

Background Material

On

Information Systems Audit 2.0 Course

Volume I



The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronic mechanical, photocopying, recording, or otherwise, without prior permission, in writing, from the publisher.

DISCLAIMER:

The views expressed in this material are those of author(s). The Institute of Chartered Accountants of India (ICAI) may not necessarily subscribe to the views expressed by the author(s).

The information in this material has been contributed by various authors based on their expertise and research. While every efforts have been made to keep the information cited in this material error free, the Institute or its officers do not take the responsibility for any typographical or clerical error which may have crept in while compiling the information provided in this material. There are no warranties/claims for ready use of this material as this material is for educational purpose. The information provided in this material are subject to changes in technology, business and regulatory environment. Hence, members are advised to apply this using professional judgement. Please visit cit portal for the latest updates. All copyrights are acknowledged. Use of specific hardware/software in the material is not an endorsement by ICAI.

Revised Edition : June 2014

Committee/Department : Committee on Information Technology

E-mail : cit@icai.in

Website : www.icai.org/http://cit.icai.org

Price : ₹ 1000/- (For Vol-I and Vol-II, including DVD)

ISBN : 978-81-8441-336-6

Published by : The Publication Department on behalf of the Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi - 110 002.

Printed by : Sahitya Bhawan Publications, Hospital Road, Agra-282 003.

June/2014/2000 Copies (Revised)



Foreword

Information technology (IT) plays a vital role in supporting the activities of any organization. The growth and changes that have come about as a result of these technological trends have important implications. Mobile and cloud computing are converging to create a new platform—one that has the potential to provide unlimited computing resources. Social networks have quickly become the key organizing principle of Internet communication and collaboration. While Internet-enabled social networks offer tremendous opportunities, widespread interest in and growth of these systems raises new risks and growing concerns.

The new company law regulatory framework prescribes management and inspection of documents in electronic form, electronic voting, electronic notices, etc that require a techno legal compliance on the part of Indian companies. The Companies Act 2013 also specifically made applicable many provisions of the IT Act 2000 and thereby expanding the scope of regulatory compliances under the 2013 Act.

Stakeholders like Banks, Insurance Companies, Electricity Companies, Companies incorporated under Special Acts, Companies notified by Central Government, etc are required to comply with the techno legal requirements as prescribed under the Companies Act 2013, Information Technology Act, 2000 and other applicable laws of India.

As much as IT has enabled business, the increasing use of IT has also led to e-crimes like cyber warfare, hacking data thefts, DDoS (Distributed Denial of Service) and other computer related frauds. Lack of proper controls/ knowledge has encouraged frauds at higher scales. Frauds are being committed by the organisations as wells as against an organisation. Consequently, there are various e-Governance, regulatory and compliance issues which are required to be looked into. These technological changes have put more focus on the role performed by Chartered Accountants, especially in the field of Information Systems Audit.

The Committee on Information Technology (CIT) of the Institute of Chartered Accountants of India (ICAI) acknowledging the need for IS Audits is conducting Post Qualification Course on Information

Systems Audit since 2001. In view of the dynamism of the IT sector, a revised edition of the background material for the Post Qualification Course on Information Systems Audit is being brought up by the CIT which will enable the members to discharge their duties as per the regulatory compliance.

The background material contains various practical aspects, new technologies along with case studies related to Information Systems Audit, which will make this a great learning guide. I appreciate the efforts put in by CA. S. Santhanakrishnan, Chairman IT Committee, members of the Committee, all the faculty members, and staff of the IT Committee for bringing out the revised background material.

I hope that it will be a useful learning material and will assist the members in understanding the nuances of the Information Systems Audit. I wish our members great success in the field of Information Systems Audit.

Best Wishes

CA. K.Raghu
President



Preface

It is a matter of immense pleasure for me that the Committee on Information Technology of the Institute has come out with the updated ISA Course 2.0 to equip members with unique body of knowledge and skill sets so that they become Information Systems Auditors (ISAs) who are technologically adept and are able to utilize and leverage technology to become more effective in their work and learn new ways that will add value to clients, customers and employers. This will also meet the increasing need of CAs with solid IT skills that can provide IT enabled services through consulting/assurance in the areas of designing, integrating and implementing IT Solutions to meet enterprise requirements.

The ISA Course 2.0 has been prepared based on inputs from senior faculty members, industry experts and professionals. The updated course material has taken into consideration the latest curriculum of similar professional courses and the recent/emerging developments in the field of Information Technology and IS Auditing and has been updated taking into consideration all the suggested changes and encompasses existing modules, contents and testing methodology.

The specific objectives of the updated ISA course 2.0 is: “To provide relevant practical knowledge and skills for planning and performing various types of assurance or consulting assignments in the areas of Governance, Risk management, Security, Controls and Compliance in the domain of Information Systems and in an Information Technology environment by using relevant standards, frameworks, guidelines and best practices.”

The updated ISA Course 2.0 has a blend of training and includes eLearning, facilitated e-Learning, hands on training, project work in addition to class room lectures. This background material also includes a DVD which has e-Learning lectures, PPTs and useful checklists. The focus is to ensure that practical aspects are covered in all the modules as relevant. I am sure the updated ISA course 2.0 will be very beneficial to the members and enable them to offer IT assurance and advisory services.

I would like to take this opportunity to place on record my deep appreciation of the efforts put in by authors of the various modules: CA. A. Rafeq, CA. M.S. Mehta, CA. Rajeev Gupta, CA. Anand Prakash Jangid, CA. Vishakha, CA. Atul Gupta and Mr. Sunil Bakshi. In this endeavour, Mr. I.P. Singh, CA. Riaz Ahmed, CA. Babu Nambi, and CA. P. Selvamoorthy provided guidance to the authors by reviewing the material and offering useful inputs in ensuring that learning objectives are achieved and the publications including the DVD meets the requirements. A number of subject matter experts including most of the senior faculty members of ISA course have reviewed the material and provided their valuable feedback which was considered in updating the material. This has gone a long way in enhancing quality, relevance and usefulness of the material. I would like to place on record my sincere appreciation for CA. A. Rafeq for his dedicated efforts and for providing overall guidance for this project from conception to completion. I would also like to thank the Committee members for supporting this initiative. The Committee Secretariat including CA Amit Gupta who was the overall coordinator and Mrs. Indu Arora, Secretary, Committee on Information Technology deserve special mention for their untiring efforts in providing necessary administrative support.

I am sure that this updated background material on Information Systems Audit Course 2.0 would be of immense help to the members by enhancing efficiency not only in providing compliance, consulting and assurance services but also open out new professional avenues in the areas of IT Governance, assurance, security, control and assurance services.

Information Technology is a dynamic area and we have to keep updating our auditing methodologies and skill-sets in tune with emerging technologies. We hope this updated ISA 2.0 course is a step in this direction. We welcome your comments and suggestions.

CA. S. Santhanakrishnan

Chairman

Committee on Information Technology

CONTENTS: VOLUME I

INTRODUCTION TO BACKGROUND MATERIAL	xi
MODULE 1: PRIMER ON INFORMATION TECHNOLOGY, IS INFRASTRUCTURE AND EMERGING TECHNOLOGIES (12%).....	15
E-LEARNING	15
SECTION 1: OVERVIEW	15
SECTION 2: CONTENTS.....	19
Chapter 1: Introduction to Computer Hardware and Software.....	19
Part 1: Computer Hardware.....	19
Part 2: Systems Software	39
Part 3: Database and Database Management Systems	65
Part 4: Hardware/Software Deployment Strategies	87
Chapter 2: Introduction to Computer Networks.....	99
Part 1: Network Basics.....	99
Part 2: Network Standards And Protocols.....	125
Part 3: The IP Networks.....	143
Chapter 3: Securing Networks.....	159
Part 1: Firewalls.....	159
Part 2: Configuring Personal Firewalls and IDS	177
Part 3: Cryptography and PKI	193
Part 4: Application of Cryptographic Systems.....	205
MODULE 1: PRIMER ON INFORMATION TECHNOLOGY, IS INFRASTRUCTURE AND EMERGING TECHNOLOGIES (6%)-Facilitated E-Learning	231
SECTION 1: OVERVIEW	231
SECTION 2: CONTENTS.....	233
Chapter 1: Overview of E-Learning and FAQs	233
Part 1: Overview of E-Learning.....	233
Part 2: FAQs of E-Learning.....	241
Chapter 2: IT Enabled Services and Emerging Technologies	253
Part 1: IT Assurance Services and Role of CAs in BPO-KPO.....	253

Part 2: Emerging Technologies: BI, Data Warehouse, ERP and E-Commerce.....	265
Chapter 3: Overview of Cloud Computing and Mobile Clouding: Challenges and Opportunities for CAs	281
Part 1: Cloud and Mobile Computing.....	281
Part 2: Emerging Technologies: BYOD, XML-XBRL and Social Media	293
Chapter 4: Overview of Business Information Systems and Risk and Controls in Newer Technologies	307
Part 1: Business Information Systems.....	307
Part 2: Emerging Technologies: Risks, Control and Audit	323
MODULE 2: INFORMATION SYSTEMS ASSURANCE SERVICES	343
SECTION 1: OVERVIEW	343
SECTION 2: CONTENTS.....	351
Chapter 1: Concepts of IS Audit	351
Chapter 2: IS Audit in Phases	369
Chapter 3: IT Enabled Services	439
SECTION: 3 APPENDIX	457
Checklists and other related materials.....	457
Appendix 1: RFP from Bank for IS Audit of Application software	458
Appendix 2: Response to RFP for Logical Access Controls Review of SAP	459
Appendix 3: Sample IS Audit Finding	466
Appendix 4: CAAT Report using SQL.....	468
Appendix 5: Sample IS Audit Report	469
Appendix 6: Questionnaire for Providing Assurance services in.....	472
E-Commerce	472
MODULE 3: GOVERNANCE AND MANAGEMENT OF ENTERPRISE INFORMATION TECHNOLOGY, RISK MANAGEMENT AND COMPLIANCE (12%)	487
SECTION 1: OVERVIEW	487
SECTION 2: CONTENTS.....	495
Chapter 1: Concepts of Governance and Management of Information Systems	495
Chapter 2: GRC Frameworks and Risk management practices	517

Chapter 3: GEIT and GRC	547
Chapter 4: Key Enablers of GEIT	561
Chapter 5: Performance Management Systems	583
Chapter 6: Implementing Governance and Management Practices	607
SECTION 3: APPENDIX	627

INTRODUCTION TO BACKGROUND MATERIAL

Need for DISA 2.0 Course

Enterprises today in the rapidly changing digital world are inundated with new demands, stringent regulations and risk scenarios emerging daily, making it critical to effectively govern and manage information and related technologies. This has resulted in enterprise leaders being under constant pressure to deliver value to enterprise stakeholders by achieving business objectives. This has made it imperative for management to ensure effective use of information using IT. Senior management have to ensure that the investments and expenditure facilitate IT enabled change and provide business value. This can be achieved by ensuring that IT is deployed not only for supporting organisational goals but also to ensure compliance with internally directed and externally imposed regulations. This dynamic changing business environment impacted by IT provides both a challenge and opportunity for chartered accountants to be not only assurance providers but also providers of advisory services.

The updated ISA course 2.0 has been designed for CAs to provide IT enabled services with the required level of confidence so that management can have trust in IT and IT related services. The ISA course 2.0 builds on the existing core competencies of CAs and provides the right type of skills and toolsets in IT so that CAs can start exploring the immense potential of this innovative opportunity. A key component of this knowledge base is the use of globally accepted good practices and frameworks and developing a holistic approach in providing such services. The background material has been designed with practical perspective of using such global best practices.

Need for updation to DISA 2.0 course

The need for DISA course updation has been extensively discussed considering the objectives and utility of the course. It was decided to update the contents based on suggestions received considering the latest developments in the field of IT and IS Auditing. The updated course has revised modules with key areas of learning as practically relevant for CAs which will enable them to be more effective in their practice for regular compliance audits and also enable to provide IT assurance or consulting services. The updated syllabus has also considered the IT knowledge acquired by the latest batch of CA students who have studied IT in IPCC and Final and have also gone through practical IT trainings. A bridge DISA course is expected to be developed to help existing DISAs to update their knowledge and skills as per the latest course.

Objective of updated DISA Course

The objective of the updated DISA course 2.0 is to equip CAs with a unique body of knowledge and skill-sets so that they can become Information Systems Auditors (ISAs) who are technologically adept and are able to utilize and leverage technology to become more effective in their work and learn new ways and thus add value to their clients or employers. The updated DISA 2.0 course will also meet the increasing market need of CAs with solid IT skills who can provide consulting/assurance in the areas of designing, integrating and implementing IT Solutions to meet enterprise requirements. The updated syllabus of the DISA Course 2.0 has been prepared based on inputs from senior faculty and has undergone numerous reviews over a period of more than two years. The latest curriculum of similar professional courses and the recent/emerging developments in the field of IT and IS Auditing were also referred in updating the course.

Objective of updated DISA Course Material

The primary objective of the updated study material for DISA course is to ensure that DISAs are well versed with the latest IT concepts and practice in the areas of Governance of Enterprise IT, GRC, Assurance, risk, security and controls. The study material has a companion DVD which includes all the reading material and supplementary reference materials and checklists in soft copy. The DVD also includes the eLearning content available as on date. All the contents in the DVD are presented and linked to aid in easy access of required material. Hence, the DVD and background material will be useful not only as a reading material for passing the DISA exam but also as a reference material for providing IT assurance and consulting services. The sample checklists given in the material can be customized based on scope, objectives of the assignment and considering the nature of business and the technology platform or the enterprise architecture.

Reading of this material is not a one-time exercise but has to be repeated and supplemented with other relevant material and research on the internet. As IT is a rapidly changing area, it will be endeavoured that the material is updated regularly. Although technology and the services provided using technology undergo rapid changes, the key concepts and requirements for risks, security and control will always remain whether it was the main-frame environment earlier or the mobile computing environment now. Hence, the need for audit and IS audit will always be there.

Use of structured approach

The updated syllabus has been developed by using process oriented structured approach based on the bloom taxonomy of learning and other global best practices. This covers the process/guidelines to be adapted in development of updated study material.

Overall Objectives

The IT knowledge and skills acquired in the DISA course would enable DISAs to be more effective in using IT for auditing in a computerised environment in existing domains of compliance, consulting and assurance services. The overall objective of the DISA course 2.0 is: **“To provide relevant practical knowledge and skills for planning and performing various types of assurance or consulting assignments in the areas of Governance, Risk management, Security, Controls and Compliance in the domain of Information Systems and in an Information Technology environment by using relevant standards, frameworks, guidelines and best practices.”**

Course Coverage

The DISA Course will provide basic understanding of how information technology is used and deployed. It facilitates understanding of how an IS Auditor is expected to analyse, review, evaluate and provide recommendations on identified control weaknesses in different areas of technology deployment. However, it is to be noted that the DISA course is not oriented towards teaching fundamentals of technology. The DISA course is conducted through a good blend of e-learning (online and facilitated), class room training, hands-on training with practical case studies and project work to ensure practical application of knowledge. The DISA course combines technology, information assurance and information management expertise that enables a DISA to become trusted Information Technology advisor and provider of IS Assurance services. The DISA with the unique blend of knowledge would serve as the "bridge" between business and technology leveraging the CA's strategic and general business skills. The class room training has been supplemented with hands on training. Aspiring DISAs need to remember that the class room training is not expected to be comprehensive but as aid to facilitate understanding. Considering the extensive coverage of the course, duration and the diverse level of participants, the faculty will not be able to cover the material in depth. **Please read the background materials of the specific modules prior to attending the classes to derive maximum benefit from the class room training.**

DISA Certification

DISA Certification through judicious blend of theoretical and practical training provides CAs with better understanding of IT deployment in enterprises which will enable them to be more effective not only in auditing in a computerised environment covering traditional areas of financial/compliance audits but also in offering IT enabled services. The DISA exam is designed to assess and certify CAs for conducting IS Audit. After successfully completing the course, the DISA candidates are expected to have required knowledge and skills to perform various assurance and consulting assignments relating to Governance, Risk management, Security, Controls and Compliance in the domain of Information Systems, Information Technology and related areas.

DISA Course: Basic competency requirements

The competency requirement of the DISA 2.0 course are mapped with the detailed body of knowledge encompassing all the key tasks an IS Auditor has to perform in specific areas and the related knowledge required for performing these tasks. The skill requirements are represented as task statements and knowledge is represented by the knowledge statements. After successful completion of the course, the DISA candidates will have conceptual clarity and will demonstrate basic competency in the following key areas:

- Overall understanding of information system and technology: concepts and practice
- Risks of deployment of information system and technology
- Features and functionalities of security and controls of IT components and IT environment.
- Controls which could be implemented using the security features and functionalities so as to mitigate the risks in the relevant IT components and environments.
- Recommend IT risk management strategy as appropriate.
- Apply appropriate strategy, approach, methodology and techniques for auditing technology using relevant IS Audit standards, guidelines and procedures and perform IS Assurance and consulting assignments.

Modules of the DISA Course

The updated ISA certification is granted exclusively to CAs who demonstrate considerable expertise in domain areas of IT Governance, Security, Control and assurance through their knowledge, skills and experience. The primary purpose of the ISA exam is to test whether the candidate has the requisite knowledge and skills to apply IS assurance principles and practices in the following modules:

No.	Name of Module	Weightage (%)
1	Primer on Information Technology, IS Infrastructure and Emerging Technologies	18
2	Information Systems Assurance Services	12
3	Governance and Management of Enterprise Information Technology, Risk Management and Compliance Reviews	12
4	Protection of Information Systems Infrastructure and Information Assets	18
5	Systems Development: Acquisition, Maintenance and Implementation.	12
6	Business Applications Software Audit	12
7	Business Continuity Management	6
	Project report	10

Learning Objectives

The DISA course is not expected to be an in-depth comprehensive coverage of different aspects of IT such as computer hardware, operating system, network, databases, application software, etc. but is focussed on training on how to review IT controls and provide assurance on secure technology deployment.

The key learning objectives are:

1. Demonstrate understanding of functioning of key components of existing and emerging information technology and their practical deployment.
2. Provide IS assurance or IT Enabled services and perform effective audits in a computerised environment by using relevant standards, guidelines, frameworks and best practices.
3. Evaluate structures, policies, procedures, practices, accountability mechanisms and performance measures for ensuring Governance and management of Information Technology, risk management and compliance as per internal and external stakeholder requirements.
4. Provide assurance, consulting or compliance services to confirm that enterprise has appropriate security and controls to mitigate risks at different layers of technology as per risk management strategy.
5. Provide assurance or consulting services that the management practices relating to systems development: acquisition, maintenance and implementation are appropriate to meet enterprise strategy and requirements.
6. Provide assurance or consulting services to validate whether required controls have been designed, configured and implemented in the application software as per enterprise and regulatory requirements and provide recommendations for mitigating control weaknesses as required.
7. Provide assurance or consulting services to confirm whether the Business continuity management strategy, processes and practices meet enterprise requirements to ensure timely resumption of IT enabled business operations and minimize the business impact of a disaster.
8. Plan and perform IS assurance or consulting assignments by applying knowledge learnt by presenting project assignment relating to allotted case study to confirm understanding.

Skill Levels

The updated syllabus provides specific skills in each of the three categories of skill areas. The suggested skill levels ensure that the updated syllabus through all the modules has right blend of concepts and practice. The skill levels will be considered by the authors of study material and also in testing methodology through the eligibility tests and assessment test.

Weightage and category of skills

No.	Skills Category	Weightage (%)
1	Knowledge and Understanding	30 to 40
2	Application of the Body of Knowledge	55 to 60
3	Written communication	5 to 10

Summary of revised DISA Training

No.	Mode of Training	Weightage (%)
1	e-Learning Online (self)	12
2	e-Learning facilitated (lectures)	12
3	Classroom Training (lectures)	42
4	Hands-on Training (on laptop)	24
5	Project Work (self in groups)	10
	Total	100

Key highlights of DISA training

DISA Training includes eLearning, hands on training, project work in addition to class room lectures.

- Candidates will have to successfully complete e-learning mode before joining class room training.
- The training in classroom and hands-on training will follow the order in sequential order of the modules. This includes an inter-mix of classroom lectures and hands-on training. The hands-on training pre-supposes and builds on understanding of concepts of the classroom lectures.
- The training includes mandatory E-Learning of 12 hours for Module-1 and 6 hours for Module-2 and passing in the online test is mandatory and part of the eligibility score.
- Module-4 will have class room lectures of 2 days and hands on training of 2 days. Module-6 will have hands on training of 2 days. **Supplementary e-Learning Lectures covering Modules 4 and 6 are also included.** These will be added in due course and will be made available through DVD or online.
- **Hands on training for Module 4 and 6 will be conducted by the experienced faculty at same venue as class rooms with all participants performing exercises on their own laptops with pre-loaded software and sample/test data as specified in advance.**

DISA 2.0 Course Background Material

The DISA Course 2.0 Background Material is intended to assist in preparing for the DISA exam. The material is a one source of preparation for the exam, but should not be considered as the only source nor should it be viewed as a comprehensive collection of all the information that is required to pass the exam. Participants are encouraged to supplement their learning by using and researching the references provided the material.

Structure of material

The DISA background material has contents as per module. Each of the module has 3 sections.

- **Section 1:** Provides the detailed Table of Contents, module objective, task statements, knowledge statements, task and knowledge mapping statement and knowledge reference guide. The Objective of task knowledge statements is to outline what DISAs will learn to do and knowledge statements are oriented towards providing knowledge for specific tasks. The mapping will provide relationship between each task to one/more knowledge statement. The knowledge reference guide provides content reference from the chapters for each of the knowledge statement/areas.
- **Section 2:** Provides the content as per the chapter. Each of the chapter/parts has the learning objectives followed by topics which are covered in brief or detail as required. At the end of each chapter, there are sample questions followed by answers and explanations.
- **Section 3:** Provides appendices which has checklist/templates as referenced in the material.

DISA 2.0 Course DVD

The Reading material for the DISA 2.0 course includes a DVD which is comprehensive collection of educational material for revised DISA Course 2.0. This DVD will aid self-learning and includes Background Material, Reference Material, e-Lectures, PowerPoint Presentations, Podcasts/MP3 Files and Self-Assessment Quiz. This DVD is designed to be supplementary to the background material. It has to be used for self-learning and also as a training aide for the DISA Course 2.0 and DISA candidates are strongly advised to use this for studying for the ISA course.

Standard PPTs for each of the modules of the DISA 2.0 course have been prepared by the authors based on the background material. These are provided in the DVD only and are expected to serve as reference material during the class. Additional references materials and checklists of the course are only included in the DVD. The PPTs may be customised or updated by the faculty as required. Participants are encouraged to copy the DVD contents in their laptops and use this as reference in the classroom training.

Feedback and updates

We compliment you on choosing to join the DISA 2.0 Course and wish you a great learning experience. Please make best use of the material and the training. **Please note that the training is expected to supplement your reading of the material prior to attending the course.** Please participate actively in the training to make the best use of the training. The material will be useful to you not only to aid you in preparing for exam but also for providing services in the area of Governance, Assurance and consulting.

Please note that the **background material has been contributed by practising professionals who have shared their expertise and reflects different writing styles of the authors.**

Please provide your feedback on areas of improvement of the course and the reading material in the specified format so that further improvements can be made. Please email your feedback or queries to: isa@icai.in. Please visit CIT portal <http://cit.icai.org/> for the latest updates of the DISA course. We wish you a great learning experience and a rewarding career as an IS Auditor.

Committee on Information Technology, ICAI

The course material includes references to some specific companies, hardware or software. This reference is only for educational purposes and is not in any way endorsement of the company or products. All copyrights are acknowledged and belong to the rightful owners.

Module-1

Primer on Information Technology, IS Infrastructure and Emerging Technologies

TABLE OF CONTENTS

MODULE 1: PRIMER ON INFORMATION TECHNOLOGY, IS INFRASTRUCTURE AND EMERGING TECHNOLOGIES (12%).....	15
E-LEARNING	15
SECTION 1: OVERVIEW	15
Objective:	15
Task Statements.....	15
Knowledge Statements (Knowledge of)	15
Relationship between Task and Knowledge Statements	16
Knowledge Statement Reference Guide	17
SECTION 2: CONTENTS.....	19
Chapter 1: Introduction to Computer Hardware and Software.....	19
Part 1: Computer Hardware.....	19
Learning Objectives.....	19
Overview of the e-Learning Material	19
1.1 Introduction	20
1.2 Overview of components of IS Infrastructure/ IS layers	20
1.2.1 People -Users	21
1.2.2 Application Software	21
1.2.3 Database Management Systems (DBMS)	21
1.2.4 System Software -Operating Systems.....	22
1.2.5 Network	22
1.2.6 Hardware	22
1.3 Components of a Computer.....	23
1.3.1 Computer Peripherals.....	23
1.3.2 What is inside the Computer?	24
Central Processing Unit (CPU)	24
Bus Lines.....	25
Instructions within processor	25
1.3.3 Memory.....	26

Internal memory	26
Primary Memory	26
Cache Memory	27
Virtual Memory	27
Secondary Memory	28
1.4 Data representation in Memory- Bits and Bytes.....	28
Data storage media	29
Semiconductor	29
Magnetic	29
Optical storage	29
1.5 Hardware Asset Management.....	30
1.5.1 Hardware Acquisition	30
Evaluation Criteria	30
ITT or RFP	31
ITT or RFP evaluation.....	31
Metrics for selecting Hardware.....	32
1.5.2 Hardware Maintenance Program	32
1.5.3 Hardware Monitoring Procedures	33
1.5.4 Data and Capacity Management	33
1.5.5 Hardware Retirement.....	35
1.6 Auditing Hardware	35
1.7 Summary	36
1.8 References	37
Part 2: Systems Software	39
Learning Objectives.....	39
2.1 Introduction.....	39
2.1.1 Software	39
1. System Software	39
2. Application Software	40
2.2 Operating System.....	40

2.2.1	Types of Operating Systems	41
2.2.2	Functions of Operating Systems	42
	Processor Management	42
	Memory Management.....	42
	Device Management.....	43
	File Management	43
	Secondary Storage Management	43
	Networking.....	44
	Protection System	44
	Other tasks of an Operating System.....	44
	Kernel and Shell.....	45
2.3	Other Type of System Software	45
2.3.1	Program Development Software	45
	First-generation language 1GL: Machine Language	45
	Second-generation language 2GL: Assembly Language	45
	Third-generation language 3GL	46
	Fourth-generation language 4GL.....	46
	Fifth-generation language 5GL	46
	Program development tools	46
2.3.2	Access Control Software	47
2.3.3	Data Communications Software	47
2.3.4	Utility Programs.....	48
2.4	Security and Controls in Operating System	48
2.4.1	Access Controls in OS.....	48
2.4.2	Access Control in Windows.....	49
	User Creation	50
	Assign Roles	50
	Assign Password.....	51
	User rights and permissions.....	51
	Permissions	52

Security Auditing: User Access	53
2.5 Software Acquisition	53
Requirements Definition	54
Software Alternatives	54
2.5.1 System Software Acquisition	54
System Software Implementation	55
System Software Change Control Procedures	55
Software Licensing Issues	55
2.5.2 Application System Acquisition	55
Software Development	56
2.6 Software Asset Management (SAM).....	56
Benefits of SAM	57
2.6.1 Endpoint Management	58
What is an Endpoint?	58
Why Endpoint Management	59
Key Benefits of endpoint management.....	59
2.6.2 Digital Rights Management	59
Scope of DRM	60
Why DRM.....	60
Examples of DRM and DLP	60
2.7 Auditing Software.....	60
2.7.1 Auditing Operating System Software.....	60
2.7.2 Auditing Software Asset Management (SAM).....	62
2.8 Summary.....	62
2.9 References	63
Part 3: Database and Database Management Systems	65
Learning Objectives.....	65
3.1 Introduction.....	65
3.2 Data Management.....	65
3.2.1 DIKW	65

3.2.2 Hierarchy of Data	66
3.2.3 Why do we need Databases?	66
3.2.4 What is a Database?.....	66
3.2.5 What is Database Management System?	67
Advantages of a DBMS	67
Disadvantages of a DBMS	68
3.2.6 Database Models	69
Hierarchical Database Model	69
Network Database Model	70
Relational Database Model	71
3.3 Relational Data Integrity.....	71
3.3.1 Database Schemas.....	74
External Schema.....	74
Conceptual Schema.....	74
Internal Schema	74
3.4 Database Languages	75
3.4.1 Data Definition Language (DDL)	75
3.4.2 Data Manipulation Language (DML)	77
3.4.3 Data Control Language (DCL).....	78
3.5 Key concepts of Database	78
3.5.1 Meta Data	78
3.5.2 Data Dictionary	78
3.5.3 Data Administrator and Database Administrator	79
3.6 Database Applications-Linking Databases to the Web.....	80
3.7 Database Security and Control	80
3.7.1 Database Security	81
3.8 Auditing Databases.....	83
3.8.1 Need for Auditing Databases	83
Auditing Database.....	83
Areas of review by IS Auditor	83

Step by step approach for auditing database.....	84
3.8.2 Database Auditing Tools.....	85
3.9 Summary.....	86
3.10 References	86
Part 4: Hardware/Software Deployment Strategies	87
Learning Objectives.....	87
4.1 Introduction.....	87
4.2 Different Deployment Strategies.....	87
4.2.1 Centralised Approach	87
Benefits:.....	88
Disadvantages:	88
4.2.2 Decentralised Approach	88
Benefits:.....	89
Disadvantages:	89
4.3 IT Components in a CBS (Core Banking Solution) Data Centre.....	89
4.3.1 Application Solutions Components	90
4.3.2 Hardware Components and OS	91
4.3.3 Network and Security Components	91
4.3.4 Enterprises Management System Components	92
4.3.5 Environmental Components	93
4.4 Configuration Management of IS Components	93
4.4.1 Configuration Identification	94
4.4.2 Configuration Control	94
4.4.3 Configuration Status Reporting	95
4.4.4 Configuration Audit	95
4.5 Hardening of Systems	95
4.6 Risks and Controls in Deployment of IS Infrastructure	96
4.7 Auditing IS Infrastructure	97
Audit all hardware and software to assess	97

4.8	Summary.....	98
4.9	References	98
	Chapter 2: Introduction to Computer Networks.....	99
	Part 1: Network Basics.....	99
	Learning Objectives.....	99
1.1	Introduction.....	99
	Benefits of Computer Networks	100
1.2	Basics of Communication.....	100
1.3	Transmission Modes	101
	Simplex	101
	Advantages	101
	Disadvantages	101
	Half Duplex	102
	Advantages	102
	Disadvantages	102
	Full Duplex.....	102
	Advantage.....	102
	Disadvantage.....	102
	Serial transmission.....	102
	Asynchronous Transmission.....	103
	Synchronous Transmission	103
1.4	Network Categories	104
	1.4.1 Local Area Networks (LAN)	104
	1.4.2 Metropolitan Area networks (MAN)	104
	1.4.3 Wide Area Networks (WAN)	105
	Differences between LAN and WAN	105
1.5	Network types	105
	1.5.1 Client-Server Architecture	106
	Functions of a Client	106

Functions of a Server	106
Middleware	107
Characteristics of Client- Server Model	107
1.5.2 Peer-To Peer Networks	108
1.6 LAN Topologies and Network Components	109
1.6.1 Media Used In Communication	109
Factors that influence the use of media	109
Factors that degrade a signal	109
Guided Transmission Media	109
Coaxial Cable	110
Twister pair cable	110
Unshielded Twisted Pair (UTP)	110
Shielded Twisted Pair	110
Optical Fibre Cable	110
Unguided Transmission Media	112
1.6.2 Network Devices	113
Network Interface Card (NIC)	113
Hub	114
Switches	114
Bridges	114
Multi-station Access Unit (MAU)	114
Routers	114
Gateway	115
1.6.3 Network Topologies	115
Bus Topology	115
Star Topology	116
Ring Topology	117
Mesh Topology	118
Hybrids	119
1.7 WAN Message Transmission Technologies	119

1.7.1	Switching	119
	Circuit Switching.....	120
	Packet Switching.....	120
	Message Switching	121
1.7.2	Multiplexing	121
	Frequency Division Multiplexing (FDM).....	122
	Time Division Multiplexing (TDM)	122
	Wavelength Division Multiplexing (WDM)	123
1.8	Selecting a Suitable Network Topology	123
1.9	Summary.....	124
1.10	References	124
Part 2: Network Standards And Protocols.....		125
Learning Objectives.....		125
2.1	Introduction.....	125
2.2	Network Standards and Protocols	125
	Internet	125
2.2.1	Network Standards	126
2.2.2	Protocols.....	127
2.2.3	Standards creation committees.....	128
2.2.4	The OSI Architecture	128
	What is OSI Model?	128
	Why OSI Model?	128
	Concepts of layers	129
	OSI Model is a layered model.	130
	Vertical (Adjacent Layer) Communication	131
	Horizontal (Corresponding Layer) Communication.....	132
2.2.5	Transmission Control Protocol / Internet Protocol (TCP /IP).....	134
	Application Layer.....	135
	Protocols used in Application Layer	135
	E-mail protocols	136

Transport Layer.....	136
Network Layer	137
Data Link Layer	138
Physical Layer	139
2.3 Wireless Networks	139
2.3.1 Wi-Fi	140
2.3.2 Blue Tooth	140
2.4 TCP/IP Security and Controls.....	141
2.5 Summary.....	141
2.6 References	141
Part 3: The IP Networks.....	143
Learning Objectives.....	143
3.1 Introduction.....	143
3.2 IP Networks	144
3.2.1 IP Addressing.....	144
IP Version 4 (IPv4).....	144
3.2.2 Public and Private Addresses	149
Network Address Translation (NAT):.....	150
Static and Dynamic Addresses	151
Reserved addresses.....	151
Subnet Mask	152
3.2.3 Internet Protocol Version 6 (IPv6).....	152
3.3 Ports	153
Service Ports	153
Source Ports.....	153
Destination Ports.....	153
3.4 The Domain Name System	153
3.5 Network Services	155
3.6 On Demand Computing.....	155
3.7 Public Global Internet Infrastructure	156

3.8	Factors Impacting Quality of Network Service.....	156
3.9	Summary.....	157
3.10	References	157
	Chapter 3: Securing Networks.....	159
	Part 1: Firewalls.....	159
	Learning Objectives.....	159
1.1	Introduction.....	159
1.2	Firewall.....	159
1.2.1	Firewall Functionalities	160
	Access Control Techniques.....	161
	Access Control Policy	161
	NAT Technique in Firewalls	161
1.2.2	Firewall types	162
	Network Based Firewall	162
	Host Based Firewalls	162
	Advantages of Host Based Firewall	162
	Personal Firewalls.....	162
	Some key terms related to Firewalls	163
1.2.3	Firewall Configurations	163
	Packet Filtering Router Firewall	163
	Stateful Inspection Packet Filtering Firewall	165
	Circuit Level Gateways	166
	Application Level Gateway Firewall	166
1.2.4	Common Implementation Structures of Firewalls	168
	Packet Filtering Routers	168
	Single Homed Firewalls	168
	Dual-Homed Host Firewalls.....	169
1.2.5	Limitations of Firewalls	171
1.2.6	Firewall Product Types	172
	Appliance Based Firewall	172

Software Based Firewall	172
1.2.7 Unified Threat Management.....	172
How UTM secures the network	173
UTM Functionalities	173
1.2.8 Firewall Life Cycle	174
1.2.9 Baseline Configuration for Firewalls	174
1.3 Summary.....	174
1.4 References	175
Part 2: Configuring Personal Firewalls and IDS	177
Learning Objectives.....	177
2.1 Introduction.....	177
2.2 Personal Firewalls	177
Common Features	177
Limitations	178
2.2.1 Configuration of Personal Firewall in Windows Environment	178
Some Windows 7 Firewall features	178
Configuring Windows 7 Firewall	179
Overview of Advanced Configuration Settings	182
2.2.2 General Controls Associated With Firewalls	188
2.2.3 Pitfalls with Firewalls.....	189
2.3 Intrusion Detection Systems (IDS)	189
Types of IDS.....	190
Detection Methodologies	190
2.4 Summary.....	191
2.5 References	191
Part 3: Cryptography and PKI	193
Learning Objectives.....	193
3.1 Introduction.....	193
3.2 Cryptography	193
3.2.1 Need for Cryptography.....	193

3.2.2	Objectives of Cryptographic Systems.....	194
3.2.3	Elements of Cryptography.....	194
3.2.4	Symmetric Key Cryptography.....	195
3.2.5	Asymmetric or Public Key Cryptography.....	196
3.2.6	Message Hash Functions.....	197
3.3	Digital Signatures.....	198
3.4	Public Key Infrastructure (PKI)	199
3.4.1	Elements of PKI	200
3.4.2	Digital Certificates	202
3.4.3	Certifying Authority (CA).....	202
3.4.4	Registration Authority (RA).....	203
3.4.5	Certificate Revocation List (CRL).....	203
3.4.6	Certification Practice Statement.....	203
3.4.7	Key Storage and Security.....	203
3.5	Cryptanalysis	204
3.6	Summary.....	204
3.7	References	204
	Part 4: Application of Cryptographic Systems.....	205
	Learning Objectives.....	205
4.1	Introduction.....	205
4.2	Uses of Cryptographic Systems	205
4.2.1	Secure Socket Layer (SSL) / Transport Layer Security (TLS)	206
4.2.2	Hyper Text Transfer Protocol Secure (Https).....	207
4.2.3	Internet Protocol Security (IPSEC)	208
4.2.4	Secure Shell (SSH).....	209
4.2.5	Secure Electronic Transaction (SET)	210
4.2.6	Secure Multipurpose Internet Mail Extension (SMIME).....	211
4.3	Generic Enterprise-Wide Network Architecture in a Bank	212
4.4	Risks and Controls in Network Environment	216

4.5	Securing Enterprise Network	217
4.6	Auditing Networks.....	217
4.7	Summary.....	218
4.8	References	218

MODULE 1: PRIMER ON INFORMATION TECHNOLOGY, IS INFRASTRUCTURE AND EMERGING TECHNOLOGIES (12%)

E-LEARNING

SECTION 1: OVERVIEW

Objective:

Demonstrate understanding of functioning of key components of existing and emerging information Technologies and their practical deployment.

Task Statements

- 1.1 Identify deployment of different components of IT and their functions: Computer Hardware, Operating system software, database management software, application software, middleware, Client Server Model, Communications technologies and networks, internet, peripherals, devices, accessories, etc.
- 1.2 Recognise the configuration of hardware, operating system software, database management software and application software.
- 1.3 Recognise function of Telecommunications and Network security including wireless, encryption, firewalls, Cryptography etc.
- 1.4 Analyze baseline security procedures, firewall configurations, user administration and user management.
- 1.5 Distinguish the technology architecture of a typical data centre in a centralised environment identifying different layers/components of technology and their functions.

Knowledge Statements (Knowledge of)

- 1.1 Information Technology components of Information Systems Infrastructure and related processes in the context of practical deployment in enterprises.
- 1.2 Fundamental concepts of different components of IT and their functions: Computer Hardware, Operating system software, database management software, application software, middleware, Client Server Model, Communications technologies and networks, internet, peripherals, devices, accessories, etc.
- 1.3 Configuration management of hardware, system software, database management software and application software.
- 1.4 Telecommunications and Network security including wireless, encryption, firewalls, Cryptography etc.

- 1.5 Concepts related to applied cryptography, including plain-text, cipher-text, symmetric cryptography, asymmetric cryptography, digital signature, message authentication code, hash functions, and modes of encryption operations.
- 1.6 Baseline security procedures, firewall configurations, user administration and user management.
- 1.7 Information Technology components of a Data Centre in centralised environment

Relationship between Task and Knowledge Statements

The task statements are what the ISA Candidate is expected to know how to perform. The knowledge statements delineate each of the areas in which is ISA candidate must have a good understanding in order to perform the tasks. The task and knowledge statements are mapped in the chart below. Note that although there is often overlap, each task statement will generally map to several knowledge statements.

Task Statement	Knowledge Statement
1.1 Identify deployment of different components of IT and their functions: Computer Hardware, Operating System Software, Database Management Software, application software, middleware, client server Model, communications technologies & networks, internet, peripherals, devices, accessories, etc.	1.1 Information Technology components of Information Systems infrastructure & related processes in the context of practical deployment in enterprises. 1.2 Fundamental concepts of different components of IT and their functions: Computer Hardware, Operating System Software, Database Management Software, application software, middleware, client server Model, communications technologies & networks, internet, peripherals, devices, accessories, etc.
1.2 Recognize the configuration of hardware, operating system software, database management software and application software.	1.3 Configuration management of hardware, operating system software, database management software and application software.
1.3 Recognize function of Telecommunications and network security including wireless, encryption, firewalls, cryptography etc.	1.4 Telecommunications and network security including wireless, encryption, firewalls, cryptography etc. 1.5 Concepts related to applied cryptography, including plain-text, cipher-

	text, symmetric cryptography, asymmetric cryptography, digital signature, message authentication code, hash functions, and modes of encryption operations.
1.4 Analyze baseline security procedures, firewall configurations, user administration & user management	1.6 Baseline security procedures, firewall configurations, user administration & user management
1.5 Distinguish the technology architecture of a typical data centre in a centralised environment identifying different layers/components of technology & their functions.	1.7 Information technology components of a Data centre in centralised environment.

Knowledge Statement Reference Guide

Each knowledge statement is explained in terms of underlying concepts and relevance of the knowledge statement to the ISA Candidate. It is essential that the candidate understand the concepts. The knowledge statements are what the IS Auditor must know in order to accomplish the tasks. Consequently, only the knowledge statements are detailed in this section. The sections identified in the matrices are described in greater detail in the forthcoming part of this module.

1.1 Information Technology components of Information Systems infrastructure & related processes in the context of practical deployment in enterprises.

Knowledge area	Reference
Information Technology components, Information Systems infrastructure & related processes	Chapter1, Part 1: 1.1 to 1.4

1.2 Fundamental concepts of different components of IT and their functions: Computer Hardware, Operating System Software, Database Management Software, application software, middleware, client server Model, communications technologies & networks, internet, peripherals, devices, accessories, etc.

Knowledge area	Reference
Components of IT and their functions: Computer Hardware, Operating System Software, Database Management Software, application software, middleware, client server Model, communications	Chapter1: Part 1 to 3

technologies & networks, internet, peripherals, devices, accessories.	

1.3 Configuration management of hardware, operating system software, database management software and application software

Knowledge area	Reference
Configuration management of hardware, operating system software, database management software and application software	Chapter1: 2 to 4

1.4 Telecommunications and Network security including wireless, encryption, firewalls, cryptography etc.

Knowledge area	Reference
Telecommunications and Network security, wireless, encryption, firewalls and cryptography.	Chapter 3, Part 1 to 3

1.5 Concepts related to applied cryptography, including plain-text, cipher-text, symmetric cryptography, asymmetric cryptography, digital signature, message authentication code, hash functions, and modes of encryption operations.

Knowledge area	Reference
Applied cryptography, plain-text, cipher-text, symmetric cryptography, asymmetric cryptography, digital signature, message authentication code, hash functions, and modes of encryption operations.	Chapter 3, Part 1 to 3

1.6 Baseline security procedures, firewall configurations, user administration and user management.

Knowledge area	Reference
Baseline security procedures, firewall configurations, user administration and user management.	Chapter 3, Part 2 to 3

1.7 Information Technology components of a Data Centre in centralised environment

Knowledge area	Reference
IT components of a data centre in CBS environment	Chapter 1, Part 4, topic 4.3

SECTION 2: CONTENTS

CHAPTER 1: INTRODUCTION TO COMPUTER HARDWARE AND SOFTWARE

PART 1: COMPUTER HARDWARE

Learning Objectives

- To gain understanding of components of Information Systems (IS) Infrastructure
- To understand working of computer and peripheral devices
- To understand Data Representation in memory and storage
- To gain understanding of Hardware Asset Management
- To understand Auditing Hardware

Overview of the e-Learning Material

Module 1 of updated ISA course 2 has two parts: eLearning of 12 hours and facilitated eLearning of 6 hours. This reference material covering chapters 1 to 3 is an aid to understanding the eLearning presentations. CAs who take up the ISA course may already have understanding of IT. However, the level of understanding may vary. The objective of the material is to cover all the fundamental concepts. Hence, CAs who already have good understanding of these concepts may do a quick review of the reading material and then take up the eLearning module directly. It is important for DISAs to read this reference material before taking up the eLearning as this complements and provides a more detailed coverage of eLearning topics. This material has been prepared as a reference guide to the eLearning and follows the same presentation style and structure of the presentations covered in the eLearning. **This material is not written in the style of text book material but is written in simple style to enable quick and easy understanding. The primary purpose of the material is to be supplementary reading material for the eLearning presentation. Hence, the content closely follows the presentations and is provided as bullet points and further explained as required. Further, the focus is on windows environment as it is most prevalent.**

DISAs are advised to refer this material before eLearning and also after completing the eLearning presentations to get more clarity on the topics discussed. However, this material is not expected to be comprehensive but is prepared as a starting point for understanding IT. Readers are advised to refer to the references provided here to get clarifications on specific areas as required. IT is a dynamic field and is continuously evolving. The material covers IT environment prevalent and

relevant at the time of its preparation. However, it is expected to be updated on regular basis. Please visit the CIT portal of ICAI (<http://cit.icaai.org>) for the latest updated material.

1.1 Introduction

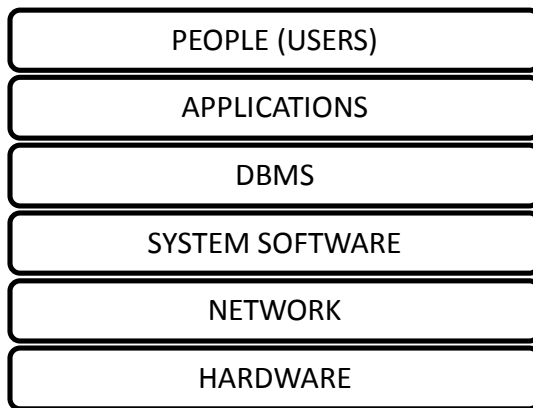
We cannot think of any enterprise today without Information systems and the critical infrastructure for developing and maintaining Information Systems is provided by Information Technology (IT). IT is a key enabler for increasing operational excellence, customer and supplier relations, better decision making and competitive advantage. In short, IT is required not only to thrive but to survive in the modern IT age. When IT is integrated with organisation and management, it can provide better ways of conducting business that empower organisations with a strategic advantage.

Business today is growing exponentially and this growth of business is propelled by information. The more information a business acquires, the more difficult it becomes to make decisions. In the past, people could rely on manual processes to make decisions because they had limited amount of information to process. Today, with massive volumes of available information, it is almost impossible for management to take decisions without the aid of information systems. Highly complex decisions must be made in increasingly shorter time frames. All this and more has made adoption of IT an imperative for running any enterprise.

1.2 Overview of components of IS Infrastructure/ IS layers

Any information system will have interaction amongst Hardware, System Software, Application Software, Database Management systems (DBMS), Network links and People. These are the key components of IT Infrastructure in Information system. The components of IS Infrastructure are given here:

In deploying IT, management has to determine what types of hardware and software will satisfy their current and future business needs, the right time to buy the equipment, and how to protect their IT investments. Auditors also have to understand how the management has deployed IT for their business and whether it helps them meet their business objectives. This does not imply that auditors need to be experts in all areas of technology; however, a working knowledge of IT hardware and software in terms of features and functionalities can help auditors to review and evaluate whether IT is meeting business needs and is implemented with right level of security at optimum cost. In the following sections we will understand these various layers of IS. A good understanding of how technology works and how this can be deployed in organisations to meet business objectives will enable auditors to offer new IT enabled services. List of sample services which can be provided by a CA in the IT areas are covered in the second part of this module (overview of eLearning and IT Enabled services).



Components of IS Infrastructure

1.2.1 People -Users

People are the most important element in most computer-based information systems. The people involved include users of the system and information systems personnel, including all the people who manage, run, program, and maintain the systems.

1.2.2 Application Software

Application software is the software that causes a computer to perform useful tasks beyond the running of the computer itself. It is a collection of programs which address a real life problem, business, scientific or any other, for its end users. The various types of application software are:

- **Application Suite:** e.g. MS Office 2013 etc.
- **Enterprise Software:** e.g. ERP Applications like SAP, etc.
- **Enterprise Infrastructure Software:** e.g. email servers, Security software.
- **Information Worker Software:** e.g. CAAT (Computer assisted audit tools), etc.
- **Content Access Software:** e.g. Media Players etc.
- **Educational Software:** e.g. eLearning, Examination Test CDs
- **Media Development Software:** e.g. Desktop Publishing, Video Editing etc.

1.2.3 Database Management Systems (DBMS)

- Every organisation has to manage its information.
- DBMS are software that aid in organizing, controlling and using the data needed by the application programs. They provide the facility to create and maintain a well-organized database. Applications access the DBMS, which then accesses the data. Commercially available Data Base Management Systems are Oracle, MySQL, SQL Servers, MS Access and DB2 etc.

- Data bases are being used at Front end (A front end to a database usually refers to the user interface that is working with that database). A back end database is the database "behind" an application. Most of web based applications would be having some or the other database at back end.
- We are these days in learning revolution and Databases provide life blood to information economy.

1.2.4 System Software -Operating Systems

System software is computer software that is designed to operate the computer hardware and to provide and maintain a platform for running application software. One of the most important and widely used system software is computer operating systems like Windows, UNIX and Linux.

System Software coordinates instructions between applications and hardware

- Enables computer to work
- Controls computer's working
- Enables connecting I/O devices
- Includes:
 - Operating system
 - Utility programs

1.2.5 Network

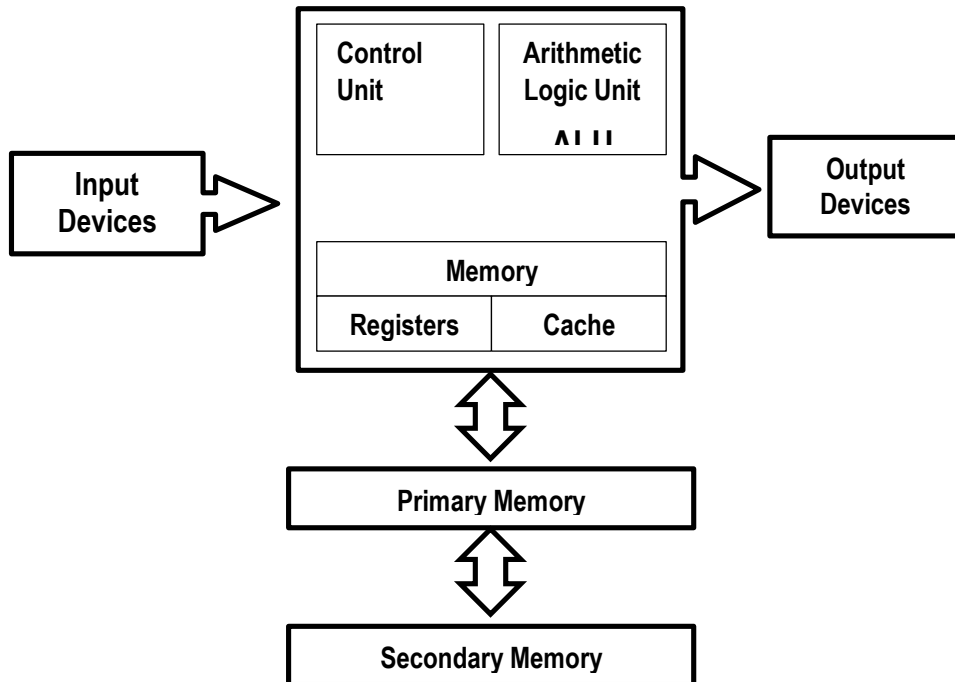
- In today's high speed world, we cannot imagine an information system without an effective communication system. Effective and efficient communication is a valuable resource which helps in good management. To enable this communication, we need communication networks.
- **Computer Network** is a collection of computers and other hardware interconnected by communication channels that allow sharing of resources and information. Where at least one process in one device is able to send/receive data to/from at least one process residing in a remote device, then the two devices are said to be in a network. Physically it would be devices which are connected but logically it would be a process in one device transmitting data to another process in another device. A network is a group of devices connected to each other.

1.2.6 Hardware

- Hardware is the tangible portion of our computer systems, something we can touch and see and it consists of devices that perform the functions of input, processing, data storage and output activities of the computer.
- The keyboard, monitor, CPU, HDD (Hard Disk drive) etc. are all hardware components of a computer.

1.3 Components of a Computer

Hardware is the tangible portion of our computer systems, something we can touch and see and consist of devices that perform the functions of input, processing, data storage and output activities of the computer.



1.3.1 Computer Peripherals

Input devices are peripheral devices which are used to interact with the computer systems and include devices such as:

- Keyboard (helps us with text based input)
- Mouse and other pointing devices (helps us in position based input)
- Scanners and webcams (helps us in image based input)
- Bar Code, MICR readers (helps us in automatic input)
- Microphone (helps us in voice based input)
- Stylus/ Touch Screen (helps us in touch based input)

Output devices are devices through which system responds.

Computers systems provide output to decision makers at all levels in an organisation to solve business problems, the desired output may be in visual, audio or digital forms.

Visual output devices like, a display device visually conveys text, graphics, and video information.

- **Cathode-ray tube (CRT)**

A vacuum tube that uses an electron gun (cathode) to emit a beam of electrons that illuminates phosphors on a screen as the beam sweeps across the screen repeatedly. A monitor is often called a CRT.

- **Liquid crystal display (LCDs)**

A low-powered display technology used in laptop computers where rod-shaped crystal molecules change their orientation when an electrical current flows through them.

- **Laser printer**

A printer that forms images using an electrostatic process, the same way a photocopier works.

- **Ink-jet Printer**

A printer that makes images by forcing ink droplets through nozzles.

- **Plotter**

A printer that uses computer-directed pens for creating high-quality images, blueprints, schematics, etc.

- **Speaker**

Gives an audio output

Processing devices include computer chips that contain the central processing unit and main memory. Processing caters to the desire of users and displays results. It consists of CPU and Main Memory.

Storage Devices are available in huge sizes. Programs and data can be stored on storage devices.

Secondary storage differs from primary storage in that it is not directly accessible by the CPU. Examples of secondary storage are,

- Hard drive
- Flash drive
- CD-ROM drive (mostly outdated) or DVD-ROM drive

1.3.2 What is inside the Computer?

Central Processing Unit (CPU)

The central processing unit (**CPU**) (or microprocessor) is the actual hardware that interprets and executes the program (software) instructions and coordinates how all the other hardware devices work together. The CPU is built on a small flake of silicon and can contain the equivalent of several

million transistors. We can think of transistors as electronic switches that allow a current to pass through i.e. “on” or “off” i.e. taking a value of 1 or 0.

The processor or **Central processing Unit (CPU)** is the brain of the computer. The main function of CPU is to execute programs stored in memory. It consists of three functional units:

1. Control Unit (CU)

Fetches Program from the memory and determines their type

- Controls the flow of data and instruction to and from memory
- Interprets the instructions
- It simply controls which ones to execute and when

2. Arithmetic and Logical Unit

Performs Mathematical and Logical operations

- Performs arithmetic operations such as addition, subtraction, multiplication, logical comparison of numbers equal to, greater than, less than, etc.

3. Registers

Small High Speed Memories that store temporary results

- High-speed memory units within CPU for storing small amount of data (Mostly 32 or 64 Bits)
- Registers could be
 - **Accumulators:** they can keep running totals of arithmetic values.
 - **Address Registers:** they can store memory addresses which tell the CPU where in memory an instruction is located.
 - **Storage Registers:** they can temporarily store data that is being sent to or coming from the system memory.
 - **Miscellaneous:** general purpose used for several functions

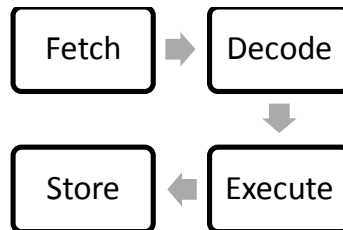
Bus Lines

The CPU is connected through Bus lines with main memory and I/O Devices. The computer buses of one form or another move data between all of these devices. The basic job of Bus is to move data from one location to other within the computer.

Instructions within processor

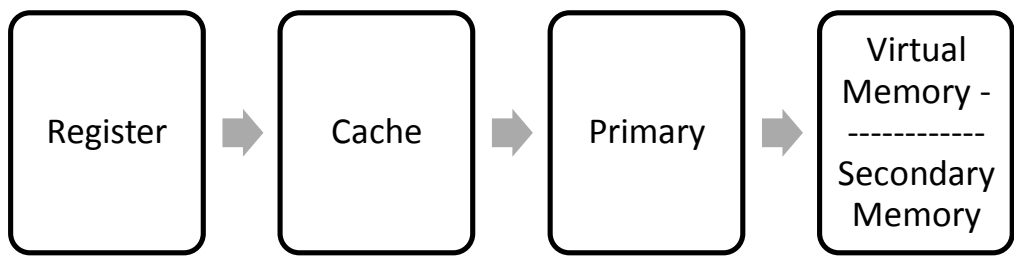
The CPU -- the centrepiece of the computer's architecture -- is in charge of executing the instructions of the currently loaded program. These instructions tell the CPU to carry out various calculations, to read and write values from and into the memory, and to conditionally jump to execute other instructions in the program.

Machine Cycle: is the steps performed by the CPU for executing an instruction. The steps are Fetch-Decode-Execute and store which gets executed within CPU.



These phases, **fetch** and **decode** are done by **CU** or Control Unit whose job is explaining to **ALU** or Arithmetic Logic Unit whose job is to **execute** and the results are **stored** in **Register**

1.3.3 Memory



Memory Hierarchy

Memory is where data and programs are stored. Various types of memory devices are

Internal memory

Registers are internal memory within CPU, very fast and very small

Primary Memory

These are devices in which any location can be accessed in any order (in contrast with sequential order). These are of primarily two types:

- **Random access memory (RAM)**

It is a Read write memory.

Information can be read as well as modified.

Volatile in nature, means Information is lost as soon as power is turned off.

- **Read Only Memory (ROM)**

It is a Non Volatile in nature (Contents remain even in the absence of power). Usually these are used to store small amount of information for quick reference by CPU. Information can be read not modified.

ROM is generally used by manufacturers to store data and programs.

- **PROM** (Programmable Read only memory) Non-volatile, Desired data and program must first be programmed e.g. used by video game manufacturers for game instructions.
- **EPROM**(Erasable Programmable Read only memory)-can be erased using UV light and reprogrammed e.g. used in Industrial Robots by car Manufacturers, can be changed with change of car model
- **EEPROMS**(Electrically Erasable Programmable Read only memory)-where chip is erasable electrically by using higher electric current e.g. used in pen drives

Cache Memory

There is a huge speed difference between Registers and Primary Memory, to bridge these speed differences we have cache memory. Cache (Pronounced kăsh) is a smaller, faster memory which stores copies of the data from the most frequently used main memory locations and processor/registers can access it more rapidly than main memory.

Cache memory is something like, we record frequently used telephone numbers in our mobile which we can access quickly otherwise we have to go to telephone directory which takes a longer time. Cache memory works on the same principle frequently used data is stored in easily accessible cache memory instead of slower memory like RAM. Because, there is less data in cache, processor can access it more quickly. There are two types of Cache memory

- **Level 1 (L1)** cache which is available in CPU
- **Level 2 (L2)** cache which is available on mother board of most systems

Now with multi-core chips, Level 3 (L3) cache has also been introduced.

Virtual Memory

Virtual Memory is in fact not a separate device but an imaginary memory area supported by some operating systems (for example, Windows) in conjunction with the hardware. If a computer lacks the random access memory (RAM) needed to run a program or operation, the OS uses a predefined space on hard disk as an extension of RAM. Virtual memory combines computer's RAM with temporary space on the hard disk. When RAM runs low, virtual memory moves data from RAM to a space called a paging file or swap file. Moving data to and from the paging file frees up RAM to complete its work.

Thus, Virtual memory is an allocation of hard disk space to help RAM. With virtual memory, the computer can look for areas of RAM that have not been used recently and copy them onto the hard disk. This frees up space in RAM to load the new applications. Area of the space on hard disk which acts as an extension to RAM is called a page file or swap file. In some operating systems an entire disk or partition can be devoted to virtual memory.

Secondary Memory

CPU refers to the main memory for execution of programs, but these main memories are volatile in nature and hence cannot be used to store data on a permanent basis. Moreover, they are very small in sizes. The secondary memories are available in huge sizes. Thus programs and data can be stored on secondary memories.

Secondary storage differs from primary storage in that it is not directly accessible by the CPU. The computer usually uses its input/output channels to access secondary storage and transfers the desired data using intermediate area in primary storage. Secondary storage does not lose the data when the device is powered down—it is non-volatile.

The features of secondary memory devices are

- **Non-volatility:** Contents are permanent in nature
- **Greater capacity:** These are available in large size
- **Greater economy:** The cost per unit information of these is lesser compared to RAM.
- **Slow:** Slower in speed compared to registers or primary storage

Storage devices could differ amongst each other in terms of:

- Speed and access time
- Cost / Portability
- Capacity
- Type of access

Based on these parameters most common forms of secondary storage are:

- Hard Drive
- DAT Tapes
- Pen Drives
- CD, DVD and Blue ray Disks
- Smart card

The kind of storage we need would depend on our information system objectives.

1.4 Data representation in Memory- Bits and Bytes

The computer has switches to represent data and switches have only two states: ON and OFF. Binary has two digits to do the counting: 0 and 1 - a natural fit to the two states of a switch (0 = OFF, 1 = ON). Everything (instructions, numeric and character data) in memory is stored in binary form. How it is interpreted is determined by the data or instruction format.

- This Binary Digit has been abbreviated to **Bit**. And a combination of 8 bits is called a **Byte**.
- Some other Binary Units are:
 - **Kilobyte (KB)** = 1024 bytes,
 - **Megabyte(MB)** =1024 KB

- **Gigabyte (GB)** =1024 MB
- **Terabyte (TB)** =1024 GB

ROM and RAM are composed of electronic components that can be in one of two states "on" and "off". So the memory chips are divided into small compartments containing bits, each bit is either "on" or "off" i.e. a 0 or 1.

Memory consists of consecutive bytes it can be more considered like a spreadsheet format. We have columns and rows. They are 8 bits across and could be millions of rows long depending on how much memory we have. The CPU tells the memory controller what column and row it wants for data and the Memory Controller can find it in RAM

Character encoding

To represent numeric, alphabetic, and special characters in a computer's internal storage and on magnetic media, a coding system has to be used. With 8 bits there are 2^8 or 256 possible combinations of "on" or "off" in a byte.

- **ASCII** (American Standard Code for Information Interchange) is essentially a 7-bit code which allows the 8th most significant bit (MSB) to be used for error checking.
- **ANSI (American National Standard Institute) Character set** was used by windows. ANSI is a modified ASCII
- **UNICODE** has replaced all major coding schemes and used 16 bits for character encoding.

Data storage media

Semiconductor

Semiconductor memory uses semiconductor-based integrated circuits to store information, could be volatile or non-volatile. Primary storage like RAM is volatile semiconductor memory. Secondary memory like Flash memory (Pen drives) and now flash-based solid-state drives (SSDs) are Non-Volatile semiconductor memories. Data is represented with switches.

Magnetic

Magnetic storage uses different microscopic magnets of different polarities to store information. Magnetic storage is non-volatile. Hard Disks, Tape Drives provide Magnetic Storage. In Magnetic Storage, data (0 or 1) is represented with polarity of Magnetic field.

Optical storage

Optical storage stores information by creating microscopic pits on the surface of a circular disc and reads this information by illuminating the surface with a laser diode and observing the reflection. Optical disc storage is non-volatile CDs, DVDs and Blue-ray all use optical means to store Data.

1.5 Hardware Asset Management

Information systems acquisition, development, and maintenance should be considered in the context of the organisation's IT long- and short-range plans. COBIT* (Control Objectives for Information and Related Technology) framework provides best practices for hardware policy areas for IT functions. Some key factors to consider are:

- Acquisition: How is hardware acquired from outside vendors?
- Standards: What are the hardware compatibility standards?
- Performance: How computing capabilities should be tested?
- Configuration: Where client/servers, personal computers, and others are be used?
- Capacity Monitoring: Is capacity monitored for efficient operations?
- Service providers: Should third-party service providers be used?

** COBIT is a business framework created by ISACA (Information System and Control Association) for the governance and management of enterprise Information Technology. ISACA provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems.) COBIT is available as a free download at www.isaca.org.*

1.5.1 Hardware Acquisition

Acquisition of Hardware might be necessitated due to: initial deployment or expansion of existing capacities or in response to demands of a new Application like ERP or could even be a replacement for retired computer systems. Hardware acquisition is not only limited to computers but also to all equipment and peripherals associated with the entire computer system, such as printers, scanners, modems, routers, and DVD-ROMs. Before providing specifications on what is needed to vendors in the form of an Invitation to Tender (ITT), it is essential to prepare a checklist based on the following evaluation criteria.

Evaluation Criteria

- Compatibility and Industry Standards
 - Is the hardware to be procured compatible with the existing one and does it take care of future applications?
 - Have the workload and performance requirements been calculated and is the hardware suggested capable of fulfilling them?
 - Are there any industry standards for the same, and do the hardware components comply with them?
- Ease of Operations
 - Can the hardware be installed and maintained by locally available engineers?
 - Can the hardware be serviced, maintained, and upgraded locally?
 - Does the hardware need any special training for its operation or will the users be able to access/use it with minimal additional technological competence?

- Support
 - What type of technical support will be provided by the vendor?
 - Are appropriate manuals for various operations available?
 - If so, are they available in a variety of media?
 - Can the manuals be understood by intended users?
 - Does the vendor have a strong Research and Development Division with adequate staff?
 - Will the vendor help in the smooth transition from the existing application to the new one?
 - What is the quantum of training that the vendor will provide?
 - What is the backup facility that the vendor will provide?
- Cost
 - Is the cost quoted competitive and comprehensive?
 - Are all the requested components included in the purchase price?
 - Are there any hidden costs?
 - Will the vendor provide support at an affordable cost?
- For acquiring Hardware any organisation would issue, an ITT (Invitation to Tender) or RFP (Request for Proposal).

ITT or RFP

The ITT or RFP documents the requirements of organisation. It has to inter alia include the following:

- **Information processing requirements:** In terms of workload and performance requirements in accordance with applications which are proposed to be implemented.
- **Hardware requirements:** In terms of Processing Speed, peripheral Devices and Network capability required as per business need.
- **System software applications:** In terms of Operating System, Database management Software and other system software requirements.
- **Support requirements:** In terms of post implementation support and training.
- **Adaptability requirements:** In terms of Compatibility with existing infrastructure and up gradation capabilities.
- **Constraints:** In terms of Delivery dates
- **Conversion requirements:** In terms of testing, pricing, structure and schedule.

ITT or RFP evaluation

The bids received from vendor in response to ITT/ RFP have to be analysed based on defined evaluation criteria for:

- Existing User Satisfaction
- Vendor Financial condition
- Maintenance facilities

- Delivery schedules
- Up gradation capabilities
- Benchmarking
- Contract terms (Right to audit)
- Price

Metrics for selecting Hardware

Some of the key metrics which are considered in selecting hardware are:

- **Turnaround Time:** Length of time for submission of the job and receipt of completed output.
- **Response Time:** Length of time between submission of transaction and first character of output.
- **Throughput:** The amount of work done over the period of time.
- **Compatibility:** Hardware to be procured compatible with the existing one.
- **Capacity:** In accordance with workload and performance requirements.
- **Utilisation:** Fit for the purpose it is to be acquired.

1.5.2 Hardware Maintenance Program

It is common for organisations to outsource the maintenance of computer hardware, which includes any or all of desktops, servers, networks, cabling, etc. One of the important criteria that need to be considered before finalizing the vendor is the issue of maintenance.

The organisation must have a hardware maintenance program that takes into consideration the following:

- Which company takes care of what IT resource? For example, computers may be serviced by one company and printers by another.
- How many times during a year does the vendor provide preventive maintenance and when?
- Was any problem reported in the past, and what corrective steps were suggested? This has to be documented.
- What is the cost of maintenance? Has, at any time during the year, the amount spent on maintenance exceeded the budgeted amount? If yes, the details have to be documented.
- Apart from the preventive maintenance schedule, how many times during the year did the vendor come for servicing the equipment because of some snag failure?
- What is the **MTBF** (Mean-Time-Between-Failure) and **MTTR** (Mean-Time-To-Repair) value? Typically, MTBF value must be high and MTTR value must be low.

1.5.3 Hardware Monitoring Procedures

Hardware monitoring procedures help in the hardware maintenance program. Malfunctioned hardware causes server downtime. It is important to employ tools for hardware monitoring. A good monitoring solution leverages investment in existing hardware and monitoring agents.

- Benefits of hardware Monitoring:
 - Flexible monitoring options
 - Enhanced server uptime and proactive alerting
 - Accurate root-cause diagnosis
 - Reduce time to investigate and resolve
 - Lower Total Cost of Ownership (TCO)
 - Fast Return On Investment (ROI)
 - Higher Quality of Service
- The following are the typical reports that are generated:
 - **Hardware Error Reports:** These reports provide details of failures, if any, of hardware resources in an organisation.
 - **Availability Reports:** These reports provide details on the availability of the hardware, software and all associated systems. Being the life-line of the organisation, the availability of IT division must be as per business requirement. If there is any break-down, this report provides details on the same.
 - **Utilisation Report:** All IT resources must be optimally used. If there is excessive utilisation of a resource, steps have to be taken to correct it. Details on utilisation parameters are automatically provided by tools used for monitoring utilisation.

These reports not only help in maintenance but also in effective planning for the future.

1.5.4 Data and Capacity Management

Capacity requirements for a Chartered Accountant's firm are very different from that of a stock broking firm or a retail grocery store. Capacity monitoring is essential to ensure that the challenge of selecting the right size or capacity of the computing architecture (capacity of the various computer systems and components) are appropriate to meet the business requirements. Capacity planning also ensures that the expansion or reduction of resources takes place in line with the overall organisational growth or reduction. Some of the key factors that influence the requirements of each of the key components such as the input devices, RAM, CPU architecture and speed, HDD, output devices, networking capability and capacity are:

- Volume of transactions,
- Complexity of computations, and
- Mode of input and output delivery.

For example, the choice of inappropriate and inadequate software can significantly reduce the operational efficiency of a business and its productivity, which in turn can affect the achievement of its objectives. In the present age, one of the main issues an organisation has to face is the

constant and never-ending growth of data and requirement for greater storage capacity along with the problem of data safety, security and integrity. In modern day enterprises, which employ large scale database applications or multimedia applications, the requirements for disk storage run from gigabytes to terabytes. If a proper data and storage management mechanism is in place, problems of downtime, business loss on account of lost data and insufficient storage space can be avoided.

The key issues in data and capacity management are:

- How to effectively manage rapidly growing volume of data?
- How to leverage data and storage technology to support business needs?
- What is the best data and storage management framework for an enterprising business environment?
- How to optimize the performance of the data storage hardware and software to ensure high availability?
- What is the best way to achieve greater storage capacity?
- How effective is the current data backup and storage management system?

Capacity Planning is planning and monitoring of the computer resources to ensure that the available resources are being used efficiently and effectively, in terms of

- CPU utilisation
- Computer Storage Utilisation
- Telecommunication and Wide Area Network bandwidth utilisation
- Terminal utilisation
- I/O channel utilisation etc.

Like every other investment in an organisation, IT investment too has to be justified on the basis of Returns on Investment (ROI). The capacity of IT resources required, such as processor power, CPU clock speed, hard disk capacity and number of terminals have to be planned meticulously keeping the business requirements of the current and the near future and also the rate of technology obsolescence so that the benefits from IT investments are realised.

Proper capacity planning has the following advantages:

- It assures appropriate infrastructure capacity levels to support existing and future business functions.
- It reduces resource expenditures and IT operating costs.
- It improves application infrastructure availability.
- It enables prioritization and reallocation of existing applications, systems, and network components.
- It projects future resource needs, protecting the infrastructure from slow-downs as capacity demands increase.
- It facilitates improved support of new and existing applications.

1.5.5 Hardware Retirement

Computer Systems have a functional life. They should be replaced at the end of their useful life or when the hardware becomes a barrier to the user. This occurs primarily when the Applications, or the software required for business activity will not run effectively on the existing hardware; or when the existing hardware has begun to malfunction on a repeated basis. Some of the key issues to be addressed in hardware retirement are:

- What to do with the older assets as newer systems come online.
 - Retiring IT equipment possesses data that may be sources of significant economic return; Need to be recycled according to regulations.
- Improper disposing of data and other IT assets
 - Can cause embarrassing security breaches
 - Increase costs
 - Pose the risk of regulatory penalties.
- Policy is needed for
 - Designating a system to be retired
 - Establishing Data Archiving Requirements (data, code, etc.)
 - Establishing Security Requirements (disposal, disposition, sensitive data, etc.)
 - Removal of Data from System Hardware
 - Removal of end-user devices or other equipment (racks, cradles, scanners, etc.)
 - Closure of licensing and/or contracts
 - Reallocation of resources (hardware, memory, support staff, etc.)
 - Finalizing program budget
 - Taking care of e-waste regulations
 - Minimizing Environmental impact.

1.6 Auditing Hardware

- Review the hardware acquisition plan to determine:
 - Whether the hardware acquisition plan is compared to business plan.
 - Whether the environment is adequate for the current installed hardware and provision made for new hardware to be added under the approved acquisition plan.
 - Whether the acquisition plan has taken into consideration deficiencies noted in the former.
 - Whether the acquisition plan has taken into consideration technological obsolescence of the installed equipment, as well as the new equipment in the plan.
 - The adequacy of documentation for hardware and software specifications, installation requirements and the likely lead-time associated with planned acquisitions.

- Review the Microcomputer (PC) Acquisition Criteria to determine:
 - Whether Management has issued written policy statements regarding the acquisition and use of PC's and that these statements have been communicated to the users.
 - Criteria for acquisition of PC's have been developed and that procedures have been established to facilitate the acquisition approval process.
 - Requests for acquisition of PC's are supported by cost benefit analysis.
 - All PC's are purchased through the IS purchasing department to take advantage of volume discounts and standardization.
- Review of the Capacity Management Policy and Procedures for hardware
 - Whether the procedure in place will ensure continuous review of hardware and system software performance and capacity.
 - Whether the criteria issued in the performance monitoring plan are based on historical data obtained from problem logs, processing schedules, accounting system reports, preventive maintenance schedules and reports.
- Review Hardware performance-monitoring plan to determine, whether it
 - Includes a review of problem logs, processing schedules, system reports, and job accounting reports.
- Problem log review
 - The problem log assists in identifying hardware malfunctions, operator actions, or system resets that negatively affect the performance of the IT infrastructure. The IT organisation should regularly monitor the problem log to detect potential IT resource capacity issues.
- Review Hardware availability and performance reports
 - Review and ensure that the services required by the organisation (CPU utilisation, storage utilisation, bandwidth utilisation, and system uptime) are available when needed and that maintenance procedures do not negatively impact the organisation's operations.

1.7 Summary

Modern organisations are heavily dependent on automated information systems for performing processing of transactions whether it is related to delivery of product or services. The basic infrastructure required to develop, maintain and sustain Information Systems is IT. Hardware is one of the important components and includes the input, output, processing and storage devices. It is important to understand functionality of various components of hardware as hardware is the important resource in managing capacities for effective and efficient working of an enterprise. Investment in IT hardware is a major investment and its maintenance is a major component of expenditure. Hence, effective and optimum utilisation of IT asset is important function in in any organisation to ensure organisational goals are achieved.

1.8 References

- <http://www.cio.in>
- Ralph M. Stair, George W. Reynolds, 'Principles of Information Systems', Cengage Learning
- www.whatis.com
- www.howstuffworks.com
- www.google.com
- www.wikipedia.com
- www.youtube.com

PART 2: SYSTEMS SOFTWARE

Learning Objectives

- To gain understanding of system software and application software
- To understand operating systems
- To understand various types of system software
- To gain understanding of software asset management
- To understand how to audit software

2.1 Introduction

Computer hardware constitutes the physical components and works based on the instruction input given by the users and other programs. These set of instruction input are called software. The term software in its broad sense refers to the program that the machine executes. Software is an intangible portion whereas hardware is tangible part which we can touch and see. Computer Software is the collection of computer programs, procedures and documentation that perform different tasks on a computer system. Program software performs the function of the program it implements, either by directly providing instructions to the computer hardware or by serving as input to another piece of software.

2.1.1 Software

Software consists of clearly-defined instruction sets that upon execution, tell a computer what to do. It is a set of instructions which when executed in a specified sequence accomplishes desired task. The most critical function of software is to direct the working of computer hardware. This causes a computer to perform useful tasks. There are two broad categories of software:

1. System Software
2. Application Software

1. System Software

System software is a collection of computer programs used in design, processing and control of application software. System software coordinates instructions between applications and hardware. It is the low-level software required to manage computer resources and support the production or execution of application programs but is not specific to any particular application.

- These refer to the set of programs that -
 - Enable a computer to work.
 - Control the working of a computer.

- Provide facilities for programmers to develop applications.
- Enable various I/O devices to be connected
- Help in the efficient use of computer resources.
- Includes:
 - Operating System
 - Data communication
 - Data Base management software (DBMS)
 - Access control
 - Tape and disk management systems
 - Program library management systems
 - Network management software
 - Program Development Software
 - Job scheduling
 - Middleware
 - Utility programs

2. Application Software

Users interact with Application Software. It refers to the set of software that performs a specific function directly for the end-user. It is a collection of programs which address a real life problem for its end users, may be business or scientific or any other problem. There are varieties of application software for different needs of users. Some of the Application Programs could be

- Application Suite: E.g. MS Office etc.
- Enterprise Software: E.g. ERP Applications like SAP, etc.
- Enterprise Infrastructure Software: E.g. email servers, Security software.
- Information Worker Software: E.g. CAAT (Computer assisted audit tools), etc.
- Content Access Software: E.g. Media Players etc.
- Educational Software: E.g. ELearning, Examination Test CDs
- Media Development Software: E.g. Desktop Publishing, Video Editing etc.

2.2 Operating System

One of the prominent System Software is Operating System. Operating system is a set of programs implemented in software, hardware and firmware that permits sharing and use of resources. It is a set of programs which act as intermediary agent between the user and the computer hardware. It controls and manages the computer hardware resources among various processes. Also called a Resource Manager, an Operating System helps in the efficient management of the important resources of RAM, CPU, and various I/O devices (which include secondary storage devices also) and the information that is held in the machine.

The Operating System also enables users to interact with the machine and takes care of technical aspects of a computer's operation. It shields the user of the machine from low-level details of the machine's operation and provides frequently needed facilities.

2.2.1 Types of Operating Systems

- Single User OS
 - One user uses system at a time. It could do single or multiple tasks.
 - Single task operating system e.g.: MS-DOS (now outdated)
 - Multi Task system e.g.: MS Windows 7 or 8
- Multi User OS
 - Several users use System at a time.
 - Example: Unix, Windows 7 or 8
- Multi-Processing OS
 - OS operates on system with more than one processor.
 - Multiprocessor systems, also known as Parallel systems or Tightly-coupled systems have more than one processor in close communication, sharing the computer bus, the clock, and sometimes memory and peripheral devices.
 - The main advantages of multiprocessor systems are:
 - Increased throughput: By increasing the number of processors, more work can be done in lesser time.
 - Economies of scale: Multiprocessor systems save more money than multiple single-processor systems, because they can share peripherals, mass storage, and power supplies.
 - Increased reliability: If functions can be distributed properly among several processors, then the failure of one processor will not halt the system, only slow it down.
- Real time OS
 - Used in embedded systems with only small set of tasks.
 - In these systems time is very critical and has to operate in real time.
 - A real time system is used when rigid requirements are placed on the operation of a processor or the flow of data; thus, it is often used as a control device in a dedicated application.
 - Some automobile-engine fuel-injection systems, home-appliance controllers and weapon systems are also real time systems.
 - A real time system has well-defined, fixed time constraints. Programs must be done within the defined constraints, or the system will fail.
 - Micro C/OS-II is a typical example of RTOS

Some major OS capabilities are:

- Multi-tasking
 - Refers to multiple tasks running simultaneously by sharing the CPU time.
 - Allows computing systems to run two or more tasks, applications concurrently.
 - At any point in time the CPU is executing one task only while other tasks wait for their turn.
 - The illusion of parallelism is achieved when the CPU switching of tasks takes place.

- Multi-processing
 - Links more than one processor (CPU)
 - If the underlying hardware provides more than one processor then that is multiprocessing.
- Multi-threading
 - It is an execution model that allows a single process to have multiple code (threads) run concurrently within the context of that process
 - Runs several processes or threads of a program simultaneously.
 - Threads can be imagined as child processes that share the parent process resources but execute independently.

2.2.2 Functions of Operating Systems

- Processor management
- Memory management
- Device management
- File management
- Secondary storage management
- Networking
- Application programme interface
- User interfaces with system

Processor Management

In multitasking environment, OS decides which task (process) gets the processor when and for how much time. This function is called process scheduling.

Operating System does the following activities for processor management.

- Keeps tracks of processor and status of process.
- Allocates and de-allocates the processor (CPU) to a process.
- Creating and deleting both user and system processes by suspending and resuming processes.
- Providing mechanisms for process synchronization.
- Providing mechanisms for process communication.
- Providing mechanism for deadlock handling.

Memory Management

Memory management refers to management of Primary Memory or Main Memory. Main memory is a large array of words or bytes where each word or byte has its own address. Main memory provides a fast storage that can be accessed directly by the CPU. So, for a program to be executed, it must be in the main memory.

- Operating System does the following activities for memory management.
 - Keeping track of the parts of memory that are currently being used and by whom.
 - Deciding the processes that are to be loaded into memory when memory space becomes available.
 - Allocating and de-allocating memory space as per need.
- Operating systems also supports **virtual memory** which carves an area out of hard disk to supplement the functional memory capacity of RAM i.e. it augments memory or RAM.

Device Management

One of the purposes of an operating system is to hide the peculiarities of specific hardware devices from users, which is done by I/O subsystem itself.

- The I/O subsystem consists of:
 - A memory management component that includes buffering, caching and spooling.
 - A general device called driver interface.
 - Drivers for specific hardware devices
- OS manages device communication via their respective drivers.
- Operating System does the following activities for device management.
 - Keeps tracks of all devices. Program responsible for this task is known as the I/O controller.
 - Decides which process gets the device when and for how much time.
 - Allocates and de-allocates the device in the efficient way.

File Management

A file system is normally organized into directories for easy navigation and usage. These directories may contain files and other directories.

- Operating System does the following activities for file management.
 - Keeps track of information, location, uses, status etc. The collective facilities are often known as file system.
 - Decides who gets the resources.
 - Allocates and De-allocates the resources.
 - Creating and deleting files.
 - Creating and deleting directories.
 - Mapping files onto secondary storage.
 - Backing up files on stable storage media.

Secondary Storage Management

The operating system is responsible for the following activities in connection with the disk management:

- Free space management.
- Storage allocation.
- Disk scheduling.

Networking

The processors in the system are connected through a communication network, configured in a number of different ways. Different protocols are used to communicate between different computers.

Protection System

Protection is a mechanism for controlling the access of programs, processes or users to the resources defined by a computer system. This is achieved by means of password and similar other techniques, preventing unauthorised access to programs and data. This mechanism provides means for specification of controls to be imposed and means for enforcement. Protection mechanism improves reliability by detecting latent errors at the interfaces between computer subsystems.

Other tasks of an Operating System

- **Control over system performance:** Recording delays between request for a service and response from the system.
- **Job accounting:** Keeping track of time and resources used by various jobs and users.
- **Error detecting aids:** Production of dumps, traces, error messages and other debugging and error detecting aids.
- **Coordination between other software and users:** Coordination and assignment of compilers, interpreters, assemblers and other software to the various users of the computer systems.
- **Providing user interfaces:** An important job of any operating system is to provide user interface. If we remember DOS days, it had a Command based User Interface (UI) i.e. text commands were given to computer to execute any command. But today we are more used to Graphic User Interface (GUI) which uses icons and menus like in the case of Windows. So, how we interface with our system will be provided by operating system.
- **Hardware independence:** Every computer could have different specifications and configurations of hardware. If application developer would have to rewrite code for every configuration he would be in a big trouble. Fortunately, we have operating system which provides Application Program Interfaces (API) which can be used by application developers to create application software, thus obviating the need to understand the inner workings of OS and hardware. Thus, OS gives us hardware independence.

Kernel and Shell

Operating System is like Glue which holds a computer together. If we think of it one side of operating system is Hardware and on other side is Application. We can primarily divide operating system into two layers.

- Kernel Layer
 - Controls access to hardware
 - Schedules system resources, memory, CPU.
 - Enforces security to system resources
 - Responds to service calls(How program accesses services from OS) e.g. Accessing hard disk, let's say that a program wants to access hard disk, it will call Kernel of OS for the same and kernel will facilitate it.
- Shell Layer
 - Surrounds kernel
 - Provides Interface for applications
 - Creates environment for application execution and user interface

2.3 Other Type of System Software

2.3.1 Program Development Software

Programming software usually provides tools to assist a programmer in writing computer programs and software by using different programming languages in a convenient way. Software tells computer what to do, and then obviously this program has to be written. This program is written in some programming languages. There have been various generations of programming languages.

First-generation language 1GL: Machine Language

- First-generation language is machine language or the level of instructions and data that the processor is actually given to work on (which in conventional computers is a string of 0s and 1s).
- The first generation program language is pure machine code, that is just ones and zeroes,
- Long Instructions
- Machine dependent.

Second-generation language 2GL: Assembly Language

- Second-generation language is assembly language.
- By using codes resembling English programming becomes much easier.
- Use of mnemonic codes such as LDA for load and STA for store means the code is easier to read and write.
- Machine dependent.

Third-generation language 3GL

- High Level language and English like.
- Problem oriented, for scientific problems we had FORTRAN, for business Problems-COBOL
- Third-generation programming languages brought many programmer-friendly features.
- It has to be told what to do and how to do.
- Can be platform independent

Fourth-generation language 4GL

- Still more English like.
- Easier to use
- Many pre-programmed functions
- It uses declarative language i.e. it has only to be told what to do, not how to do.
- Includes Data Management features

Fifth-generation language 5GL

- Used mainly in Artificial Intelligence (AI)
- Designed to make the computer solve a given problem without the programmer.
- Programmer only has to bother about problems to be solved and conditions to be met.
- It primarily ended as hype due to expectation mismatch.
- Subsequently vendors tried to use the term to sell their packaged 4GL products.
- Languages like PROLOG, LISP, KL-1, Mercury etc.

Program development tools

Assembler: A computer will not understand any program written in a language, other than its machine language. The programs written in other languages must be translated into the machine language. Such translation is performed with the help of software. A program which translates an Assembly language (2GL) program into a Machine language (1GL) program is called an assembler.

Compiler: It is a program which translates a high level language program into a machine language program. A compiler is a computer program (or a set of programs) that transforms the source code written in a High level language (the source language) into Machine language (Binary language) called Object Code. In a compiler debugging is difficult, because a compiler goes through the entire program and then translates the entire program into machine codes. The machine codes generated by compiler are saved permanently for future reference.

Interpreter: An interpreter is a computer program that executes instructions line by line, i.e. performs instructions written in a programming language. An interpreter is a program which translates statements of a program into machine code. It reads only one statement of program,

translates it and executes it, thus Debugging is easier. It occupies less memory space. The machine codes produced by interpreter are not saved.

SQL Engine: It converts SQL statement to Machine Code.

Debugger: A debugger is a utility that helps in identifying any problem occurring during execution. By using the debugger utility, one can pinpoint when and where a program terminates abnormally, indicates the value of the variables used, and in general provides information so that the programmer can locate bugs.

Linker: Linking is the process of combining various pieces of code and data together to form a single executable unit that can be loaded in memory. The process of linking is generally done during compilation of the program. After linking, the loading process takes place by using loader software.

Loader: A loader is a program which loads the code and data of the executable object file into the main memory, goes to the very first instruction and then executes the program.

Editor: An editor program is a system software utility that allows the user to create and edit files. During the editing process, no special characters are added. On account of this, the editor utility is used to create the source code.

2.3.2 Access Control Software

Access control software is now generally embedded as functions in Operating Systems and DBMS. Access Control Software is used for:

- Analysing who is accessing and using data.
- Who is controlling the data,
- Secure access to data, files, system resources
- Assign ownership of all data for accountability
- Logging access activity

2.3.3 Data Communications Software

Communications software is generally embedded in the computer operating system.

- Communications software assists Operating System in managing local and remote terminal access
 - to host resources,
 - to manage security
- E.g. terminal emulators, file transfer programs

2.3.4 Utility Programs

Utility software is a computer software designed to help manage and tune the computer hardware, operating system or application software by performing a single task or a small range of tasks. Some types of utility software are integrated into the major operating systems.

The functions of Utility software are:

- To manage a computer's functioning
- To improve operational efficiency e.g. Defragmenters
- To understand application systems.
- To facilitate assessing or testing data quality.
- To test a program's ability to function correctly and maintain data integrity.
- To assist in fast program development.

Some utility software are:

- Disk Storage Utilities including Disk defragmenters, Disk checkers, Disk cleaners, Disk partitioners, Backup, Disk compression, file managers and Archive.
- Data Compression Utilities
- Cryptographic Utilities
- Network managers
- Registry cleaners

2.4 Security and Controls in Operating System

Operating System should be robust, reliable, and free of Integrity flaws. Operating system's processes and kernel do the designated task as instructed. A malicious program could make these process do malicious tasks. OS can be secured through proper user access and it has to be protected through anti-virus, firewalls, anti-spyware and patch management.

2.4.1 Access Controls in OS

Access control is the process of authorizing users, groups, and computers to access objects which could be files, directories etc. on the computer. Operating system access controls is the first layer of access controls which mainly rely on hardware features of processor which control which memory addresses a process can access. The access controls provided with an operating system typically authenticate users using some mechanism such as passwords etc. then mediate their access to files, communications ports, and other system resources.

Access Control in most of operating systems is operated through Access Control Lists (ACL). ACL is a list of "who" has "what" access to an Object. An access control list (ACL) is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. As the operating system works with files, this will usually be the smallest object with which its access control mechanisms can deal. ACLs are widely used in

environments where users manage their own file security. ACL is a matrix of access permissions, with columns for files, objects and rows for users and related capabilities.

	File A	File B	Prog. X
Role A	Read Write	Write	
Role B	Read	Read Write	
Role C			Execute

Access control lists are widely used, often with Roles. Where Role = set of users, which could be Administrator, User, Guest. In a Role Based access Control, permissions are given based on roles and through roles each user gets permissions based on Roles they are assigned to.

2.4.2 Access Control in Windows

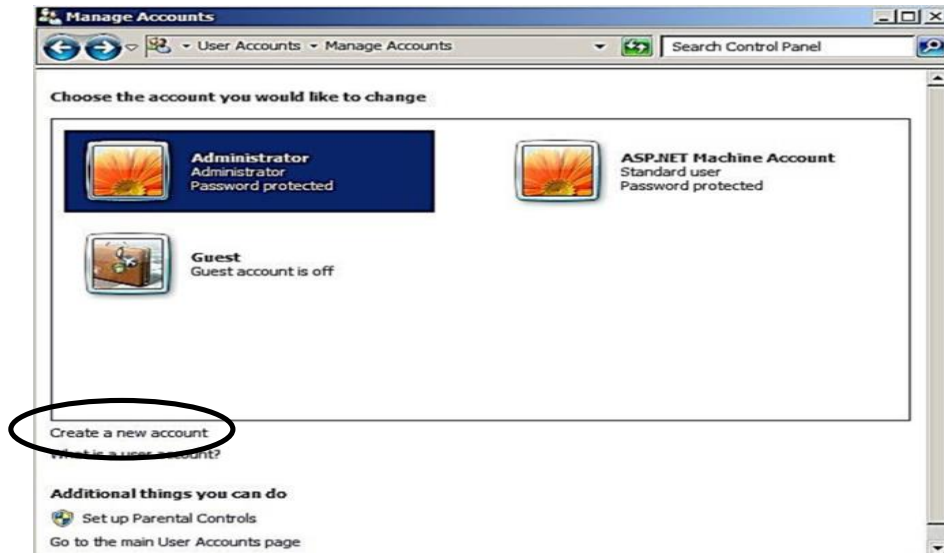
Implementing right level of access is most critical to ensure that access to information is provided to employees and other users as per organisation needs and based on the organisation structure. The principle of ensuring proper segregation of duties is also implemented through access controls. As operating system software is the first entry point for the user, the key functions of OS relating to user management has to be properly implemented as per security policy of the organisation. Auditors have to review whether these are as per policy outlined by the senior management. It is highly advisable that auditors become familiar with the whole process of user management right from user creation to deletion. How to create users, how to define specific roles, grant access to specific modules and functions, how to grant permissions and how to review and enable security auditing are covered here for Windows OS. Similar functions would be available in other operating systems but the way functionality works would vary from one OS to another:

- User creation
- Assign roles
- User rights and privilege
- Permissions
- Security auditing

The topic of Access Controls is covered in more detail in Chapter-5: Logical Access Controls in Module-4: Protection of Information assets of ISA 2 course. This is also covered in hands on training of Module-4.

User Creation

In Windows 7 we can create a user by going to Control Panel > User Accounts > Manage accounts as shown in the next page.



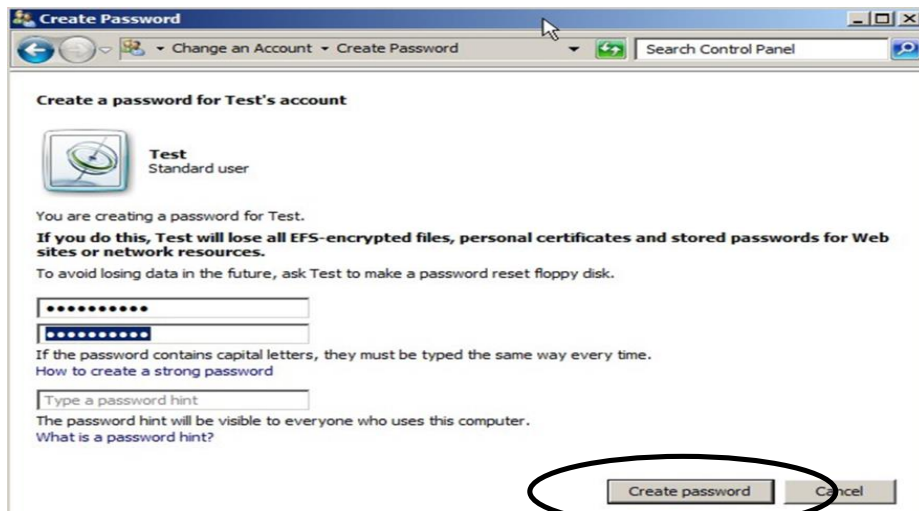
Assign Roles

In Windows 7 we can assign roles by going to Control Panel > User Accounts > Manage accounts. The default Roles could be Standard User or Administrator



Assign Password

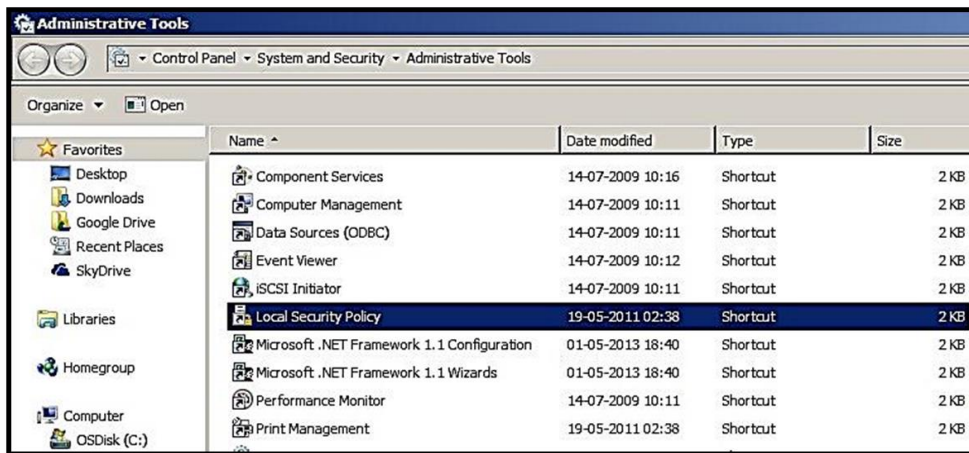
In Windows 7, we can assign password by: Control Panel > User Accounts > Manage accounts



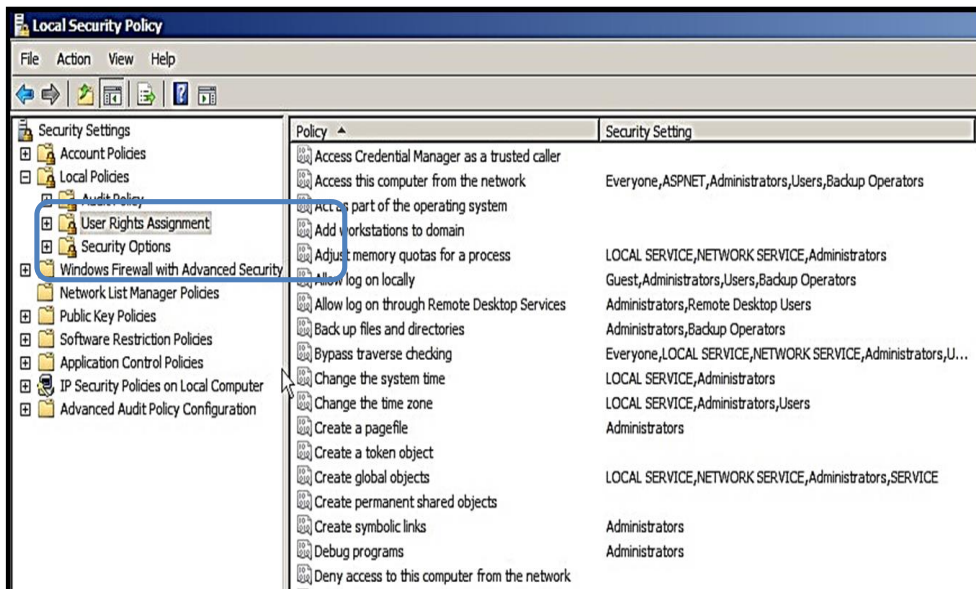
User rights and permissions

User Rights apply to user accounts, and Permissions are attached to objects. For assigning User Rights we go to Start > Control Panel > System and security > Administrative Tools > Local Security Policy

Module 1: e-Learning

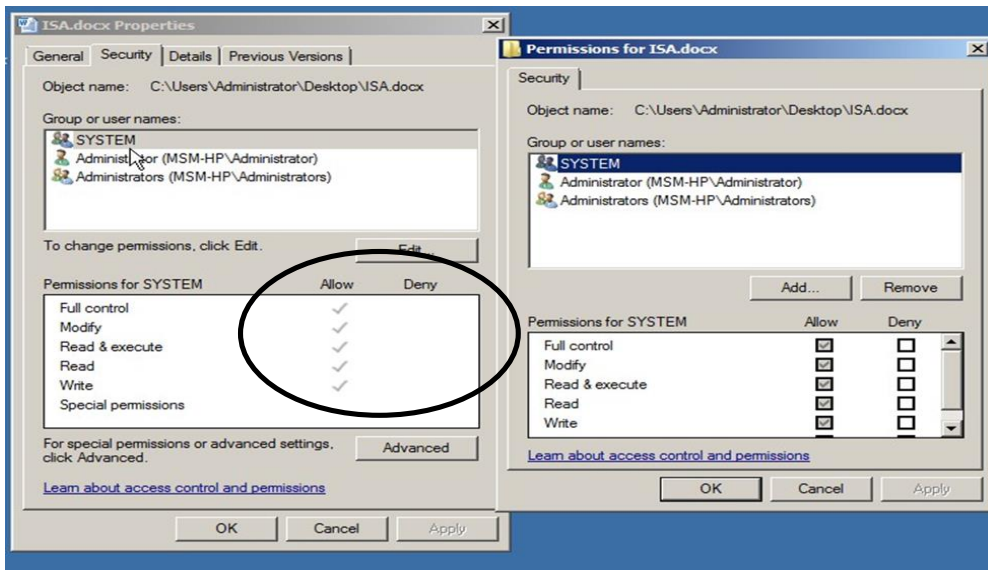


Click on User Rights assignment



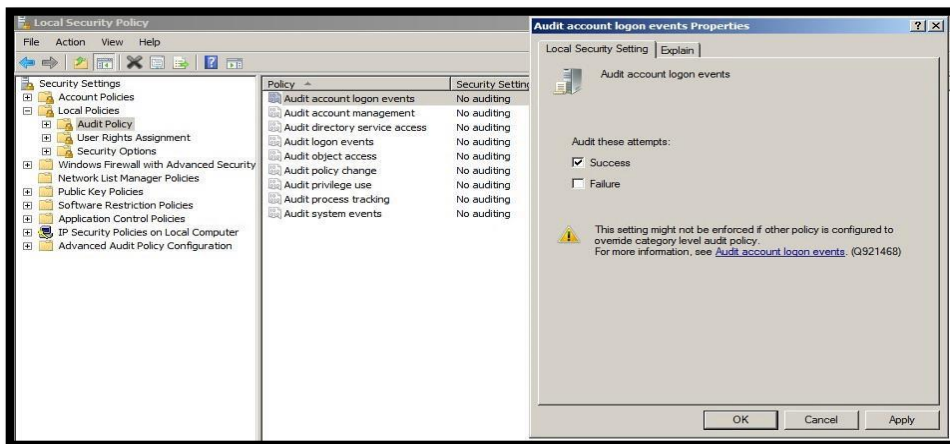
Permissions

Permissions are attached to objects. Right Click on Properties > Security Tab > Advanced or Edit



Security Auditing: User Access

Audit access to Object, Logon, System events. For Logging User Events: Go to Start> Control Panel>System and security> Administrative Tools>Local Security Policy>Local Policies> Audit Policy



2.5 Software Acquisition

The software (operating systems, applications, database-management systems, and utilities) must meet the needs of the organisation. With a wide variety of software products available, their acquisition, implementation, maintenance, and integration is a challenge for any organisation.

Some of the critical factors to be considered by an organisation would be considering during software acquisition are discussed here. **This topic is covered in more detail in chapters 1 and 5 of Module-5: Software development, acquisition and maintenance.**

Requirements Definition

The key tasks that should be considered for requirement definitions:

- Establish the scope, objectives background and project charter.
- Establish business requirements.
- Develop a conceptual model of the base computer environment that will support the efficient application development and processing required to meet the business needs and structure.
- Develop security, control and performance requirements.
- Consolidate the definition of all requirements.
- Analyse and evaluate alternative solutions.

Software Alternatives

The key tasks that should be considered in evaluating software alternatives are:

- Criteria for selecting or rejecting alternatives.
- Cost factors in development vs. purchase decision.
- Software cost.
- Initial and continuing support availability.
- Delivery schedule including lead time requirements.
- Requirements and constraints in order to use the software.
- Capabilities and limitations of the software.
- Potential risk of using a package in terms of future costs and vendor access to the organisation.
- Selection advice from vendors, comparable installations and consultants.
- Compatibility with existing in-house system software.
- Financial stability of the software suppliers.
- Technical expertise of the software suppliers.
- Cost/Benefit Analysis

2.5.1 System Software Acquisition

When acquiring system software, we have to consider the following:

- Business, functional and technical needs and specifications
- Cost and benefit(s)
- Obsolescence
- Compatibility with existing systems
- Security

- Demands on existing staff
- Training and hiring requirements
- Future growth needs
- Impact on system and the network performance

System Software Implementation

It has to be ensured that all appropriate levels of software have been implemented. Any patches or service packs have been implemented and any predecessor updates have taken place.

System Software Change Control Procedures

- All software must follow a formal change-control process.
- System software changes are scheduled when they least impact transaction processing.
- A written plan is in place for testing changes to system software.
- Tests are completed as planned.
- Problems encountered during testing are resolved and the changes are re-tested.
- Test procedures are adequate to provide reasonable assurance that changes applied to the system correct known problems and do not create new problems.
- Software will be identified before it is placed into the production environment.
- Fall-back or restoration procedures are in place in case of production failure.

Software Licensing Issues

Organisations need to ensure that all software used are licensed to ensure compliance. Proof of ownership should be supplemented with following documents::

- Software License Terms -End User License Agreement (EULA)
- Certificate of Authenticity (COA)
- Original media and manuals
- Purchase invoice and/or receipt

2.5.2 Application System Acquisition

Application software could be off the shelf purchase or could involve Software Developments.

Off the Shelf Purchase

Some of the factors to be considered when making off the shelf purchase are:

- Compatibility
- Reliability
- Benchmarks

- Cost
- Functionality
- Vendor support
- Viability of vendor
- Flexibility
- Documentation
- Response time
- Ease of installation

Software Development

If we have planned for Software development the steps involved are:

- **Requirement Definition-** Business requirements are gathered in this phase. Questions answered are: Who is going to use the system? How will they use the system? What data should be input into the system? What data should be output by the system?
- **Requirement Analysis-** These requirements are analysed for their validity and the possibility of incorporating the requirements in the Application and a Requirement Specification document is created
- **Design-** software design is prepared from the requirement specifications
- **Coding-** Based on the Design, code is produced by the developer and is the longest phase.
- **Testing-** Code produced is tested against the requirements to make sure that the product is actually solving the needs addressed and gathered during the requirements phase
- **Changeover and Implementation-** After successful testing the product is deployed in the live environment.
- **Post Implementation Review:** Once the user starts using the developed system then the actual problems crop up and these have to be solved from time to time.
- **Maintenance-** The process where the corrections and up gradations for the developed product is known as maintenance.

2.6 Software Asset Management (SAM)

ITIL (Information Technology Infrastructure Library) defines Software Asset Management as: “the entire infrastructure and processes necessary for the effective management, control and protection of the software assets within an organisation, throughout all stages of their lifecycle.” In simple terms it means

- Purchasing,
- Deploying,
- Managing, and Tracking of software from purchase to retirement of the software

Software Asset Management (SAM) is the business practice of using people, processes, and technology to systematically track, evaluate, and manage software licenses and software usage. SAM is a key process for any organisation to meet its legal, financial and reputational responsibilities. SAM answers the following key questions:

- What is installed in the environment?
- What is supposed to be installed?
- Who is using the Software?
- How much are they using it?
- Are they supposed to be using it?
- How are they using it?
- Can they prove they're allowed to use it?

Benefits of SAM

Software is a critical and valuable asset and needs effective management. Key benefits of implementing SAM are:

- Cost Savings
 - With SAM we can control cost through Standardisation.
 - Get volume discounts by going in for volume licensing
 - We might be having redundant programs but once we analyse our programs we might reduce Redundancy.
 - With awareness we have a more streamlined operations
- Risk Management
 - Reduce business, reputational and legal risks.
 - When we go for genuine software is used then the reputational and legal risk is reduced.
 - With updated programs, chances of malware also reduce, reducing the business risk.
- Streamlined Operations
 - Proper software deployment makes software trouble free, leading to better productivity.
 - With genuine software we'll have peace of mind and infrastructure optimisations are possible.
- Good Governance
 - With better compliance with responsibility under regulations will lead to better Governance
- Disaster Protection
 - Updated inventory lets us know what we have.
 - We could also organise offsite backups of the software media that we have.
 - Faster restoration is possible.

Steps to software asset management:

- Take Inventory
 - First, we need to know what we already have.
 - Could be done manually or through tools.
- Get Organized
 - We would also need to build inventory of software assets we have
- Create Policies, procedures and standards for software Life Cycle.
 - Software acquisition
 - Software storage
 - Software implementation and use
 - Software retirement
- Maintain The Plan
 - The SAM plan should be maintained through regular software inventories and regular updates.

2.6.1 Endpoint Management

What is an Endpoint?

An endpoint device is an Internet-capable computer hardware device on a TCP/IP network. Where an information stream is generated or ends. This could be a:

- Computer
- Laptops
- smart phones
- Thin clients,
- POS terminals etc.

In any Distributed environment endpoints need to be deployed, configured, patched, secured and supported.

Endpoint Management solutions encompass

- Patch delivery,
- inventory,
- software distribution,
- OS deployment,
- remote control capabilities, and
- near real-time visibility into the state of endpoints Including advanced capabilities to support server endpoints

Issues

- Difficult to manually identifying systems that require OS migrations, upgrades, or replacements

- Information is not easily available to track hardware and software assets to verify software and hardware contracts
- Managing remote offices with high on-site IT support costs

Why Endpoint Management

- Analyse vulnerabilities (patched or insecure configurations)
- Easily and automatically remediate all the networked endpoints
- Establish and enforce configuration policies across the endpoints
- Distribute and update software packages
- View, modify, and audit properties of the endpoints

Key Benefits of endpoint management

- Cross platform support- handle windows, Unix etc.
- Centralised management for greater control
- Standardised systems to drive consistency
- Streamlined software management to simplify compliance
- Leveraged asset management to improve service levels
- Managed change using best practices,
- Quickly responds to end user needs
- Understanding what you have and where it is
- Optimised client and server software assets
- Simplified software license audits
- Creates detailed asset reports
- Measured and improved IT performance
- Easily created advanced analytics
- Automated IT processes-increased end user satisfaction and better service levels
- Enabled end user self-service
- Empowers the end user

2.6.2 Digital Rights Management

Digital Rights Management refers to technologies and systems that prevent users from doing thing with content that the content provider does not wish them to do. This means ensuring controlled access to information as defined.

We borrow a book from a library for two days, we can't read it in two days, what we can do is get a photocopy of the book but the quality would be poor, would need spiralling to hold the pages together and perhaps cost more than the cost of book itself. But if the book is in digital form i.e. it's an eBook would not cost us a paisa to create a perfect copy. This is where Digital Rights

Management (DRM) comes into play, what is there to protect the Intellectual Property Rights (IPR) relating to the digital content.

DRM removes usage control from the person in possession of digital content and puts it in the hands of a computer program. It refers to any scheme that controls access to copyrighted material using technological means. This is also associated with concept of Data leak prevention (DLP), which is a strategy for making sure that end users do not send sensitive or critical information outside of the corporate network.

Scope of DRM

Digital Rights management consists of all activity conducted in relation to the rights governing the:

- Digital content creation
- Distribution
- Storage
- Retrieval
- Use
- Disposal

Why DRM

- To protect the property rights of an enterprise's assets
- Primarily for protecting data from leak
- To establish the awareness of Intellectual Property Rights (IPR) in society.

Examples of DRM and DLP

- A company sets its servers to block the forwarding of sensitive e-mail.
- An e-book server restricts access to, copying of and printing of material based on constraints set by the copyright holder of the content.
- Software on DVDs that limits the number of copies a user can make.
- A music label releases titles on a type of CD that includes bits of information intended to confuse ripping software.

2.7 Auditing Software

2.7.1 Auditing Operating System Software

When auditing operating system software procurement and implementation procedures, review of configuration, patch management, change control and the documentation, the following approach may be adopted:

- Review system software selection procedures to determine that they:

- Address both, the Information System (IS) requirements and business plans.
 - Include an overview of the capabilities of the software and control options.
 - Same selection criteria are applied to all proposals.
- Review cost/benefit analysis of system software procedures to determine the following:
 - Total cost of ownership has been considered while deciding for System software
 - Hardware requirements
 - Training and technical support requirements.
 - Impact on data security.
 - Financial stability of the vendor's operations.
- Review controls over the installation of changed system software to determine the following:
 - System software changes are scheduled when they least impact transaction processing.
 - A written plan is in place for testing changes to system software.
 - Tests are being completed as planned.
 - Problems encountered during testing were resolved and the changes were re-tested.
 - Fall-back or restoration procedures are in place in case of failure.
- Review Configuration Management and OS Hardening would involve:
 - A review of the pre-defined/default user accounts,
 - Whether the multi-boot option is required, if not whether disabled or not
 - Whether services enabled are as per organisation's business requirements,
 - What devices to be allowed/disallowed
 - What resources are accessible by default by all users?
 - What are the procedures for controlling application of patches?
 - Are the user accounts and particularly the Admin/Super User accounts accessed through a secured access control mechanism?
 - At a PC level, is a personal firewall enabled or not?
- Review system software maintenance activities to determine the following:
 - Changes made to the system software are documented.
 - Current versions of the software are supported by the vendor.
 - Vendor's maintenance activities are logged.
- Review systems documentation specifically in the areas of:
 - Parameter tables.
 - Activity logs/reports.
- Review and test systems software implementation to determine the adequacy of controls in:
 - Change procedures.
 - Authorisation procedures.
 - Access security features.
 - Documentation requirements.
 - Documentation of system testing.
 - Audit trails.

- Access controls over the software in production.
- Review authorisation documentation to determine whether:
 - Additions, deletions or changes to access authorisation have been documented.
 - Attempted violation reporting and follow-up have been documented.
- Review system software security for the following:
 - Procedures have been established to restrict the ability to circumvent logical security access control.
 - Security provided by the system software.
 - Existing physical and logical security provisions are adequate to restrict access to the master consoles.
 - Vendor-supplied installation passwords were changed at the time of installation.

2.7.2 Auditing Software Asset Management (SAM)

The steps involved in auditing SAM include identifying the application to audit, using a tool to generate current usage report followed by analysing the report to:

- Identify non-usage of application – recommendation to remove application.
- Identify any users that haven't used the application for 60+ days – recommendation: Enquire if user needs else remove.
- Ensure users are using the correct version/suite of the application – recommendation: If full suite is not required then buy single application.
- Update audit report.
- Run a new install report and obtain updated compliance figures
- Recommendation for rectifying any non-compliance by purchasing new licenses.

The topics of auditing SDLC and Software are covered in more detail in chapter 8 of Module-5: Software development, acquisition and maintenance and Chapter-6: Auditing Logical Access controls of Module-4 respectively. The hand on training of Module-4 provides practical training on auditing software.

2.8 Summary

Hardware becomes functional only with the software which runs on it. The cost and complexity of software has been continuously increasing over the years. The two most important types of software for any organisation are System Software and Application software. System software includes both operating systems and utility programs. System software controls how various technology tools work with application software. Operating system is one of the important system software as it controls how hardware devices work together and interfaces with applications software. Utility Software provides additional functionality to operating systems. Application Software fulfils the specific information processing needs of an organisation. Software is crucial to the success of any organisation and hence has to be effectively and constantly managed.

Understanding how software works in terms of various features and functionality helps us in optimally managing all the software assets throughout the economic lifecycle.

2.9 References

- Ralph M. Stair, George W. Reynolds, 'Principles of Information Systems', Cengage Learning
- ITAssetManagement.Net
- BSA.org
- <http://www.gcflearnfree.org/computerbasics/2>

PART 3: DATABASE AND DATABASE MANAGEMENT SYSTEMS

Learning Objectives

- To gain understanding of Data Base Management Systems
- To understand Database Models
- To understand Database Languages
- To gain understanding of People involved with DBMS
- To understand Controls features in Database Management Systems
- To understand how to audit DBMS

3.1 Introduction

Every organisation has to manage its information i.e. any organisation should know what it needs in terms of information, acquire that information, organize that information in a meaningful way, assure information quality and provide software tools so that users in the organisation can access information they require. To achieve the above objectives, the organisation has to use Data Base Management Systems (DBMS)

3.2 Data Management

3.2.1 DIKW

For any organisation to survive today the crucial need is to have data and ability to process it.

- The word **Data** is derived from Latin for “to give”, thus “Data” in really gives facts from which additional facts can be inferred.
- **Information** is the data that has been processed within a context into a form to give it meaning or useful for user
- **Knowledge** is the information that has been analysed, assimilated.
- **Wisdom** is the application of knowledge

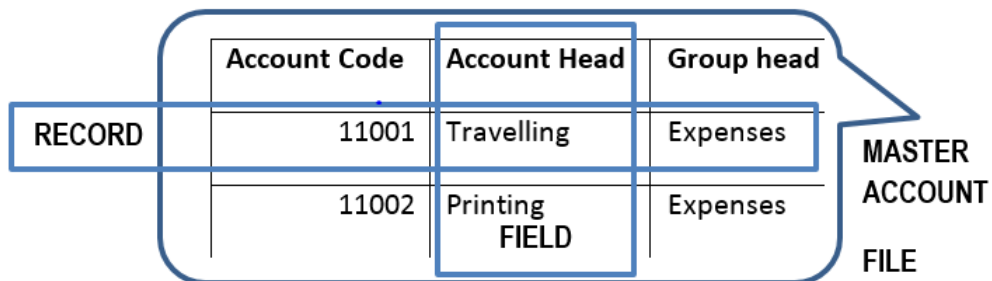
Data Management involved managing the process of data conversion in various states from right from data origination to its conversion as knowledge:

Data > Information > Knowledge > Wisdom.

Data management includes all aspects of data planning, handling, analysis, documentation and storage, i.e. development, execution and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information assets. Let us understand the hierarchy of data base.

3.2.2 Hierarchy of Data

- **Database:** is a collection of related files. For example: accounting database could be a collection of master account file, opening balance file, etc.
- **File:** is a collection of related records
- **Record:** is a collection of related data fields. A record describes an entity, e.g. PAN Number, Name, Gross Salary, Tax Payable are the attributes of the IT Return.
- **Field:** is a collection of characters
- **Characters:** are collection of bits.



3.2.3 Why do we need Databases?

In a traditional file system, the Applications make reference to specific files containing relevant data, e.g. invoicing application would have its invoicing file and accounting application would have its accounting file. But this leads to whole lot of problems:

- **High Redundancy**- Customer details would be recorded in invoicing file as well as accounting file.
- **Limited Data Sharing**- Each application would reference its own file.
- **Low Data Integrity** – Let's say a customer changes address, data might have been updated in invoicing file but not accounting file.
- **High Dependence between Data and Application**- If any change in the data structure or format is made in the data file, a corresponding change has to be made in the application program and vice-versa.

The problems with file systems led to database approach to data management.

3.2.4 What is a Database?

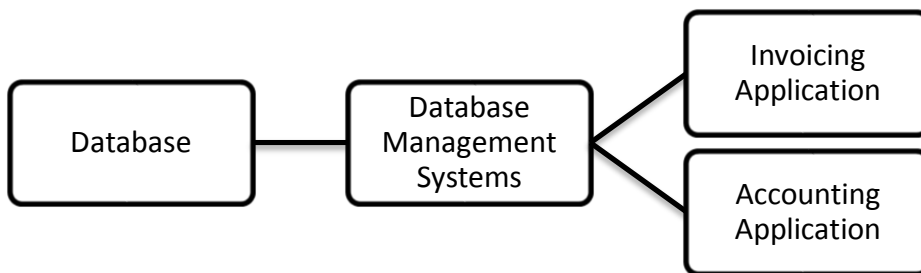
A **database** is a collection of data, typically describing the activities of one or more related functions of an organisation(s). Database is just like an electronic filing cabinet i.e. a collection of computerised data files. Some databases appear a single file to the OS, the database file then becomes a container for entire file structure.

The Database system helps us do various operations on these files such as:

- Adding new files to database
- Deleting existing files from database
- Inserting data in existing files
- Modifying data in existing files
- Deleting data in existing files
- Retrieving or querying data from existing files.

3.2.5 What is Database Management System?

Data Base Management Systems are software that aid in organizing, controlling and using the data needed by the application programmes. A Database Management System is a software system for creation and control of a database and manipulation of the data in the database. They provide the facility to create and maintain a well-organized database. DBMS can mean Data repository or the application bundled with the data repository to act as front-end. Applications access the DBMS, which then accesses the data. Commercially available Data Base Management Systems are Oracle, MySQL, SQL Servers and DB2, etc.



With this Database approach, applications would access a common database through Database Management Systems.

Advantages of a DBMS

- **Permitting Data Sharing:**
One of the main advantages of a DBMS is that the same information can be made available to different users.
- **Controlling Data Redundancy:**
In a DBMS duplication of information or redundancy is, if not eliminated, carefully controlled or reduced i.e. there is no need to repeat the same data over and over again. Minimizing redundancy can, therefore, significantly reduce the cost of storing information on hard drives and other storage devices, as also avoid data inconsistency.

- **Integrity can be maintained:**

- Integrity constraints can be applied to database so that the correct data can be entered and updated into database. The constraints may be applied to data item within a single record to ensure domain and relational integrity or they may be applied to relationships between records to ensure referential integrity. This also ensures consistent data across the database.
- Data integrity is maintained by having accurate, consistent, and up-to-date data.

The chances of making a mistake increase if the same data has to be changed at several different places than making the change in one place. Updates, in a database need to be made only at one place.

- **Program and file consistency:**

Using a DBMS, file formats and programs are standardised. This makes the data files easier to maintain because the same rules and guidelines apply across all types of data. The level of consistency across files and programs also makes it easier to manage data when multiple programmers are involved.

- **User-friendliness:**

DBMS makes the data access and manipulation easier for the user. DBMSs also reduce the reliance of users on computer experts to meet their data needs.

- **Improved security:**

DBMSs allow multiple users to access the same data resources which could lead to risk to an organisation if not controlled. Security constraints can be defined i.e. Rules can be built to control access to sensitive data. Some sources of information need to be protected or secured and only viewed by select individuals. Through the use of passwords, database management systems can be used to restrict data access to only those who are authorised.

- **Achieving program/data independence:**

In a DBMS, the data and the programs required to update and maintain those data items are not coupled. Programs being independent of data files can be modified independently of the data files, since In a DBMS data does not reside in applications but data bases program and data are independent of each other.

- **Faster application development**

In the case of deployment of DBMS, as the data in a database is independent of the applications, the latter can be developed to access the database through application interface. Thus, Application development becomes fast. If any change in the data structure or format is made in the data file, a corresponding change need not be required in the application program and vice versa.

Disadvantages of a DBMS

There are two major downsides to using DBMSs. These are Cost and Threat to data security.

- **Expensive**
 - Implementing a DBMS system can be expensive and time-consuming, especially in large organisations.
 - Training requirements alone can be quite costly.
 - Other disadvantage could be cost of data conversion from legacy Non-DBMS solutions, requirement of specific skill sets to manage the DBMS (need for a DBA).
 - DBA is required to fine tune the DBMS from time to time with increased volumes and changing requirements.
- **Security:**
 - In the absence of proper safeguards in place, it may be possible for some unauthorised users to access the database. If one gets access to database then it could be an all or nothing proposition.
- **DBMS failure: Single point of failure**
 - As the whole data may be stored in the DBMS, it becomes a single point of failure resulting in disruption of services/non-availability of data.

3.2.6 Database Models

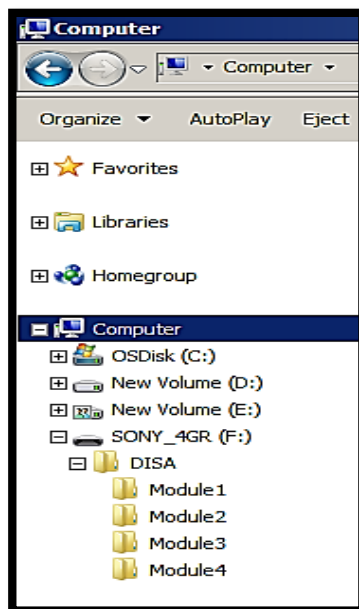
A database should be designed to store all data relevant to business to facilitate quick and easy modifications. A **database model** is a type of data model that determines the logical structure of a database and fundamentally determines in which manner data can be stored, organized, and manipulated.

Following are the database models,

- Hierarchical Database
- Network Database
- Relational Database (RDBMS)

Hierarchical Database Model

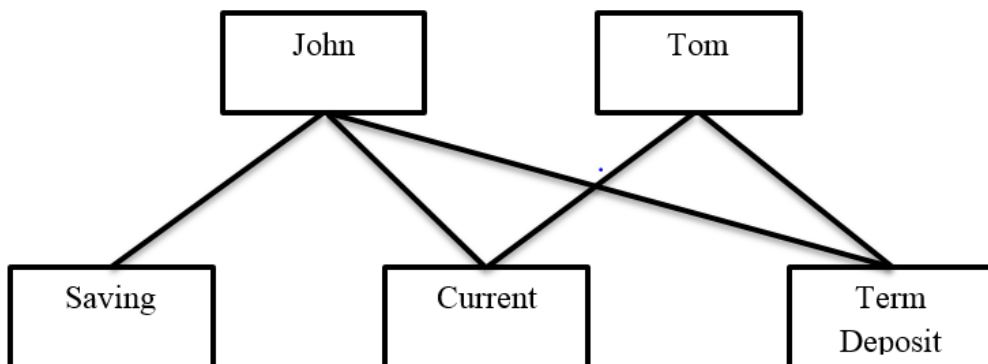
Data is organized in a tree structure. The records have a one-to-many relationship (1: n), **one** record type is the **root**, all other record types is a **child** of **one parent** record type **only**.



One typical Hierarchical structure could be your Directory (folders) in Windows OS.

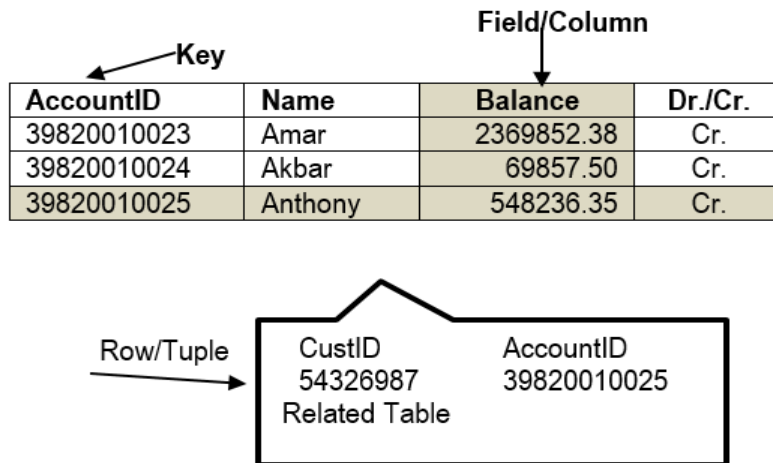
Network Database Model

Records have a many-to-many relationship. For example many customers have multiple accounts. The main disadvantage of this model is its complexity. Also, when the database is re-organized, there is every possibility that data independence might be lost.



Relational Database Model

The **Relational Database Model** is very simple and elegant; a **relational** database is a collection of one or more relations, where each relation is a table with rows and columns which is a logical equivalent of files. It permits the use of simple, high-level languages to query data.



This model represents the database as a collection of Relations and is governed by these rules:

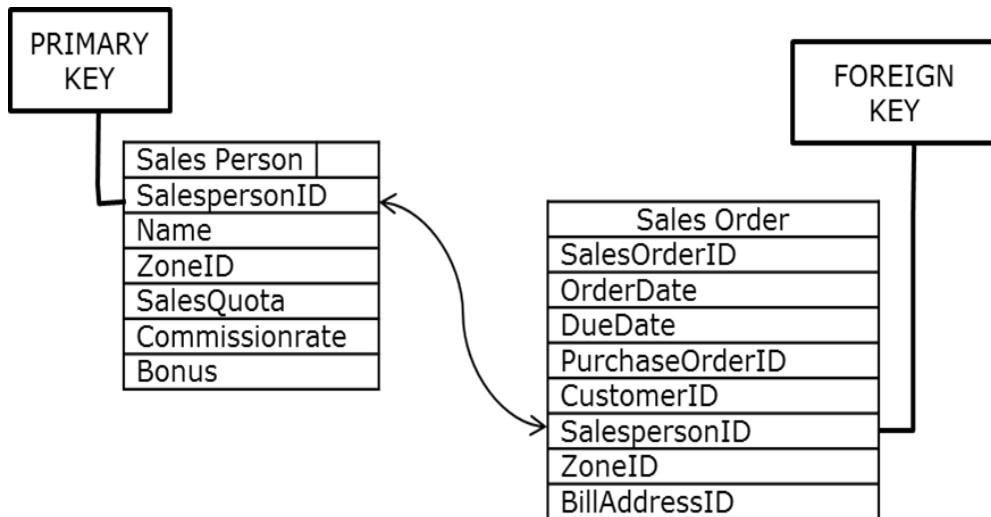
- Data is represented in a two-dimensional table, in rows and columns.
- Columns describe the attributes.
- Each column in the table has a unique name.
- All the entries in any column are of the same type or same domain.
- Each column has a domain, a set of possible values that can appear in that column.
- All the entries in any column are of the same type or same domain.
- A row in the table is called Tuple.
- Ordering of rows and columns is insignificant.
- Duplicate rows are not allowed.
- All data items stored in the columns are atomic in nature, that is, they cannot be split further without loss of information.
- In many tables, there is a column called the Key Column whose value is unique and cannot be null.

3.3 Relational Data Integrity

In order to maintain integrity (accuracy) of data in the database, relational model specifies several types of integrity constraints. Its major types are:

- **Domain constraint:** This means that all the values in the column of a table must be from the same domain. Example: In Income Tax Assessee Database Column of First Name would have all First names and Date of Birth would have all Date of Births in Date format.

- **Entity Constraint:** This rule is to ensure and assure that the data values for the primary key are valid and not null. Example: In Income Tax Assesse Database the primary key would be PAN Number which is unique and never null.
- **Referential Integrity:** In a relational data model, associations between tables are defined by using foreign keys. The referential integrity rule states that if there is a foreign key in one table, either the foreign key must match the primary key of the other table or else the foreign key value must be null.



In the above case SalesPersonID in Sales Order Table is foreign key but is primary Key in Sales Person Table. This Constraint says that if in Sales Order Table for a transaction, SalesPersonId is 0033 then that value should exist as Primary key in Sales Person Table. There might also be a case where there is direct order, in such a case SalesPersonID would be Null (in the Sales Order table). Thus Referential Integrity Constraint would not allow someone to create an order booked by a non-existent salesman.

People Associated With DBMS

- **Data Owners:** Owners of database
- **Database Designers:** Help in Database design and Structure
- **Application Developers:** Implement Database Design and application programs
- **Database Administrators:** Manage Database management systems(discussed later)
- **End Users:** Who query and update databases

Normalisation

“Norma” in Latin means **Carpenter Square** whose job is to set it at right angle.

Similarly, normalization is used to set the table right. Database normalization is a conceptual Database design technique which involves process of organizing the fields and tables of a relational database to minimize redundancy and dependency on non-key elements. Objective is all non-key items are related on key fields. It is the process of Conceptual Database Design achieved through - identification of relationships among various data items, Grouping data items and establishing relationships and constraints. Normalization usually involves dividing large tables into smaller and still smaller (and less redundant) tables and defining relationships between them in order to improve storage efficiency, data integrity and scalability. The objective is to have data Tables in such a way that additions, deletions, and modifications of a field can be made in just one table and then propagated through the rest of the database using the defined relationships.

BEFORE NORMALISATION

StudentID	StudentName	Address	Subject	SubjectCost	Grade
12345678	Amar Akbar	1 Wall street	Accounts	1500	B
			Economics	2000	A
			Management	1500	B+

AFTER NORMALISATION

StudentID	StudentName	Address
12345678	Amar Akbar	1 Wall street

Subject		SubjectCost
Accounts		1500
Economics		2000
Management		1500

**SUBJECT TABLE (KEY=Subject)**

StudentID	Subject	Grade
12345678	Accounts	B
12345678	Economics	A
12345678	Management	B+

RESULT TABLE (KEY= StudentID + Subject)

The **advantages** of the normalization are:

- Reduced redundancy.
- More efficient data structure.
- More flexible data structure i.e. we are able to add new rows and data values easily.
- Better understanding of data.

3.3.1 Database Schemas

DBMS is responsible for access of Database; one of the initial steps would be “telling” the DBMS the logical and physical structure of data and relationships among data for each user. This Description of database is called **Schema**. The data in a DBMS is described at three levels of abstraction or schemas:

External Schema

It is the user's view of the database. This level describes that part of the database that is relevant to each user.

External level is the one which is closest to the end users. Individual users are given different views according to the user's requirement.

Let's say an HR person's requirement in terms of data would be EmployeeID, EmployeeName, DateofBirth, DateofJoining, Department, Designation, Basic Pay. Whereas Payroll Persons would be interested in EmployeeID, EmployeeName, Department, Designation, Basic Pay, leave, TDS, Deduction. These would be different user's view of data or External Schema.

Conceptual Schema

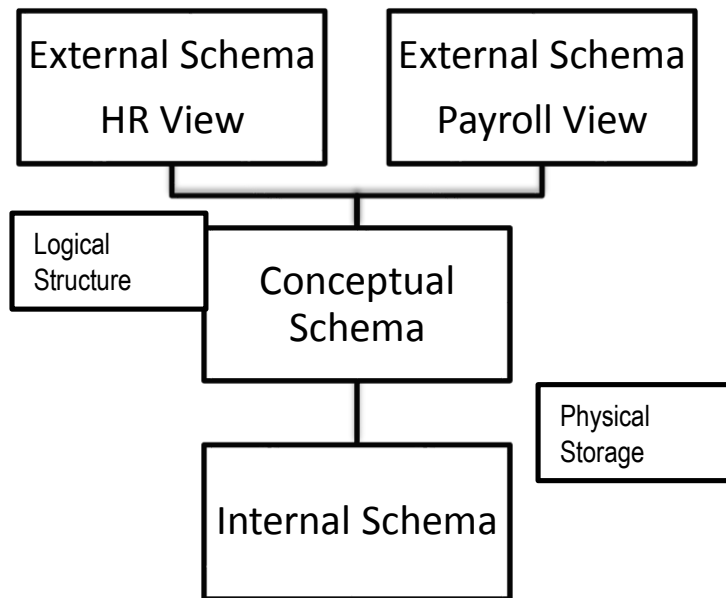
This level describes what data is stored in the database and the relationships and constraints among the data. This level contains the logical structure of the entire database. The conceptual level represents all entities, their attributes and their relationships.

The conceptual schema in above case would consist of EmployeeID, EmployeeName, DateofBirth, DateofJoining, Department, Designation, Basic Pay, Leave, TDS, Deduction and relationship amongst them i.e. incorporates view of community of users HR as well as payroll.

All these data items would be in the form of Normalized small Tables with relationships and constraints.

Internal Schema

It is the physical representation of database on the computer. This level describes how the data is physically stored in the database. The internal level is concerned with storage space allocation, Record descriptions, Records placement, Data Compression and Data Encryption Techniques.



3.4 Database Languages

A DBMS provides a comprehensive set of facilities to perform the following actions:

- Creating, Modifying, Deleting database objects.
- Inserting, Updating and deleting data in the database.
- Performing the process of querying the database.
- Controlling access to the database.
- Providing facilities for data integrity and consistency.

These facilities are grouped under database languages. **Structured Query Language or SQL** is a language that provides an interface to relational database systems. The three important classifications of database languages are:

- Data Definition/Description Language (DDL);
- Data Manipulation Language (DML); and
- Data Control Language (DCL).

3.4.1 Data Definition Language (DDL)

The schemas discussed above need to be entered into the DBMS. This would be done using **Data Definition Language (DDL)**. It is a collection of instructions and commands used to define and describe the data and relationships in a specific database.

Module 1: e-Learning

Data Definition Language (DDL) is used by the DBA (Database Administrator- explained later) and by database designers to define both conceptual and internal schemas. DDL does not deal with data.

It is a set of SQL commands used to create, modify and drop database structure. These commands are not generally used by a common user.

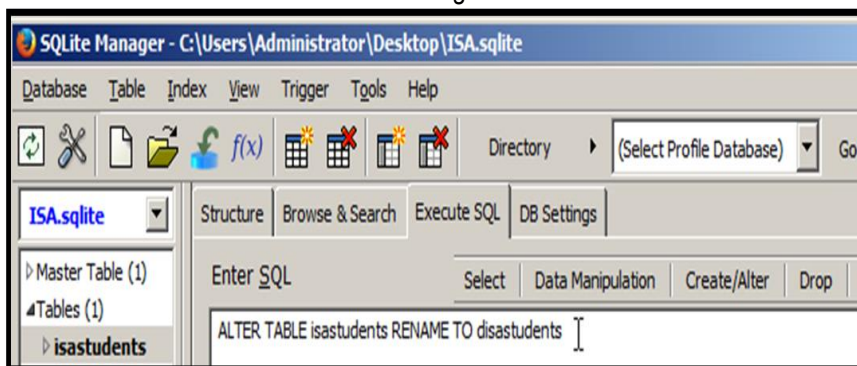
Example: To create schema, SQL statement CREATE Table is used or to Modify Schema ALTER Table is used. All these statements are used to define Database



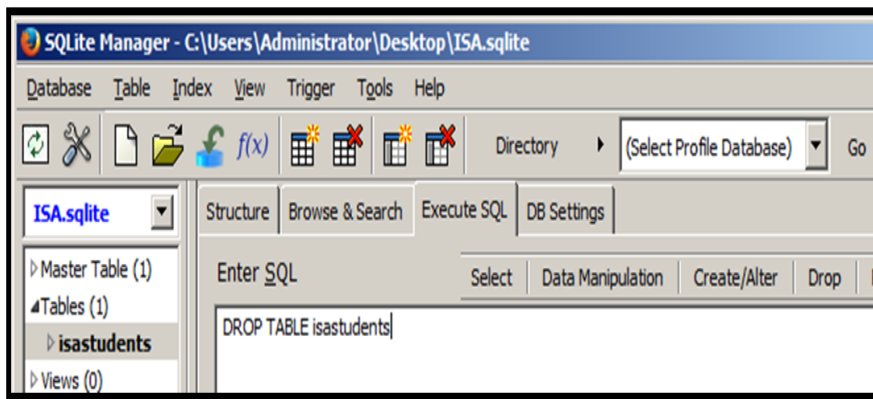
In the above example: CREATE table isastudent (StudentID varchar (20), roll_no number (10))

This means that we want to create a table with the name 'isastudent' with two columns - StudentID and roll_no. The name field will have attributes of type of: data: character, Maximum size of 20 characters. Similarly, roll no will be a number type with maximum length of 10.

Use of ALTER with RENAME for Renaming Table



Use of DROP for Deleting Table



3.4.2 Data Manipulation Language (DML)

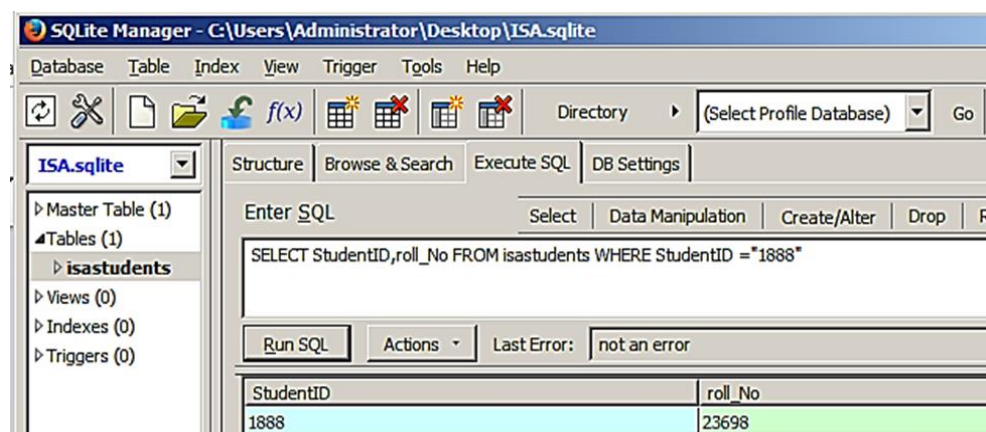
Subsequent to installation of DBMS, Users like managers would like to review reports and access information.

To query the databases, the commands used to manipulate the databases are part of **Data Manipulation Language (DML)**. Typical manipulations include retrieval, insertion, deletion, and modification of data. DML statements are used to maintain and query a database.

Applications access data through DML.

It is the area of SQL that allows changing data within the database i.e. enable users to manipulate data in existing schemas' objects.

Example: SQL statement like AVG (Average) MAX (find Largest Value) are used to query the database



In the above example: SELECT StudentID, roll_No FROM isastudents WHERE StudentID ="1888"

In the table name isastudents, StudentID and roll_No refer to two fields containing StudentID and Roll number respectively in the table and we are trying to extract data relating to Student with ID "1888".

3.4.3 Data Control Language (DCL)

After Database has been setup and being able to manipulate data there is also a need to control a database, including administering privileges and committing data this is done using statements forming part of **Data Control Language (DCL)**. DCL is a database language used to control access to data in a database.

- Example: To give privileges and roles SQL statements like GRANT.

SQL>GRANT SELECT ON isastudents TO Pyare.Lal

To grant the user Pyare.Lal ability to retrieve information from the isastudents Table, we use GRANT with SELECT

3.5 Key concepts of Database

3.5.1 Meta Data

Meta Data is critical to DBMS. It data is data about it provides data about:

- Where data came from
- How data were changed
- How data are stored
- How data are mapped
- Who owns data
- Who can access data
- Data usage history
- Data usage statistics

3.5.2 Data Dictionary

It is the documentation of database providing detailed description of every data in database. It covers the following:

- Way data is defined
- Types of data that is present
- Relationship among data
- Keys for databases
- People Accessing data and Access rules

The typical uses of a data dictionary are:

- Provide a standard definition of terms and data elements that can be referenced by programmers, database administrators, and users to maintain data integrity
- Assist programmers in designing and writing programs
- Simplify database modification

3.5.3 Data Administrator and Database Administrator

- **Data Administrator**- Administrative and Policy Functions
- **Data Base Administrator**- Technical Functions

Database administrator (DBA) manages the DBMS for an organisation. As organisation Database Systems are important and complex, the task of designing and maintaining the Database requires a skilled Database Administrator who has a thorough knowledge of the business of the organisation, is well versed in the use of DBMS and who keeps abreast with new emerging technologies and methodologies. The DBA designs schemas, provides security, restores the system after a failure, and periodically tunes the database to meet changing user needs.

Data management tasks

- Perform the process of liaising with management.
- Perform the process of liaising with database users for their needs.
- Perform the process of liaising with database vendors.
- Perform the process of liaising with the Data Administrator (DA).
- Acquire latest information on database technologies and tools.
- Prepare the project status report on the usage of databases.

Security tasks

- Monitoring and maintaining security of databases.
- Granting access rights and revoking them to users.

Technical Tasks

- Monitoring the databases, perform database tuning and optimizing database performance.
- Maintaining availability (24 x 365) and ensuring integrity of databases.
- Installing any patch software, if necessary.
- Managing database backups and restorations.
- Guiding application programmers in their work.
- Performing the process of capacity planning.
- Performing the process of normalization, demoralization, indexing, and defining views.
- Framing procedures for purging and archiving data.

Some Enterprises have a separate position **Data Administrator** which is a non-technical position. Job of Data Administrator relates to data rather than Database. All administrative and policy matters rest with DA. Thus, the primary responsibility of defining External and Conceptual Schema is jobs of DA, whereas the primary responsibility of defining internal schema rests with DBA.

3.6 Database Applications-Linking Databases to the Web

Front-end application: These directly interact with people or users.

Back-end application: Interacts with other programs or applications.

Web provides interactive interface (to the clients) to the business information stored in back-end databases. Databases are the functional muscle of the web. System designers are increasingly using the Web as the front end to database systems. Ability to produce useful information from the underlying data is the strength of database applications. These could involve searching, filtering, dicing, slicing and integrating data which is facilitated by Database Applications.

These Database Applications these days allow us to link company databases to internet help in establishing data marts and warehouses, helping in remote access and manipulation of data, use online processing to increase productivity for any organisation. One prominent example of Database application could be ERP application SAP. Most retail store Web sites like EBay and Amazon use database systems to store, update and present data about products for sale. The popular Web-based "Facebook" application is essentially a database built upon the "MySQL" database system and is an indication of the increasing usage of database applications as foundations for Web-based applications. In short, one of the reasons of popularity of internet is the ability to link databases. Today a large number of corporate databases are accessed over internet through a standard web browser.

3.7 Database Security and Control

Database Controls could be in terms of:

- Database Roles and Permissions
 - Segregation of duties
 - Roles and Permissions allow control of operations that a user can perform on database,
- Concurrency Control
 - Addresses conflicts relating to simultaneous accesses
- Views
 - Views enable data access limitations. A view is a content or context dependent subset of one or more tables. e.g. – A view might be created to allow a sales manager to view only the information in a customer table that is relevant to customers of his own territory and restrict user from views of the database.

- Stored Procedures
 - Database servers offer developers the ability to create and reuse SQL code through the use of objects called as Stored Procedures (Group of SQL statements).
 - These are available to applications accessing a database system and are actually stored in database. Stored procedures reduce the long SQL queries to a single line.
- Triggers
 - These are designed to be automatically 'fired' when a specific action/event takes place within a database. E.g. On execution of code to delete an employee from Master File, a trigger would be executed (automatically) to scan the Employee Liability Table to check whether any liability against this employee exists.

3.7.1 Database Security

The objective of Data base security would be Authorised people should be given Right access to the Right data. In this context user management becomes very important. There could be different types of database users

- Application programmers
- Specialized users
- Naive users

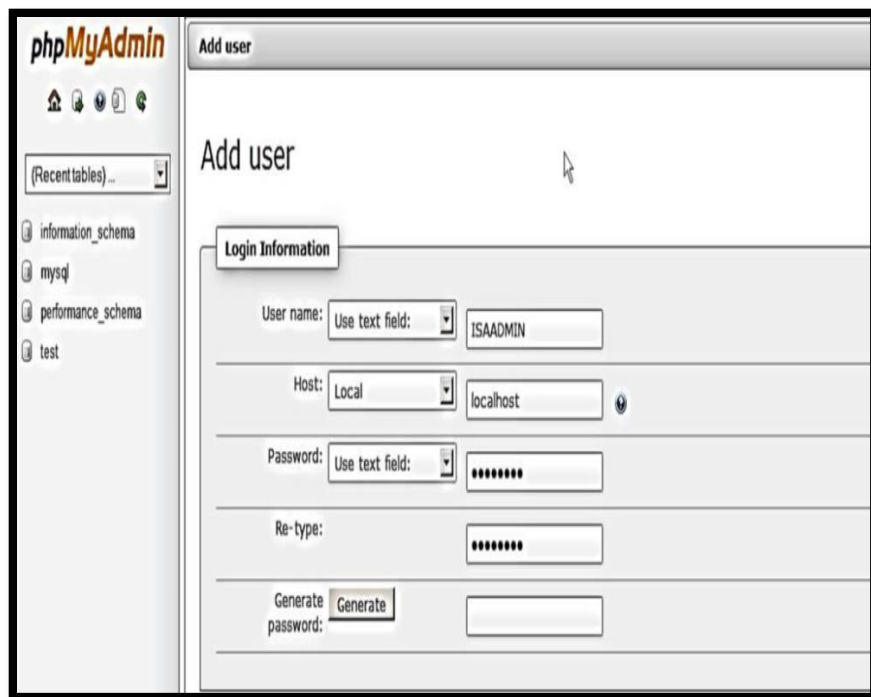
This user management is achieved through Authorisation and access control

Basic model for accessing control involves:

- Subjects (Right People)
- Objects (Right data)
- Access Rights (Right Access)

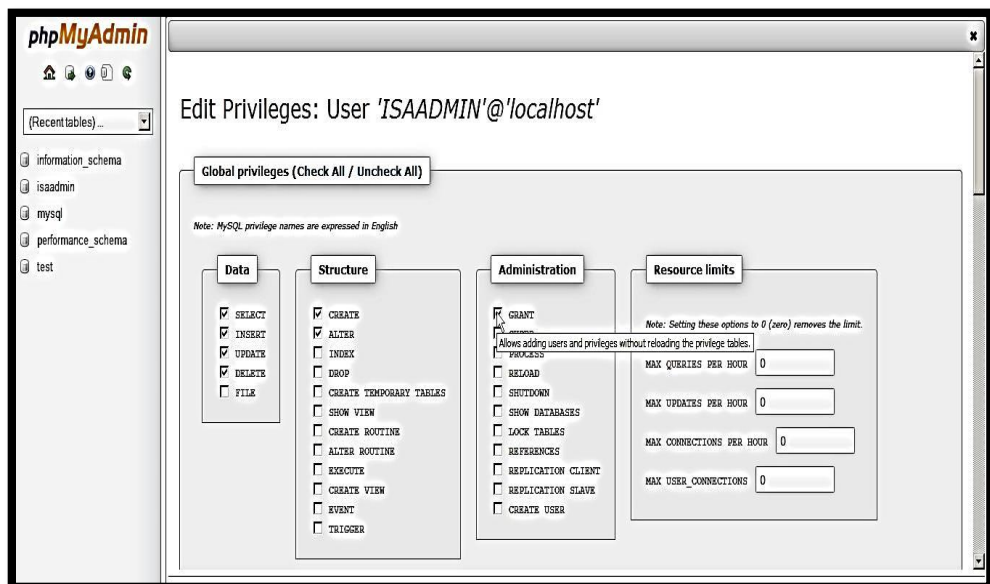
To access the database, a user must specify a valid database user account and successfully authenticate as required by that user account

Normally, a database administrator first uses CREATE USER to create an account, then GRANT to define its privileges and characteristics. For Example in Oracle, The SYS and SYSTEM accounts have the database administrator (DBA) role granted to them by default. These are predefined all other users have to be created. Thus there is a need to create user and assign some authentication mechanism like a Password.



The screenshot shows the 'Add user' form in phpMyAdmin. The left sidebar contains the 'phpMyAdmin' logo, navigation icons, and a list of databases: 'information_schema', 'mysql', 'performance_schema', and 'test'. The main content area is titled 'Add user' and contains a 'Login Information' section. This section includes fields for 'User name' (set to 'ISAADMIN'), 'Host' (set to 'localhost'), 'Password' (masked with dots), and 'Re-type' (also masked). There is a 'Generate password' button and a corresponding empty text field.

Data base Administrator will then grant access rights or privileges to user as shown below.



The screenshot shows the 'Edit Privileges' form for user 'ISAADMIN'@'localhost' in phpMyAdmin. The left sidebar is the same as the previous screenshot. The main content area is titled 'Edit Privileges: User 'ISAADMIN'@'localhost''. It features a 'Global privileges (Check All / Uncheck All)' button and a note: 'Note: MySQL privilege names are expressed in English'. Below this, there are four panels: 'Data', 'Structure', 'Administration', and 'Resource limits'. The 'Data' panel has checkboxes for SELECT, INSERT, UPDATE, DELETE, and FILE. The 'Structure' panel has checkboxes for CREATE, ALTER, INDEX, DROP, CREATE TEMPORARY TABLES, SHOW VIEW, CREATE ROUTINE, ALTER ROUTINE, EXECUTE, CREATE VIEW, EVENT, and TRIGGER. The 'Administration' panel has checkboxes for GRANT, PROCESS, RELOAD, SHUTDOWN, SHOW DATABASES, LOCK TABLES, REFERENCES, REPLICATION CLIENT, REPLICATION SLAVE, and CREATE USER. The 'Resource limits' panel has input fields for MAX QUERIES PER HOUR, MAX UPDATES PER HOUR, MAX CONNECTIONS PER HOUR, and MAX USER CONNECTIONS, all set to 0. A note at the bottom right states: 'Note: Setting these options to 0 (zero) removes the limit.'

3.8 Auditing Databases

3.8.1 Need for Auditing Databases

- Cost of Breach
 - The cost of data breach is very high.
 - There is a huge risk of data stolen from the organisation and risk of identity theft.
 - In a number of cases, records containing sensitive personal information are involved in security breaches, raising huge privacy issues.
- Regulatory Compliance
 - There are many regulations and Standards which provide for audit of Data Bases like PCI-DSS HIPAA, ISO 27001 etc.
 - Database monitoring is key requirement.
- Database Leak Prevention
 - Sensitive data needs protection.
 - There is an ever increasing number and type of threats which need to be mitigated.
 - Attackers are targeting databases where data can be captured in bulk.
- Open Accessibility
 - Web applications have melted traditional perimeter controls.
 - Databases become vulnerable to breaches.

Auditing Database

The databases may be Front End or Back end. It is important to audit application controls. Applications facilitate access by customers, employees, and business partners. Many different applications may be accessing the same database and be subject to differing sets of controls. It is important to audit the management of controls and also segregation of duties relating to these applications.

- Perimeter Controls: Data access is distributed in most organisations. Perimeter controls (Firewalls, IDS etc.) protect the databases from malicious users. It is essential to audit these perimeter controls.
- Database Controls: Segregation of duties, concurrency control and possibility of anybody access data without going through application are some of the controls which need to be examined.

Areas of review by IS Auditor

- Definition standards
- Separate test database and live database
- Access controls, Database user rights should be need based
 - Changes in authorisation IDs

- Changes to the structure of data (such as dropping a table)
 - Changes to data values (such as updating or inserting data)
 - Access attempts by unauthorised IDs
- Controls to handle concurrent access problems.
- Monitoring database performance
- All database logs should be periodically verified
- Documentation regarding database incidents
 - What activities were performed in the database by both users and administrators
- Checkpoints to minimize data loss
- Data backup and recovery procedures
- Whether backups are tested

Step by step approach for auditing database

- Understand application system / network infrastructure
 - While planning an audit it is important to understand how the architecture components inter-relate.
 - Need to understand application systems and network architecture in which it operates.
- Identify database administrators
- Identify database environments and versions
 - Operating system hosts
 - Database configuration files / documentation
 - Database schemas
- Arrange database access
 - Access should be provided for system table and system views.
- Look at Logs
 - System Access
 - Logins – Success / Fail
 - Account / Role / Permissions changes
 - Password changes
 - Data Access
 - SELECT – Success / Fail
 - Data Change
 - INSERT, UPDATE, DELETE
 - Schema / Object Changes
 - CREATE, ALTER, DROP
 - Privileged User Activity
 - All

3.9 Summary

At the very heart of most of management information systems are a database and a database management system. A database maintains information about various entities and a database management system (DBMS) is software through which users and application programs interact with a database. We can very well say that Databases and Database Management Systems form the foundation of information economy. DBMS is crucial for any organisation and has to be controlled, monitored and assessed.

3.10 References

1. C J Date, An Introduction to Database Systems (8th Edition), Addison-Wesley.
2. Raghu Ramakrishnan, Database Management Systems, 3rd Edition, McGraw-Hill
3. <http://asktom.oracle.com>
4. <http://www.java2s.com/Code/SQLServer/CatalogSQLServer.htm>

PART 4: HARDWARE/SOFTWARE DEPLOYMENT STRATEGIES

Learning Objectives

- To gain understanding of deployment strategies for IS Infrastructure
- To understand Information Technology Components of a Data Centre in CBS Environment
- To understand Configuration management of IS Components
- To gain understanding of Hardening of Systems
- To understand Auditing IS Infrastructure.

4.1 Introduction

Any business organisation would like to have its goals and objectives achieved. To meet these business objectives it will have some business processes, these business processes would need some IT Services. These IT Services would require IT infrastructure. After considering this top down approach, the business organisations plan for its IT infrastructure, since only a well-designed IT infrastructure can help an organisation achieve its objectives. After making an IT plan it is imperative to implement the plan, the term which is used more often for this implementation is "Deployment". Deployments in this background involves acquiring new software and Hardware and have it up and running including installation, configuration, running, testing and necessary customisations and modifications.

4.2 Different Deployment Strategies

The strategy for deployment of IT infrastructure could involve different possibilities, centralised or decentralised. Each has its own merits and demerits, the best approach would depend on the kind of organisation as well as the tone at the top.

4.2.1 Centralised Approach

In Centralised approach decisions are taken at the most senior or central level. There is a central database. Content that has to be globally shared are at the central level. Applications are deployed on single hardware/ software platform. Servers are at the central level. There is requirement of a single middleware to connect client server at the central level. All user communication and traffic is directed to the central point. Centralisation might be appropriate wherever the system is critical to the functioning of the organisation, system is used by more than one department, Data is drawn

from several different sources, and/or there are particular technical issues such as the design of the network. Example could be most of CBS banks.

Benefits:

- Resource Sharing
 - Data used across organisation in one place,
 - Easier to undertake organisation-wide activities.
 - Exchange of hardware, software.
- Avoidance of duplication
- Better security
- Achieving economies of scale.
- All data is at central level so it can be fully replicated for higher availability and disaster recovery purposes.
- Policy enforcements can be done at central level.
- Security like patch management anti-virus management etc. can be done at central level.

Disadvantages:

- Single Point of Failure
 - Central server and databases could be single points of failure. Thus, there is a need for proper controls in the form of database mirroring, back-up sites, component redundancies, access controls etc.
- Inflexibility
 - Less flexibility to cope with local internal or external changes
- Increased dependence and vulnerability
 - Greater numbers of staff rely on single information systems,
 - Greater reliance on a few key staff who plan, develop and run those systems,
 - Greater technical complexity that makes problems harder to diagnose, and
 - Greater potential impact of data security breaches.

4.2.2 Decentralised Approach

In Decentralised approach decision making is delegated. The database is localised for an office/region/zone/country depending upon the business strategy. Content is of local relevance. Applications can be implemented on different platforms. Middle-ware is required at each set-up. There will not be a single point of failure. Policy administration is at decentralised level. Decentralised set up might be appropriate for areas where the system is relevant only to the individual user / department, Data is drawn only from an existing centrally-managed database or from a proposed locally-managed database, and/or Processing or reporting requirements are subject to frequent change. Example could be a Multi-National Company having operations in different countries.

Benefits:

- Greater fit between systems and local needs
 - Proximity of user and developer helps meet the users' real needs.
- Higher usage of computerised systems
 - Fit local needs, users are motivated
- Faster system development
 - less distance between system user and system developer
- No single point of Failure
 - One unit can work as a back-up site for the other unit.
- Reduced CAPEX
 - Deployment can be done in phases, and hence can be matched with budget cycles since all deployment need not be at one go.
 - Up gradations can be done in phases

Disadvantages:

- Barriers to sharing data
 - Information systems could be mutually incompatible.
- Barriers to sharing other resources, including human resources
 - Inability to share resources other than data
- Duplication of effort
 - Databases replication would be required at all decentralised locations, could consume more resources.
- Lack of Centralised Control like
 - Patch management, version control, security implementation, Antivirus updates etc.
- Latency
 - Because of distributed architecture there may be latency, due to the amount of routing involved between distributed setups.

4.3 IT Components in a CBS (Core Banking Solution) Data Centre

A bank's data centre or an IPF (Information Processing Facility) is a facility used to house computer systems and associated components, to cater to its information processing needs. In addition to the computers, the Data Centre (DC) has storage, security and communication links. The Data Centre is equipped with redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices. The IT components, in a Data Centre depend upon the corporate objectives of the bank, the type of services it plans to offer, the risk management and control mechanism it wishes to embed into

IT processes and meet compliance/regulatory requirements, as also to leverage upon technology to act as a differentiator for maximizing business and profit.

In the context of CBS, the IT components will depend upon the type of services the solution offers, the committed/expected response time for customer transactions and the availability requirements of services. This also depends upon the layers of security implemented for securing IT assets and the processes in place for building customer confidence through efficient and secure processes. Therefore, other applications/solutions requiring interface to the CBS solution are also hosted at the Data Centre. In addition to meeting availability requirements, the banks have a DR site and may have near-site also. Usually near site is used for data replication only.

The IT components can be broadly listed under the following categories,

- Application Solutions and Services
- Hardware and OS Components
- Network and Security Components
- EMS Components
- Environmental Components

4.3.1 Application Solutions Components

The following applications/services are normally deployed in data centre of a bank

- (i) CBS – including Internet Banking
- (ii) RTGS/NEFT/Integrated Risk Management solution/Integrated Treasury Solution/Anti-Money Laundering System/Asset Liability Management Solution/Mobile Banking/ Automated Data Flow and MIS/ Data Archival System/New Pension Scheme/Govt. Business/OLTAS etc.
- (iii) Web Services
- (iv) Customer Call Centre services
- (v) Customer Relationship Management
- (vi) Human Resources Management
- (vii) Email System
- (viii) Data Warehouse
- (ix) Biometric Authentication of branch users in CBS
- (x) Second factor Authentication (for Internet Banking Users)
- (xi) Cheque Truncation System and MICR Clearing System
- (xii) Financial Inclusion

The applications which are not a part of the Core Banking Solution have an interface built (through middleware) with CBS. These applications may be housed in the same data centre or elsewhere. Usually, the bank's WAN is also interfaced with the following external networks for facilitating the seamless integration of CBS with other applications.

- ATM (Automatic Teller Machine) Switch

- Reserve Bank of India's MPLS (Multi-Protocol label switching) network and NPCI(National Payments Corporation of India)
- SWIFT (Society for Worldwide Interbank Financial Telecommunication)
- Master/VISA/American Exchange
- National Clearing Cell and Cheque truncation system
- Utility services networks like telephone companies, mobile companies, electricity companies, water department etc.,
- Government Tax Departments
- Other Govt. agencies like Central Board of Excise and Customs, Director General Foreign Trade.

4.3.2 Hardware Components and OS

In a Data Centre, we have Server Farm i.e. a number of servers connected together. These servers would broadly fall into following categories:

- **Core Banking Servers** - in High Availability (HA) mode. Number of servers depends upon transaction volume, response time requirement and these are clustered.
- **Database Servers** - in High Availability (HA) mode.
- **Web Servers, Email, Anti-virus servers**
- **Application Servers** for the other applications

All the servers normally have redundant power supply from different UPS system and high speed Network interface cards. Some banks implement virtualization for the Web Servers, Database Servers and other Application servers. This helps to achieve scalability, reliability and high availability for these servers.

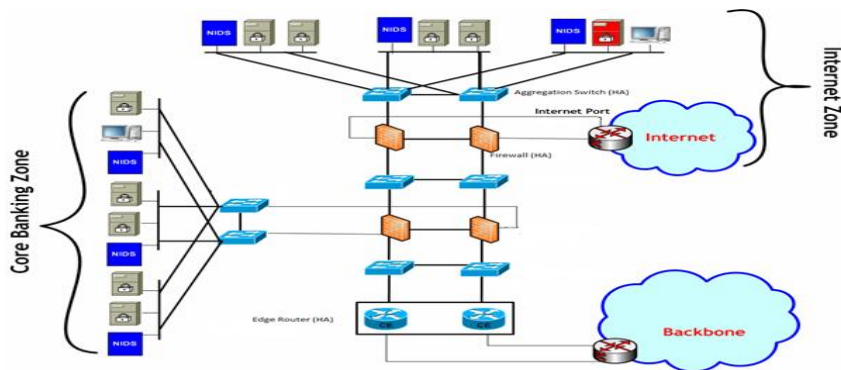
Storage: For storage of production, test/development, migration and training data at the Data Centre. Usually, the DRC (Disaster Recovery Centre) storage is sized for just the production environment. Tape Library is used for taking backups.

4.3.3 Network and Security Components

The network design in the DC (Data Centre) is such that there are two distinct zones; one of which caters to the Private Segment (Core Banking Zone), and other - the Public Segment (Internet Zone). The architect is such that each of the two zones has different sub-nets through VLANs (Virtual Local area Networks). Following networking devices are installed,

- **Core Routers** – 2 numbers to connect (back to back) the DC to the (Edge Routers) WAN. These are configured in a HA (High Availability) mode, and have IPsec implemented on them.
- **Core Switches** – 2 nos. in each of the two zones to provide for VLANs.
- **ISDN Routers** – To connect to branch routers to ISDN back up line.
- **Top of Rack Ethernet Switch** – for each of the racks.
- **Encryption Devices**

- **ACS Server** for Terminal Access Controller Access-Control System (TACACS) – For authentication, authorisation and accounting services of all network devices including branch routers.
- **Firewalls** – (Core and Segment) - Each of the 2 zones is protected by 2 separate clusters of high performing firewalls
- **Internet Router** – To connect DC/DR to ISPs.
- **Intrusion Detection and Protection Systems** – Separate for each of the two zones.
- **Two Factor Authentication** – Hardware and software to provide second factor authentication for internet banking users.
- **Security Solutions** for email, and web.
- **End-Point Security solutions.**



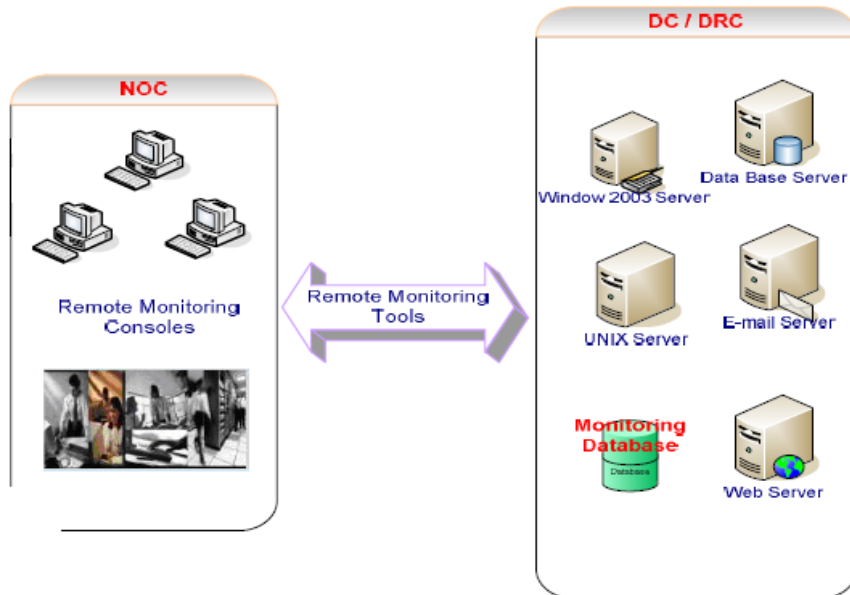
A generic DC/DR Architecture

4.3.4 Enterprises Management System Components

The EMS solution is deployed to act as an interface for the Network Operations Centre (NOC) and is used to monitor the servers, network and security components at DC, DRC, Near Site, WAN Links and branch Infrastructure. It is a set of hardware and software solution(s) for the purpose of:

- Application Monitoring
- Server Monitoring
- Network Monitoring
- Patch Management
- Asset Management
- SLA(Service Level Agreement) Management
- Change Management
- Interface to Helpdesk Module

The NOC (Network Operations Centre) is usually at a different location for carrying out above activities. A generic depiction of EMS deployment is given below:



4.3.5 Environmental Components

- Racks - to house all the servers and the network equipment like Switches. Routers etc.
- Power ducts, cables, LAN (structured cabling) usually running below false floor.
- Smoke Detection and Fire Suppression Systems
- Motion Sensors
- Biometric and proximity card readers
- Video Camera Surveillance and Security Breach Alarms systems
- UPS power conditioning devices – to protect the servers and other critical network and system equipment from brownouts, spikes, blackouts, noise, and over-voltages.
- Power, Water and Optic Fiber cables – from two redundant sources.
- Redundant air conditioning equipment – to maintain a continuous temperature of 20 ± 2 Centigrade.
- Humidity control equipment
- Diesel storage for power back-up.

4.4 Configuration Management of IS Components

For an enterprise (just like a bank) using technology, it is imperative to keep a track, at central level, of all IS components i.e. Hardware, Software etc., their configurations, versions etc., so that control could be exercised over their lifecycle. Configuration management refers to relative management of parts or elements of IT components. Configuration management covers the

identification of all significant components within the IT infrastructure and recording the details of these components in the Configuration Management Database. The configuration management system also records relationships between these components. It provides comprehensive information about all components in the infrastructure that enable all other processes to function more effectively and efficiently. In configuration management, we record functional and physical characteristics of hardware and software. Configuration management is applied throughout the lifecycle of IS components (Hardware, Software etc.).

Configuration management defines Configuration Items (CI), Items that require change control and process for controlling such change. It is concerned with the policies, processes and tools for managing changing IS Components. Special configuration management software is available commercially. When a system needs hardware or software upgrade, a computer technician can access the configuration management program and database to see what is currently installed. The technician can then make a more informed decision about the upgrade needed.

Configuration Management System has the following aspects

- Configuration identification
- Configuration control
- Configuration status reporting
- Configuration audit

4.4.1 Configuration Identification

It is impossible to control something we don't know. Therefore, identification of IS components is important. In a restaurant with 100 tables the captain takes an order for food and waiter serves the food, if there are no table numbers imagine the mess waiter would be in. He would not be able to correlate food to be served with table, so it is important to have some unique way of identifying the tables with orders.

Configuration Identification (CI) is the identification of all IS Components and typically includes the versions and updates that have been applied to installed software packages and the locations and network addresses of hardware devices. It helps us to know:

- Items (HW/SW) which are under configuration management.
- Configuration of components of these Items.
- Configuration, version of these items, e.g. Track of all software (Name, Version, Licence, Configuration, Related Documentation, etc.)
- Details of hardware (Type, CPU, Memory etc.)

4.4.2 Configuration Control

Products in any organisation need to be maintained due to evolution, or the changes in user needs. As change is inevitable, controlling the changes in the CIs is necessary.

Configuration control is the activity of managing configuration Items and their related documentation throughout the life cycle of these products. This activity helps us understand:

- Items which are controlled
- Process of controlling these changes
- Version control
- Who controls these changes
- Ensures that latest approved version of items are used.

4.4.3 Configuration Status Reporting

This involves recording and reporting of all changes in IS components. This provides a complete record of:

- Status of proposed changes.
- What changes were made and at what time.
- Effect of those changes on different components, e.g. if we have upgraded operating system then it will need corresponding change in Antivirus Solutions or other software or may require a hardware upgrade.

4.4.4 Configuration Audit

This involves verifying the correctness of the IS components to examine whether these are in accordance with requirements as also verifying the configuration status reporting. It measures effectiveness of configuration management and ensures that:

- All Items are correctly identified, and
- All changes are correctly registered, approved, tracked and implemented.

An advantage of a configuration management application is that the entire collection of systems can be reviewed to make sure any changes made to one system do not adversely affect any of the other systems.

4.5 Hardening of Systems

Hardening of systems is the process of securely configuring computer systems, to eliminate as many security risks as possible. The objective is that the system architecture should be designed to prevent attacks/intrusions. There are many default settings in systems which introduce much vulnerability. Moreover, default settings may make operations easier but expose system to vulnerabilities which could compromise the system. Hardening of system may involve, among other measures, applying patches; disabling unnecessary services; closing open network ports; and setting up intrusion-detection systems, firewalls and intrusion-prevention systems, etc.

Some important steps to harden operating systems are:

- Latest patches, service packs and hotfixes should be installed.
- Automatic notification of patch availability should be ensured.
- For authentication: set minimum password length and complexity
- Configure event log settings: logging should be enabled to detect any un-desired events.
- Operating systems contain some privileged administrator, SuperUser or Root Accounts which have ability to access any information and change it. Such Ids should be suitably controlled with strong passwords and should be used only for reconfiguring and software updating. Their activity should be logged.
- Disable the guest account.
- Disable or uninstall unused services.
- Use the Internet Connection Firewall or other methods to limit connections to the server.
- Configure file system permissions. For all important files, the permissions could be made read only.
- Configure registry permissions.
- Install and enable Security Suite. (Like Microsoft has a Microsoft Security Essentials which has to be activated and kept up-to-date)
- Secure Web Browsers like Google Chrome could be used which have a sandboxing capability (Sandboxing helps prevent malware from installing itself on user computer, or using what happens in one browser tab to affect what happens in another. The sandbox adds an additional layer of protection against malicious web pages that try to leave programs on computer)
- Some OS like Windows have capability of encrypting drives; this should be used especially for laptops in an organisation.
- Configure a screen-saver to lock the console's screen automatically if the host is left unattended.
- If the machine is not physically secured against unauthorised tampering, set a BIOS/firmware password to prevent alterations in system start-up settings.
- Configure the device boot order to prevent unauthorised booting from alternate media.

Vulnerability assessment tools like Microsoft Baseline Security Analyser or Bastille Linux may be used.

4.6 Risks and Controls in Deployment of IS Infrastructure

Risks in deployment of IS Infrastructure could be:

- Improper design –
 - Design of infrastructure has to be in accordance with business considerations.
- Disruption of services-
 - System Failure,
 - System damage,

- Denial of Service (DOS) attacks,
- Security Breaches-
 - Unauthorised access,
 - Unrestricted insider access,
 - Unnecessary services,
 - Non-authentication of web contents,
- Poor response times-
 - Inadequate capacity monitoring
 - Misconfiguration,

Controls to mitigate the above risks could be in terms of:

- Proper site selection,
- Redundancy at each layer: network, servers, network segmentation/zoning.
- Replication of data,
- Backup procedures,
- Proper Network Operating Centres (NOC) for network monitoring and control
- Security solutions,
- Secured connections to extranets,
- Deployment of firewalls,
- Intrusion Detection Systems/ Intrusion Prevention Systems for monitoring network traffic
- Tested applications,
- EMS and monitoring

4.7 Auditing IS Infrastructure

Audit all hardware and software to assess

- Whether a Hardware list with configurations is available?
- Appropriateness of hardware in accordance with computational requirements, performance, levels of redundancy
- Analysis of environmental controls for hardware
- Whether effective hardware maintenance is there, to reduce downtime?
- Test all infrastructure devices for compliance with all applicable policies.
- Whether operating system has been hardened?
- Whether proper access controls are operational for operating Systems
- Whether there are backup systems hardware, software and data sets for disaster readiness?

4.8 Summary

Information Technology forms the backbone of any organisation. For which, IT Infrastructure has to be deployed, this could be centralised or decentralised depending on the needs of the organisation. We have studied the relative advantages and dis-advantages of centralised and decentralised approach. We also had an overview of IT infrastructure in a CBS Bank. Every organisation has to keep a track and control changes in configurations through Configuration Management (CM). We also understood how to harden our systems and risks and controls in deployment of IT infrastructure and auditing thereof.

4.9 References

- http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml
- <http://www.configurationkit.com/index.htm>
- <http://www.sans.org/critical-security-controls>

CHAPTER 2: INTRODUCTION TO COMPUTER NETWORKS

PART 1: NETWORK BASICS

Learning Objectives

- To gain understanding of basics of communication
- To understand transmission modes
- To understand different categories and classification of Networks
- To gain understanding of LAN topologies
- To gain understanding of WAN transmission technologies
- To understand factors impacting selection of a suitable topology.

1.1 Introduction

In today's highly geographically dispersed organisations we cannot imagine an information system without an effective communication system. Effective and efficient communication is a valuable resource which helps the management in achieving its objectives. This communication is facilitated with communication networks. Computer network is a collection of computers (Servers / Nodes), communication medium, software that help them to communicate and the transmission methods used in such communication, software and communication protocols. Where at least one process in one device is able to send/receive data to/from at least one process residing in another device, then the two devices are said to be in a network. Physically Devices are connected but logically it is the processes which send or receive data. A network is a group of devices connected to each other.

Each component, namely the computer, printer, etc. in a computer network is called a node. Computer networks are used for exchange of data among different computers and also to share the resources. The field of computer networks is one of the most interesting and rapidly growing fields in computer science. With advantages of faster and better processing capabilities, existing computer systems are connected to each other to form a computer network which allows them to share CPU, I/O devices, storages, etc. without much of an impact on individual systems.

The main reason is resource sharing and communication. Other **reasons** for networking computers could be:

- Users can save shared files and documents on a file server rather than storing them in their individual computers.

- Users can share resources like network printer, which costs much less than having a locally attached printer for each user's computer.
- Enables sharing of data stored in a central database.
- Users can share applications running on application servers, which enable users to share data and documents, to send messages, and to collaborate.
- Better Security- The job of administering and securing a company's computer resources can be concentrated on a few centralised servers

Benefits of Computer Networks

The following are the important **benefits** of a computer network.

- **Distributed nature of information:** There would be many situations where information has to be distributed geographically. E.g. In the case of Banking Company, Account information of various customers could be distributed across various branches but to make Consolidated Balance Sheet at the yearend it would need networking to access information from all its branches.
- **Resource Sharing:** Data could be stored at a central location and can be shared across different systems. Even resource sharing could be in terms of sharing peripherals like printers, which are normally shared by many systems. E.g. In the case of a CBS bank data is stored at a Central Data Centre and could be accessed by all branches as well as ATMs.
- **Computational Power:** When working in a client server mode facilitated through networking, the computation activity is shared amongst server and clients thus reducing the load on one.
- **Reliability:** Many critical applications should be available 24X7, if such applications are run across different systems which are distributed across network then the reliability of the application would be high. E.g. In a city there could be multiple ATM machines so that if one ATM fails one could withdraw money from another ATM, as ATMs are connected to the ATM switch over network.
- **User communication:** Networks allow users to communicate using e-mail, newsgroups, and video conferencing etc.

1.2 Basics of Communication

Any communication system needs:

1. Sender, who wants to transmit a message,
2. Receiver, for whom the message is intended,
3. Content or Message,
4. Medium used for sending the message, and
5. Protocol, that is, the set of rules for making communication possible.

The main **goal** of a communication system is that the message

1. Must be accurately delivered only to the intended recipient(s),
2. Must be delivered always on time, and
3. The contents of the message must not change during transmission.

To communicate, message or content has to be transmitted. **Data transmission** or Digital communications is the physical transfer of data (a digital bit stream) over a point-to-point or point-to-multipoint communication channel. Examples of such channels are copper wires, optical fibre, wireless communication channels, and storage media. The data is often represented as an electro-magnetic signal, such as an electrical voltage signal, a radio wave or microwave signal or an infra-red signal. Data transmitted may be a digital message originating from a data source, like a computer or a keyboard. It may also be an analog signal such as a phone call or a video signal, digitized into a bit-stream. Digital signals are discreet signals whereas analog signals have varying frequencies.

1.3 Transmission Modes

A given transmission on a communications channel between two machines can occur in several ways. The transmission is characterised by:

- a) The direction of the exchanges.
- b) The number of bits sent simultaneously.
- c) Synchronisation between the transmitter and receiver.

Based upon the above, transmission modes could be:

Simplex

In Simplex communication, data transmission is always unidirectional; that is, the signal flows in one direction from any node A to any node B. Example is keyboard to computer connections.

Advantages

This mode of channel is -

- Simple, (including software)
- Inexpensive, and easy to install.

Disadvantages

Simplex mode has restricted applications, for it is -

- Only a one-way communication.
- There is no possibility of sending back error or control signals to the transmitter.

Half Duplex

In Half-Duplex communication, there are facilities to send and receive, but at a time, only one activity can be performed at a time, either send or receive. Example can be Line between a desktop workstation and a remote CPU. If another computer is transmitting to a workstation, the operator cannot send new messages until the other computer finishes its message to acknowledge an interruption.

Advantages

This mode of channel:

- Helps to detect errors and request the sender to retransmit information in case of corruption of information.
- Is less costly than full duplex.

Disadvantages

- Only one device can transmit at a time.
- Costs more than simplex.

Full Duplex

In Full-Duplex, data can travel in both directions simultaneously, we can also think of duplex as two simplexes, each travelling in a different direction. Example: Ethernet connections (The kind of networks we have in our offices) work by making simultaneous use of two physical pairs of twisted cable.

Advantage

- It enables two-way communication simultaneously.

Disadvantage

- It is the most expensive method in terms of equipment because two bandwidth channels are needed.

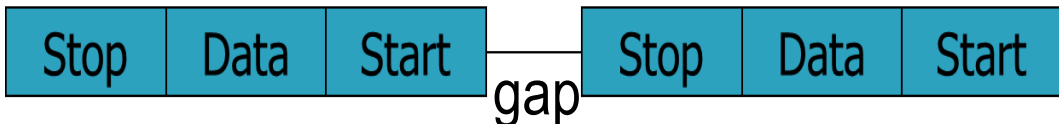
Serial transmission

Serial transmission can be either Synchronous or Asynchronous on the basis of the synchronisation between the receiver and sender. In Serial Transmission, as single wire transports information, the problem is how to synchronise the sender and receiver.

Asynchronous Transmission

Also termed as **Start-Stop communication**, an asynchronous communication technique is a technique in which the timing of a signal is unimportant and is most widely used by computers to provide connectivity to printers etc. Any communication between devices of dissimilar speeds will be of asynchronous one. In asynchronous transmission, the transmitter sends 1 start bit (0) at the beginning and 1 or more stop bits (1s) at the end of each byte. There may be a gap between each byte. The basic characteristics of an Asynchronous Communication System are:

- Sender and receiver have independent transmit and receive clocks.
- Simple interface and inexpensive to implement.
- Limited data rate, typically < 64 kbps.
- Requires start and stop bits that provide byte timing.
- Increased overhead.
- Parity often used to validate correct reception.



Advantages

- It is simple and does not require synchronisation of the two communication sides.
- Since timing is not critical for asynchronous transmission, hardware can be cheaper.
- Its set-up is fast and well suited for applications where messages are generated at irregular intervals, like data entry from the keyboard.

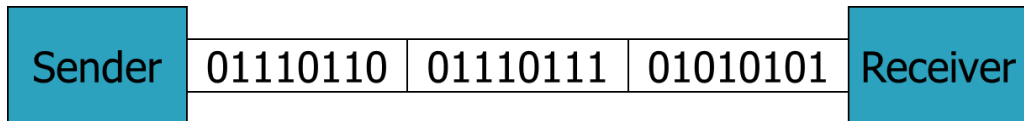
Disadvantages

- Slower-Because of the insertion of start and stop bits into the bit stream, asynchronous transmission is slower than other forms of transmission that operate without the addition of control information.

Synchronous Transmission

In synchronous transmission, we send bits one after another without start/stop bits or gaps. It is the responsibility of the receiver to group the bits. In synchronous communication, the clock of the receiver is synchronised with the clock of the transmitter. On account of this, higher data transmission rates are possible with no start-stop bits. The characteristics of synchronous communication are:

- There is synchronisation between the clocks of the transmitter and receiver.
- It supports high data rates.
- It is used in communication between computer and telephony networks.



Advantages

- The advantage of synchronous transmission is speed. With no extra bits or gaps to introduce it is faster than asynchronous transmission.

Disadvantages

- In synchronous transmission, the data is to be recognized at the receiver's end, as there may be differences between the transmitter and receiver clocks. That is why each data transmission must be sustained long enough for the receiver to distinguish it.
- Slightly more complex than the asynchronous one.
- Its hardware is more expensive than that of asynchronous one.

1.4 Network Categories

1.4.1 Local Area Networks (LAN)

Local Area Networks (LAN) interconnects a variety of devices and provides a means for information exchange among them. LAN interconnects devices within a single building or cluster of buildings within a limited geographic area.

Some features of LAN are:

- Uses regular topology.
- Permanently connected.
- Security is high.
- Installation and maintenance which can be centralised or distributed is relatively easy.
- Low error rates.
- Owned and maintained by the organisation.
- Majority of the installations uses guided media like UTP, Optical fiber, etc.,
- Traditional LANs-provide data rates of 1 to 20 Mbps
- High-speed LANS-provide data rates of 100 Mbps to 1 Gbps

1.4.2 Metropolitan Area networks (MAN)

Traditional point-to-point and switched network techniques used in WANs are inadequate for growing needs of organisations for high capacity and low costs over large area. These are met through MANs. The key characteristics are:

- Service to customers in large areas.
- Generally include provisions for both voice and data transmissions.

- Provides required capacity.
- Lower cost and greater efficiency than equivalent service from Telephone Company.

1.4.3 Wide Area Networks (WAN)

Wide Area Networks (WAN) covers large geographical areas. In WAN, circuits provided by a common carrier and high-capacity backbones interconnect at various Network Access Points. One simple example could be Internet. WAN consists of interconnected switching nodes. Some other features of WAN are:

- It usually has an irregular topology.
- It can be connected on demand or be permanently connected.
- Most WANs are not owned by any one organisation
- WAN uses public or private networks.
- Higher-speed WANs use optical fibre and transmission technique known as asynchronous transfer mode (ATM)-10s and 100s of Mbps are common.

Differences between LAN and WAN

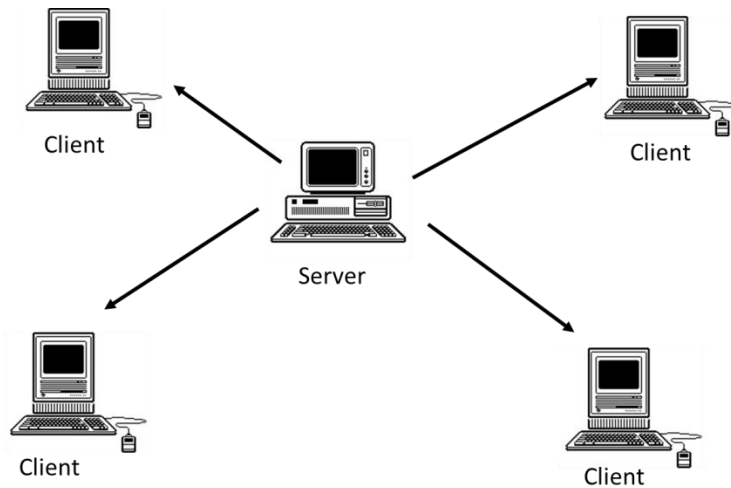
- Scope of a LAN is smaller
LAN interconnects devices within a single building or cluster of buildings
- LAN is usually owned by organisation that owns the attached devices
For WANs, most of network assets are not owned by same organisation
- Internal data rate of LAN is much greater.
- All devices in a LAN will have same NetworkID.

1.5 Network types

Based on Node Relationships there are broadly two types of networks.

- **Client Server Architecture:** In this there is a dedicated file server that runs the network, granting other nodes or clients access to resources.
- **Peer - to - Peer Architecture:** In this every node can act as a client and server; that is, all nodes are treated on par.

1.5.1 Client-Server Architecture



The Client-Server architecture separates an application into at least two processes. One process plays the role of the client, the other plays the role of the server. In this architecture, the client process requests services from server process. Client also shares the processing load of the server. The application also has to be designed to work in Client Server mode. In this model there is separation of computational logic from interface-oriented logic. This model is not about how computers or nodes are connected but more about processes or computational logic being split. i.e. there are client processes which typically request for information and there are server processes which take request for information gather that information and send it to client. Thus it is not about hardware it is about applications and their processes.

Functions of a Client

- Client process is implemented on hardware and software environments better suited for humans
- A client can request services from one or more servers
- Client executes in a different address space from the server
- Usually manages the GUI
- Manages the display of data
- Performs data input and validation and all tasks that can be handled locally.
- Dispatches requests to server(s)
- Manages local environment, Display, Keyboard etc.

Functions of a Server

- A server is a supplier of services to clients

- Serves one or more clients
- Each client can be on different platform
- A program that carries out client requests
- Usually manages some unique resources such as:
 - RDBMS
 - Business Logic and Files

Middleware

Middleware are a kind of programs that help in clients communicate with Server applications. This is like plumbing which joins clients with server. It consists of all the software that supports connectivity between clients and servers. Middleware controls communication, authentication and message delivery.

Middleware does the job of Transporting, Queuing, and Scheduling. Let's say that a client request for information- Middleware does the job of conveying this request to server, when middleware takes the request from client, client is in a way free to do other jobs, middleware then schedules the request of client to server, maintain a queue of requests and after getting the required response from server hands over the responses back to client.

Middleware has the capability to connect to diverse platforms thus providing platform independence.

Characteristics of Client- Server Model

- Separation of service into client and server roles
- A server permits sharing of resources by many clients
- Clients always initiate the requests with the server
- One server serves many clients
- Server is independent of the client, such that it may reside on the same or different machine
- Clients and servers are independent of hardware or operating systems.
- Better security
- Clients and servers are loosely coupled and communicate via messages
- Scalable architecture i.e. it can scale horizontally by adding more clients or vertically by adding more server layers.
- Server code and data are centrally managed for better maintenance capabilities and integrity of shared resources.

Advantage of Server Based Networks:

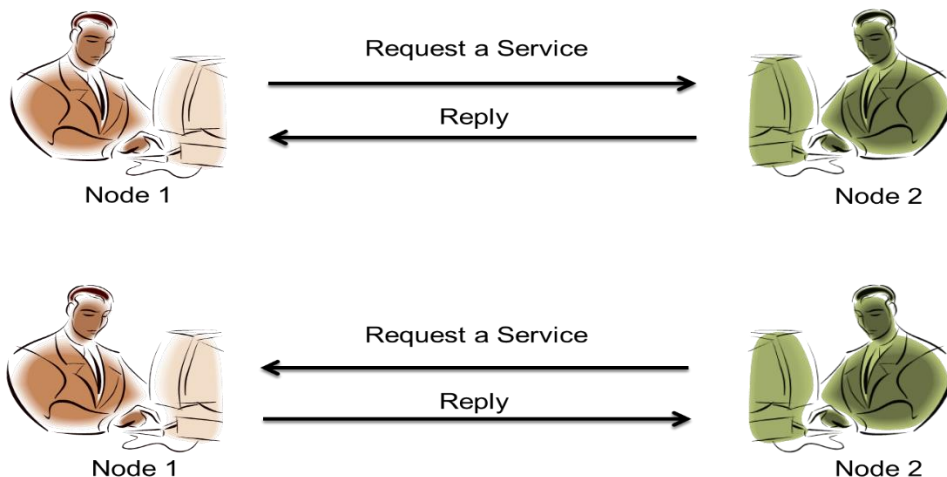
- Strong central security
- Central file storage
- Ability to pool available hardware and software

- Less intrusive security
- Easy manageability of large no. of users
- Central organisation

Disadvantage of Server based networks:

- Expensive dedicated Hardware
- Expensive network operating system software and client licenses
- A dedicated network administrator (usually required)

1.5.2 Peer-To Peer Networks



Peer -to-Peer Networking is where two or more computers are connected and share resources without going through a separate server computer. In this approach all computers share equivalent responsibility for processing data.

Advantages of Peer-to-Peer Networks are:

- No extra investment in server hardware or software
- Easy setup
- No network administration required
- Ability of users to control resource sharing
- No reliance on other computers for their operation
- Lower cost for small networks

Disadvantages of Peer-to Peer Networks are

- Additional load on computers because of resource sharing
- Lack of central organisation
- No central point of storage for file archiving

- Users own administration of their computers
- Weak and intrusive security
- Lack of central management
- Not meant for large networks

1.6 LAN Topologies and Network Components

1.6.1 Media Used In Communication

Medium through which data is transmitted is transmission media. For connecting devices in a network some or the other transmission media would be required. Media used in computer networks are broadly classified into Guided and Unguided.

Factors that influence the use of media

The main factors that influence the use of appropriate media include:

- **Cost:** initial, expansion and maintenance
- **Quality:** quality needed over some estimated distance
- **Attenuation:** weakening of signal
- **Speed:** data rate and response time
- **Security:** vulnerability to eaves dropping
- **Immunity from Electromagnetic Interference (EMI)**

Factors that degrade a signal

Three factors that degrade the quality of a signal are:

- **Attenuation:** In attenuation, as the signal travels through the medium, it loses its strength.
- **Delay Distortion:** This problem is of a composite signal (multiplexed signal), as it consists of multiple signals of varying frequencies. When all of them arrive at the same time, there is no distortion. But if they arrive at different times, then there is delay distortion.
- **Noise:** Any unwanted stray signal that is present in a signal is called noise. Sometimes the noise signals interfere with the regular ones, making it difficult for the receiver to interpret the signal correctly.

Guided Transmission Media

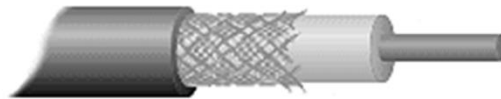
They are also known as Bound Media. They use a "cabling" system that guides the data signals along a specific path.

- Coaxial Cable
- Twisted Pair Cable
- Fiber Optic Cable

Coaxial Cable

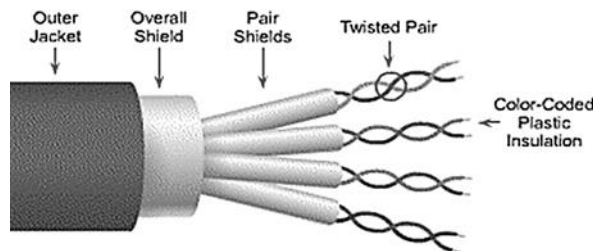
Co-axial cable consists of a central core conductor of solid or stranded wires. The central core is held inside a plastic cladding with outer wire mesh and an outer plastic Cladding providing a shield. The axis of both the conductors is same hence the name; Co-Axial. This is the kind of Cable we generally see being used for Cable TV.

- Thinnet- Flexible used for internal cabling
- Thicknet: Used for external cabling



Twister pair cable

A twisted pair cable is a type of cable made by putting two separate insulated wires together in a twisted pattern and running them parallel to each other. Benefits - Reduced EMI



Unshielded Twisted Pair (UTP)

This is the most commonly used media used in networks. This consists of two wires twisted over one another which reduce the interference in signals.

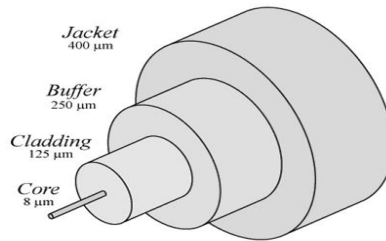
Shielded Twisted Pair

In case of shielded twisted pair (STP), there is a metallic shield either in the form of a foil or a braid over the twisted pair. The shield reduces the penetration of electro-magnetic stray signals (noise), to some extent.

Optical Fibre Cable

Optic Fibre Cable uses light based signalling. The significant benefits are low attenuation and very high integrity over much longer distances than metallic options. In an optical fibre, the inner core

consists of a pure glass material or plastic/polymer/acrylic about the diameter of a human hair. An optical fibre has the following parts:



- **Core:** a thin glass centre of fibre through which light travels ;
- **Cladding:** the outer optical material surrounding the core that reflects the light back into the core.
- **Buffer coating:** plastic coating that protects fibre from damage and moisture

Advantages of Optic Fibre are:

- Optical fibre can be drawn to smaller diameters than copper wires.
- Higher carrying capacity: Because optical fibre are thinner than copper wires, more fibre can be bundled into a given diameter cable than copper wires. This allows more packing.
- Less signal degradation: The loss of signal in optical fibre is less than in copper wire.
- Low power: Because signals in optical fibre degrade less than in others like coaxial cables lower power transmitters can be used.

Disadvantages of Optic Fibre are:

- Very fragile than wires.
- Costlier than other guided media.
- Difficult to splice (i.e., it is extremely difficult to join optical fibre cables).

Comparison among Guided Media

Factor	UTP	STP	Co-axial	Optical Fibre
Cost	Lowest	Moderate	Moderate	Highest
Installation	Easy	Fairly easy	Fairly easy	Difficult
Bandwidth	Typically 100Mbps	Typically 16Mbps	Typically 16Mbps	Typically 100Mbps
Attenuation	High	High	Lower	Lowest

EMI	Most vulnerable	Less vulnerable compared to UTP	Less vulnerable compared to STP	Not affected
Security	Easy to eavesdrop	Vulnerable to eavesdrop	Vulnerable to eavesdrop	Extremely difficult to eavesdrop

Unguided Transmission Media

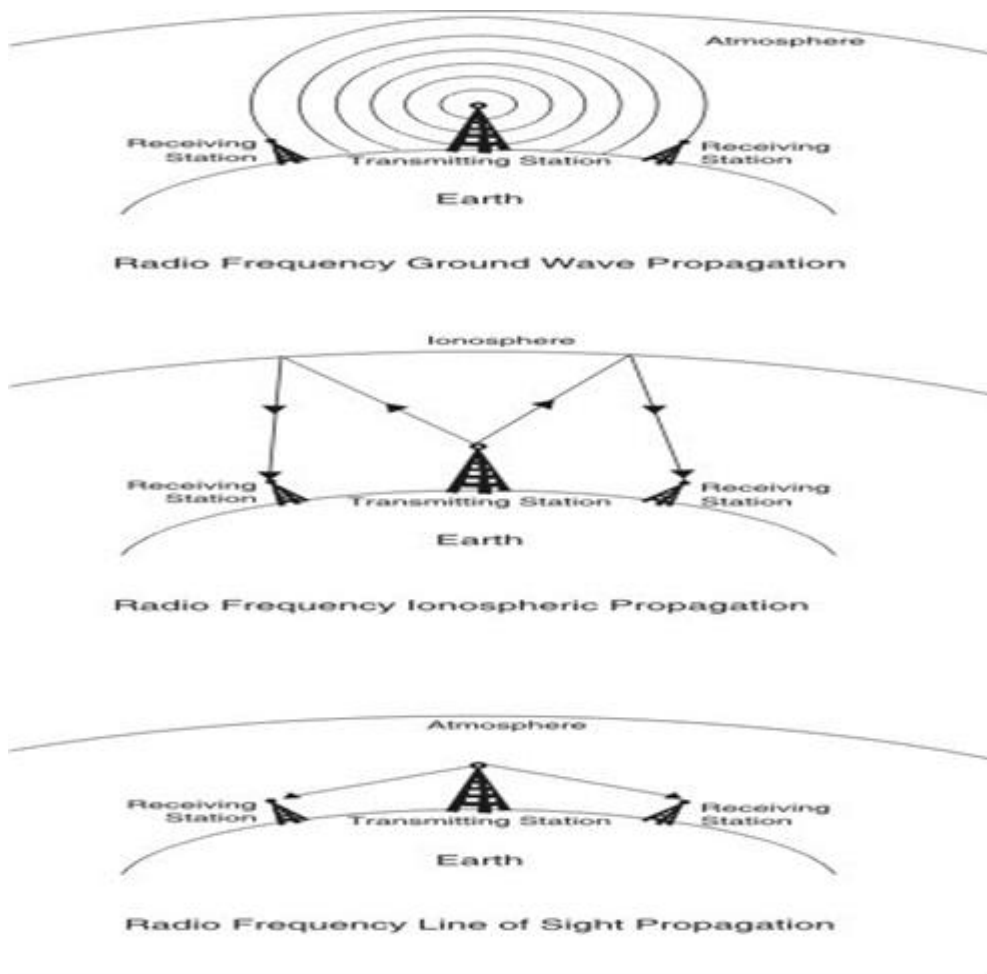
In Unguided Transmission Media, data signals travel without any guidance along a specific path. These are not bound to a cabling media and do not take a fixed path. Signals are broadcasted by transmitters and picked by receivers. A signal radiated from an antenna travels along one of three routes: ground wave, ionospheric, or line of sight (LOS).

Ground Wave Propagation-more or less follows the contour of the earth and can propagate considerable distances, well over the visual horizon.

Ionospheric Propagation, a signal from an earth-based antenna is reflected from the ionized layer of the upper atmosphere (ionosphere) back down to earth. Ionospheric propagation can travel through a number of hops, bouncing back and forth between the ionosphere and the earth's surface. A signal can be picked up thousands of kilo-meters from the transmitter.

Line of Sight (LOS) propagation: In this, the transmitter and the receiver face each other. This is sometimes called space waves or tropospheric propagation.

- **Radio Waves**: Could be Ground Wave propagation, Ionospheric propagation, Line of Sight (LOS) propagation
- **Microwave**: Line of Sight transmission with receiving Station
- **Satellite**: Signals are reflected from Geo-stationary Satellites
- **Cellular Telephony**: Uses radio waves



Various types of Propagation

1.6.2 Network Devices

Network Interface Card (NIC)

Network Interface Card (NIC) is a device that enables computers to connect to the network. It provides one or more ports for connection of the network cable. It transmits and receives data onto the network cable. Each NIC Card has a unique hard coded 48 Bit physical address which is called MAC (Media Access Control) Address. It is generally of the type e.g. 40-2C-F4-0B-24-9E, where it is being represented in hexadecimals and each hexadecimal is represented with 4 bits thus a 48 Bit address. We can see MAC addresses of our computer by command `C:\ipconfig /all` in command prompt mode.

Hub

Hub is a hardware device that contains multiple, independent ports that match the cable type of the network. It provides multiport connectivity. Networks using a Star topology require a central point for the devices to connect.

Some features of hubs are:

- Hubs offer an inexpensive option for transporting data between devices
- Don't offer any form of intelligence.
- Transmission is broadcast
- Hubs can be active or passive.
- **Active hub** amplifies and regenerates the incoming signals before sending the data on to its destination.
- **Passive hubs** do nothing with the signal

Switches

Switches are a special type of hub that offers an additional layer of intelligence. Switch reads the MAC address (described above, it is address of NIC Card) of each frame it receives. It maintains its Switching Table. This information allows switches to transmit only to nodes to which a frame is addressed. This speeds up the network and reduces congestion, reduces collisions. Since this provides point to point connectivity multiple connections are possible.

Bridges

Bridges are used to extend or segment two networks. They sit between two physical network segments and manage the flow of data between the two segments by looking at the MAC address of the devices connected to each segment, Bridges can elect to forward the data or block it from crossing.

Multi-station Access Unit (MAU)

Special type of hub used for token ring networks. On the outside, the MAU looks like a hub. This performs the token circulation inside the device. It connects to multiple network devices, each with a separate cable.

Routers

Routers are networking devices used to extend or segment networks by forwarding packets from one logical network to another. A router can be a dedicated hardware device or a computer system with more than one network interface and the appropriate routing software. Routers contain internal tables of information called routing tables that keep track of all known network addresses and possible paths throughout the internetwork, along with number of hops of reaching each network. When a router receives a packet of data, it reads the header of the

packet to determine the destination address. Once it has determined the address, it looks in its routing table to determine whether it knows how to reach the destination and, if it does, it forwards the packet to the next hop on the route.

Static routing, routes and route information are entered into the routing tables manually.

Dynamic routing: The router decides about the route based on the latest routing information gathered from connected routers.

Gateway

Gateway is a device that translates one data format to another. It is used to connect networks using different protocols. Key point about a gateway is that only the data format is translated, not the data itself. Example could be Email Gateways.

1.6.3 Network Topologies

The term topology, or more specifically, network topology, refers to the arrangement or physical layout of computers, cables, and other components on the network.

Physical topology refers to the placement of the network's various components, including device location and cable installation, while **logical topology** shows how data flows within a network, regardless of its physical design

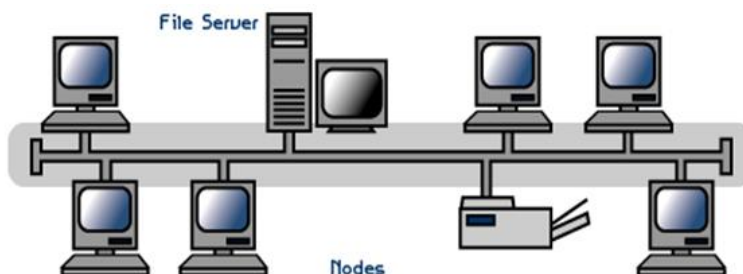
Importance of Logical Topologies- The media access method, the way network access is controlled and collisions prevented is based on the logical topology rather than the physical topology. To effectively troubleshoot communications problems, it is important to know not only the physical topology of a network but also the logical topology, so that we know what path the data packets take as they travel from one computer to another.

All network designs stem from four basic topologies:

- Bus
- Star
- Ring
- Mesh

Bus Topology

The bus topology computers are connected on a single backbone cable.



This is the simplest method of networking computers. The cable runs from device to device by using “tee” connectors that plug into the network adapter cards. Terminator is used at the end to stop the signal from bouncing. A device wishing to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message. Because only one computer at a time can send data on a bus network, the number of computers attached to the bus will affect network performance.

Advantages

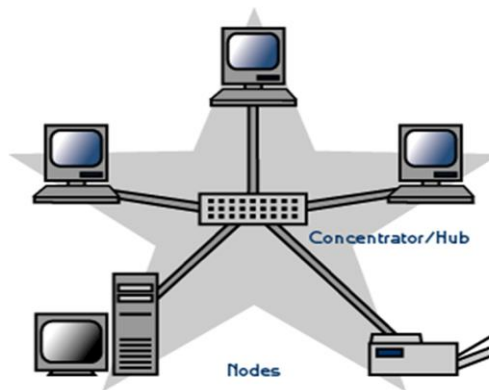
- Less expensive when compared to star topology due to less cabling and no network hubs.
- Good for smaller networks not requiring higher speeds.
- Networks can be extended by the use of repeaters.
- Easy to install.

Disadvantages

- Limited in size and speed.
- Attenuation
- One bad connector or failure of the backbone cable shuts down entire network.
- Difficult to troubleshoot.
- Addition of nodes negatively affects the performance of the whole network, and if there is a lot of traffic throughput decreases rapidly.

Star Topology

Star topology contains a central hub or Switch to which each and every node is connected.



This necessitates drawing of a separate cable from each and every node to the central hub. All inter-node data transmission has to pass through it.

Advantages

- Easy to troubleshoot.

- Allows mixing of cabling types.
- Easy to install and wire.
- No disruptions to the network when nodes are down.
- No disruptions to the network while connecting or removing devices.

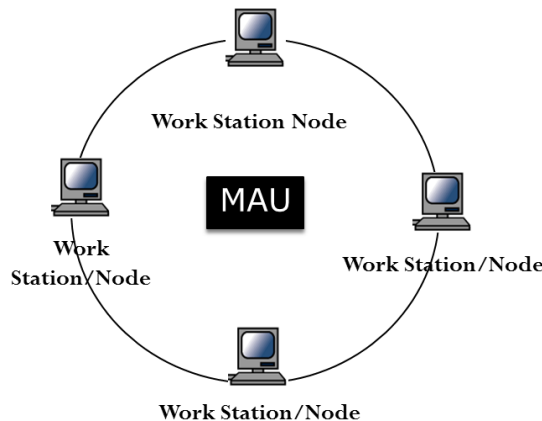
Disadvantages

- Hubs become a single point of failure.
- Cabling is expensive because individual cables have to be drawn from nodes to hubs.
- More expensive than bus topology because of the cable.
- The capacity of the hub determines the number of nodes that can be connected.

Ring Topology

The ring topology connects computers on a single circle of cable

In a ring network, every device has exactly two neighbours for communication purposes.



All messages travel through a ring in the same direction (effectively either "clockwise" or "anti-clockwise").

A token, or small data packet, is continuously passed around the network. Whenever a device has to transmit, it holds the token. Whosoever holds the token has the right to communicate.

The Token Ring is a network with different logical and physical topologies. Physical Topology is wiring diagram and logical topology is the channel access method. Here, the physical topology is a star bus; that is, there is a length of cable from each computer that connects it to a central hub (called a Multi-Station Access Unit, or MAU). Inside the hub, however, the ports are wired together sequentially in a ring, and they send data around the ring instead of sending it out to all ports simultaneously as it would if the network were a logical star. The MAU makes a logical ring connection between the devices internally.

Advantages

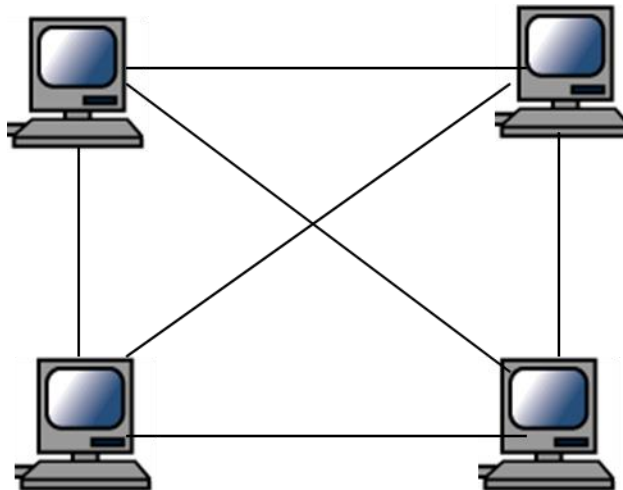
- Every device gets an opportunity to transmit.
- No computer can monopolise
- Every node gets fair share of network resources.
- Performs better than the star topology under heavy network load.
- Caters to heavy network load

Disadvantages

- One malfunctioning workstation or bad port in the MAU can create problems for the entire network.
- Moves, additions and change of devices can affect the network.
- Network adapter cards and MAUs are much more expensive than Ethernet cards and hubs.

Mesh Topology

In this topology, every node is physically connected to every other node.



This is generally used in systems which require a high degree of fault tolerance, such as the backbone of a telecommunications company or an ISP.

Advantages

- Highly fault tolerant
- When one node fails, traffic can easily be diverted to other nodes.
- Guaranteed communication channel capacity
- Easy to troubleshoot

Disadvantages

- It requires maximum number of cables for connecting devices than any other topology.
- It is complex and difficult to set up and maintain.
- It is difficult to introduce or remove nodes from the system as it necessitates rewiring.
- Its maintenance is expensive.

Hybrids

Hybrid networks use a combination of any two or more topologies in such a way that the resulting network does not exhibit any one of the standard topologies (e.g., bus, star, ring, etc.). For example two star networks connected together create a hybrid network topology. A hybrid topology is always produced when two different basic network topologies are connected.

Two common examples for Hybrid network are: Star Ring network and Star Bus network.

- **Star Ring Network:** A Star Ring network consists of two or more star topologies connected by using a multi-station access unit (MAU) as a centralised hub.
- **Star Bus Network:** A Star Bus network consists of two or more star topologies connected by using a bus trunk (the bus trunk serves as the network's backbone).

1.7 WAN Message Transmission Technologies

Some of the scenarios where you need a Wide Area Networks (WAN) could be:

- A bank with branches all over the world – gather transactions into central database.
- Regional sales representatives needing to submit sales files to their HQ in other states/countries
- A clothing manufacturer selling products through Internet to their customers throughout the world.

1.7.1 Switching

For data transfer across WAN, Switching Techniques are required, Switching implies sending on a path.

Following are the switching techniques used for WAN:

- Circuit Switching
- Packet Switching
- Message Switching

Circuit Switching

Circuit Switching is a type of communication in which a temporary physical connection is established between two devices, such as computers or phones, for the entire duration of transmission usually a session.

In circuit switching, the entire bandwidth of the circuit is available to the communicating parties. The cost of the circuit is calculated on the basis of the time used. Circuit switching networks are ideal for real-time data transmissions. Example: Telephone connections

How it works

- Communication via circuit switching networks involves 3 phases:
- Circuit establishment – an end-to-end connection must be established before any signal can be transmitted via the channel.
- Data transfer – the transmission may be analog voice, digitalized voice or binary data depending on the nature of the network.
- Circuit disconnection – once the transmission is complete, the connection will be terminated by one of the end station.

Advantages	Disadvantages
Compatible with voice	No routing techniques, call subject to blockage
No special training / protocols are needed to handle data traffic	Devices at both ends must be compatible in terms of protocols and data flow.
Predictable, constant rate of data traffic	Large processing and signal burden on the network

Packet Switching

It is a Network technology that breaks up a message into smaller packets for transmission. Unlike circuit switching which requires point to point connection establishment, each packet in the packet switched network contains a destination address. Thus, packets in a single message do not have to travel the same path and can arrive out of order. Destination computer reassembles them into proper sequence. Example is internet communication and most computer networks.

How it works

- Data is transmitted in blocks, called packets
- Message is broken into a series of packets
- Packets consists of a portion of data plus a packet header that includes control information
- At each node en-route, packet is received, stored briefly and passed to the next node.

Advantages	Disadvantages
Provide speed conversion, Two devices of different speed can communicate	Complex Routing and control
Efficient path Utilisation	Delay in data Flow during time of load

Packet switching networks support two kinds of services:

1. **Datagram:** In which each packet is treated independently and packet path is chosen based on the information received from neighbouring nodes on traffic, line failures etc. Each independent packet referred as a datagram.
2. **Virtual circuit:** Pre-planned route is established before sending any packets. Once the route is stabled, all packets follow the route but it is logical connection for fix duration and referred as virtual circuit.

Message Switching

Message switch is also known as store-and-forward switching. No physical path is established in advance between the sender and the receiver. Data is sent which is concentrated at switching point and whenever path is available it is sent forward.

Its cost is determined by the length of the message being transmitted.

Example: SMS (Short Message Service) on mobiles

How it Works

- Not necessary to establish circuit all over the network from source to destination
- When the sender sends a block of data, it is stored in the switching point
When the appropriate route is available, it is transferred to the next switching point, one hop at a time until the message reaches its destination.
- Each block is received in its entirety, inspected for errors, and then retransmitted.

1.7.2 Multiplexing

Multiplexing is a set of techniques that permit the simultaneous transmission of multiple signals on a single carrier. With increase in data-and-telecommunications usage, there is increase in traffic and also the need to accommodate individual users. To achieve this, we have to either increase individual lines each time a new channel is needed, or install higher capacity links and use each to carry multiple signals. If the transmission capacity of a link is greater than the transmission needs of the devices connected to it, the excess capacity is wasted. Multiplexing is an efficient system that maximizes the utilities of all facilities.

A device that performs multiplexing is called a multiplexer (MUX), and a device that performs the reverse process is called a de-multiplexer (DEMUX). Prominent kinds of multiplexing are:

- Frequency Division Multiplexing (FDM)
- Time Division Multiplexing(TDM)
- Wave division Multiplexing(WDM)

Frequency Division Multiplexing (FDM)

This is a form of signal multiplexing which involves assigning non-overlapping frequency ranges to different signals or to each “user” of a medium. FDM is an analog technique that can be applied when the bandwidth of a link is greater than the combined bandwidths of the signals to be transmitted.

Features of FDM are:

- All signals are transmitted at the same time.
- A multiplexer
 - Accepts inputs and assigns frequencies to each device.
 - Is attached to a high-speed communications line.
- A corresponding de-multiplexer
 - Is at the end of the high-speed line.
 - Separates the multiplexed signals into their constituent component signals.
- The channel bandwidth is allocated even when no data is to be transmitted.

Time Division Multiplexing (TDM)

Time-Division Multiplexing (TDM) is a type of digital or rarely analog multiplexing in which two or more signals or bit streams are transferred apparently simultaneously as sub-channels in one communication channel, but take turns on the channel. The time domain is divided into several concurrent timeslots of fixed length, one for each sub-channel. TDM is applied when the data rate capacity of the transmission medium is greater than the data rate required by the sending and receiving devices.

TDM is of two types:

1. **Synchronous TDM:** In this scheme, the multiplexer allocates exactly the same time slot to each device at all times, no matter whether a device has anything to transmit or not.
2. **Asynchronous TDM:** The disadvantage of Synchronous TDM is that it does not assure use of the full capacity of a link, as the time slots are allotted to each of the sending device irrespective of whether it has any data to send or not. In Asynchronous TDM need based time is given to only those devices that have data to transmit.

Wavelength Division Multiplexing (WDM)

Wavelength Division Multiplexing (WDM) is conceptually like the FDM, which multiplexes multiple optical carrier signals on a single optical fibre by using different wavelengths (colours) of laser light to carry different signals.

1.8 Selecting a Suitable Network Topology

In real world we see lot of networks like Telephone/ mobile network, postal networks etc. If we look at these systems we can analyse that networks could be of two types:

- **Connection Oriented networks-** wherein a connection is first established and then data is exchanged like it happens in Telephone networks
- **Connectionless Networks-** where no prior connection is made before data exchanges. Data which is being exchanged in fact has a complete contact information of recipient and at each intermediate destination, it is decided how to proceed further- as happens in the case of postal networks in real life.

These real world networks have helped model computer networks. Each of these networks is modelled to address the following basic issues

- **Routing:** Refers to the process of deciding on how to communicate the data from source to destination in a network.
- **Bandwidth:** refers to the amount of data which can be sent across a network in given time.
- **Resilience:** The ability of a network to recover from any kind of error like connection failure, loss of data etc.
- **Contention:** The situation that arises when there is a conflict for some common resource. For example network contention could arise when two or more computer systems try to communicate at the same time.

A network's topology affects its capabilities. The choice of one topology over another will have an impact on the:

- Type of equipment the network needs.
- Capabilities of the equipment.
- Growth of the network.
- Way the network is managed.

Some Design Considerations to consider before deciding on Network

- Performance
- Cost Reduction
- Security/Auditing
- Availability/Reliability

- Manageability and Monitoring
- Quality of Service/Class of Service
- Support for Business Recovery Planning

Before any network topology is designed, the network design engineer considers these goals:

- To provide maximum possible reliability by providing alternative routes if a node fails.
- To be able to pinpoint faults promptly.
- To give the end users the best possible response time and throughput. This is especially important for interactive sessions between user applications.
- To route network traffic through the least cost path within the network. This is usually provided in two ways:
 1. By minimising the actual length of the channel between its components; it entails routing the traffic through very few intermediate components.
 2. By providing the least expensive channel option for a particular application; for instance, transmitting low priority data over low cost dial up lines, in contrast to using an expensive high speed satellite channel.

1.9 Summary

We can very well say that in today's competitive market, responsiveness to customer or supplier demand is often a decisive factor in the success of an organisation. This market responsiveness requires communication which is facilitated through computer networks. Computer networks are considered one of the most critical resources in any organisation.

In this chapter we have learnt about communication which is facilitated through data transmission over computer networks. We have also learnt about the network components which help in constituting structure of networks or network topologies. We have also had an overview of some WAN transmission technologies. Knowledge of these technologies helps us in selecting a suitable network topology.

1.10 References

- Ralph M. Stair, George W. Reynolds, 'Principles of Information Systems', Cengage Learning
- <http://www.di.unisa.it/~vitsca/RC-0809/ch04.pdf>
- http://www.tutorialspoint.com/unix_sockets/client_server_model.htm
- <http://magazine.redhat.com/2008/03/11/what-is-middleware-in-plain-english-please/>
- <http://pluto.ksi.edu/>

PART 2: NETWORK STANDARDS AND PROTOCOLS

Learning Objectives

- To gain understanding of network standards and networking protocols
- To gain an overview of OSI Layers and understand layering concept
- To understand TCP/IP Model
- To gain understanding of Wireless Networks

2.1 Introduction

A network may be described as a group or collection of computers connected together for sharing resources and information. Where individual networks are connected by different types of network devices, such as routers and switches, it is called Internetwork. Enabling effective and secure communication of various systems with disparate technologies is a challenging task. Networks are a complicated subject and when we talk of internetwork i.e. two different networks having different technologies, problem is compounded. Understanding of these complicated systems was made easier by splitting the communication process to small portions via a reference model called OSI. The Open Systems Interconnection (OSI) model enables easy integration of various technologies and provides solutions for managing the internetworking environment. A practical model or more appropriate a suite of specific network protocols is TCP/IP, on which Internet has been built. We would understand these concepts.

2.2 Network Standards and Protocols

Internet

The Internet is a worldwide system of interconnected computer networks. Its origins can be traced to the creation of ARPANET (Advanced Research Projects Agency Network) as a network of computers under the auspices of the U.S. Department of Defence in 1969. ARPA established a packet-switching network of computers linked by point-to-point leased lines that provided a basis for early research into networking. The conventions developed by ARPA to specify how individual computers could communicate across that network became TCP/IP. As networking possibilities grew to include other types of links and devices, ARPA adapted new TCP/IP to meet the demands of the new technology. As involvement in TCP/IP grew, the scope of ARPANET expanded to become what is now known as the Internet.

An internet under TCP/IP operates like a single network connecting many computers of any size, type and shape. Internally, an Internet is an interconnection of independent physical networks

linked together by internetworking devices. Initially NSF (National Science Foundation) created the first backbone for Internet, but now there are many companies that operate their own high-capacity backbones, and all of them interconnect at various Network Access Points (NAPs) around the world. This ensures that anybody who is on Internet, irrespective of area they are in and the company they use, are able to communicate through Internet with everybody else. The Internet is thus a giant agreement between different companies to help communication between different participants.

There is no governing body in control of Internet. But if anything has to function then some rules and regulations need to be followed. Some organisations develop technical aspects of this network, set standards for creating applications on it. Some bodies help in managing the Internet. These are:

- **The Internet Society (ISOC)**, (www.isoc.org) a non-governmental international organisation providing coordination for the Internet, and its internetworking technologies and applications.
- **The Internet Architecture Board (IAB)** (www.iab.org) governs administrative and technical activities on the Internet.
- **The Internet Engineering Task Force (IETF)** (www.ietf.org) has the primary responsibility for the technical activities of the Internet, including writing specifications and protocols.
- **The Forum of Incident Response and Security Teams** (www.first.org) is the coordinator of a number of Computer Emergency Response Teams (**CERTs**) representing many countries, governmental agencies, and ISPs (Internet Service Providers) throughout the world.
- **The World Wide Web Consortium (W3C)** (www.w3.org) takes a lead role in developing common protocols for the World Wide Web to promote its evolution and ensure its interoperability.
- **The Internet Corporation for Assigned Names and Numbers (ICANN)**. (www.icann.org) This body handles governance of generic Top Level Domain (gTLD), registration of Domain names and anything relating to Names and Numbers on Internet.

2.2.1 Network Standards

Standards are documented agreements containing technical specifications or other precise criteria to be used consistently as rules, guidelines, or definitions of characteristics, to ensure that materials, products, processes and services are fit for their purpose. These provide a model for development that makes it possible for a product to work regardless of the individual manufacturer. These are essential for creating and maintaining an open and competitive market for manufacturers and provide guidelines to vendors, government agencies and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.

To take a simple example, let us look at an electric plug and socket where there are no standard specifications. In this case, the plugs of two manufacturers can never fit into each other's socket.

So there are standards which define the distance and angle between pins, diameter of pin etc. so that one plug could fit into socket manufactured by the other manufacturer. The benefits of standardisation are:

- Allows different computers to communicate.
- Increases the market for products adhering to the standard.

2.2.2 Protocols

A networking protocol is defined as a set of rules that governs data communication over a network for:

- What is communicated,
- How it is communicated and
- When it is communicated.

To take a simple example, if we are speaking with somebody, for the other person to understand it is important that we are speaking the same language governed by same grammar and the speed of communication should be such that the other person can comprehend. Similarly, communication in networks is facilitated by these common rules called protocols.

The key elements of protocol are:

- **Syntax:**
 - Represents What is communicated
 - It is the structure or format of the data, that is, the order in which they are presented.
 - In simple terms it means which portion of packet is address and which is content.
 - As an analogy, in a Post Card it is pre-defined which part will carry address and which part the content.
- **Semantics:**
 - Represent how it is communicated.
 - It means each section of bits, how a particular pattern is to be interpreted, and based on that, what action to be taken.
 - In simple terms it could represent even in address which portion is senders address and which is receivers address
- **Timing:**
 - Represents When it is communicated
 - It indicates when the data is to be transmitted and how fast it can be sent.

Even though both these terms are interchangeable a bit of difference could be a protocol defines a set of rules used by two or more parties to interact between themselves. A standard is a formalised protocol accepted by most of the parties that implement it.

2.2.3 Standards creation committees

Standards are developed through the cooperation of standards creation committees, forums, and government regulatory services. Some prominent Standard setting Bodies are:

- International Organization for Standardization (ISO)
- Internet Engineering Task Force (IETF)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Telecommunication Union (ITU)
- American National Standards Institute (ANSI)
- National Institute of Standards and Technology (NIST)

The Standard Setting process is a pretty democratic process with participation from users. Let's say IETF is to set a standard, the process in brief would be

- A protocol is proposed by a vendor.
- IETF working group studies the proposal.
- IETF issues a request for comment (RFC).
- IETF reviews the comments.
- IETF proposes an improved RFC.
- The RFC becomes a proposed standard.
- The proposed standard becomes a draft standard if two or more vendors adopt it.

That's the reason all IETF Standards start with RFC.

2.2.4 The OSI Architecture

What is OSI Model?

Very simply this model attempts to explain how computers network. Open Systems refers to a cooperative effort to have development of hardware and software among many vendors that could be used together. Developed by ISO(International Organisation for Standardization), the Open System Interconnection (OSI) Reference Model describes how information from a software application in one computer moves through a network medium to a software application in another computer. In other words, the model describes the concepts involved when the message or data or instruction from the sender's computer or device moves over a range of network environments and reaches the receiver's computer or device, as the sender sent it.

Why OSI Model?

OSI Model is a reference model used to understand data communication in networks. In today's complex computing environment, messages are sent across heterogeneous networks with a large variety of hardware technologies, networking devices and protocols, device drivers, operating systems, application software, and so on. So there is a need for resolving these complexities universally, without causing worries to the users. The answer is the Open Systems Inter-connection

Reference Model that makes inter-operability across heterogeneous technology environments possible.

Concepts of layers

Internetwork is a network of networks, these networks might not be on same platforms, technologies. Imagine windows based system communicating with Apple Macintosh or UNIX/Linux based systems, where technologies are different and perhaps languages are different. In these cases what becomes important is each side should have knowledge of steps taken for communication so that it could do a reverse process irrespective of technologies. This is where layering concepts come into play.

Imagine you want to send an audit report to your client in Berlin, Germany. The key steps are:

- First we will write a report.
- Then the dispatch department in our office will put the report in an envelope, seal the envelope, write senders and receivers addresses, put a postage stamp on the envelope and post it.
- Postal staff will take out all the letters from the letter box and sort them. Letter meant for Berlin is put in a bag, which itself is put in another bag meant for Germany.
- The air cargo takes those bags to central postal hub in Frankfurt, Germany.
- The German postal office people open the bag and see the bag meant for Berlin.
- This bag goes to Berlin where it is opened and out comes an envelope meant for the client address
- It is handed over to person delivering letters to that clients address.
- The administrative staff of the client opens the envelop takes out the report and delivers to the client.

Sending our report to our Berlin client involves so many steps, lot of action has been done on it so that it can reach the other end. Similarly when a message is sent from one computer to another again lots of action and processes happen for it to reach other end. In our case there have been various phases, report writing phase, envelopment phase, sorting phase, similarly at the other end there have been sorting phase, de-envelopment phase and all. These different phases in network terminology could be considered analogous to Layers.

Each phase consists of some actions to be taken, in envelopment phase, actions are to put the report in an envelope, seal the envelope, write senders and receivers addresses, put a postage stamp on the envelop and post it. Similarly, in each layer some actions are done on data after which it passes to the next layer or phase. Each layer knows the form of data which it will get and also knows the form of data it has to pass on to the next layer and the function the layer has to do. A layer is not concerned about actions taken at previous layer or actions to be taken by next layer so that there is a form of independence amongst different layers.

The dispatch section in our office knows the form of data it will get i.e. a report and functions it has to perform, i.e. to put the report in an envelope, seal the envelope, write senders and receivers

addresses, put a postage stamp on the envelop and post it . It also knows the format of data it has to give to the next layer i.e. an Envelope. Our dispatch section is not bothered about actions we have taken, whether we have written report by hand or using a printer, it only knows that a data in the form of letter will be received by it. Neither is dispatch section bothered about the sorting process adopted by postal staff, whether it is automated sorting or manual sorting, it just knows the format of data in which it has to send.

Each layer talks to its upper layer, lower layer and there is also peer to peer communication with corresponding layer. Layering concept is important so that the layers could be independent of each other and technological advancements could take place at each layer independent of other layers. Also irrespective of technology, if a layer understands the action taken by corresponding layer at other end it could do a reverse job. If a layer knows encryption has happened at other end, then it knows that it will have to decrypt. This information of action undertaken is passed on by use of headers and trailers added to the data. Layers also help the process become technology independent. At our end and at German end technologies could be different but what is important is that phases are understood by the other end.

Our dispatch section is manual and letters are sealed manually whereas the German client could have automated letter openers i.e. technologies are different. What is important is that clients' staff when they receive the envelope knows that if there is an envelope there is bound to be a letter in the envelope provided they have understanding of the process. They will know that envelope has to be opened to extract the letter. At our end, we have put the report in an envelope and have put envelop in a bag i.e. performed encapsulation of the message. At the other end bag is opened and envelop taken out, envelop is opened and report taken out i.e. de-capsulation of the message. So, at one end encapsulation would be done and headers attached; at the other end de-capsulation would be done, i.e. the headers have been removed.

OSI Model is a layered model.

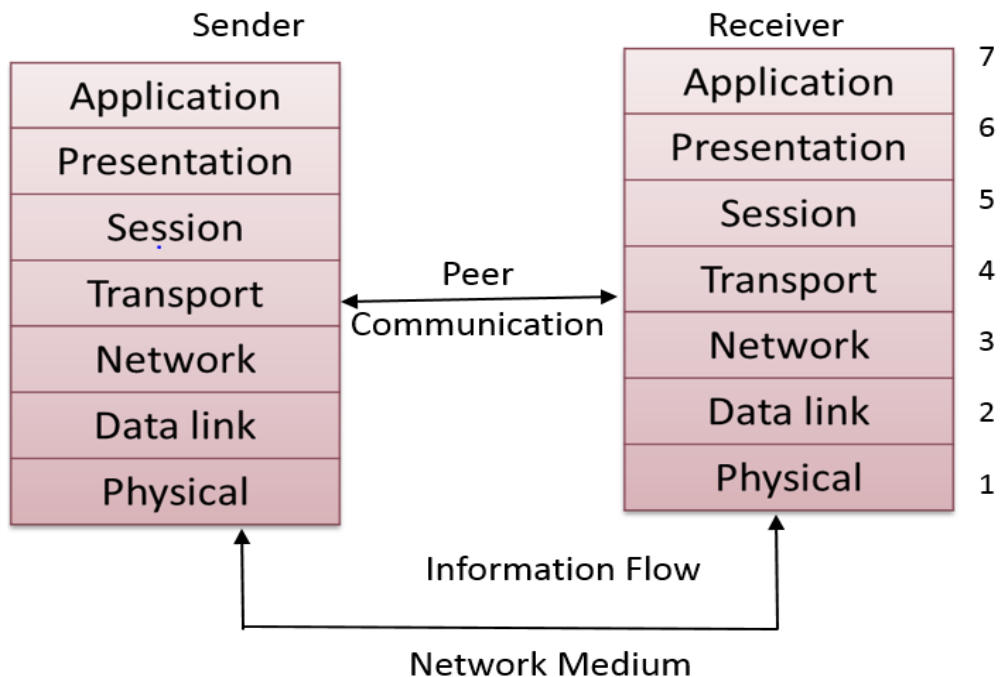
The OSI reference model is a layered model of seven layers, each specifying particular network functions. The model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of tasks is then assigned to each of the seven OSI layers. Each layer is reasonably self-contained so that the tasks assigned to it can be implemented independently. Two key Terminologies to know are:

Interfaces: describe (vertical) communication between adjacent layers.

Protocols: describe (horizontal) communication between layers,

The numbering of layers always starts from Physical Layer, i.e. layer no. 1 and ends at Application Layer which is layer no. 7. Application Layer should not be confused with Applications but yes, it is closest to Applications and the Physical Layer is closest to hardware.

OSI is a 7 Layered Model. The Layers are:



The sequence of layers can be remembered by mnemonic “All people seem to need data processing”

- All (Application)
- People (Presentation)
- Seem (Session)
- To (Transport)
- Need (Network)
- Data (Data Link)
- Processing (Physical)

Vertical (Adjacent Layer) Communication

Data is sent down from Application to Physical at sender's end and up from Physical to Application at recipient's end every time something is transmitted across the network. To understand if we as a user are working in an application that is sending information to another user who at this time is also working in the same application, but on a different computer, data will get transmitted down the layers all the way from the Application layer at the top (Layer 7) down to the Physical layer (Layer 1) at the bottom, where the data can actually be transmitted. When it reaches the other user, the process is reversed, and data transmits vertically upwards until it reaches its destination in Application Layer (layer7).

Horizontal (Corresponding Layer) Communication

Happens logically on the same layer (between hosts) e.g. when a web browser establishes communication with a web server, a session (layer 5) between the two must be established. Important point is that only layer 1 (physical) will actually allow the session layer on the host to reach the session layer on the web server. This means that data must transfer vertically down to layer 1 on the host, and up from layer 1 to layer 5 on the web server.

Thus, the layers are logically connected even though they don't have a physical connection. That is, they are connected via software (hence logical), which is the case for all layers with the exception of layer 1. Let us now try to understand OSI Model. Continuing with the same Example, we want to send an audit report to our client in Berlin, Germany. The key steps are:

OSI Layer	Report to be sent to Client in Germany		Functions
7	The report has to be sent by mail so we use SMTP (Simple Mail Transfer protocol used by emails) Decide on a service that Report is to be sent by mail, courier Report could be dictated on phone also but we decide on service i.e. courier	Application	Service to Application Interface to User/ application File Transfer access Management Virtual Terminal Mail Services
6	The client is in Germany so let's translate it in German and format it as a report.	Presentation	Coding and Converting Compression and Decompression Encryption and Decryption Not interested in content – Format and Syntax
5	Let's call them first to ensure that they are available. We will monitor the transmission and when the message has reached will terminate.	Session	Establishes, Maintains and Terminates Sessions, Synchronisation
4	Message is big, so let's segment it into small segments and sequence them. And also request the partner at other end to acknowledge receipt.	Transport	Flow Control Segmentation-De-segmentation Error Handling End to End Message Integrity
3	Let's add our office address and the clients address on these packets. And decide on the path(Courier) where to send	Network	Control Passage of packets over Routes Logical addresses Selects best path- Congestion Control

2	Courier will add its Local UniqueID and the Local UniqueID of clients also lets add a seal to see packet is not tampered en route.	Datalink	Reliable transit of data Data Framing Add MAC Address Error Detection
1	Mail is urgent so it is sent by air cargo	Physical	Deals with 0s and 1s Converts Bits to Voltages Transmission rates Contains physical components
1	Mail is received and unloaded by courier Company	Physical	
2	Courier Ok, UniqueID is mine so meant for me Check the seal which its intact so no tampering	Datalink	
3	Delivered by couriers, Ok it's from India Auditors.	Network	
4	Will reorder all the different segments and also tell the Indian auditor's office that I received the packet, but well the third segment is missing will have to inform auditor's office to resend the missing segment, Ok received a replacement packet now de-segment it have it as one report	Transport	
5	The Report has been received so let's terminate the session	Session	
6	Admin Staff reads the letter and formats it the way client CEO wants i.e. an executive summary he doesn't have much time.	Presentation	
7	It's a report so will use appropriate services to give it to CEO.	Application	

This is only a simplistic example of how data gets across to different computers on network. Although there is no exact mapping between the postal system and OSI layers but this comparison provides a broad idea of steps involved. We had an over view of the working done at different layers. OSI is theoretical model, a reference model which can be used only to understand how different layers function and what happens to any communication through all these different Layers.

2.2.5 Transmission Control Protocol / Internet Protocol (TCP /IP)

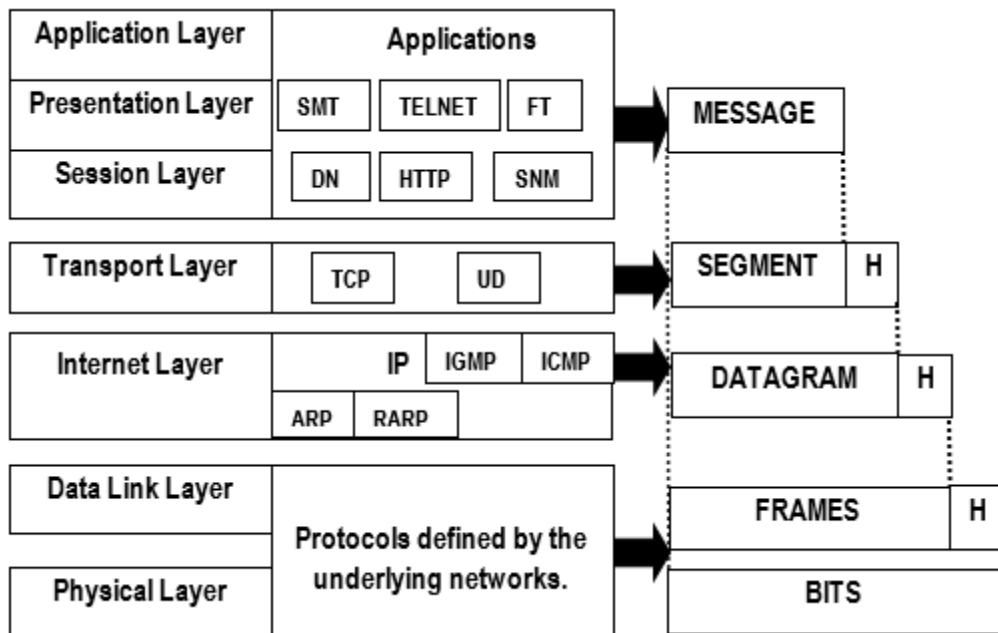
The practical model or the protocol suite which comes into play in data communication between devices on a network is **TCP/IP**. The internet's technological success depends on its principal communication tools, the Transmission Control Protocol (TCP) and the Internet Protocol (IP), generally known as TCP/IP. TCP/IP is a set of protocols developed to allow cooperating computers to share resources across the networks. It establishes the standards and rules by which messages are sent through the networks.

TCP/IP (Transmission Control Protocol/Internet Protocol) is a Suite of communication protocol, whose development began in the early 1970s by (D)ARPA, the United States Defence Advanced Research Projects Agency. They called it Arpanet. By 1982, the DOD (Department of Defence) declared TCP/IP the standard for all military computer networking. By the late '80s, TCP/IP became the dominant market player.

These standards are the protocol of the Internet and the global standard for local area networks and wide area networks, the major exception being the traditional networks of the telephone companies. However, telephone companies that deploy voice over IP (VoIP) networks are, in fact, using TCP/IP as well. TCP/IP protocol suite is a bundle of protocols that are segmented into five layers.

5. Application Layer
4. Transport layer
3. Internet Layer
2. Data link layer
1. Physical layer

These layers of TCP/IP can be mapped with layers of OSI as follows



Application Layer

The Application layer is the topmost layer of the TCP/IP protocol suite and runs various applications which provide them the ability to access the services of the other layers and define the protocols that applications use to exchange data. There are many Application layer protocols, and new ones are always being developed.

Protocols used in Application Layer

HTTP: Stands for Hyper Text Transfer Protocol and is used for Web browsing. For example, when you enter a web address in our browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. *For example: when browsing, the internet services are being provided by HTTP.*

TELNET: It is an abbreviation of Terminal Network and with the help of this protocol user can login to a remote server. *For example: when we login to Income tax site, the protocol which is working is TELNET*

FTP (File Transfer Protocol): Helps in transferring files from one computer to another which is one of the most common tasks performed in a networking or internetworking environment. *E.g. FTP is often used to upload or download files to remote systems*

SMTP: It stands for Simple Mail Transfer Protocol which provides a mechanism for sending messages to other computer users based on e-mail addresses. *E.g. whenever we are sending a mail the services is provided by SMTP Protocol.*

DNS: Domain Name System maps a name to an address and an address to a name. The addressing system on the Internet uses IP addresses, which are usually indicated by numbers such as 220.227.161.85. Since such numbers are difficult to remember, a user-friendly system that has been created is known as the Domain Name System (DNS). It provides the mnemonic equivalent of a numeric IP address and ensures that every site on the Internet has a unique address. For example: <http://www.icaai.org>. If this address is accessed through a Web browser, it is resolved to 220.227.161.85.

TIP: As an experiment try going to the site of ICAI by just writing 220.227.161.85 in your browser.

SNMP: It stands for Simple Network Management Protocol, network administrators use SNMP to monitor and map network availability, performance, and error rates.

E-mail protocols

MIME (Multipurpose Internet Mail Extensions)

Allows images, audio and non-ASCII formats to be included in email messages (any file format). It enables use of non-ASCII character sets. It is also used by HTTP.

POP3 (Post Office Protocol)

POP3 is used for retrieving email. Downloads mail from the (mail) server and stores it locally, then deletes it from the server.

IMAP (Internet Message Access Protocol)

IMAP is also for retrieving email. The difference is that unlike POP, IMAP supports (among other things) synchronization across multiple devices. This means that if we reply to an email on our smartphone, then IMAP checks email on your Laptop, our reply will show up there and vice versa.

Transport Layer

The Transport layer (also known as Host-to-Host Transport layer) is responsible for ensuring logical connections between hosts, and transfer of data. In other words, it acts as the delivery service used by the application layer above.

Protocol data unit (PDU) is segment.

Data can be delivered with or without reliability. The main protocols used are

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP).

User Datagram Protocol (UDP): Example - letter dropped in letterbox, Unreliable delivery

UDP provides a one – to - one or one – to - many, connectionless, unreliable communications service. It is used when the data to be transferred is small (such as the data that would fit into a single packet), and the overhead of establishing a TCP connection is not desired or the applications or upper layer protocols provide reliable delivery.

UDP is connectionless, meaning that A doesn't initiate a transport connection to B before it starts sending data. If B detects an error, it simply ignores it (rather than acknowledge the error to A), leaving any potential fix entirely up to A.

E.g. small queries, VOIP, Streaming data, etc.

Transmission Control Protocol (TCP): Example- Speed Post with POD

TCP provides a one to - one, connection-oriented, reliable communications service. It is responsible for the establishment of a TCP connection, the sequencing and acknowledgment of packets sent, and the recovery of packets lost during transmission. It is responsible also for breaking up the message into datagrams, reassembling datagrams at the other end, resending anything that gets lost, and putting things back in the right order.

If A is sending a stream of data to B, TCP will split it into smaller blocks called segments. Each segment is checked for errors, and retransmitted if any are found. A knows whether a segmented contains errors depending upon the acknowledgement it receives from B. TCP is reliable because there is a mechanism in it called PAR (Positive Acknowledgment with Re-transmission), which sends the data to the recipient again and again until it receives a Data OK signal from the recipient.

Network Layer

The Network layer enables us to find the best way from source to destination. The objective of Network layer is to decide which physical path the information should follow from its source to its destination (routing). This layer ensures routing of data between different networks and subnets. Its key tasks are:

- Message addressing (Logical addressing, IP Addressing)
- Path determination between source and destination nodes on different networks
- Routing messages between networks
- Controlling congestion on the subnet
- Translating logical addresses into physical addresses

Protocol data unit (PDU) is Packet.

Protocols used in Network Layer IP, ARP, RARP, ICMP and IGMP.

Internetwork Protocol (IP):

Internet Protocol (IP) is an Internet layer protocol that uses unique addresses (called IP Addresses which are discussed in next part) for the destination computer and for our computer. IP provides the means for our computer to determine whether the destination Computer is a local computer or a computer located somewhere on the Internet. To reach a destination computer on the Internet, IP protocol also allows computer to figure out how to reach the Internet destination computer via our default gateway.

It is an unreliable and connectionless datagram protocol which provides no error checking or tracking. This is like the delivery service of a post office. The post office does its best to deliver mail

but does not always succeed. If an unregistered letter is lost, it is up to the sender or would-be recipient to discover the loss. The post office itself does not keep track of every letter and cannot notify a sender of loss or damage. When the letter is delivered, the receiver mails the postcard back to the sender to indicate that he got it. If the sender does not receive the postcard, he or she assumes the letter has been lost and sends another one.

Address Resolution Protocol (ARP):

Address Resolution Protocol maps IP addresses to physical (MAC) addresses. It is used by hosts to find MAC address of other hosts whose IP address is known.

Reverse Address Resolution Protocol (RARP)

RARP allows a host to discover its IP address if it knows its physical address (MAC).

Internet Control Message Protocol ICMP

ICMP is a mechanism used by hosts and routers to send notification of datagram problems back to the sender. ICMP allows IP to inform a sender that a datagram is undeliverable. *Many of us would have at some time or other used PING command PING sends out ICMP (Internet Control Message Protocol) messages to verify both the logical addresses and the physical connection, Looks for any congestion on the route.*

Internet Group Message Protocol (IGMP)

IGMP is a companion to the IP Protocol. IGMP helps a multicast router identify the hosts in a LAN that are members of a multicast group.

Data Link Layer

Data Link Layer provides reliable transit of data over local networks. The Data Link Layer performs the task of delivery over local networks and error detection. The protocol data unit (PDU) is called Frame.

Main tasks of Data Link Layer

Framing: The DLL divides the stream of bits received from the network layer into manageable data units called frames.

Physical Addressing: If frames are to be distributed to different systems on the network, the DLL adds a header to the frame to define the physical address (MAC) of the sender (source address) and/or receiver (destination address) of the frame.

Flow Control: If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender, the DLL imposes a flow control mechanism to prevent overwhelming the receiver.

Error Detection Error detection is the process of detecting whether errors occurred during the transmission of the bits across the media. The Data Link layer uses a calculated value called the CRC (Cyclic Redundancy Check) that's placed into the Data Link trailer that's added to the

message frame. The receiving computer recalculates the CRC and compares it to the one sent with the data. If they match data received is error free.

Access Control: When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

Physical Layer

The physical layer deals in zeroes and ones and voltages. Physical layer provides the path through which data moves among devices on the network. The protocol data unit (PDU) is called a Bit.

The physical layer is concerned with the following:

Physical characteristics of interfaces and media: The physical layer defines characteristics of the interface between the devices and the transmission medium and also defines the type of transmission medium.

Representation of bits: The physical layer data consists of a stream of bits (0 and 1) without any interpretation. To be transmitted, bits must be encoded into electrical or optical signals.

Data Rate: The transmission rate – the number of bits sent each second, is also defined by the physical layer.

Synchronization of bits: The sender and receiver must be synchronized at the bit level.

Line Configuration: The physical layer is concerned with the connection of devices to the medium.

Transmission Mode: The physical layer also defines the direction of transmission between the two devices: simplex, half-duplex and duplex.

2.3 Wireless Networks

The term wireless networking refers to technology that enables two or more computers to communicate using standard network protocols, but without network cabling. Strictly speaking, any technology that does this could be called wireless networking. The current buzzword however generally refers to wireless LANs. However WANs could be also wireless WWAN (Wireless Wide Area Networks).

Wireless Wide Area Networks (WWANs)

WWANs refer to technology that enables users to establish wireless connections over remote private or public networks using radio, satellite and mobile phone technologies instead of traditional cable networking solutions like telephone systems or cable modems. These connections can be maintained over large geographical areas, such as cities or countries, through the use of satellite systems or multiple antenna sites maintained by wireless service providers. Networks connected over large Geographical areas using Radio/Satellite Technologies could be the only viable alternative for rural or remote areas. E.g.: Banking networks, ATMs thru VSAT

Wireless Local Area Networks (WLANs)

WLANs generally use Radio waves to connect devices to a business network. Example: when we connect a laptop to a Wi-Fi hotspot at a cafe, hotel, airport, or other public place, we're connecting to that business's wireless network.

Benefits

- **Convenience:** It allows accessing network resources from any location within wireless network's coverage area or from any Wi-Fi hotspot.
- **Mobility:** User is no longer tied to desk, as compared to wired connections. He can even be connected whilst in there is no tying with desk or wires.
- **Productivity:** Wireless access to the Internet and the organisations' key applications and resources helps the staff even when not in office and encourages collaboration.
- **Easy setup:** No need to install cables, so installation can be quick and cost-effective.
- **Expandable:** Wireless networks can be easily expanded with existing equipment, whereas a wired network might require additional wiring.
- **Security:** Advances in wireless networking technologies couple with encryption all provide security protections.
- **Cost:** With reduced wiring costs, they can cost less to operate than wired networks.

2.3.1 Wi-Fi

Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. Wi-Fi networks have limited range. A typical wireless access point might have a range of 32 m (120 ft.). Security in Wi-Fi can be improved using WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access).

2.3.2 Blue Tooth

The name came from a Danish King, whose name was translated to Harold Bluetooth. King Bluetooth had unified some warring factions and the idea behind Bluetooth is to unify different platforms and devices.

Bluetooth technology was invented in 1994 by engineers at Ericsson, a Swedish company. Bluetooth is a wireless technology standard for exchanging data over short distances up to 50 meters (164 feet) from fixed and mobile devices. It is a feature which is used every day through a number of compatible devices. These include USB, handheld PDA, Phone headset and the most popular, the mobile phone. Through the use of a mobile phone we can send pictures, videos, exchange business cards and also transfer files to our PC. Both data and voice transmissions can be sent and received through the use of short range networks. Bluetooth is really like a very low-power, short-range radio signal. The system is fairly secure.

Few devices that utilise Bluetooth technology are:

- Keyboards and mice

- Printers
- Cell phones and headsets
- PDAs (Personal Digital Assistants)
- Desktop and laptop computers
- Digital cameras

2.4 TCP/IP Security and Controls

TCP-IP, which are very widely used for Internet were built to facilitate communication. It has lots of vulnerabilities inherent in the protocols, which could be exploited through different kinds of attacks. Some of the Attacks are:

- Sniffing
- Denial of Service Attacks
- Spoofing, hijacking

Controls could be in the form of:

- Encryption,
- VPN IPsec
- Firewalls
- One Time Passwords
- Network Monitoring Tools, Port Scans
- Updated Security Patches

2.5 Summary

In this part we have learnt about Internet and technologies helping in working of Internet which is a set of heterogeneous networks and to facilitate interoperability we have network standards and protocols. Understanding OSI model helped us gain an insight into the different phases or layers in network communication. We also gain an understanding on the main technology on which internet is built TCP/IP and related protocols. Networking is increasingly becoming wireless, and we learnt about some wireless technologies in everyday use.

2.6 References

- http://www.tcpipguide.com/free/t_TCPIPOverviewandHistory.htm
- <http://www.garykessler.net/library/tcpip.html>
- http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/wireless_networking_overview.mspx?mfr=true

PART 3: THE IP NETWORKS

Learning Objectives

- To gain understanding of IP Networks
- To gain an overview of IP Addressing Scheme
- To gain an understanding of Domain Name Services, Ports
- To understand Network Services
- To get an overview of Public Global Internet Infrastructure
- To understand Factors Impacting Quality of Service

3.1 Introduction

Imagine posting a letter with an address 16, Civil Lines, will it reach the address? Answer to this question depends on whether we have posted the letter in the Green Letter boxes meant for local delivery at GPO or Red letter boxes which are meant for general delivery across the world. If we have posted in Green letter boxes, yes it will reach the address even if city is not specified. If we are posting a letter in Red letter box which has to be delivered across the world, proper address with City, Country need to be specified.

Communication between hosts (Devices) can happen only if they can identify each other on the network. In a single network, hosts can communicate directly via MAC address (MAC address we have already discussed, is a factory coded 48-bits hardware address which can uniquely identify a host in the world). On the other hand, in case; if a host wants to communicate with a remote host which is not on the same network, we require a means of addressing to identify the remote host uniquely; i.e. we must know the address of the network as well the host.

A logical address is given to all hosts connected to Internet and this logical address is called Internet Protocol Address (IP Address). In TCPIP Model; we have also understood that the network layer is responsible for carrying data from one host to another. It facilitates providing logical addresses to hosts and identifies them uniquely using the same.

The Internet layer takes data units from Transport Layer and cuts them in to smaller units called Data Packets which are a PDU (Protocol Data Unit) for Network Layer. Internet layer defines IP addressing also selects the path that the packets should follow to reach the destination. Routers work on Internet layer and facilitate routing of data to its destination.

3.2 IP Networks

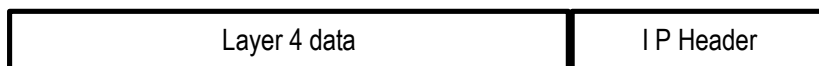
An IP network is a communication network that uses Internet Protocol (IP) to send and receive messages between one or more computers. An IP network is implemented in internet networks, local area networks (LAN) and enterprise networks. All hosts or network nodes must be configured with the TCP/IP suite and must have an IP address.

3.2.1 IP Addressing

Internet Protocol has the responsibility of identification of hosts based upon their logical addresses and routing of data between these hosts over the underlying network. For identification of hosts Internet Protocol Addressing Scheme gives the address of a device attached to an IP network (TCP/IP network).

Every client, server and network device are assigned an IP address, and every IP packet traversing an IP network contains a source IP address and a destination IP address.

IP encapsulates data unit received from above and adds its own header information



IP Encapsulation

IP header contains all the necessary information to deliver the packet at the other end like Version of IP, Protocol, Source IP Address, Destination IP Address etc.

IP Version 4 (IPv4)

IP Address (IPv4) is an address which is 32-bits in length of the type

01110101 10010101 00011101 11101010

It is written in form of 4 Octets or Bytes separated by a dot. Using these 32 bits we can have 2^{32} permutations and combinations i.e. in all 4,29,49,67,296 different and unique IP Addresses.

IP address can be a value from 00000000.00000000.00000000.00000000

to 11111111.11111111.11111111.11111111

If thought of in binary terms 0 means 00000000 and 255 in binary is 11111111 and all permutation and combination in between. Thus, each of these Octets can be any value from 0 to 255, both inclusive i.e. in all 256.

0	.	0	.	0	.	0
to		to		to		to
255	.	255	.	255	.	255

IPv4 addresses are usually represented in "dotted decimal" notation, separated by decimal points like xxx.xxx.xxx.xxx or 117.149.29.234

IP Addressing Scheme-Classes

IP addressing system is designed in such a way that it contains information of three fields: class type, netid, and hostid. IPv4 addressing Scheme is a classful addressing scheme

Classful network design allowed for a larger number of individual network assignments. There are 5 classes of Addresses

- Class A
- Class B
- Class C
- Class D
- Class E

The first three bits of the most significant octet of an IP address was defined as the class of the address. Three classes (A, B, and C) were defined for universal Unicast Addressing.

Class D is reserved for Multicasting.

Class E is reserved for experimental purposes only like for research and development or study.

Unicast Addressing Mode: In this mode, data is sent only to one destined host. The destination address field contains 32-bit IP address of the destination host.

Broadcast Addressing Mode: In this mode the packet is addressed to all hosts in a network segment. IP address having host bit all ones is the Broadcast IP, for example in class A, the address XXX.255.255.255

Multicast Addressing Mode: This mode is a mix of previous two modes, i.e. the packet sent is neither destined to a single host nor the entire hosts on the segment. In this packet, the destination address contains special address. Example is online games.

Network IP and Broadcast IP

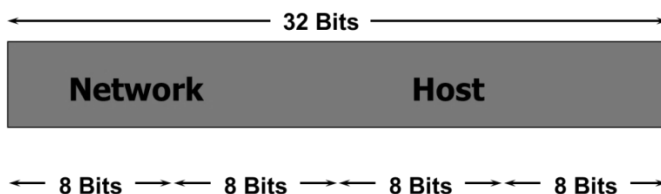
IP address having host bit all zeroes is the Network IP.

IP address having host bit all ones is the Broadcast IP.

Both these addresses cannot be physically used on any system. Given any IP address, a network IP and broadcast IP can be associated with it.

Network and Host ID

Each of the IP address of Class A, B and C will have a Network and Host portion of the Address



That is out of 32 Bit address some bits or more specifically Octets or Bytes will represent Network Address and some octets will represent Host ID

Class A Address

Class A address is wherever the first octet of an IP address is any number ranging from 0-127.

XXX.XXX.XXX.XXX

0-127

If we consider in binary then it means first octet is 00000000 (decimal equivalent 0) to 01111111(Decimal Equivalent 127) and all the permutations and combinations in between. It means, when we move from 00000000 to 01111111 all the bits will keep on changing between 0 and 1 whereas 1st bit will remain constant at 0, which is called a Higher Order Bit.

Where ever it's a class A address



First octet represents NetworkID and remaining 3 octets represent HostID. Earlier while discussing Broad Cast and Network IP addresses we had discussed that in network and host portion of an IP Address all changing Bits can never be all 0s or all 1s. Thus network portion of Class A address can never be 00000000 and never be 01111111, since in these cases all changing bits will be 0s or 1s. Therefore in Class A the first octet ranges from 1 – 126, i.e. Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only.

The IP range 127.x.x.x is reserved for loopback IP addresses. This implies that Class A addressing can have 126 networks (2⁷-2) and each network can have 16777214 hosts (2²⁴-2) since address space for host ID is 24Bits and all changing bits can never be 0s or 1s.

Class A IP address format thus, is 0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

This is meant for big networks needing huge number of hosts e.g. Microsoft

Class A address is wherever the first octet of an IP address is any number ranging from 128 to 191, i.e.

XXX.XXX.XXX.XXX

128-191

If we consider in Binary then it means first octet is 10000000 (decimal equivalent 128) to 10111111(Decimal Equivalent 191) and all the permutations and combinations in between.

It means, when we move from 10000000 to 10111111 all the bits will keep on changing between 0 and 1 whereas 1st two bits will remain constant at 10, which are called a Higher Order Bits

Class B Address

Where ever it's a class B address



First two octet represents NetworkID and remaining two octets represent HostID. Again in network and host portion of an IP Address all changing Bits can never be all 0s or all 1s. Thus, network portion of Class B address can never be 10000000 00000000 and never be 1011111111111111, since in these cases all changing bits will be 0s or 1s. This implies that Class B addressing can have 16384 networks ($2^{14}-2$) since address space for NetworkID is 16Bits and only 14 bits are changing Bits and all changing bits can never be 0s or 1s

Each network can have 65534 hosts ($2^{16}-2$) since address space for host ID is 16Bits and all changing bits can never be 0s or 1s. Class B IP address format is, 10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

Class C Address

Class C address is wherever the first octet of an IP address is any number ranging from 192 to 223, i.e.

XXX.XXX.XXX.XXX

192

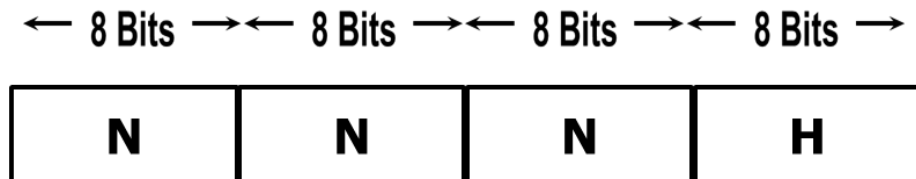
To

223

If we consider in Binary then it means first octet is 11000000 (decimal equivalent 192) to 11011111(Decimal Equivalent 223) and all the permutations and combinations in between.

It means, when we move from 11000000 to 11011111 all the bits will keep on changing between 0 and 1 whereas 1st three bits will remain constant at 110, which are called Higher Order Bits

Where ever it's a class C address



First three octet represents NetworkID and remaining one octet represents HostID. Again in network and host portion of an IP Address all changing Bits can never be all 0s or all 1s. Thus network portion of Class C address can never be 11000000 00000000 00000000 and never be 101111111111111111111111, since in these cases all changing bits will be 0s or 1s. This implies that Class C addressing can have 2097150 networks ($2^{21}-2$) since address space for NetworkID is 24Bits and only 21 bits are changing Bits and all changing bits can never be 0s or 1s .

Each network can have 254 hosts (2^8-2) since address space for host ID is 8Bits and all changing bits can never be 0s or 1s

Class C IP address format is 110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

Class D Address

Class D address is wherever the first octet of an IP address is any number ranging from 224 to 239, i.e.

XXX.XXX.XXX.XXX

----- 224-239

Very first four bits of the first octet in Class D IP addresses are set to 1110 which are called Higher Order Bits

Class D has IP address range from 224.0.0.0 to 239.255.255.255.

Class D is reserved for Multicasting.

In multicasting data is not destined for a particular host, that's why there is no need to extract host address from the IP address.

Class E Address

This IP Class is reserved for experimental purposes only like for research and development or study. IP addresses in this class range from 240.0.0.0 to 255.255.255.254. To summarise

Class	1 st Octet Decimal Range	1 st Octet High Order Bits	Network/Host ID N=Network H=Host	Default Subnet Mask	Number of Networks	Hosts per Network (Usable Addresses)
A	1 – 126*	0	N.H.H.H	255.0.0.0	126 ($2^7 - 2$)	1,67,77,214 ($2^{24} - 2$)
B	128 – 191	10	N.N.H.H	255.255.0.0	16,382 ($2^{14} - 2$)	65,534 ($2^{16} - 2$)
C	192 – 223	110	N.N.N.H	255.255.255.0	20,97,150 ($2^{21} - 2$)	254 ($2^8 - 2$)
D	224 – 239	1110	Reserved for Multicasting			
E	240 – 254	1111	Experimental; used for research			

Although people identify the class by the first number in the IP address, a computer identifies class by the first three bits of the IP address (A=0; B=10; C=110).

More than twenty lacs Class C networks are possible, but have least number of hosts.

The fewest are Class A networks, which are reserved for government agencies and huge companies.

Class division shows that class A networks can accommodate far more hosts than class B or class C networks.

Thus the major purpose of Classful addressing scheme is to reduce inefficiency in address allocation.

3.2.2 Public and Private Addresses

One of the steps taken to conserve the IP address was concept of Public and Private Addresses.

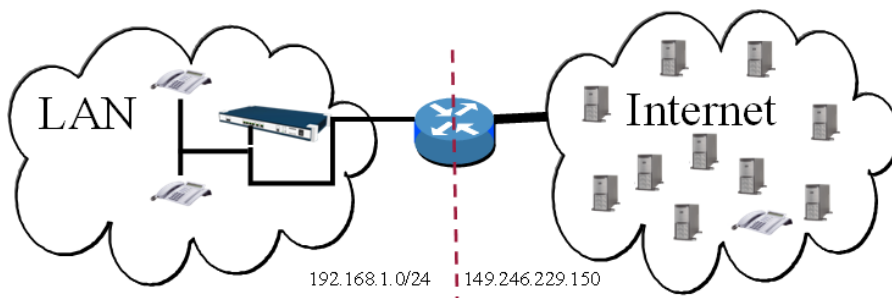
Every IP address that is exposed to the public Internet is unique. In contrast, IP addresses within a local network can use the same private addresses.

Thus a user's computer in company A can have the same address as a user in company B and thousands of other companies. However, private IP addresses are not reachable from the outside world.

An IP address is considered private if the IP number falls within one of the IP address ranges reserved for private networks such as a Local Area Network (LAN). The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private networks (local networks). These addresses cannot be routed on Internet so packets containing these private addresses are dropped by the Routers. Most ISPs will block the attempt to address these IP addresses. These IP addresses are used for internal use by companies that need to use TCP/IP but do not want to be directly visible on the Internet.

Class	Private Networks Start address	Private Network Finish Address	No of Addresses
A	10.0.0.0	10.255.255.255	1, 67, 77, 216
B	172.16.0.0	172.31.255.255	10, 48, 576
C	192.168.0.0	192.168.255.255	65,536

In order to communicate with outside world, internet, these IP addresses must have to be translated to some public IP addresses using NAT (Network Address Translation) process can be used



Network Address Translation (NAT):

NAT works like a receptionist who transfers any external call to an internal intercom number and vice versa.

Network address translation is a mechanism by which multiple PCs/hosts with private IP addresses are enabled to access using one or few public IP addresses.

In other words, we operate with two sets of addresses: we would have our private addresses configured on hosts throughout our network, and then a public routable block of addresses

would be configured on our NAT device. NAT would be responsible for correlating the Private and Public addresses and translating as needed to support communications.

NAT allows a single device, such as a router, to act as an agent between the Internet (or "public network") and a local (or "private") network. This means that only a single, unique IP address is required to represent an entire group of computers

Static and Dynamic Addresses

Network infrastructure devices such as servers, routers and firewalls are typically assigned permanent "static" IP addresses. If we call a Radio Taxi for a Cab and it sends us a cab. Next time if we call for a cab will it send the same cab as last time? Most likely answer would be No. Radio Taxi is maintaining a pool of cabs out of which one cab is assigned to us as and when it is released it is now available for assignment to some other customer. Similarly, ISPs which allocate IP addresses to us, maintain a pool of IP addresses out of which one is assigned to us. As soon as we disconnect it is released and assigned to perhaps some other customer. These are Dynamic IP addresses.

When we E-file an Income Tax Return its acknowledgement shows IP Address on left hand bottom. Next time we file a return, the IP address changes.

We can know our IP address at the site www.whatismyipaddress.com. The client machines can also be assigned static IPs by a network administrator, but most often are automatically assigned temporary "dynamic" IP addresses via software that uses the DHCP (Dynamic Host Control Protocol).

DHCP allows us to define a range from which the server is allowed to give out IP's. For example, 192.168.1.100 – 150. Computers connecting to the network are assigned an IP with a lease time.

Cable and DSL modems typically use dynamic IP with a new IP address assigned to the modem each time it is rebooted.

Reserved addresses

The following are reserved addresses:

IP address 0.0.0.0 refers to the default network and is generally used for routing. The network address 0.0.0.0 designates a default gateway. This is used in routing tables to represent "All Other Network Addresses".

IP address 255.255.255.255 is called the Broadcast address.

IP address 127.0.0.1 is called the Loopback address. It is used to simplify programming, testing, and troubleshooting. It allows applications to communicate with the local host in the same manner as communicating with a remote host, without the need to look up the local address

In every network the host address which is all zeroes identifies the network itself. This is called the Network IP Address and is used in routing tables to refer to the whole network.

A host address which is all ones is called the Broadcast Address or Announce Address for that network. For example, on the Class C network 205.217.146.0, the address 205.217.146.255 is the broadcast address.

Packets addressed to the broadcast address will be received by all hosts on that network. The network address and the broadcast address are not used as actual host addresses. These are invalid addresses on the internet. Routers don't route them.

Subnet Mask

We are now moving towards classless addresses i.e. network and host portion of address can be derived using IP Address with a subnet mask.

The 32-bit IP address contains information about the host and its network. It is very necessary to distinguish both. For this, routers use Subnet Mask, which is as long as the size of the network address in the IP address. Subnet Mask is also 32 bits long.

Subnet mask helps in creating subnets.

Internet Service Providers (ISP) may face a situation where they need to allocate IP subnets of different sizes as per the requirement of customer, with the help of subnet mask; he may want to subnet the subnets in such a way that results in minimum wastage of IP addresses.

3.2.3 Internet Protocol Version 6 (IPv6)

Traditional Dominant Version of IP addressing is IP version 4 which is a 32 Bit addressing scheme i.e. it has 4,29,49,67,296 unique addresses, i.e. 2^{32} . But if we look at it the number of devices and addresses required are far exceeding these, so we are moving from IP Version 4 to IP version 6, IPv6 which is a 128 Bit addressing scheme i.e. the number of possible addresses are 2^{128} which is huge number and supposed to last long.

IETF (Internet Engineering Task Force) has redesigned IP addresses and to mitigate the drawbacks of IPv4.

IPv6 is written in form of hexadecimal like 2001:0db8:85a3:0000:0000:8a2e:0370:7334. It also offers auto configuration, higher mobility, quality service, security and privacy compatibility, efficient and capable of optimization.

Various countries, including India, are under migration to IPv6. In India, the IPv6 migration is led by the Telecom Regulatory Authority of India. Today majority of devices running on internet are using IPv4 and it is not possible to shift them to IPv6 in coming days. There are mechanisms provided by IPv6, by which IPv4 and IPv6 can coexist unless the Internet entirely shifts to IPv6.

3.3 Ports

French word *Porte* really means 'door'.

Ports can be readily explained with a simple real world example. We can think of IP addresses as the street address of a building, and the port number as the number of a particular Flat within that building. If a letter (a data packet) is sent to the building (IP) without a flat number (port number) on it, then nobody would know who it is for (which service it is for). In order for the delivery to work, the sender has to include the flat number along with the address.

A port is a 16-bit number, which along with an IP address forms a socket. Since port numbers are specified by 16-bit numbers, the total number of ports is given by 2^{16} which are equal to 65536 (i.e. from 0 to 65535).

Service Ports

A number is assigned to user sessions and server applications in an IP network. The port number resides in the TCP or UDP header of the packet.

Source Ports

The source port, which can be a random number, is assigned to the client and is used to keep track of user sessions.

Destination Ports

The destination port is used to route packets on a server to the appropriate network application. For example, port 80 is the standard port number for HTTP traffic, and port 80 packets are processed by a Web server. Destination ports are typically well-known ports (0-1023) for common Internet applications such as HTTP, FTP and SMTP. It can also be a registered port (1024-49151) that vendors use for proprietary applications.

In both TCP and UDP, each packet header will specify a source port and a destination port, each of which is a 16-bit unsigned integer (i.e. ranging from 0 to 65535) and the source and destination network addresses (IP-numbers), among other things.

3.4 The Domain Name System

DNS (Domain Name System) is a hierarchical, distributed database that contains mappings of DNS domain names to various types of data, such as Internet Protocol (IP) addresses and is an Internet Engineering Task Force (IETF) standard. DNS allows the use of friendly names, such as www.icai.org, to easily locate computers and other resources on a TCP/IP-based network.

Remembering names of our acquaintances is easy. But if we want to call them on cell phone, cell phone will call them only based on their telephone Number. 10 digits telephone Numbers

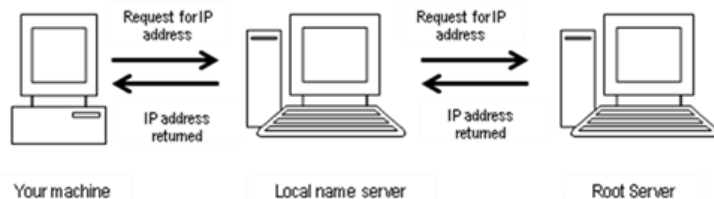
are very difficult to remember. So we feed the telephone Number in our cell phone and associate it with the name of our acquaintance. When we need to call that person we dial that person and our cell phone based on the contact list resolves it into a telephone number and calls the number. The same process happens for internet.

All hosts in the Internet are addressed using IP Addresses. Since they are 32 bits in length, almost all users find it difficult to memorize the numeric addresses. For example, it is easier to remember `www.icai.org` rather than `220.227.161.85`. The Domain Name System (DNS) was created to overcome this problem. It is a distributed database that has the host name and IP address information for all domains on the Internet.

For example, when a Web site address is given to the DNS either by typing a URL in a browser or behind the scenes from one application to another, DNS servers return the IP address of the server associated with that name.

In the above example, `www. icai.org` would be converted into the IP address `220.227.161.85`. Without DNS, we would have to type the four numbers and dots into our browser to retrieve the Website.

When we want to obtain a host's IP address based upon the host's name, a DNS request is made by the initial host to a local name server. If the information is available in the local name server, it is returned else the local name server then forwards the request to one of the root servers. The root server, then, returns the IP address.



Obtaining the numeric IP address

The DNS system is a hierarchy of database servers that start with the root servers for all the top level domains (.com, .net, etc.). These servers point to authoritative servers residing within ISPs and companies that resolve the host names to complete the name resolution.

DNS and Reverse DNS

DNS is resolving a Domain Name to its corresponding IP Address.

Reverse DNS is IP address to domain name mapping - the opposite of forward (normal) DNS which maps domain names to IP addresses. Reverse DNS is maintained in a separate set of data from forward DNS.

Reverse DNS is mostly used by humans for such things as tracking where a web-site visitor came from, or where an e-mail message originated, etc.

Generic top-level domain

A generic top-level domain (gTLD) is one of the categories of top-level domains (TLDs) maintained by the Internet Assigned Numbers Authority (IANA) for use on the Internet.

Overall, IANA currently distinguishes the following groups of top-level domains:

- infrastructure top-level domain (.arpa)
- country - code top-level domains (ccTLD)
- sponsored top - level domains (sTLD)
- generic top - level domains (gTLD)

.aero	.info	.net	.biz	.jobs	.pro	.coop	.mobi	.travel	.gov
.asia	.int	.org	.com	.mil	.tel	.edu	.museum	.xxx	.name

3.5 Network Services

Network Service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture.

For example

- Domain Name System (DNS) which translates domain names to Internet protocol (IP) addresses and the
- Dynamic Host Configuration Protocol (DHCP) to assign networking configuration information to network hosts.
- Network remote access services
- Directory services
- network management services

These are common services on local area networks. They require users to have permissions to access the shared resources.

- Printing Services
- Network File Services
- Electronic Mail Services
- FTP Services
- Web Services

3.6 On Demand Computing

On-demand computing (ODC) is an enterprise-level model of technology and computing in which resources are provided on an as-needed and when-needed basis. Generally used for outsourced services. ODC make computing resources such as storage capacity, bandwidth, computational speed and software applications available to users as and when needed for specific temporary projects, known or unexpected workloads, routine work, or long-term technological and computing

requirements. On-Demand is gaining tremendous corporate acceptance and adoption because it overcomes many of the inadequacies and increasing costs of traditional, legacy/on premise software products and support. ODC is about having our storage, our applications and our security available to us when we need them shifting the burden and cost of maintaining on-site software from us to the On-Demand vendor. The benefit of ODC is that organisation has to pay only for the computing resources they utilise. The biggest concerns about ODC are security and privacy.

3.7 Public Global Internet Infrastructure

Networks distributed world-over and interconnected through communication channels allowing exchange of information form the Internet. Users access Internet through LAN or dial-up to the POP (Point of Presence) of an Internet Service Provider (ISP). This POP is a part of the network of the ISP. These POPs of a service provider may be connected via optical fibre leased through a telephone operator or may be owned by the ISP. Thus, when connected, the user logically becomes a part of the network of the ISP.

These networks are connected to one-another through high speed backbones. Backbones are typically fibre optic trunk lines. The converge point of these backbones are called Network Access Points (NAP). These backbones, in fact, have multiple fibre optic cables combined together for increased capacity, and afford speeds in the range of 155 Mbps to 2.488 Gbps. At NAP, the edge routers divert data to the regional networks. Data travels from one regional network (ISP network), to another via NAPs using backbones. At the destination regional network, data gets transmitted to the specific network. Within this destination network, the data then travels to the specific computer/device.

3.8 Factors Impacting Quality of Network Service

Today internet is being used for many real time services also where time is critical, like Voice over IP, IP TV, Online Games, video-on-demand and other consumer service, Internet banking and all. To achieve customer satisfaction, Quality of Service QoS becomes very important in these kinds of Network Services. Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. The goal of QoS is to provide guarantees on the ability of a network to deliver predictable results. QoS involves prioritization of network traffic. QoS can be targeted at a network interface, toward a given server or router's performance, or in terms of specific applications. A network monitoring system must typically be deployed as part of QoS, to ensure that network is performing at the desired level. QoS can be classified into three categories:

- **Best Effort Basis Services:** No guarantee on delivery or throughput. This is the least priority traffic.
- **Differentiated service:** Here different type of traffic is differentiated according to the performance requirements. The devices use different queuing strategies for different priorities.

- **Guaranteed service:** Services like VoIP and Video etc. are given top priority in transmission at a guaranteed speed.

From user perspective, customer services like internet banking may have guaranteed services. Organisation's Email and access to intranet may be categorised under differentiated services and internet browsing for internal users may be categorized under best effort basis. Some organisations use least priority, priority and top priority for categorization of various services over the network for implementing QoS.

3.9 Summary

In this part, we have learnt about IP Networks the main strength behind internet. We also learnt about IP addressing scheme, concepts of Public and Private Addresses. Our use of internet is enriched by browsing various sites reaching those sites are made easy by Domain Name system as we don't have to remember IP addresses. We also saw emerging concepts of Network Services and On- Demand Computing. We also had an overview of Public Global Internet infrastructure.

3.10 References

- http://www.tcpipguide.com/free/t_TCPIPOverviewandHistory.htm
- <http://www.garykessler.net/library/tcpip.html>
- http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/wireless_networking_overview.msp?mfr=true

CHAPTER 3: SECURING NETWORKS

PART 1: FIREWALLS

Learning Objectives

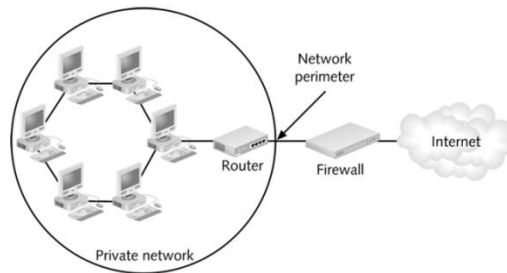
- To gain understanding of Firewalls
- To gain an overview of types of Firewalls
- To gain an understanding of Common Implementations of Firewalls
- To understand Limitations of Firewalls
- To get an overview of Unified Threat Management
- To understand Firewall Life Cycle
- To understand Baseline Configuration of Firewalls

1.1 Introduction

With the increased use of networked systems, the threat profile to organisations' information assets has increased manifold. Organisations' information resources are accessed by users from different access points. Further internal users also need to access Internet. However, while Internet access provides benefits, it enables the outside world to reach and interact with local network assets, creating a threat to the organisation. This exposes assets to attacks, both malicious and unintentional.

1.2 Firewall

Firewall is a system or group of systems to enforce Control policy. Firewalls are an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet. Firewall may be a hardware device or a software program running on a secure host computer, or a combination of hardware and software. Firewalls and associated technical controls have become fundamental security tools. Firewall is deployed at the perimeter of the network, i.e. the entry point. (The term 'Firewall' is coined after the firewalls which are used to prevent the spread of Fire from one area to another; in this case, they limit the damage that could spread from one subnet to another).



Firewall – at the perimeter of the organisation's intranet

As an access control mechanism, the firewall enforces the security policy between an organisation's secured network and the unsecured environment. Based on the rules configured, it filters the traffic both in-bound and outbound from the secured network and determines,

- Which inside machines, applications and services may be accessed from outside,
- Who outsiders are permitted access to internal and what resources, and
- Which outside services, the insiders may access.

In general, the design goals for a firewall are:

- All traffic from inside (secured) to outside (unsecured), and vice versa, must pass through the firewall.
- Only authorised traffic, defined by the local security policy, will be allowed to pass the firewall.

1.2.1 Firewall Functionalities

Fundamentally, firewalls perform the following tasks:

- **Manage and control network traffic** - Firewalls typically do so by inspecting the packets and monitoring the connections that are being made, and then filtering connections based on the packet-inspection results and connections that are observed.
- **Authenticate access** - if the authentication is not successful, the packet would be dropped even though it was permitted based on inspection and the state of the connection. Authentication can be carried through
 - User name/ID and password of the user initiating the connection prior to allowing the connection to be established. Once the connection has been authenticated and authorised by the security policy, the user is no longer prompted for authentication for that connection.
 - The use of public keys and certificates under the PKI.
 - The use of pre-shared keys among the hosts.

- **Act as an intermediary** - firewall can be configured to act as an intermediary, i.e. proxy in the communications process between two hosts.
- **Protect resources** - firewall can protect the internal resources and can be configured to inspect the actual application data itself (for example, allowing it to differentiate between legitimate HTTP traffic and malicious HTTP traffic) before presenting the data to the protected resource.
- **Record and report on events** - the firewall can be configured to maintain logs that can be examined on the happening of a security event. The firewall can also be configured to issue notifications in form of alerts on firewall policy violation.

Access Control Techniques

The firewalls generally use following techniques to control access and enforce security policy.

- **Service control:** Determines the types of internet services that can be accessed. The firewall may filter traffic on the basis of IP address and TCP port number.
- **Direction control:** Determines the direction in which particular services requests may be initiated and allowed to go through the firewall.
- **User control:** Controls access to a service according to the user who is attempting to access it. This is usually applied to inside users.
- **Behaviour control:** Controls how particular services are used. For example, it may enable external access to only a portion of the information on a local Web server.

Access Control Policy

There are two approaches in configuring the firewall rules that are manifested through the firewall policy

- **Default Deny Policy or Mandatory Access Control Policy**
Under this policy, the recommended approach is to deny everything and then selectively allow certain traffic through the firewall.
This will block all traffic on all interfaces in either direction from anywhere to anywhere unless explicitly permitted. This type of policy is normally implemented when dealing with granting access from an untrusted source to a protected system.
- **Allow All Policy or Discretionary Access Control Policy**
This policy follows the opposite approach. It allows, by default, all access and denies only the traffic that is explicitly configured to be denied. This type of security policy is frequently implemented for granting access from a trusted network to external systems (e.g. Internet).

NAT Technique in Firewalls

Network Address Translation (NAT) allows a network to use one set of network addresses internally and a different set when dealing with external networks. NAT is now a function of almost

every firewall whether in a SOHO (small office home office) environment or implemented in an enterprise. NAT firewalls automatically provide protection to systems behind the firewall because they allow connections that originate from the systems inside of the firewall only. It conceals the internal network.

1.2.2 Firewall types

Network Based Firewall

A network firewall is a device deployed between networks to restrict which types of traffic can pass from one network to another. Organisations typically use one or more network firewalls at their network perimeter to provide protection from external threats. Network-based firewall could be implemented on a perimeter router, multi-layered switch or could be a dedicated firewall.

Network firewalls work by comparing network traffic to a set of rules, each of which typically specifies a network or application protocol and the source and destination of the communication. For example, a rule might permit e-mail to reach the organisation's e-mail server from external hosts.

Host Based Firewalls

A host-based firewall is a piece of software running on a single host that can restrict incoming and outgoing network activity for that host only. They can prevent a host from becoming infected and stop infected hosts from spreading malware to other hosts. Host-based firewall runs on computer running OS such as Windows 7 or UNIX. Host-resident firewalls filter and restrict the flow of packets. These can be implemented on a server also.

Advantages of Host Based Firewall

- Filtering rules can be tailored to the host environment. Host-based firewalls are particularly important for systems that are network-connected but are not protected by network firewalls and other network-based security controls.
- They provide an additional layer of protection on the network. When a new server or host is attached to the network, it can have its own firewall, without the need to change the configuration of the network firewall.

Personal Firewalls

A personal firewall controls the traffic between a personal computer or workstation on one side and the Internet or enterprise network on the other side. Personal firewall functionality can be used in the home environment and on corporate intranets. Typically, the personal firewall is a software module on the personal computer. Personal firewalls assume that outbound traffic from the system is to be permitted and inbound traffic requires inspection.

Personal firewall capabilities are normally built into operating system. In a SOHO environment having multiple computers connected to the Internet, firewall functionality can also be housed in a router that connects all of such computers to a DSL, cable modem, or other network interface. Such a firewall is known as a Personal Firewall Appliance.

Some key terms related to Firewalls

Dual Homed

It simply means house with two doors. It is a computer that has at least two network interfaces (NIC), one connected to secure side other unsecure side.

Demilitarized Zone (DMZ)

The name comes from Demilitarized zone between North and South Korea, where neither North Korean nor South Korean military is present.

In Networks, Demilitarized Zone (DMZ) usually houses the IT components that require public access such as a mail server, web server, etc.

Bastion Host

Bastions are highly fortified projections on the outer walls of forts. Bastions are exposed to outside but are critical to a fort's security and enemy's primary effort is to break the bastions thus making security weak.

Similarly Bastion Hosts are computer systems that have Hardened systems because they are vulnerable to attack, as they are exposed to the Internet and are a main point of contact for users of internal networks.

Common characteristics of a bastion host are as follows,

- Its Operating system is hardened, in the sense that only essential services are installed on it.
- It may be configured to require additional authentication before a user is granted access to proxy services.
- It is configured to access only specific hosts.
- It can maintain detailed logs of all traffic.
- It has each proxy independent of other proxies loaded on it.

1.2.3 Firewall Configurations

Packet Filtering Router Firewall

This is the simplest firewall, and is usually implemented on a screening router deployed between the private network and the public network. A router is a device that receives packets from one network and forwards them to another network. The screening router examines the header of every

packet of data travelling between the Internet and the corporate network. Packet filtering firewalls work at the network layer of the OSI model, or the Internet layer of TCP/IP model.

The header of a packet would contain:

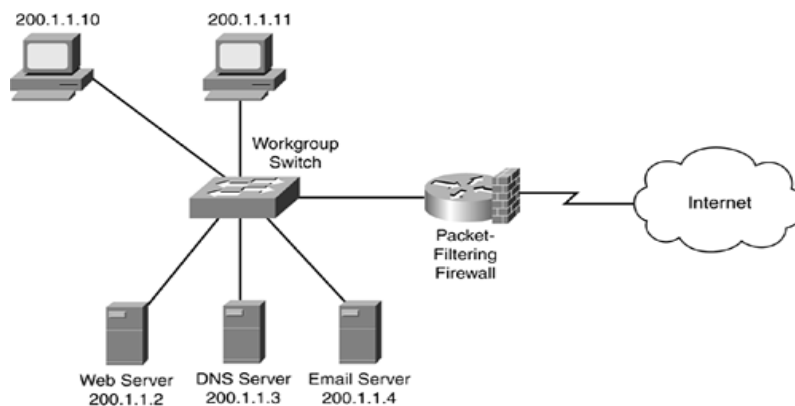
- Type of packet i.e. TCP,UDP, ICMP, IP SEC
- IP Address of Source
- Port Number of Source
- IP Address of Destination
- Port Number of Destination

Firewall rule could be based on any of these.

In case, the rule is matched, and the rule permits, the packet is passed to the next server/device as per the information in the Routing Table of the screening router. If match is found but the rule disallows, the packet is dropped. However, if match is not found, the action to forward or drop the packet is taken as per the default parameter.

Sample Access Control List (ACL)

Source Address	Source Port	Destination Address	Destination Port	Protocol	Action
Any	Any	200.1.1.2	80	TCP	Allow
Any	TCP	200.1.1.3	53	UDP	Allow
Any	TCP	200.1.1.4	25	TCP	Allow
Any	Any	Any other	Any	Any	Deny



Packet Filtering Router

In the above example, the packet filtering router allows access from outside to the Web server (port 80), DNS Server (port 53) and the Email server (port 25). In case any traffic does not meet criteria

as per the first three rules, then the last rule is followed and the packets are denied access. As per the above rules, no traffic is permitted to secured servers 200.1.1.10 and 200.1.1.11.

Advantages of Packet Filtering Firewalls

Packet filtering firewalls have two main strengths: speed, and flexibility. They are not very costly and have low impact on network performance.

Limitations of Packet Filtering Firewalls

- Configuring the packet filtering firewalls and defining the Access Criteria poses difficulty.
- Most packet filtering firewalls do not support advanced user authentication schemes.
- Many packet filtering firewalls lack robust logging facilities as only limited information is available to the firewall.

The primary focus of Packet Filtering Firewalls is to limit inbound traffic while providing for outbound and established traffic to flow unimpeded. Thus, packet filter firewalls are very suitable for high-speed environments where logging and user authentication with network resources are not important. Packet filtering firewalls are prone to following types of attacks,

IP Address Spoofing attack

In this type of attack, the attacker fakes the IP address of either an internal network host or a trusted network (outside) host so that the packet will pass the access rules defined in the firewall. For example using a TOR Browser which provides proxy services we can fake our IP address and breach a Packet filtering firewall which has rule to restrict our IP Address.

Source routing attack: In this process, it is possible to define such a route that it bypasses the firewall. To prevent such attacks, all packets wherein source routing specification is enabled may be dropped. However, this control will not be effective where the topology permits a route to be defined.

Tiny Fragment attack: Using this method, an attacker fragments the IP packet into smaller ones and pushes it through the firewall in the hope that only the first of the sequence of fragmented packets would be examined and the others would pass without review.

Stateful Inspection Packet Filtering Firewall

Stateful inspection firewalls are packet filters that incorporate added awareness of the OSI model data. The Stateful Firewalls keep track of the current connection to ensure that only permitted traffic is allowed to pass. Thus, these firewalls filter traffic based on both packet characteristics (like the packet-filtering firewall) as also session checks to make sure that the specific session is allowed.

Stateful inspection firewalls create a directory of outbound TCP connections, along with each session's corresponding client port. This "State Table" is then used to validate any inbound traffic. The Stateful inspection solution is more secure because the firewall tracks client ports individually rather than opening all "high numbered" ports for external access.

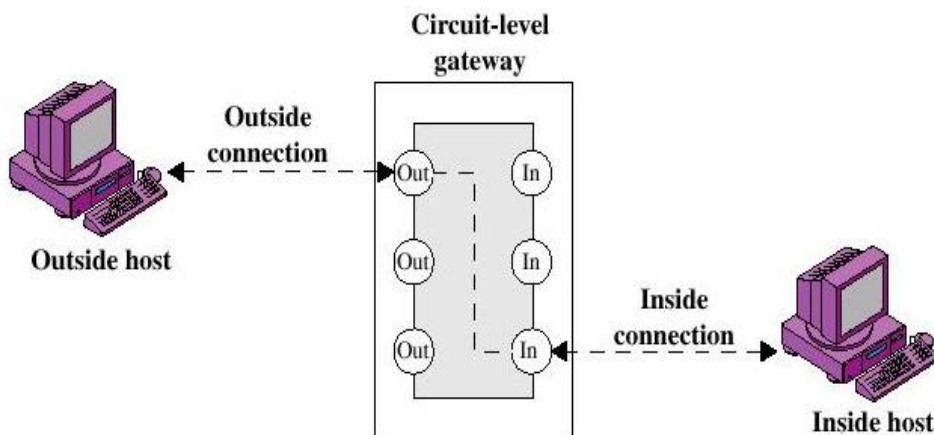
Source Address	Source Port	Destination Address	Destination Port	Action
192.168.1.0	1035	200.12.39.201	80	Established

In this example, as a connection is established between the (source port 1035), with the remote server having port 80, the Stateful inspection firewall makes an entry in the Connection Status table. This state of a connection becomes one of the filtering criteria. If an incoming packet matches an existing connection listed on the table, it will be permitted access without further checking.

Circuit Level Gateways

This type of firewall validates the connections before data is exchanged. It functions at the session layer of the OSI model. A circuit-level gateway relays two TCP connections, one between itself and an inside TCP user, and the other between itself and a TCP user on an outside host. Once the two connections are established, it relays TCP data from one connection to the other without examining its contents. The security function consists of determining which connections will be allowed.

It is typically used when internal users are trusted to decide what external services to access. Circuit level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect. On the other hand, they do not filter individual packets.



Disadvantage of a Circuit Level Gateway

A circuit-level gateway cannot examine the application-level content of the packets it relays between a trusted network and an untrusted network.

Application Level Gateway Firewall

An application-level gateway acts as a relay of application-level traffic. It operates at the Application Layer of OSI model. These are implemented on hardened operating systems. Application level

gateways, also called proxies, are similar to circuit-level gateways except that they are application specific. It forces both sides of the conversation to conduct the communication through the proxy. Application level gateway firewalls are capable of permitting or rejecting requests based on the content of the network traffic.

Examples of access control functions that the application-level gateway can process:

- Access control based on content - whether the request contains known exploits?
- Access control based on user authentication- whether the user is permitted to access the resource requested?
- Access control based on source network zone - whether the access to the requested resource from the source network is allowed? For example, certain intranet resources from the Internet may be prohibited access to particular service(s).
- Access control based on source address - whether the sender address is allowed access to the resource?

The working of an Application level gateway firewall is depicted here.

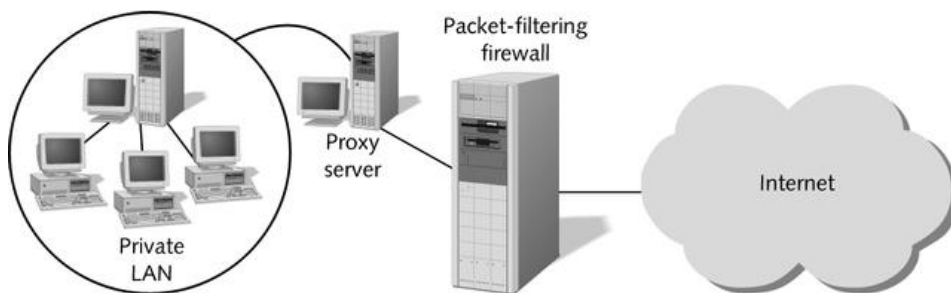


Fig: Application Level Gateway Firewall

Advantages of Application Level Gateway

- Application level gateway (and also the circuit level gateway) firewall systems employ the concept of bastion hosting. Therefore, in the event of a break-in, only the firewall system is compromised, not the entire network.
- Application-level gateways are more secure than packet filters and Stateful Inspection Firewalls as they authenticate individuals and not the devices.
- They can provide auditing and logging functions so that the network traffic can be monitored or analysed at a later time.
- Application level gateways provide complete control over type of service.

Limitations of Application Level Gateway Firewalls

- They are very process intensive and hence can cause performance issues. This can be addressed by using proxy services for critical applications only.

- They are vulnerable to bugs present in the operating system and any application running on the system.

1.2.4 Common Implementation Structures of Firewalls

The deployment strategy for a firewall in an organisation depends upon the objective of the network and the ability of the organisation to implement the architecture. Following are the most common architectural implementations of firewalls:

- Packet filtering routers
- Screened host firewalls
- Dual-homed firewalls, and
- Screened subnet firewalls (DMZ).

Packet Filtering Routers

This is the simplest implementation of a firewall configuration, and is deployed at the perimeter of the network having an untrusted (internet connection). The perimeter routers can be configured to control the passage of packets as per filtering rules defined.

Single Homed Firewalls

This architecture combines the packet filtering router with a separate, dedicated firewall, a Bastion Host acting as application proxy server. The packet filtering router screens the packets before allowing the permitted packets to the proxy server, thus reducing the network traffic and load on the proxy. The application proxy examines an application layer protocol and performs the proxy services.

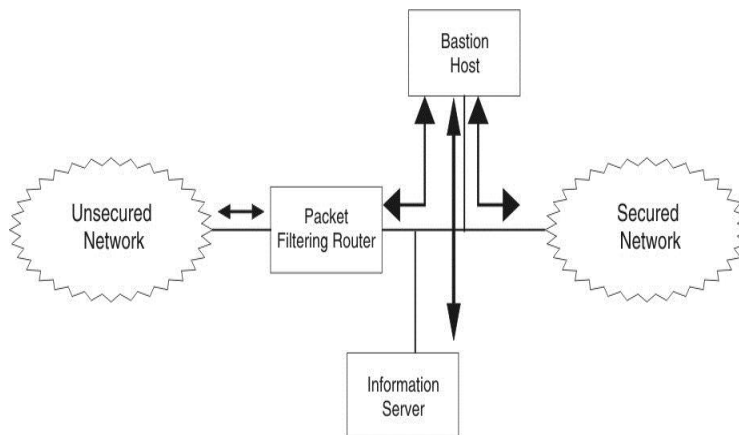


Fig: Single Homed Firewall

Advantages of a Single-homed firewall

- This architecture ensures greater security than a single packet filtering router or an application level gateway firewall alone:
- Its implementation scheme uses both packet-level and application-level filtering, allowing for considerable flexibility in defining security policy.
- An intruder has to penetrate two separate systems before the security of the internal network is compromised.

Limitations

- In this set-up, if the packet filtering router is completely compromised, traffic flows directly through the router between the internet and other hosts on the private network.

Dual-Homed Host Firewalls

In this approach the bastion host is Dual Homed i.e. contains two NICs: one connected to the external network, and one connected to the internal network providing an additional layer of protection by requiring all traffic to go through the Bastion Host to move between the internal and external networks.

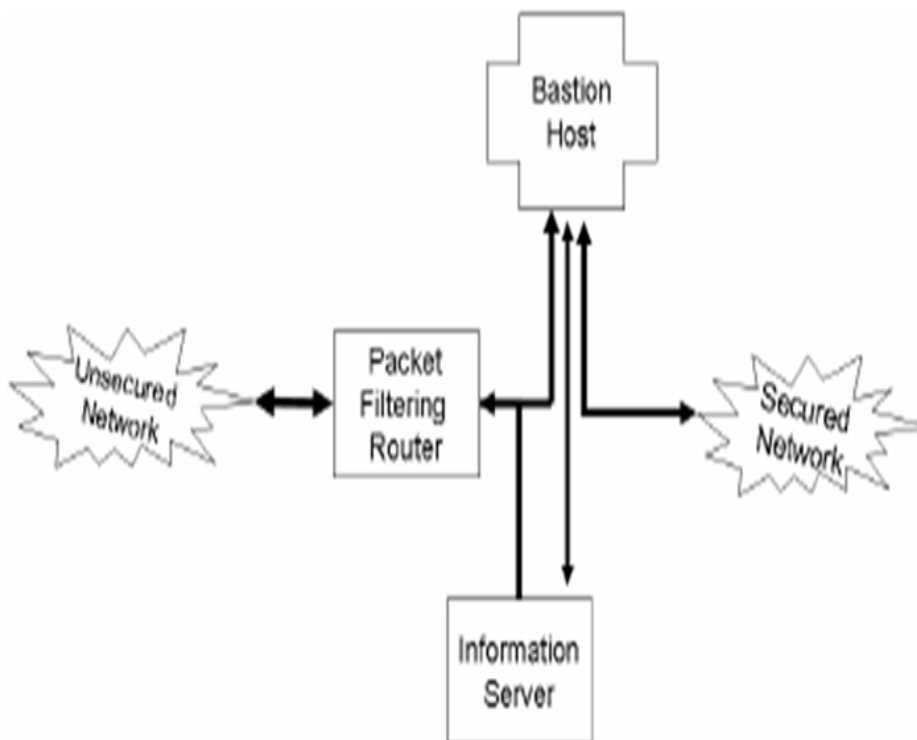


Fig: Dual-homed Firewall

Screened Subnet Firewalls (with DMZ)

The screened subnet firewall configuration is the most secured environment. It has two packet-filtering routers, one between the bastion host and the Internet and the other between the bastion host and the internal network, creating an isolated sub-net. For all incoming traffic, the outside router (the router facing the internet) directs all the packets to the bastion host. The bastion host together with the firewall does preliminary filtering and if the packet passes the test, directs the packet to the less secure or DMZ, the demilitarized zone.

However, where the packet has to travel into the secure network, which is configured as a separate segment, the inside router along with the second firewall provides a second line of defence, managing DMZ access to the private network by accepting only traffic originating from the bastion host. For outgoing traffic, the inside router manages private network access to the DMZ network. It permits internal systems to access only the bastion host. The filtering rules on the outside router require use of the proxy services by accepting outgoing traffic only from the bastion host.

It would be observed that in a screened sub-net firewall, the internal network (the private segment) is highly secured. The external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity.

The advantages of a screened subnet firewall system are explained here.

An intruder must penetrate three separate devices - the outside router, the bastion host, and the inside router to infiltrate the private network.

- Since the outside router advertises the DMZ network only to the Internet, systems on the Internet do not have routes to the protected private network. This ensures that the private network is invisible.
- Since the inside router advertises the DMZ network only to the private network, its systems do not have direct routes to the Internet. This ensures that inside users access the Internet via the proxy services residing on the bastion host.
- Packet-filtering routers direct traffic to specific systems on the DMZ network, eliminating the need for the bastion host to be dual-homed.
- Since the DMZ network is a different network than the private network, a Network Address Translator (NAT) can be installed on the bastion host to eliminate the need to renumber or re-subnet the private network.

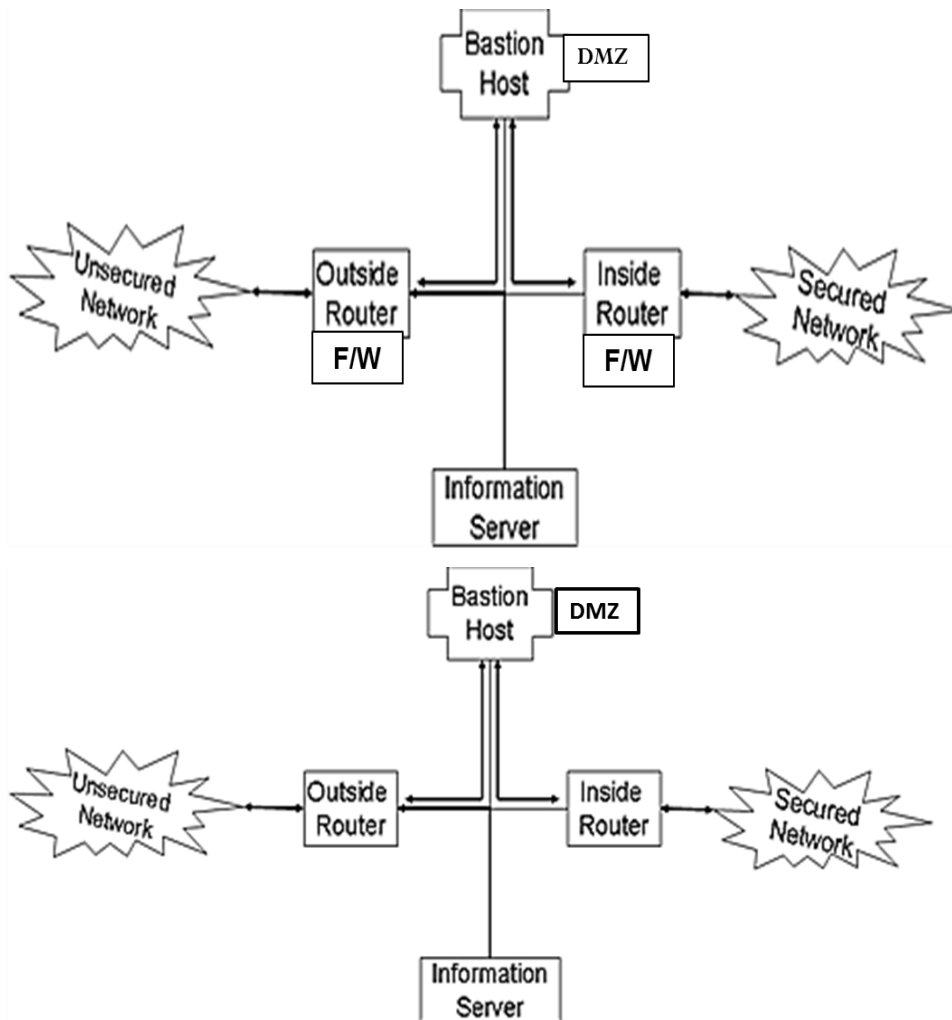


Fig: Screened subnet firewall

1.2.5 Limitations of Firewalls

A firewall is a critical component of network security. It is designed to address the issues of data integrity or traffic authentication and confidentiality of internal network.

The firewalls do have the following limitations:

- A firewall cannot prevent users or attackers with modems from dialling in to or out of the internal network, thus bypassing the firewall and its protection completely.
- Firewalls cannot enforce password policy or prevent misuse of passwords.
- Firewalls are ineffective against non-technical security risks such as social engineering.

- Firewalls cannot stop internal users from accessing websites with malicious code.
- Firewall may not have been implemented on a secured Operating system/hardened system.
- The access list configured in the firewall might not be properly defined, implemented or adequate.
- Network segmentation might not be as per security requirements of the organisation.
- Firewalls cannot provide complete protection against viruses.
- Monitoring of firewall alerts may be inadequate.

1.2.6 Firewall Product Types

The firewall can be either a stand-alone appliance system or it can be implemented on top of a commercial operating system. This depends largely upon the organisation's requirements.

Appliance Based Firewall

The appliances have the firewall software embedded as firmware, making them more secure than those implemented on top of commercial operating systems as appliance based firewalls do not suffer from security vulnerabilities associated with underlying operating systems. These firewalls are faster than firewalls implemented on top of commercial operating systems. However, these firewalls suffer from the scalability issues.

Software Based Firewall

The main advantage of implementing firewalls on top of commercial operating systems is scalability. If an environment requires improved performance, it is usually a simple matter to install a larger system on which to run the firewall software. Most appliances do not offer this level of flexibility or scalability.

The greatest disadvantage of implementing firewalls on top of commercial operating systems is the potential presence of vulnerabilities that might undermine the security posture of the firewall platform itself. In most cases, vulnerabilities in the underlying operating system are the cause of firewalls' compromise.

1.2.7 Unified Threat Management

Unified threat management (UTM) is the evolution of the traditional firewall into an all-inclusive security product able to perform multiple security functions within one single appliance. To meet new threats the organisations are required to add more security solutions or security appliances. This poses the problem of increased complexity and cost, as each new technology means a new device to deploy, a new set of policies to configure, and a new management console to monitor. And, because each new stand-alone product is not integrated with the existing product set, it also creates potential blind spots in an organisation's security strategy, through which threats could pass undetected.

How UTM secures the network

A single UTM appliance simplifies security strategy, with just one device taking the place of multiple layers of hardware and software. Also from one single centralised console, all the security solutions can be monitored and configured. The UTM has a customised Operating System holding all the security features at one place. This can lead to better integration and throughput than a collection of disparate devices.

UTM Functionalities

Following functionalities are normally supported by the UTM.

- **Firewall:** performs stateful packet inspection
- **VPN:** enables secure remote access to networks
- **Gateway anti-virus:** prevents malicious payloads
- **Gateway anti-spam:** prevents unsolicited messages from entering the network
- **Intrusion Prevention:** detects and blocks intrusions and certain attacks
- **Content filtering:** stops access to malicious, inappropriate, or questionable websites and online content.
- **Bandwidth management:** enables effective management of Bandwidth.
- **Application control:** provides visibility and control of application behaviour and content
- **Centralised reporting** as the basic features.

They can also support data-loss prevention by blocking accidental or intentional loss of confidential, proprietary, or regulated data. For enterprises with remote networks or distantly located offices, UTM's are a means to provide centralised security with complete control over their globally distributed networks.

Key advantages

- Reduced complexity: It is a single security solution integrated together that reduces the complexity.
- It makes the task of installation of various security products easier. Hence maintenance and vendor issues become simpler.
- UTM facilitates easy management of the solution. Generally, it works on simple plug and play architecture. It supports GUI interface for manageability.
- Reduced technical training requirements, one product to learn.

Key Disadvantages

- Becomes a Single point of failure (SPOF) for network traffic. In case of its failure, the complete network is exposed. The vulnerabilities in the OS or the UTM can make it the single point of compromise.
- Deployment of UTM may have impact on latency and bandwidth when the UTM cannot keep up with the traffic

Regulatory compliance: Identity-based UTMs deliver identity-based reports on individual users in the network. This offers short audit and reporting cycles and facilitates the meeting of regulatory compliance requirements in enterprises.

1.2.8 Firewall Life Cycle

The firewall life cycle can be defined in five phases. The firewall life cycle stems from the network security policy of the organisation. This policy should be maintained and updated frequently as new attacks or vulnerabilities arise or as the organisation's needs in terms of network applications change. Based on the Network Security policy, the firewall policy is developed. This policy should make the process of creating the firewall rule base less error-prone and more verifiable. The rule base should be properly mapped to the applications and the access matrix. The next phases relate to selection of the solution, its implementation, and configuration and patch management. Phases follow an iterative approach and at each stage the configuration is changed as per changing policy. Changes are effected as per the documented and approved Change Management policy.

1.2.9 Baseline Configuration for Firewalls

Before deciding upon the baseline configuration for a firewall, a general risk assessment and cost-benefits analysis should be performed on the network. This would provide a list of the network applications and the methods that will be used to secure the applications.

In the context of a commercial organisation having offices/users at various locations, a border router or other firewall should be used at the Internet connection point to create an internal DMZ. Web servers and other publicly accessible servers should be placed on the DMZ so that these are accessible as needed and still have some protections from the firewall. Internal users should be protected with an additional firewall. The default policy for the firewall should be to block all traffic and connections unless the traffic type and connections have been specifically permitted, as this approach is more secure. Remote users should be allowed access through a VPN. Firewall should be configured so that it itself is immune to penetration.

1.3 Summary

Firewall acts as security policy enforcement point for inbound and outbound access to the internal networks as packets cross network boundaries. This is done by inspecting the data that is received and tracking the connections that are made to determine what data should be permitted and what data should be denied. Stateful packet filtering examines packet data with memory of connection state between hosts. Network Address Translation (NAT) is the addressing method that hides internal network addresses. Application layer gateways (proxy servers) control how internal network applications access external networks by setting up proxy services.

For a firewall to be able to successfully protect resources, it is critical to implement a design that lends itself to protecting those resources in the most efficient manner. From a simple packet filtering to the screened sub-netting implementations, there are various implementation strategies. Although a single firewall will do an adequate job of protecting most resources, certain high security

environments may warrant using multi-firewall architecture to minimize exposure and risk. Like any other security device firewalls have to be properly configured and monitored.

1.4 References

1. http://csce.uark.edu/~kal/info/private/Networking%20Bookshelf/fire/ch06_01.htm

PART 2: CONFIGURING PERSONAL FIREWALLS AND IDS

Learning Objectives

- To gain understanding of Personal Firewalls
- To gain an understanding on configuring Personal Firewalls
- To understand Intrusion Detection systems
- To understand General Controls in firewalls.

2.1 Introduction

The only way to make a personal computer connected over Internet, 100% secure is to turn it off or disconnect it from the Internet. The real issue is how to make it secure when it is connected. At a minimum, home computers need to have personal firewall and a Security suite having Anti-Virus, Anti spyware etc. In our typical SOHO (Small Office Home Office) Environment, some protection is needed which is provided by personal firewalls. Good personal firewall software is very important because it stops unwanted visitors at the front door.

2.2 Personal Firewalls

Personal Firewalls provide the same methods and techniques as a robust enterprise firewall does, but in a simplified way for the less technically savvy persons. An enterprise firewall has to be constantly monitored whereas a personal firewall does not need much monitoring. Personal firewalls are software installed in a user's computer that offers protection against unwanted intrusion and attacks coming from the Internet. A personal firewall controls network traffic to and from a computer, permitting or denying communications based on a security policy. Personal firewalls are available from numerous security vendors, and Windows 7 includes its own firewall.

The main difference in personal and enterprise firewall is scale, whereas personal firewall focusses on one computer, enterprise firewall's focus is enterprise network and is generally installed at perimeter of network. Personal firewall is based on Security policy of a computer whereas enterprise firewall is based on security policy of the enterprise.

Common Features

- Protecting the computer from unwanted incoming connection attempts.
- Allows the user to control which programs can and cannot access the local network and/or Internet and provide the user with information about an application that makes a connection attempt.
- Block or alert the user about outgoing connection attempts.
- Monitor applications that are listening for incoming connections.

- Monitor and regulate all incoming and outgoing Internet users.
- Prevent unwanted network traffic from locally installed applications.
- Provide information about the destination server with which an application is attempting to communicate.

Limitations

- Many malwares can compromise the system and manipulate the firewall even to the extent of shutting of Firewalls. Like Bagle worm that can disable Windows XP Firewall. (Bagle worm is a Mass-mailing email worm with remote access capabilities).
- These firewalls could cause many false alerts which could irritate non tech savvy users.
- These firewalls could be impacted by vulnerabilities in OS.

2.2.1 Configuration of Personal Firewall in Windows Environment

Choice of Personal firewalls includes using the firewall built into Windows, using a third party product, choosing an Internet security suite that includes a firewall. We would be discussing configuration of a Windows 7 Firewall. The Windows 7 Firewall is a stateful, host-based firewall that filters incoming and outgoing connections based on its configuration. While typical end-user configuration of Windows Firewall still takes place through the Windows Firewall Control Panel, advanced configuration now takes place in a Microsoft Management Control (MMC).

We have already understood that there are two types of firewalls - Network Based and Host based. Windows Firewall with advanced security is a host based firewall; protects a host from unauthorised access and attack. In addition to blocking unwanted incoming traffic, we can configure Windows Firewall with Advanced Security to block specific types of outgoing traffic as well. We have already studied that stateful firewalls operate by inspecting the state of all communications between hosts and storing connection data in state tables. Windows is a stateful firewall.

Some Windows 7 Firewall features

- Inbound filtering
- Outbound filtering
- Firewall rules combined with IPsec rules
- Support for complex rules
- Support for logging

Network Location-Aware Host Firewall

Windows Firewall with Advanced Security is a network location aware application. Windows 7 identifies and remembers each of the networks to which they connect. Windows 7 stores the firewall properties based on location types.

Configuration for each location type is called a profile. In each profile we can:

- Enable or disable Windows Firewall

- Configure inbound and/or outbound connections
- Customize logging and other settings

There are three network location types in Windows Firewall with advanced security

1. **Domain** – Applicable when the connection is authenticated to a domain controller for the domain of which it is a member. (*Domain is a group of computers whose security is managed as a unit. Domain Controller makes the security decisions for the computers in the domain.*)
2. **Public**: For use when in locations such as airports or coffee shops. This is the default profile.
3. **Private**: It is a User assigned profile and is used to designate private or home networks.

By default, all other networks are initially classified as public networks. User can identify the network as either public or private. To classify a network as a private network, the user must have administrator credentials.

While a computer may be connected to multiple network locations at the same time, only one profile can be active at a time. The active profile is determined as follows:

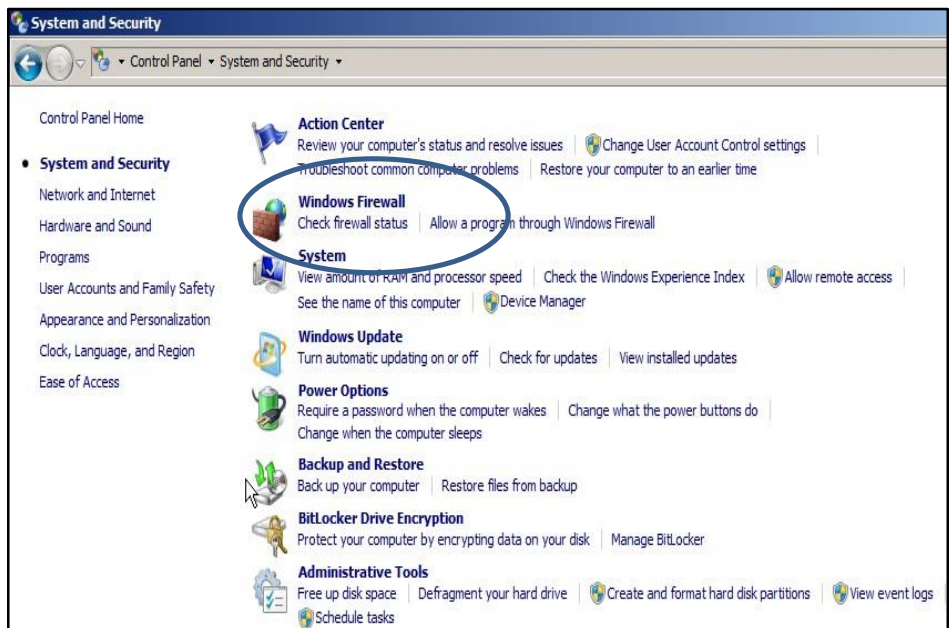
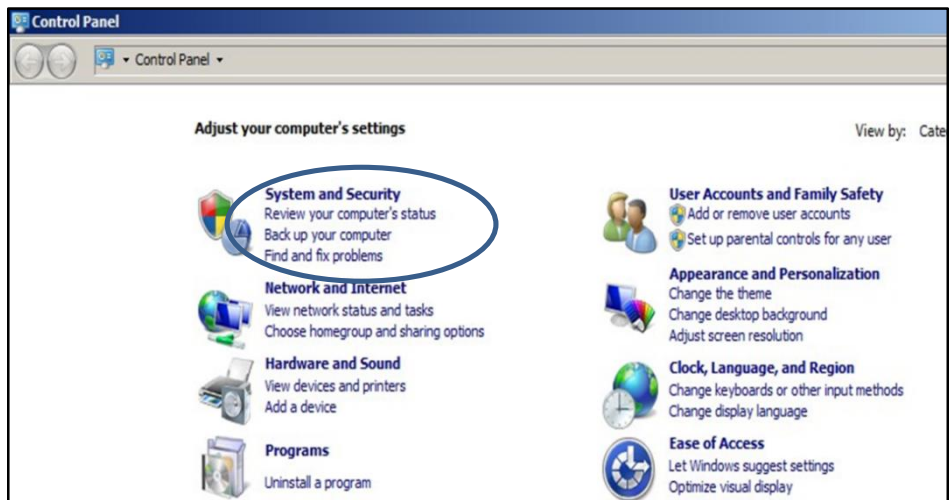
- If all interfaces are authenticated to the domain controller for the domain of which the computer is a member, the domain profile is applied.
- If at least one interface is connected to a private network location and all other interfaces are either authenticated to the domain controller or are connected to private network locations, the private profile is applied.
- Otherwise, the public profile is applied.

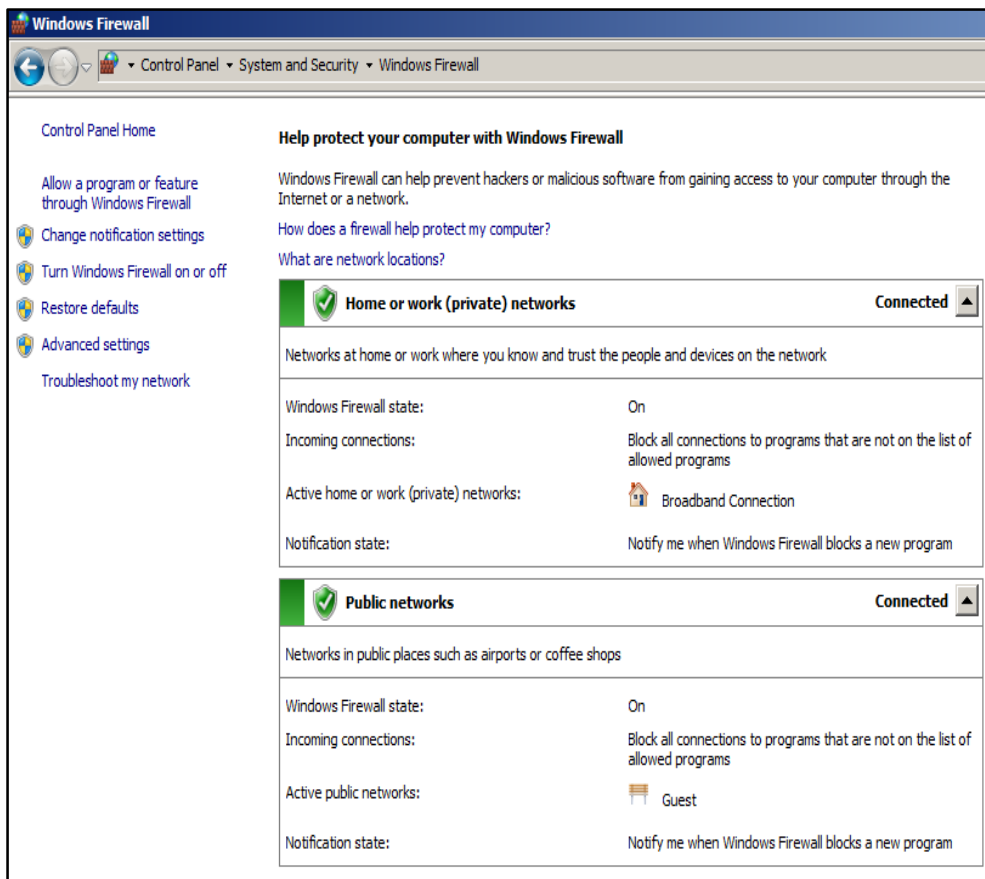
Configuring Windows 7 Firewall

We can configure a Windows 7 firewall as follows, Windows help is available and can easily be activated using function key F1

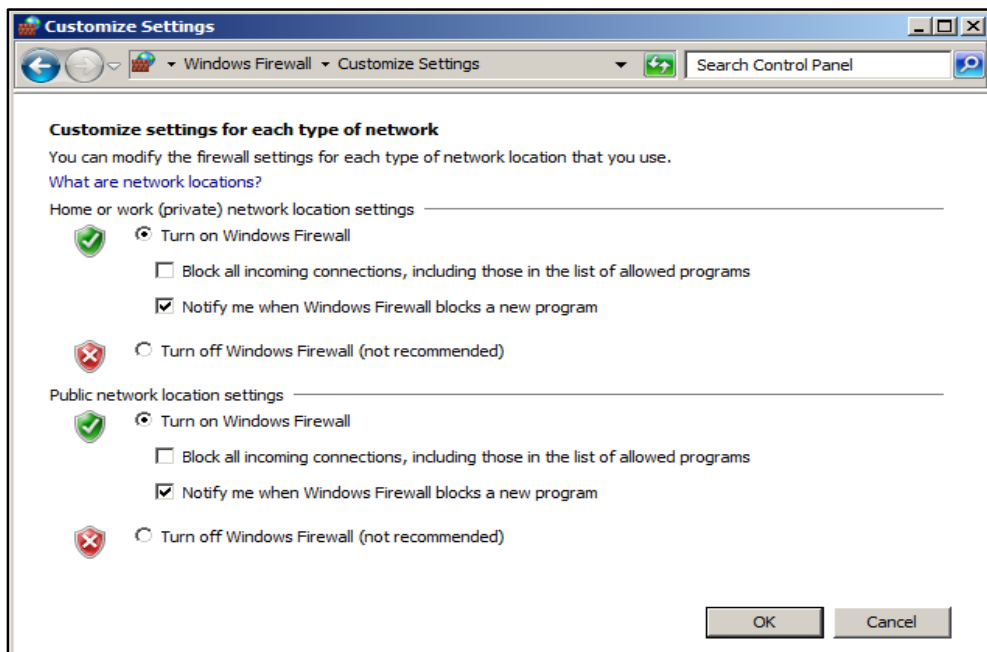
To manually Configure Firewall

- To manually allow a program through the firewall, open the **Control Panel** from the Start menu.
- Select **System and Security**, and then select **Windows Firewall**.
- Click **Allow a program** or feature through Windows Firewall in the left column of the window.





- On the left pane, we can see various links like, Change notification settings, Turn Windows Firewall on or off, Restore defaults and advanced settings etc.
- On the right pane, there are two types of networks link for which we can set firewall settings. They are Home or Work (Private) networks and Public networks.
- By default the Firewall state is **ON** for both the networks.
- Click the Change Notification settings button in the Allowed Programs window.

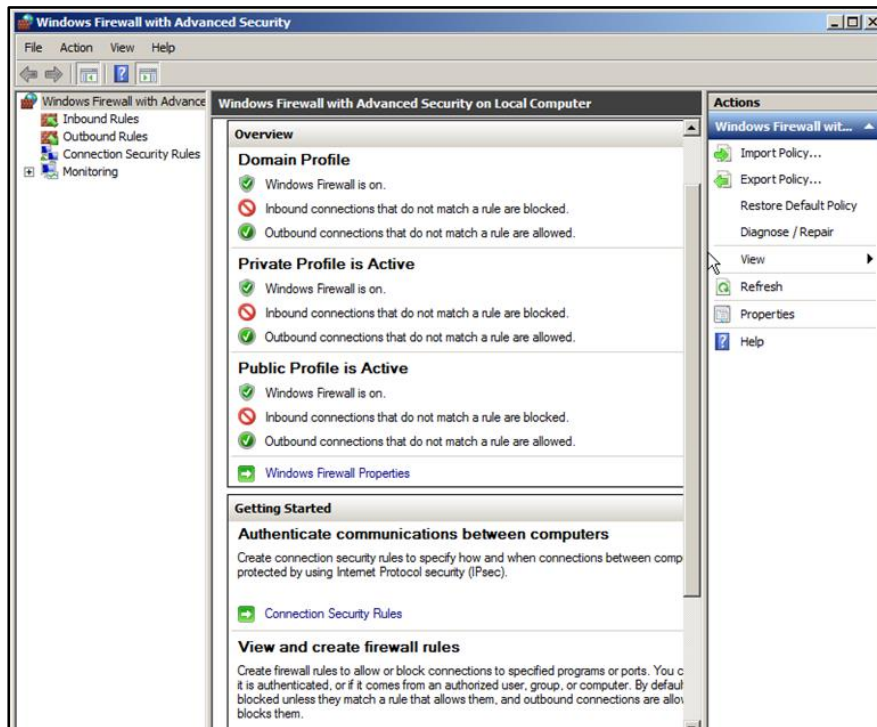


- Select the program or feature and whether we want to open it up to home/work (private), public, or both for all networks.
- Click OK to save our changes.

Overview of Advanced Configuration Settings

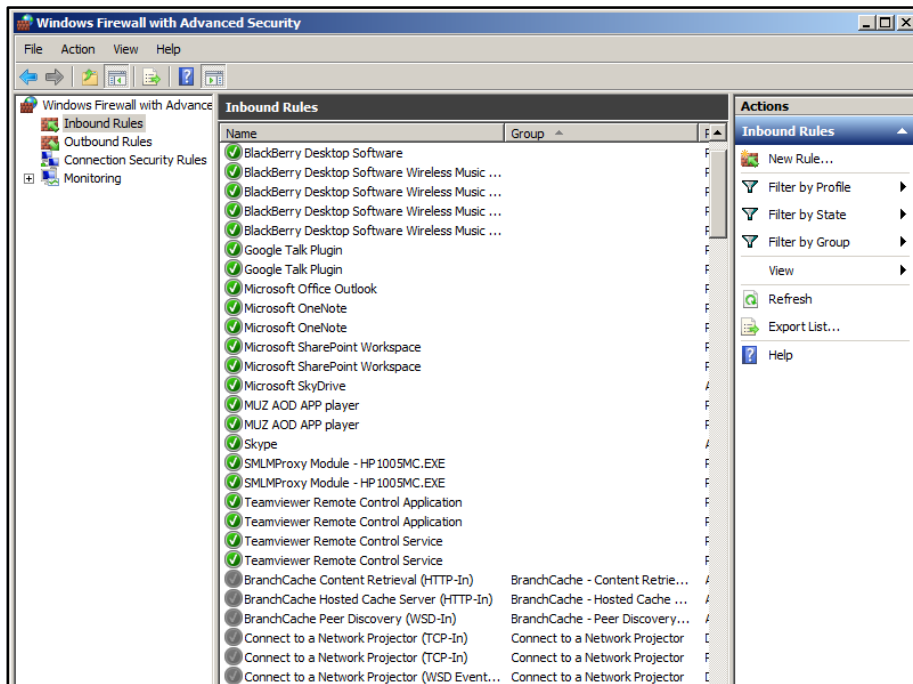


- Go to *Control Panel > System and Security > Windows firewall*
- On the left pane, Click on the **Advance Settings** link to view or change settings. The Advanced settings for the Local Computer displays as below:

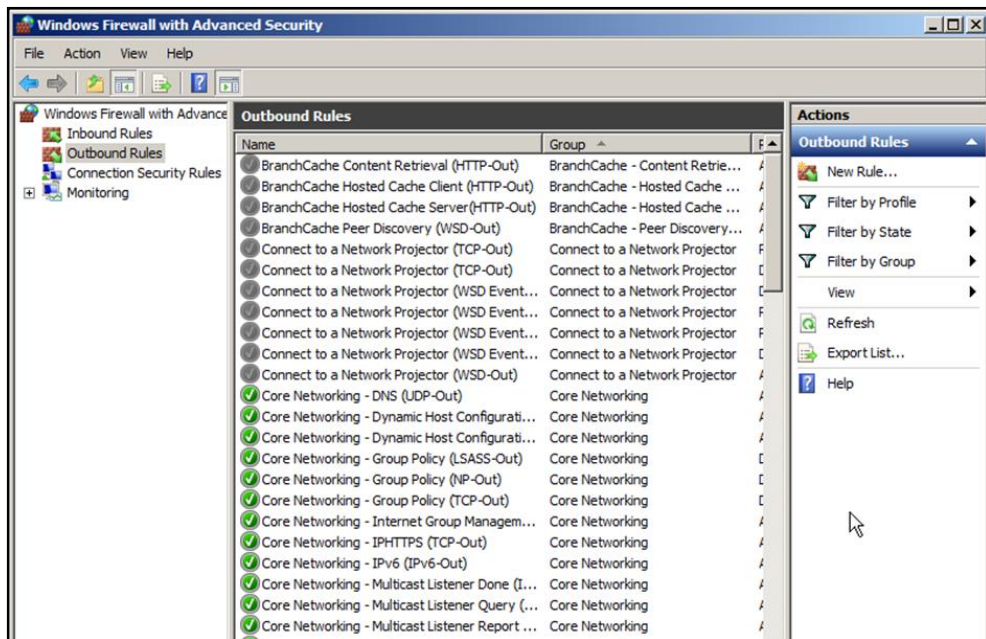


- We can see the options of *Inbound Rules*, *Outbound Rules*, *Connection Security Rules* and *Monitoring*.
- Click on the **Inbound Rules** link in the left pane. A list of all Inbound Rules is displayed.
- On clicking an enabled rule, *lists of actions are shown in the Actions Pane*. Click on *Disable Rule* to disable the selected rule. We can also Cut, Copy and Delete the rule.

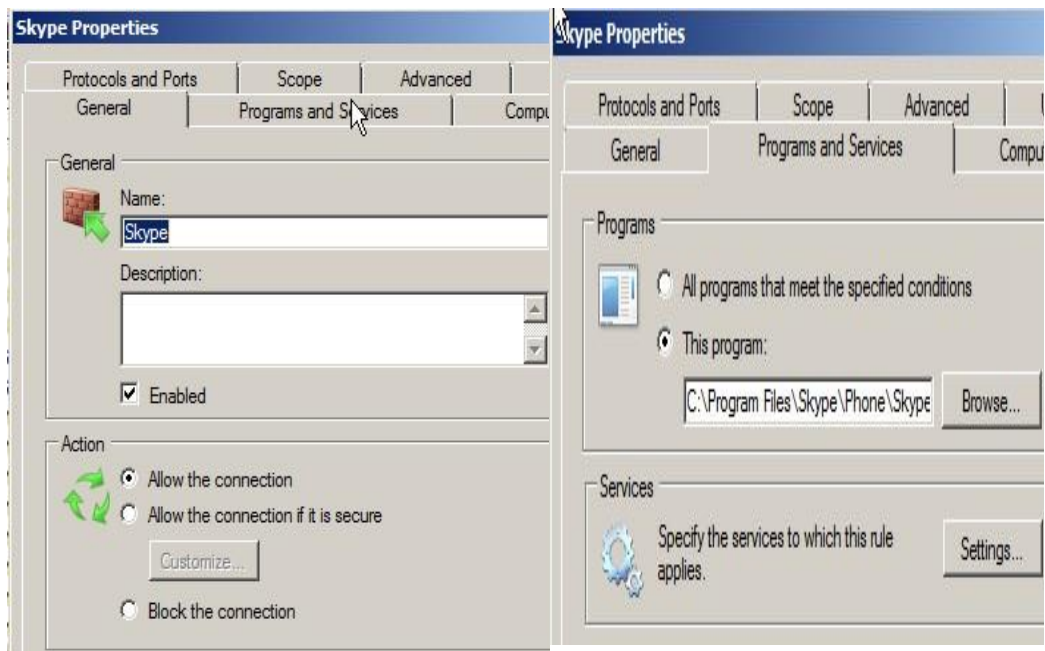
Module 1: e-Learning



- The same procedure is applicable for enabling/disabling outbound rules.



We can see the properties of a rule. In the following depicts, we see details of the rule allowing Skype in our system.



Click Monitoring in the left pane to monitor the settings like *Active Networks*, *Firewall State*, *General Settings* and *Logging settings* etc.

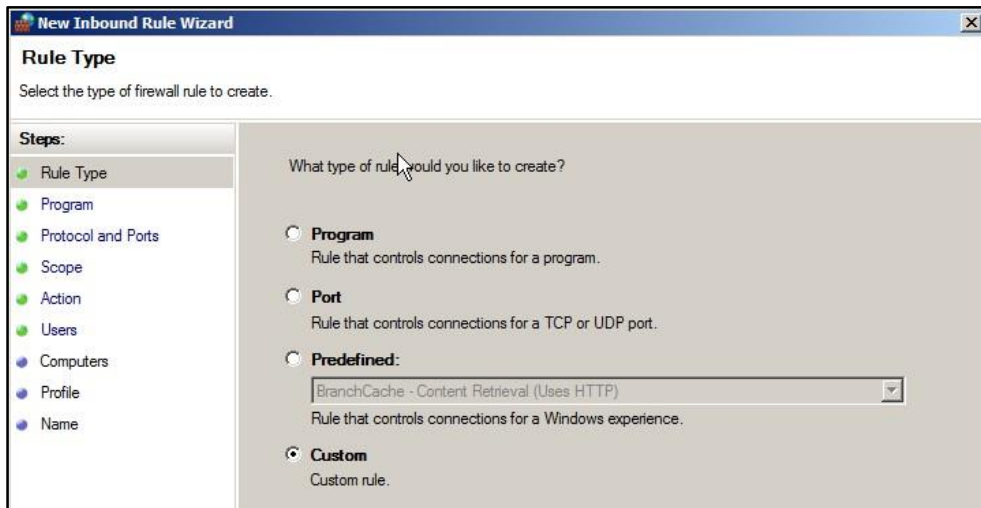
The screenshot shows the Windows Firewall with Advanced Security console. The left pane shows the 'Monitoring' tab selected. The right pane displays a list of firewall rules with the following columns: Name, Profile, Action, Override, Direction, Program, Local Address, Remote Address, Protocol, Local Port, Remote Port, and Allowed Users.

Name	Profile	Action	Override	Direction	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Allowed Users
BlackBerry Desktop Software	Public	Allow	No	Inbound	C:\Progr...	Any	Any	UDP	Any	Any	Any
BlackBerry Desktop Software	Public	Allow	No	Inbound	C:\Progr...	Any	Any	TCP	Any	Any	Any
BlackBerry Desktop Software Wireless Music ...	Public	Allow	No	Inbound	Any	Any	Local subnet	TCP	4481	Any	Any
BlackBerry Desktop Software Wireless Music ...	Public	Allow	No	Inbound	Any	Any	Local subnet	TCP	4482	Any	Any
BlackBerry Desktop Software Wireless Music ...	Public	Allow	No	Inbound	Any	Any	Local subnet	UDP	4482	Any	Any
BlackBerry Desktop Software Wireless Music ...	Public	Allow	No	Inbound	Any	Any	Local subnet	UDP	4481	Any	Any
Core Networking - Destination Unreachable (...)	All	Allow	No	Inbound	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Destination Unreachable (...)	All	Allow	No	Inbound	System	Any	Any	ICMPv4	Any	Any	Any
Core Networking - Dynamic Host Configurati...	All	Allow	No	Inbound	C:\Wind...	Any	Any	UDP	68	67	Any
Core Networking - Dynamic Host Configurati...	All	Allow	No	Inbound	C:\Wind...	Any	Any	UDP	546	547	Any
Core Networking - Internet Group Managemen...	All	Allow	No	Inbound	System	Any	Any	IGMP	Any	Any	Any
Core Networking - IPv6 (IPv6-In)	All	Allow	No	Inbound	System	Any	Any	IPv6	Any	Any	Any
Core Networking - Multicast Listener Done (...)	All	Allow	No	Inbound	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listener Query (...)	All	Allow	No	Inbound	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listener Report ...	All	Allow	No	Inbound	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listener Report ...	All	Allow	No	Inbound	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Neighbor Discovery Adve...	All	Allow	No	Inbound	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Neighbor Discovery Solicit...	All	Allow	No	Inbound	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Packet Too Big (ICMPv6-In)	All	Allow	No	Inbound	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Parameter Problem (ICMP...	All	Allow	No	Inbound	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Router Advertisement (IC...	All	Allow	No	Inbound	System	Any	fe80::/64	ICMPv6	Any	Any	Any
Core Networking - Router Solicitation (ICMP...	All	Allow	No	Inbound	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Time Exceeded (ICMPv6-In)	All	Allow	No	Inbound	System	Any	Any	ICMPv6	Any	Any	Any
File and Printer Sharing (Echo Request - ICM...	Private	Allow	No	Inbound	Any	Any	Local subnet	ICMPv4	Any	Any	Any

Create a rule to enable services.

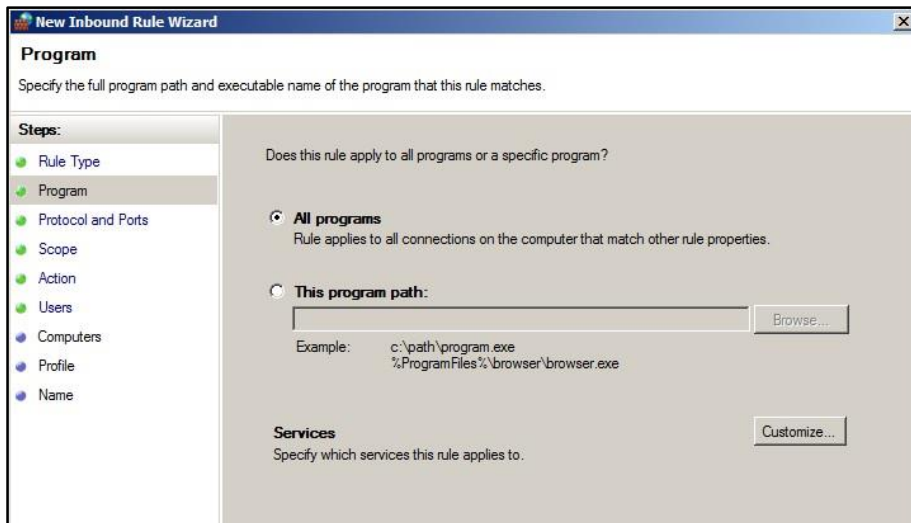
We can also create a rule. Create rule type:

- Click **Advanced settings**.
- Select **Inbound Rules** in the left column.
- Select **New Rule** on the right side of the window.



The new rule could be based on *Program*, *Port*, *Predefined* or *Custom*.

We will build a *Custom* rule: First it asks if it will apply to any specific Program or all Programs, we select the appropriate option.



Then the wizard asks for parameters for three parts of header Type i.e. TCP etc., Local Port, Remote Port.

New Inbound Rule Wizard

Protocol and Ports
Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports**
- Scope
- Action
- Users
- Computers
- Profile
- Name

To which ports and protocols does this rule apply?

Protocol type: TCP

Protocol number: 6

Local port: Specific Ports
80
Example: 80, 443, 5000-5010

Remote port: Specific Ports
50000
Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings: Customize...

The wizard now requires parameters for two remaining parts of packet header, i.e. Local and Remote IP addresses.

New Inbound Rule Wizard

Scope
Specify the local and remote IP addresses to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope**
- Action
- Users
- Computers
- Profile
- Name

Which local IP addresses does this rule apply to?

☐ Any IP address

☒ These IP addresses:
74.25.36.58
Add... Edit... Remove

Customize the interface types to which this rule applies: Customize...

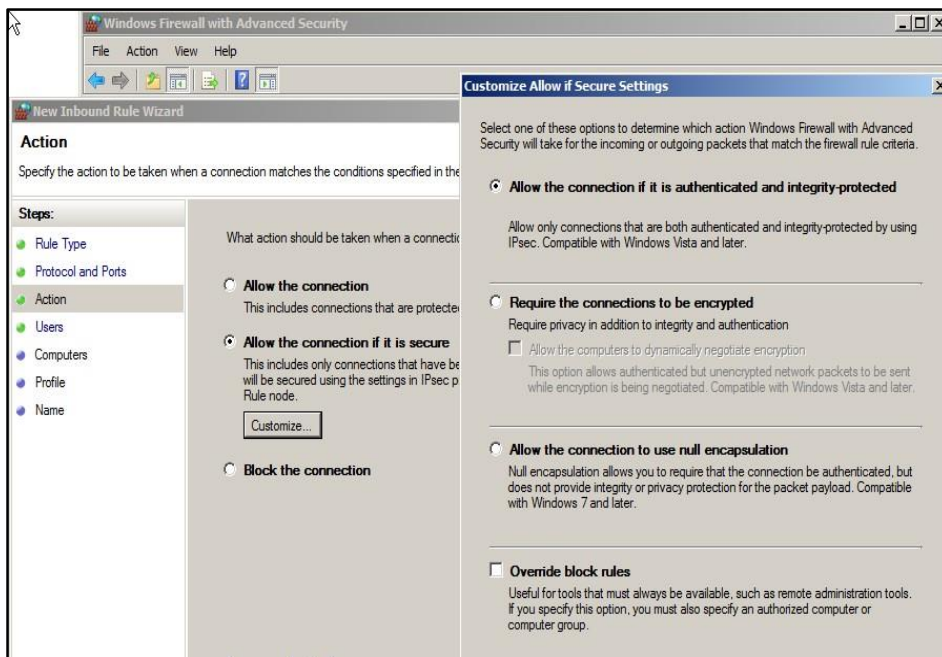
Which remote IP addresses does this rule apply to?

☒ Any IP address

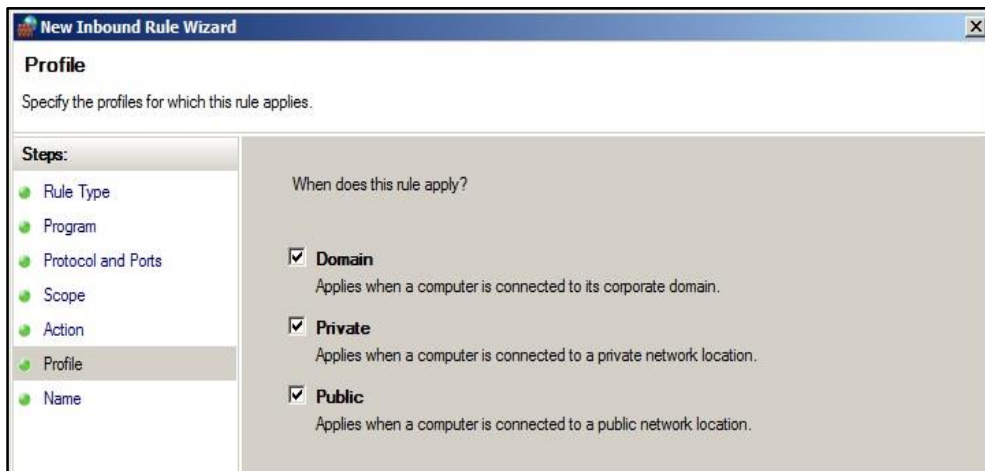
☐ These IP addresses:

Add... Edit... Remove

Based on the criteria stated, Action to be taken can, now be defined. Apart from allowing and blocking the connection, we can make access rule based on Authentication mechanism.



After specifying the rule, we can specify when this rule will apply i.e. based on Location.



Windows firewall thus has many features for advanced setup and is configurable according to our needs.

2.2.2 General Controls Associated With Firewalls

A firewall is the first level of security at the perimeter of a network. A compromise of the firewall can open the network to numerous exposures. As such, it is necessary that the controls associated

with firewall implementation must be understood and followed properly. The general controls associated with firewalls can be classified as,

- **Physical Security Controls:** The organisations are required to devise, implement and periodically review policies related to the physical security of all network components, viz. the servers, the devices, appliances etc.
- **Operating System Security:** A firewall, to be secure, has to be implemented on hardened vulnerability free operating system. The OS patches must be examined and applied without delay.
- **Configuration of firewall policy:** The firewall must be configured as per the organisation policy for allowing/denying traffic both in-bound and out-bound.
- **Change Control procedures:** The access rules must be implemented as per the access criteria defined in the firewall policy of the organisation. The configuration must be reviewed/updated from time to time.
- **Documentation:** Network diagram and configuration must be documented and updated as per changes. The documentation must be thoroughly examined to identify any lapses and vulnerabilities.
- **Log Monitoring:** Log generation facility must be enabled and these logs/alerts must be monitored as a part of regular activity. Attempted violations of the access criteria or the vulnerabilities indicated in these logs should be examined promptly for remedial action.

2.2.3 Pitfalls with Firewalls

Problems faced by organisations where firewalls are implemented could be:

- Firewalls are not clearly understood
- Firewalls are not configured properly
- Activities are not monitored regularly
- Firewalls are circumvented through the use of modems
- If the hackers are inside a corporate network, their action cannot be controlled

2.3 Intrusion Detection Systems (IDS)

Firewalls are a preventive control, which prevent any attack from outside, but what if the enemy is inside and many attacks are from inside. Another layer of control we use for monitoring traffic and events inside our network are Intrusion Detection Systems (IDS), as the name suggests it is a detective control. In simple words, IDS is more like an alarm system in the house, which will alert us when somebody intrude our house, IDS will alarm us when there are intruders in our computer (host) or across our network.

IDS monitors network traffic and host logs for signs of intrusion and by providing Alerts bring potential intrusions to the attention of administrators. It only monitors and lets us know when an event has happened, but does not itself reacts. It has no ability to prevent any intrusions. However, nowadays, there is Intrusion Detection and Prevention System (IDPS) in the market which have

the ability to prevent the intrusion. IDS can detect network scans, packet-spoofing, Denial of Service (DoS), unauthorised attempts to connect to services and improper activity on a system.

Types of IDS

There are two types of IDS which are explained below.

1. **Network Intrusion Detection Systems (NIDS):** NIDS are placed at various choke points, i.e. Routers, Switches etc. within the network and they monitor all traffic to and from devices on the network. Sensors capture all network traffic and analyze the content of individual packets for malicious traffic. These do not create much system overhead. Some possible downsides to network-based IDS include encrypted packet payloads and high-speed networks, both of which inhibit the effectiveness of packet analysis.
2. **Host Intrusion Detection Systems HIDS:** HIDS are implemented on individual hosts or devices on the network. It monitors all packets to and from the host only and alerts the administrator if suspicious activity is detected. It monitors who accessed what. Downside is that it has to be implemented on individual hosts so there is greater deployment and maintenance cost.

Detection Methodologies

Detection methods which an IDS can use could be:

- **Signature Based**
A signature based IDS monitors packets on the network and compares them against large databases of attack signatures. This is just like most antivirus software detects malware. The downside is that it could fail against new attacks, because there won't be a history or signature.

There will always be a lag between new attack being discovered and its signature added to database; during this lag IDS will not be able to detect the new threat.

- **Statistical Anomaly Based(Behaviour Based)**
Behaviour-based intrusion-detection techniques assume that an intrusion can be detected by observing a deviation from the normal or expected behaviour of the system or the users. An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is "normal" for that network- what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous, or significantly different, than the baseline.
The advantages of behaviour-based approaches are that they can detect attempts to exploit new and unforeseen Vulnerabilities. The downside is large number of false positives.

An Intrusion Detection system is only as good as the monitoring which happens, because it only issues alerts, reacting to those alerts is the task of administrator.

2.4 Summary

Personal Firewalls are an effective means of protecting personal computers and hosts. Apart from many vendor products windows 7 has a configurable firewall, which offers lot of configuration options. A firewall is like a doorkeeper protecting attacks from outside but hacker could already be inside the system. To prevent these attacks we have Intrusion Detection Systems to provide alerts while monitoring traffic and events.

2.5 References

- <http://www.giac.org/paper/gsec/1377/host-vs-network-based-intrusion-detection-systems/102574>
- <https://www.ischool.utexas.edu/~netsec/ids.html>

PART 3: CRYPTOGRAPHY AND PKI

Learning Objectives

- To gain understanding of cryptography including need and types
- To understand digital signatures
- To gain an overview of Public Key Infrastructure
- To understand Cryptanalysis

3.1 Introduction

Cryptology is the science of hiding and Cryptography means the practice and study of hiding information. Cryptography is the theory and practice of secure communication. It is the process of transforming data into something that cannot be understood without some additional information. It has been used since ages in military communications and purpose was, should the message fall into the hands of unintended person, he should not be able to decipher the contents of message. These days, in any network particularly the internet, systems are communicating over untrusted medium, and cryptography becomes necessary. It provides mechanisms for authenticating users on a network, ensuring the integrity of transmitted information and preventing users from repudiating (i.e. rejecting ownership of) their transmitted messages.

3.2 Cryptography

Cryptography is the art of protecting information by transforming it into unintelligible form and the process is called encryption. Many schemes used for encryption constitute the area of Cryptography. These are called Cryptographic Systems or Ciphers. Techniques used for deciphering a message without knowledge of enciphering details constitute cryptanalysis. A cryptanalyst is one who analyses cryptographic mechanisms and decodes messages without knowledge of the key employed in encryption. Most of Cryptanalyst are deployed in areas like Military etc.

3.2.1 Need for Cryptography

Cryptography has gained prominence because of the need to safeguard information from falling into wrong hands. It provides solutions to problems of protecting data and identity with regard to data in transit. Some key issues to be addressed for all communications taking place over network relate to:

- Confidentiality
- Integrity
- Authentication
- Non-repudiation

Cryptography helps in addresses confidentiality related issues. Cryptography when used as an element of PKI also addresses Integrity, Authentication and non-repudiation related issues.

3.2.2 Objectives of Cryptographic Systems

The main goals of any Cryptographic System are to ensure following in electronic communication:

- **Authentication:** The process of proving one's identity. The system provides facilities to the recipient of a message to convince him that the message he has received has originated only from the sender and not from any unauthorised person.
- **Privacy or Confidentiality:** Ensuring that no one can read the message except the intended receiver. Whatever is communicated between two parties should be known only to them. No unauthorised person should get to know about it.
- **Integrity:** Assuring the receiver that the received message has not been altered in any way. The system should provide facilities to the recipient that the message he has received has not been altered.
- **Non-Repudiation:** A mechanism to prove that the sender really sent this message. The system should provide facilities to the recipient to convince him that the message he has received has originated only from the sender, and the sender at a later point of time does not repudiate the same.

3.2.3 Elements of Cryptography

The following are the basic elements about messages and encryption.

- Any message that is intelligible is termed **plaintext**, also called as Cleartext.
- **Encryption** is the process of converting the given plaintext into a scrambled form.
- The encrypted message that is unintelligible is called **Ciphertext**.
- The process of turning cipher text back into plaintext is called **Decryption**.

To convert any plaintext into ciphertext we need an Algorithm (in plain speak some mathematical formula or function) and Keys.

A **Cryptographic Algorithm**, also called a Cipher, is the mathematical function used for encryption and decryption. This is used for two functions: one for encryption and the other for decryption. A cryptographic algorithm must be easy to use, but extremely difficult to crack.

Keys are additional secret data which has to be Input to the algorithm for encryption or decryption. These keys prevent the message from being decoded—even if the algorithm is publicly known. Key must be long enough to break but short enough to use and transmit.

Example: Julius Caesar used a technique called Caesar cipher to transmit message to his army. It was actually shift by 3 rule wherein alphabet A is replaced by D, B is replaced by E, and so on. That means you can encrypt the message using a formula Original Letter +3= Encrypted Letter. In this case the formula is Algorithm, but the formula will operate with a key which in this case is 3, we change the key and result changes. To decrypt we need the algorithm and the key.

Cryptography not only protects data from theft or alteration, but also ensures its authentication. There are, in general, three types of cryptographic schemes to accomplish these goals:

Secret Key or Symmetric Cryptography (SKC): Uses a single key for both encryption and decryption.

Public Key or Asymmetric Cryptography (PKC): Uses one key for encryption and another for decryption.

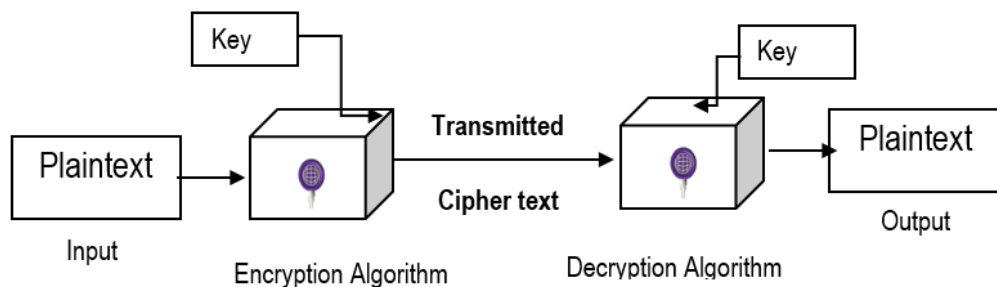
Message Hash Functions: Reduce a message of variable length to a fixed and usually much shorter length.

3.2.4 Symmetric Key Cryptography

In Symmetric Key Cryptography, the sender uses the key (and some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key (and rule set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, this cryptography is also called Symmetric Encryption.

The key must be known to both the sender and the receiver; that, in fact, is the secret, but the difficulty with this system is the distribution of the key.

DES (Digital Encryption Standard) one of the most used Symmetric Key Algorithm which was adopted by NIST (National Institute for Standards and Technology) used a 56 bit key i.e. it had 2^{56} keys, which with brute force are difficult to crack, but due to advances in technology, current NIST standard is AES (Advanced Encryption Standard) that uses a stronger key size of 128, 192 and 256 bits. Increase in number of bits increases the strength because the number of possible keys increases.

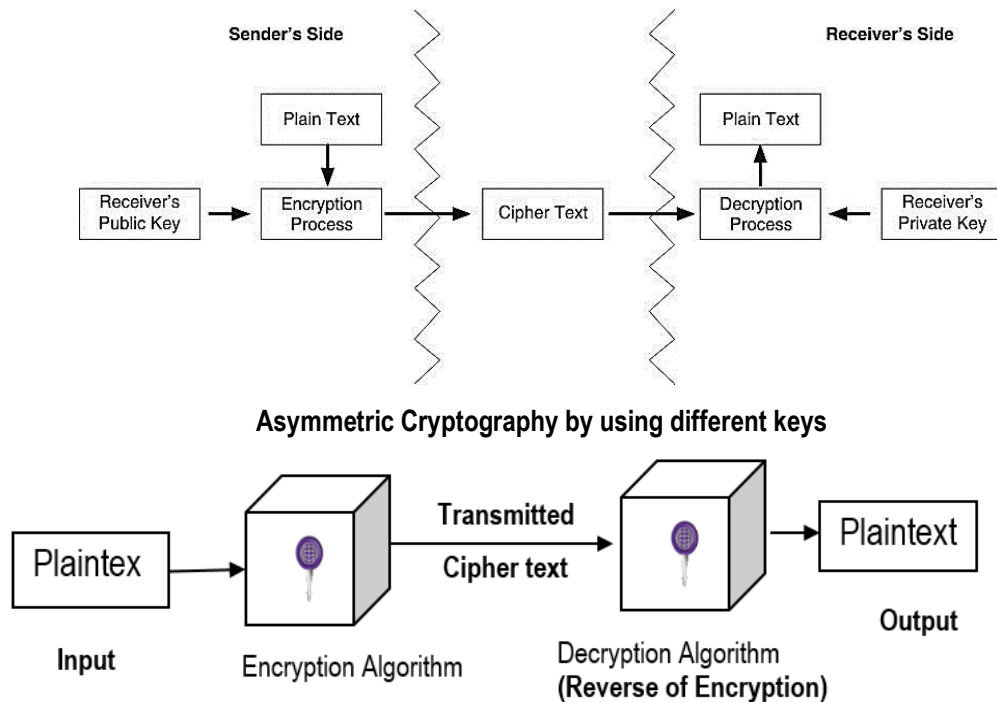


Symmetric Key Cryptography (using the same key)

3.2.5 Asymmetric or Public Key Cryptography

In symmetric key encryption system, a single key is used for both encryption and decryption. The main problem in this method is that the sender and receiver must agree on the symmetric key without anyone else finding out and the difficulty of sending the key to the recipient in a safe and secured manner. Such a process of generation, transmission and storage of keys is termed as Key Management. Where the number of users is more, the problem becomes huge.

Asymmetric Encryption uses a pair of keys generated in such a way that one key is used for encryption and another for decryption. It does not matter which key is applied first, but both keys are required. Since a pair of keys is used in this approach, the mechanism is also called asymmetric cryptography. In this concept, each person gets a pair of keys, one called the public key and the other called the private key. The public key of the individual is in public domain, while the private key is never revealed. But, this process of encryption and decryption is thousands of times slower than symmetric encryption.



In this case if Ram sends a message to Rahim encrypted with Key 1 then Rahim can only decrypt it using Key 2, the message can in no way be decrypted with Key 1.

This Asymmetric Encryption approach is used mainly for exchange of Symmetric Keys and Digital Signatures.

For example: RSA: The first, and still the most common PKC implementation, named after the three MIT mathematicians who developed it - Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. Key size used these days is 2048 bit i.e. 2^{2048} Possible keys.

Comparison between Symmetric and Asymmetric Key Encryption Algorithms

Symmetric Key / Private Key Encryption	Asymmetric Key / Public Key Encryption
Key Size is generally small as compared to public key encryption	Key Size is generally large when compared to private key encryption
Works fast	Slow compared to symmetric key
Consumes less computer resources	Uses more computer resources compared to symmetric key method
Less secure when compared to asymmetric method because of key management problem	Increased security because private keys are never revealed to anyone
Not intended for authentication	Provides facilities for authentication through digital signatures.
Efficient for encryption	Provides facilities for efficient digital signatures and key management through PKI

3.2.6 Message Hash Functions

Message Hash, also called Message Digests and One-way hash functions, are algorithms that, in some sense, use no key. Instead, a fixed length hash value is computed based upon the plaintext that makes it impossible to recover either the contents or length of the plaintext. The main purpose of Hash function or message digest is Message integrity, since at receiver's end Hash is recalculated, if they match that ensures that message has not been altered during transmission. For example: Secure Hash Algorithm (SHA): Algorithm for NIST's Secure Hash Standard (SHS). SHA-1 produces a 160-bit hash value.

3.3 Digital Signatures

We are living in a digital world, where communications are happening on networks with the help of computers. There comes the importance of trusted communication. A trusted communication should have these attributes of trust:

- **Confidentiality:** Privacy from third person
- **Integrity:** Change in message during transit should be detected
- **Authenticity:** Identity of sender should be detected
- **Non-repudiation:** Denial by sender should not be possible
- **Access Control:** Only give the keys to those authorised to use.

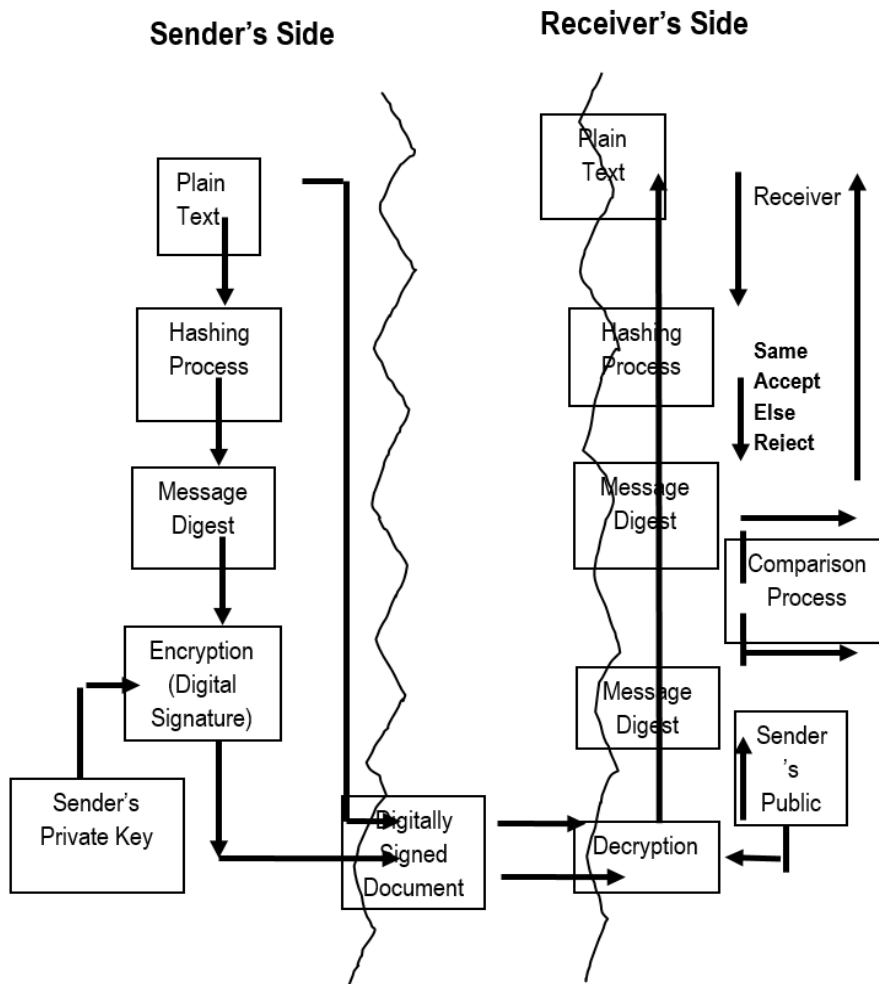
Some of these attributes of trust are provided by digital signature. Digital signature may be defined as a data string dependent on some secret known only to the signer, and additionally, on the content of the message. The process involves use of Asymmetric Keys and Hash.

Taking the above example of communication from Ram to Rahim the process would be:

- Ram subjects the message to a hash function to obtain a message digest.
- Encrypts the message digest by using his private key (Sender's Private Key). The outcome is called the digital signature of the sender (digitally signs the message digest).
- Attaches the encrypted message digest (digital signature) to the message and sends it to Rahim.
- Upon receiving the message and the encrypted message digest, Rahim decrypts the encrypted message digest using Ram's (Sender's) public key and obtains the message digest.
- Rahim subjects the message to the hash function and obtains a message digest.
- He then compares the computed message digest with the message digest he has received from Ram (derived by decrypting the digital signature of Ram). If both of them are same, the integrity of the message is established. If the integrity is suspect, then Rahim can ask Ram to resend the message.

In this example the digital signatures have served the purpose of

- Authentication (establishing the identity of the person who has signed it);
- Integrity (that the document that has been signed is unchanged); and
- Non-repudiation (that the person who has signed it can't deny it later).



Working of the Digital Signature by Using Hashing

3.4 Public Key Infrastructure (PKI)

Digital signatures achieved the objectives of authentication, integrity and non-repudiation (through PKI or trusted third party), but two more objectives required for secure communication are confidentiality and access control. These are achieved through Digital Envelopes and Public Key Infrastructure (PKI).

Digital Envelope is an encrypted message that uses both secret key and public key cryptography methods. A secret key is used to encrypt and decrypt the message, but the public key method is used to send the secret key to the other party.

PKI is a comprehensive system that provides public-key encryption and digital signature services to ensure confidentiality, access control, data integrity, authentication and non-repudiation. So the basic purpose of PKI is to help in maintaining the attributes of trust in any electronic transaction.

Today we are increasingly using electronic communication over internet for all forms of transactions, from E- Commerce to E-Filing of documents. In all these transactions the requirements are:

- Identify of users accessing sensitive information? (Authentication)
- Control who accesses information (Access Control)
- Be sure communication is private but carried over the Internet? (Privacy-Confidentiality)
- Ensure data has not been tampered with? (Integrity)
- Provide a digital method of signing information and transactions? (Non-repudiation)

3.4.1 Elements of PKI

Elements of PKI include:

- **Public/private key pair** –Asymmetric Keys
- **Digital certificate**-Contains identity and verification information
- **Certificate authority**-Trusted Third Parties (TTP) to verify and vouch for the identities of entities in the electronic environment
- **LDAP directory**-Store certificates and publicly required information so applications can retrieve them on behalf of users.
- **Authentication device**- to store the private key.
- **In addition Time stamping, Cross certification, Arbitration mechanism, Verification certificate, CRL, CPS are also part of PKI.**

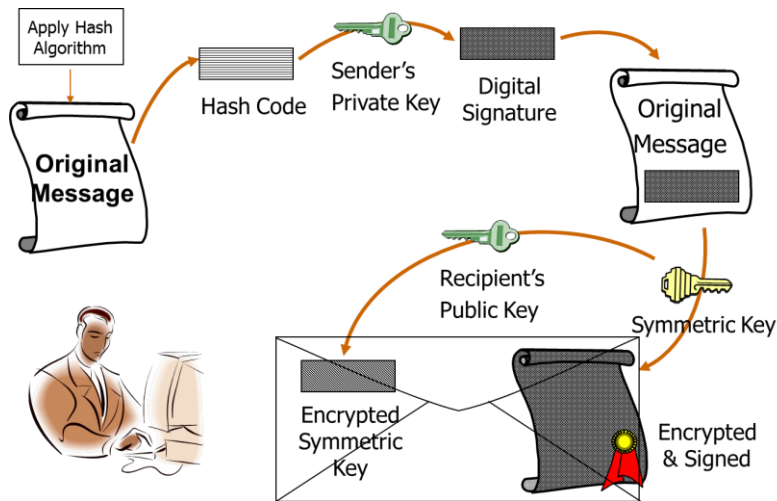
Let's look at a typical trusted communication using PKI.

To explain this method, let us go back to the example of Ram trying to send a confidential message to Rahim.

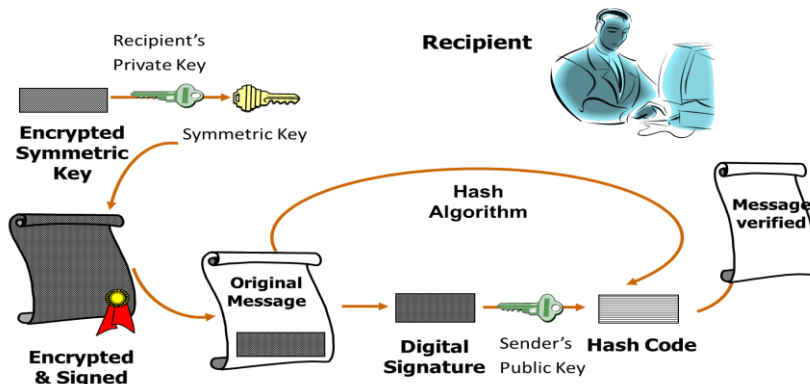
1. Ram subjects the message to a hashing function. The result is the message digest.
2. The message digest is then encrypted (signed) using the private key of Ram (Sender) (the result is the digital signature), and attaches the encrypted message digest to the message.
3. The plain-text signed message is encrypted using a randomly generated symmetric key (encryption of the message). This key is independent of the private and public keys.
4. The symmetric key used for encryption is encrypted using the Public asymmetric key of Rahim (Receiver). (Encryption of the key).
5. Then Encrypted Signed message and encrypted key (i.e. Electronic Envelope) are sent to the receiver (Rahim).
6. On receipt of the above, Rahim first decrypts the encrypted symmetric key using his (Receiver's) private key (decryption of the key) and obtains the symmetric key.

7. He uses the symmetric key so obtained to decrypt the Signed message to get the plain text (decryption of the message).
8. He then uses Ram's (Sender's) public key to decrypt the digital signature (i.e. encrypted message digest (decryption of the message digest)).
9. The plain-text so obtained in step No.7 is subjected to the hash function and the message digests are compared. If they are the same, the message is accepted. .
10. Hence he achieves message integrity, identity authentication, non-repudiation and confidentiality.

At the senders end



At the receivers end:



3.4.2 Digital Certificates

A Digital Certificate is a digitally signed document that associates a public key with a user. The certificate can be used to verify that a public key belongs to an individual. In a typical public key infrastructure (PKI) scheme, the signature will be of a certifying/ certification authority (CA). The signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together.

Contents of a Typical Digital Certificate

- Serial Number: Used to uniquely identify the certificate.
- Subject: The person or entity identified.
- Signature: The algorithm used to create the signature.
- Issuer: The entity that verified the information and issued the certificate.
- Valid-From: The date from which the certificate is valid.
- Valid-To: The expiration date.
- Public Key: The public key to encrypt a message to the named subject.
- Thumbprint Algorithm: The algorithm used to hash the certificate.
- Thumbprint: The hash itself to ensure that the certificate has not been tampered with.

3.4.3 Certifying Authority (CA)

Certifying Authorities are Trusted Third Parties (TTP) to verify and vouch for the identities of entities in the electronic environment. The trust in the CA is the foundation of trust in the certificate as a valid credential. In India, the IT Act (Information Technology Act) provides for the Controller of Certifying Authorities (CCA), the body under Ministry of Communications and Information Technology to license and regulate the working of Certifying Authorities and also to ensure that none of the provisions of the IT Act are violated.

The main role of Certifying authority is to digitally sign and publish the public key bound to a given user. Certifying Authority does this using its own private key. This brings a chain of trust i.e. trust in user's key relies on the trust in CA's key. Some Roles and responsibilities of CA include:

- Establish Certificate Practice Statement (CPS) and Certificate Policies
- Verification of registration, suspension and revocation request
- Generation, issuance, suspension and revocation of digital certificates
- Publication and archival of certificates, suspension and revocation information
- Key management
- Compliance with security standards
- Utilisation of trustworthy systems in performing its services

3.4.4 Registration Authority (RA)

A registration authority (RA) acts as the verifier for the certificate authority before a digital certificate is issued to a subscriber. The registration process begins with RA, who authenticates identity of a person based on which CA will issue Digital Certificate. Registration Authority (RA) interacts with the subscribers for providing CA services. The RA is subsumed in the CA, which takes total responsibility for all actions of the RA.

3.4.5 Certificate Revocation List (CRL)

CRL is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked, and therefore entities presenting those certificates should no longer be trusted. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. The CRL file is itself signed by the CA to prevent tampering. The CRL is always issued by the CA that issues the corresponding certificates. When a potential user attempts to access a server, the server allows or denies access based on the CRL entry for that particular user.

3.4.6 Certification Practice Statement

CPS (Certification Practice Statement): A statement of the practices, which a certification authority employs in issuing and managing certificates. A CPS may take the form of a declaration by the CA of the details of its trustworthy systems and the practices it employs in its operations and in support of issuance of a certificate.

A CPS might include the following types of information:

- Certificate policies that are implemented by the CA and the certificate types that are issued
- Policies, procedures, and processes for issuing, renewing, and recovering certificates
- Cryptographic algorithms, cryptographic service providers (CSPs), and the key length that is used for the CA certificate
- Physical, network, and procedural security for the CA
- The certificate lifetime of each certificate that is issued by the CA
- Policies for revoking certificates, including conditions for certificate revocation, such as employee termination and misuse of security privileges
- Policies for certificate revocation lists (CRLs), including where to locate CRL distribution points and how often CRLs are published
- A policy for renewing the CA's certificate before it expires.

3.4.7 Key Storage and Security

Key management includes dealing with the generation, exchange, storage, use, and replacement of keys.

Key storage and security is a huge challenge for any Certifying Authority and one of the biggest challenges is CAs root private key, because compromise of a CA private key would allow cyber criminals to start forging their own trusted certificates. Some of the measures adopted by CAs for key management include:

- CA key is stored in a Hardware Security Module (HSM).
- The machines are locked and stored in steel vaults and all with heavy physical security.
- The HSM will log all signatures.
- The machine is under 24/7 video surveillance, with off-site recording.

For Public key of subscribers, Key repositories are used to store certificates and publicly required information, so applications can retrieve them on behalf of users. LDAP (Lightweight Directory Access Protocol) is one of the protocols used to access these repositories.

3.5 Cryptanalysis

Cryptanalysis mainly deals with methods of recovering the plaintext from ciphertext without using the key. In other words, it is defined as the study of methods for obtaining the meaning of encrypted information, without access to the secret information which is normally required to do so. It also deals with identifying weakness in a cryptosystem. Cryptanalysis is also used to refer to any attempt to circumvent the security of other types of cryptographic algorithms and protocols, and not just encryption. There are many types of cryptanalytic attacks. The basic assumption is that the cryptanalyst has complete knowledge of the encryption algorithm used.

*For example **Known-plaintext attack**: In this case the cryptanalyst has access to not only the ciphertext of several messages, but also to the plaintext of those messages. Using the ciphertext and its corresponding plaintext, he deduces the key used to encrypt the messages.*

3.6 Summary

Cryptography or the science and art of coding messages provide us a method to transmit messages over open networks, like internet and still achieve the objectives of confidentiality, integrity, authenticity and non-repudiation. Digital certificates provide a means to digitally sign the message. PKI affords us the infrastructure to manage the Asymmetric keys, and a means of certifying the authenticity of holder of key.

3.7 References

- <http://www.garykessler.net/library/crypto.html>
- <http://en.wikibooks.org/wiki/Cryptography>
- <http://resources.infosecinstitute.com/role-of-cryptography/>
- http://www.di-mgt.com.au/rsa_alg.html#simpleexample

PART 4: APPLICATION OF CRYPTOGRAPHIC SYSTEMS

Learning Objectives

- To understand uses of cryptographic Systems
- To gain an overview of SSL/ TLS
- To gain an overview of cryptographic systems like IPsec, SSH, SET
- To gain an overview of generic Enterprise Network Architecture in a Bank.
- To understand risks and controls in Enterprise Network
- To understand auditing network security

4.1 Introduction

The need to send sensitive information over the Internet is increasing, and so is the necessity to secure information in transit through the Internet as also Intranets. Cryptography is used for securing transmission of messages, protection of data, authentication of sender and to provide privacy and security in any situation where information is not intended for public.

4.2 Uses of Cryptographic Systems

Cryptographic systems are techniques which use one or more forms of cryptography and/or PKI to secure electronic transmissions from threats relating to confidentiality, integrity, authentication and non-repudiation. Ram and Rahim want to talk to each other, or Ram wants to log on to Rahim's website. But they're worried about security issues like:

- How do we know we're talking to the right person?
- How do we know people can't listen to our conversation?
- How do we know people can't change our conversation?

A system is needed that protects against these security concerns. To resolve these problems, we have many applications of cryptographic systems like:

- Secure Socket Layer/Transport Layer Security
- Secure Hyper Text Transfer Protocol (HTTPS)
- IPsec
- SSH
- Secure Electronic Transaction
- Secure Multipurpose Internet Mail Extension (SMIME)

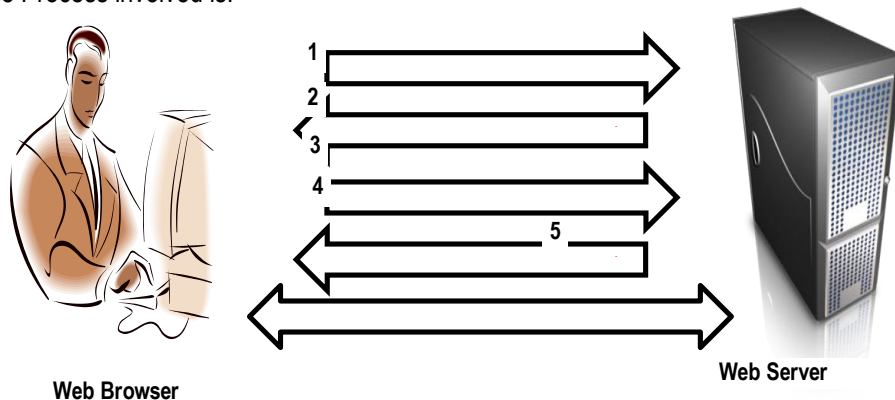
4.2.1 Secure Socket Layer (SSL) / Transport Layer Security (TLS)

The Secure Socket Layer (SSL) and Transport Layer Security (TLS) is the most widely deployed security protocol used today. SSL was first developed by Netscape and subsequently became Internet standard known as TLS (Transport Layer Security). The main differences between SSL and TLS are technical in terms of the generation of key material.

SSL/TLS are essentially protocols that provide a secure channel between two machines operating over the Internet or an internal network. In today's Internet focused world, the SSL protocol is typically used when a web browser has to securely connect to a web server over the inherently insecure Internet. SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely.

Any program using TCP can be modified to use SSL connection. SSL is flexible in choice of symmetric encryption, message digest, and authentication mechanism that can be used. SSL provides built in data compression.

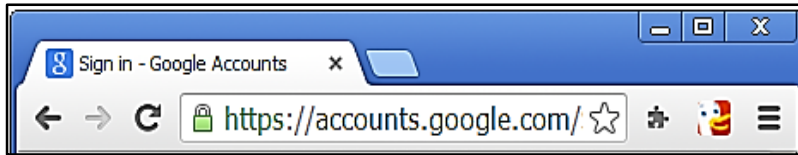
The Process involved is:



1. Browser connects to a web server (website) secured with SSL. Browser requests that the server identify itself.
2. Server sends a copy of its SSL Certificate, including the server's public key.
3. Browser checks the certificate root against a list of trusted CAs and to verify that the certificate is unexpired, unrevoked, and that its common name is valid for the website that it is connecting to. If the browser trusts the certificate, it creates, encrypts, and sends back a symmetric session key using the server's public key.
4. Server decrypts the symmetric session key using its private key and sends back an acknowledgement encrypted with the session key to start the encrypted session.
5. Server and Browser now encrypt all transmitted data with the session key.

Technically, SSL is a transparent protocol which requires little interaction from the end user when establishing a secure session. In the case of a browser for instance, users are alerted to the

presence of SSL when the browser displays a padlock. This is the key to the success of SSL – it is an incredibly simple experience for end users.



Almost any service on the Internet can be protected with SSL. SSL is being used for

- Secure online credit card transactions.
- Secure system logins and any sensitive information exchanged online e.g. secure Internet Banking session
- Secure cloud-based computing platforms.
- Secure the connection between E-mail Client and E-mail Server.
- Secure the transfer of files over https and FTP(s) services.
- Secure intranet based traffic such as internal networks, file sharing, extranets, and database connections.

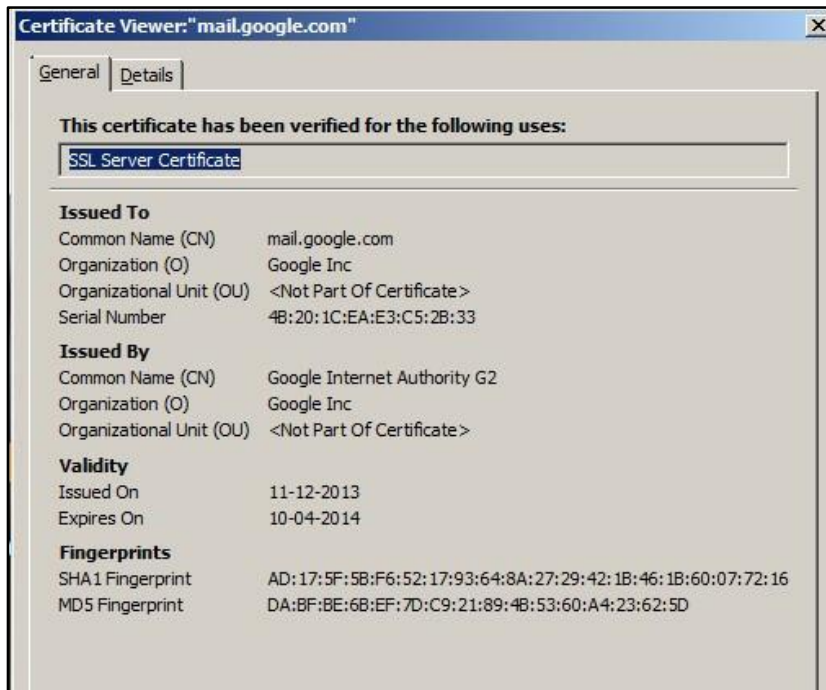
4.2.2 Hyper Text Transfer Protocol Secure (Https)

As the use of web based content and applications grow, many of them mission critical and confidential, the enterprises face mounting challenges to protect these web sites as well to provide access to it in a secured mode. This is enabled through the use of an encrypted transport mechanism, HTTPS. The secure access is required for applications ranging from database, ERP, and finance to collaboration software, such as SharePoint and WebEx.

Hyper Text Transfer Protocol over Secure Sockets Layer (HTTPS) is a secure version of the Hyper Text Transfer Protocol (http). It provides an encrypted transmission session between a Web Server and a Browser Client. HTTPS allows secure ecommerce transactions, such as online banking.

Secure HTTPS URLs begin with "https://" and uses port 443 by default.

Server verification is accomplished by providing web servers with a digitally signed certificate from a trusted Certificate Authority (CA) and then presented to the end user. Similarly, user authentication is also provided by allocating digitally signed certificates to each user, and is presented only when mutual authentication is required.



One of the limitations of HTTPS is that it slows down the web services.

4.2.3 Internet Protocol Security (IPSEC)

Virtual Private Networks (VPN)

VPNs connect private networks through untrusted networks like the Internet; they establish a tunnel and use strong encryption to provide privacy and strong authentication to guarantee identity, so they are more secure than traditional networks. The VPN can link two networks or two individual systems. It can link clients, servers, routers, firewalls, and switches. The individual networks could be private networks or the Internet. VPN provides confidentiality and integrity over insecure or untrusted intermediate networks. IPsec enables VPN and creates a virtual tunnel with encryption to ensure secure communication.

IPSec

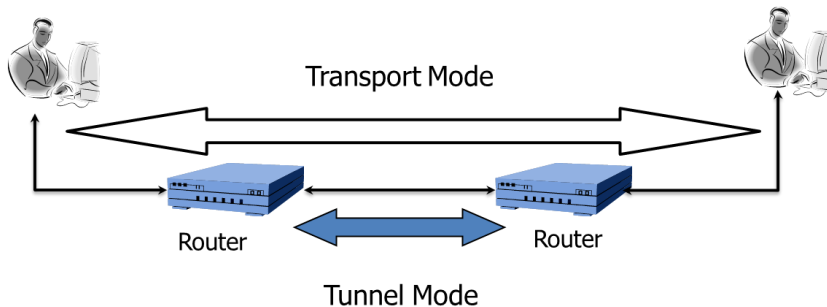
IPsec is encryption at IP (network layer); it protects any application data across IP Network. That is the reason applications need not be specifically designed for use of IPsec. IPsec is a framework for a set of protocols for security. IPsec is useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers. IPsec is implemented at end routers/firewalls.

Goals of IPsec are:

- To verify sources of IP packets--*authentication*
- To protect integrity and/or confidentiality of packets--*data Integrity/Data Encryption*

IPsec operates in two modes:

- Transport mode (for end-to-end) provides secure connection between two end points. In this mode data is encrypted but the header of the packet is not encrypted
- Tunnel mode (for VPN): With tunnel mode, the entire IP packet is encrypted and a new header is added to the packet for transmission through the VPN tunnel.



4.2.4 Secure Shell (SSH)

SSH is an end-to-end encryption technique. SSH is a protocol for secure remote login and to execute commands over an insecure network.

When we sit at a computer, everything we type goes directly to the shell. Whenever logging to a remote host telnet goes across the network to simulate the same thing. Whatever we type is picked up, sent across the network, and sent to the shell on the remote machine. But Telnet is plaintext, so anyone watching the network will see exactly what we type, including things that we don't even see on the screen (like passwords).

SSH has the same basic concept as Telnet, it takes what we type and sends it across the network to a shell on the remote computer. SSH is encrypted.

Secure Shell, SSH, is Telnet + SSL + other features.

SSH is usually used for UNIX systems and encrypts the commands getting transmitted. It works in a client server mode and both ends of the client/server connection are authenticated using digital certificates.

4.2.5 Secure Electronic Transaction (SET)

SET was originally developed by Master and Visa cards for secured electronic transactions. SET uses a system of Dual Signature. Purpose of the dual signature is to link two messages that are intended for two different recipients. In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank. The merchant does not need to know the customer's credit-card number, and the bank does not need to know the details of the customer's order. The customer is afforded extra protection in terms of privacy by keeping these two items separate. However, the two items must be linked in a way that can be used to resolve disputes if necessary. The link is needed so that the customer can prove that this payment is intended for this order and not for some other goods or service.

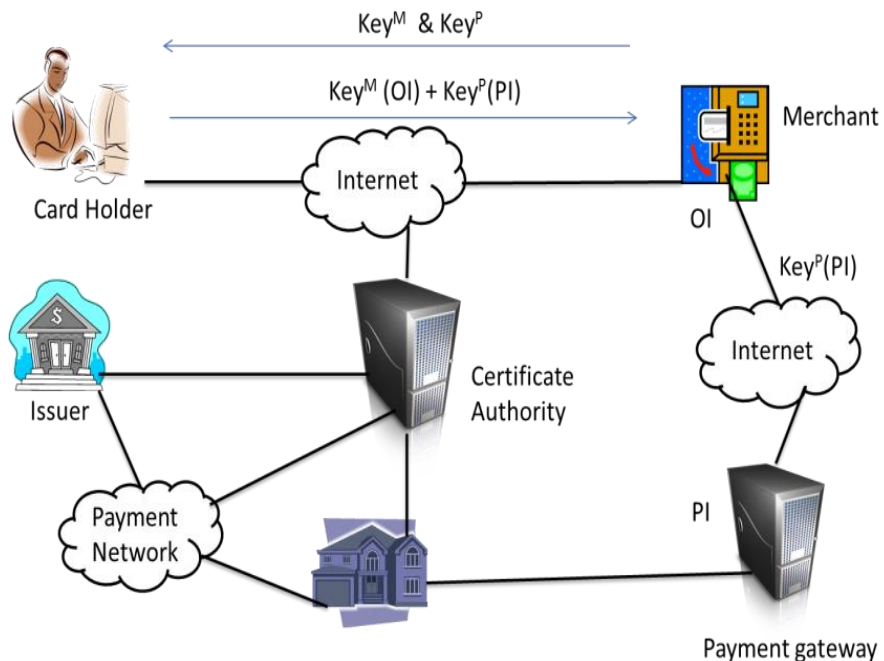
SET uses combination of RSA public key cryptography and DES private key cryptography and digital certificates to secure electronic transactions. SET provides a secure communications channel among all the parties involved in a transaction: Customer, Seller, Customer's credit provider, Seller's bank. It provides trust by the use of X.509v3 certificates.

The SET process

1. Customer opens account with Credit Company or bank.
2. Bank issues Certificate to the Customer with RSA Keys.
3. Merchant has two certificates, signing and key exchange.
4. Customer places an order.
5. The Merchant sends the customer his public key and a copy of his certificate so that the customer can verify that it's a valid store.
6. The Customer sends Order Information (OI) encrypted with Merchant's public key so the Merchant can read it, and Payment Information (PI) encrypted with Payment Gateway's Public Key so the Merchant cannot read it.
7. Merchant requests payment by sending PI to the "Payment Gateway" (who can decrypt it) and verifies Customer's credit.
8. Merchant confirms the order to the Customer.
9. Merchant ships goods to Customer.
10. Merchant sends request for payment to the Payment Gateway which handles transfer of funds.

The Dual signature allows proof that:

- Merchant has received Order Information (OI).
- Bank has received Payment Information (PI) and verified the Customer Digital signature.
- Customer has linked OI and PI and can prove later that PI was not related to a different purchase.



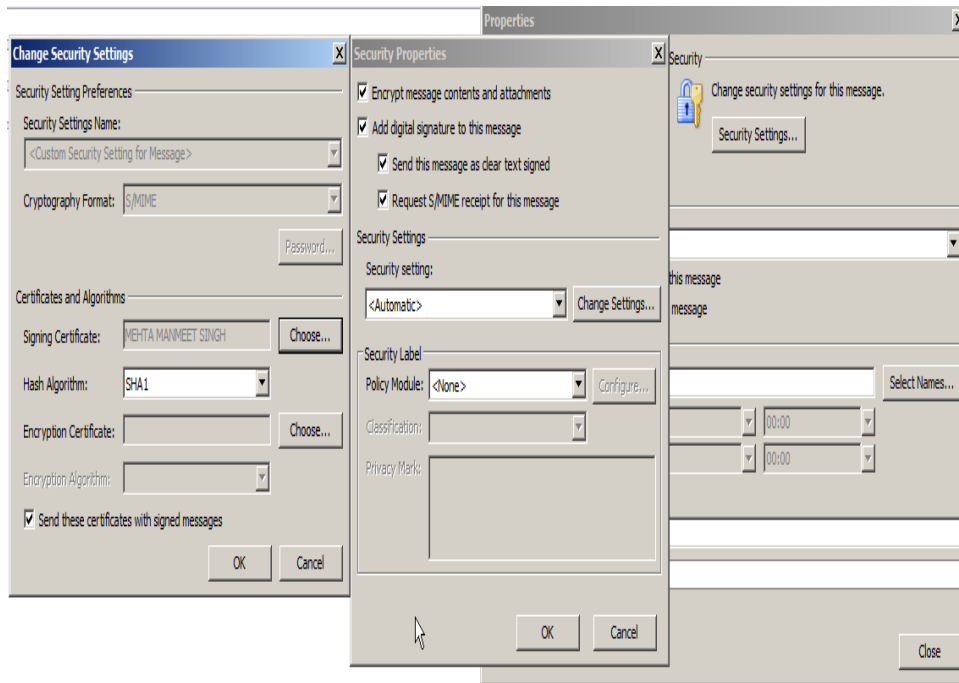
4.2.6 Secure Multipurpose Internet Mail Extension (SMIME)

A conventional email message suffers various security issues, we cannot be sure that the sender is who they claim to be; or that the message text has not been tampered with. Email text itself is not generally encrypted, meaning that if someone hacks access to our inbox, they can view our messages. S/MIME (Secure Multi-Purpose Internet Mail Extensions) is a secure method of sending e-mail and attachments that uses the RSA encryption system.

The S/MIME standard is based on public-key cryptography. In this specification, an individual user owns a digital certificate which contains a public key and a private key. The private key is held only by its owner; the public key is shared with contacts. With the keys in place, we can use our email client to attach a digital signature to outgoing emails, or to encrypt the content of an email, or both.

In Outlook Go to Message > Option > other options> Properties> Security Settings

In security settings, we have the option to add digital signatures which can be done through Change settings and choosing a digital signature.



4.3 Generic Enterprise-Wide Network Architecture in a Bank

The networking technologies have provided a platform to the banks to develop customer-centric products and services. The absorption of technology has been a major differentiator among the banks in positioning them as market leaders in meeting customer aspirations. Banks have been toying with different deployment models of networking to work as an enabler for service delivery. Any organisation-wide technology deployment strategy will depend upon the following factors

1. **Business focus** – the services, the committed delivery time and the point of service delivery. In the case of a bank, the services would comprise of front end services supported with back-end processes.

Front End Services

- Retail Banking Services,
- Portfolio Management and Investment Services
- Insurance Products
- Cash Management Services
- Foreign Trade Services.

Back-end processes - Reconciliation, Customer account management, clearing and settlements, Treasury operations, Loans origination and sanction etc.

2. **Risk Management Requirements** – Technological processes should adequately protect the bank from
 - Operational Risk
 - Systemic Risk
 - Credit Risk
 - Liquidity Risk
 - Market Risk etc.
3. **Governance and Compliance requirements** – Systems should meet regulatory requirements pertaining to
 - Financial Control
 - Audit
 - Reporting

The applications which are not a part of Core Banking solution are integrated to it. Once a network is in place, it is also used for other products and services, like

- Hosting Web portal, Intranet portal, email services etc.
- Data Warehouse, HRM, CRM solutions etc.
- Bill payments, transacting govt. business etc.,

The network is also used for Mobile Banking, SMS delivery, Phone Banking, etc. which need to be well integrated providing a seamless experience to customers of different segments and lines of business. The network architectural design has to be such that from technology perspective – the availability, scalability, resiliency and survivability issues are properly addressed. The network should also deliver, as per the management commitments, well-performing applications and services amongst varying network conditions and costs.

Layers of network architecture in a Bank: The architecture of an enterprise wide network in a bank would have the following layers,

I. The WAN Network Topology

There are broad two types of WAN topologies,

- (1) Centralised Aggregation of Network Traffic - All branches' network connections converge directly at the Data Centre/DR Centre.
- (2) Decentralised Aggregation of Network Traffic - The branches' network connections converge at regional aggregation points and these intermediate aggregation points converge at the DC and the DRC.

In view of difficulty in managing the de-centralised environment, most of the banks prefer the centralised approach. As the networks are now being used more and more for data, voice and video, the MPLS (multi-protocol label switching) technology supported networks set up by various service providers are extensively being used as the back-bone. MPLS has the advantage of

providing high availability, economics of scale and flexibility of implementing QoS (Quality of Service) for managing different types of traffic.

The back-bone is provided by the service provider which is usually optical fiber with redundant routes. These are central conduits designed to transfer network traffic at high speeds, and are designed to maximize the reliability and performance of large-scale, long-distance data communications.

The last mile primary links, in most cases, are the leased lines backed up with secondary link – normally ISDN, Wi-Fi or satellite link. The last mile connects the branch/office to the nearby POP (Point of Presence) of the Service Provider.

The DC and the DRC are in different seismic zones so that, in case of an earthquake, both of them are not impacted simultaneously. The bank may have in addition to DC and DRC, a nearby DC. This is to curtail the data loss for mission critical applications. Normally banks have separate Nearby DC at a location within 20-30 KMs of the DC. The RPO (Recovery point objective) and the RTO (Recovery time objective) determine the need for a nearby Data Centre. The Near-site DC is connected over point to point redundant links with DC through two or more different service providers for zero data loss. The DC and DR are connected to the WAN cloud (MPLS) through primary (active) and the secondary (redundant) links by using different routers working in High Availability mode. The DC and DR are connected through redundant replication links.

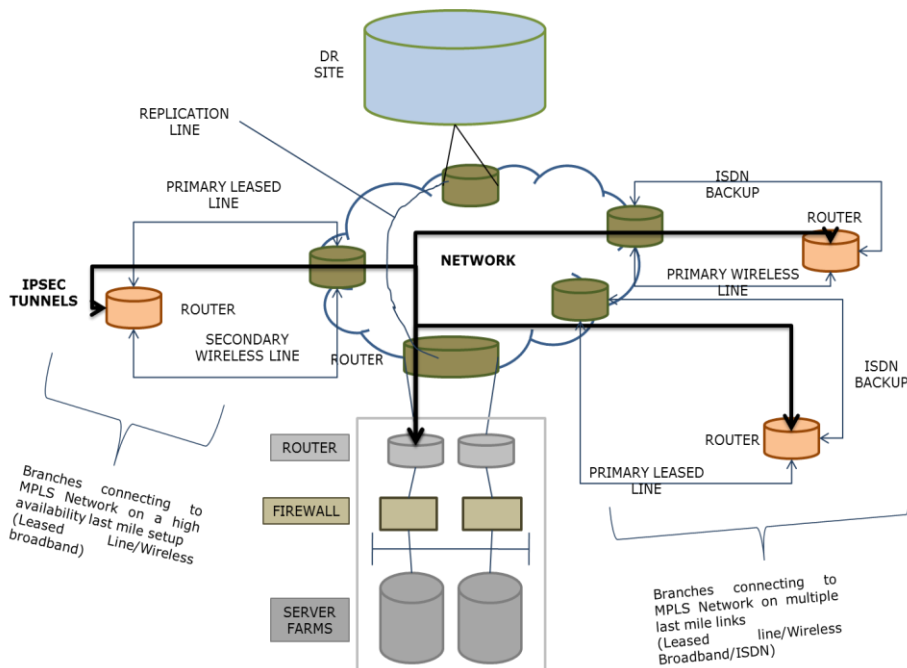
Therefore, when the production site fails, the nearby data center would contain all transactions that were executed up to the time of the outage. The Near Data Center is linked to both the DC site and the DR site through redundant links. In the event of a DC failure the backup site brings its database up-to-date by establishing a session with the Near Data Center.

II. Security

The private and public domain servers and other assets are hosted in DC, DR and near-site DC in different demilitarized zones (DMZ). The DMZs are created through sets of firewalls and VLANs implemented over multiple layer 2 switches.

All data to and from the WAN to branches and DC, DRC and near DC site is encrypted. Similarly, layers of security is implemented over all secured assets through firewalls, intrusion detection and prevention systems, database activity monitoring tools, anti-virus solutions, end-point security tools, access control systems etc. Application servers that need to be directly accessed from the Internet are placed in the DMZ between the Internet and the internal enterprise network, which allows internal hosts and Internet hosts to communicate with servers in the DMZ.

In order to have an access to internet, a minimum of two links from two different Internet Service Providers (ISPs) are commissioned at DC. This ISP level redundancy is built at DC, so that in case if one of the links/ISP is not available, then the Internet facing Servers at DC should be accessible using the second link from the other ISP. Redundant internet links are also provided at the DR.



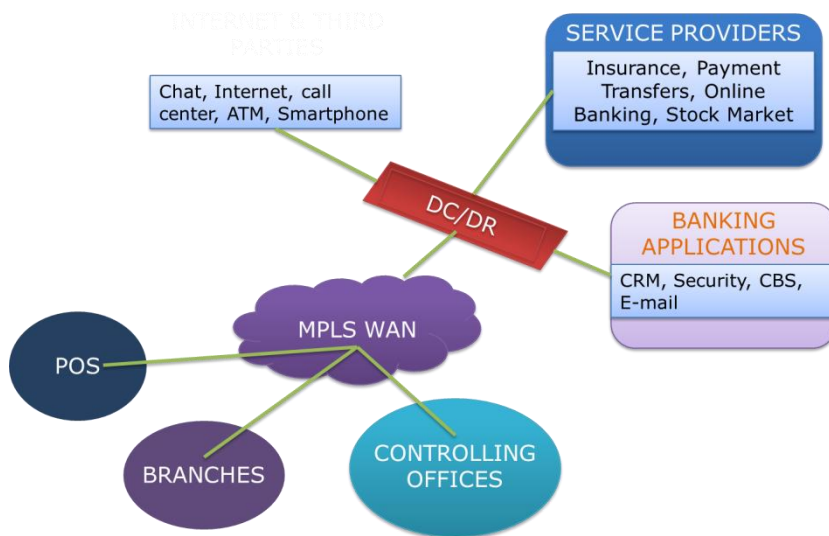
III. Interface to service delivery Channels and Internet

All the banks' WANs are connected to INFINET, the Indian Financial Network, which is the communication backbone for the National Payments System, which caters mainly to inter-bank applications like RTGS, Government Transactions, Automatic Clearing House, CTS etc.

The banks' WAN networks are also interfaced with the following external networks where ever required:

- NPCI(National Payments Corporation of India, ATM(Automatic Teller Machine) Switch
- SWIFT (Society for Worldwide Interbank Financial Telecommunication)
- Credit and Debit Card Agency
- Utility service network like telephone companies, mobile companies, electricity companies, water department etc.,
- Government Tax Departments and regulatory offices if required

A generic pictorial depiction of banking services over the WAN is given here.



Also the WAN has a point to point connectivity

- Mobile operators' network for SMS and phone banking services,
- Financial Inclusion service provider's network. Normally, the bank officials using financial inclusion application access the CBS from their endpoint through a VPN for authorisations of account openings, loan sanctioning etc. in the financial inclusion.

4.4 Risks and Controls in Network Environment

Enterprise networks are subject to a number of risks in terms of loss of privacy, confidentiality, integrity, availability and breaches of statutory or regulatory compliances. There could be a number of risks. Hacked network devices could result in data interception which could be analysed, altered, or deleted, User passwords can be compromised, Device configurations can be changed; Denial-of-service attacks could be initiated; the list is endless.

To mitigate these risks we need controls to ensure:

- Controlled Access - knowing who is on the network (authentication), what resources they are authorised to use, and applying these access controls to their traffic.
- Integrity - guaranteeing that the network itself is available as a business critical resource and that threat can be identified and mitigated. Maintain integrity of important information
- Privacy - ensuring that traffic on the network is not accessible to unauthorised users.
- Keep assets available - operational and protected from vandalism and other outages

4.5 Securing Enterprise Network

Components of Network Security include Firewalls, Intrusion Detection and Prevention Systems (IDS/IPS), DMZ, Encryption, Hashing Passwords, VPN, Antivirus software, anti-spyware programs, hierarchical passwords, and biometric verification, physical protection, Logging, Auditing and comprehensive and ongoing personnel training. Network security should be multi-layered with many different techniques used to protect the network. To limit damage, it is important to have modular architecture and security has to be implemented at all levels:

- Securing Internet connections with Firewalls, Authentication, Authorisations, Physical Security, Defining and hardening any egress or ingress points of Networks, using VPNs, SSL
- Implementing Perimeter firewall - Proper configurations
- Securing Public servers and e-commerce servers with firewalls, placing in DMZs, using reliable OS with updated patches, Anti-Virus, only required services should run on Front end servers.
- Securing Remote access networks with VPN, Authentication, Encryption, One Time Passwords.
- Securing Network devices, each device hardened against possible intrusions, Access control to devices through Authentication, using secure protocols.
- Securing Server farms using authentication, Intrusion Detection Systems (IDS), patching known OS Vulnerabilities, implementing Firewalls.
- Securing User services with security policy, personal firewalls, Anti-virus Software.
- Securing Wireless networks with firewalls, encrypted protocols and VPN.

Some key factors

- Create internal segregation to further compartmentalize traffic and access.
- Centralised network management with control and reporting facilities
- Network security policy definition and management for all software and devices

4.6 Auditing Networks

Review network security and infrastructure

- Assessing the Network design analysis and network diagram to verify that the
 - Networks are secured.
 - Access to Networks is in accordance with Network Policy of the organisation.
 - Proper Segregation in networks is in place

Review firewall capabilities and reliability

- Auditing Network firewalls, whether properly configured
- Proper Routing controls are implemented for networks.

- For monitoring internal network traffic, Intrusion Detection Systems are in place.

Please refer to Chapter-6 of Module-4 for understanding details of network security.

4.7 Summary

Cryptographic systems provide ability of secure communication over networks. Many Secure protocols and frameworks have application of cryptographic techniques like SSL, HTTPS, IPsec, SSH, SET and S-MIME to name a few. Generic Enterprise Network Architecture in a bank gave us an understanding of how network is implemented in typical bank. To mitigate the risks in an enterprise network, we need to secure networks by implementing adequate controls. Effectiveness of controls can be gauged through Auditing.

4.8 References

- <http://resources.infosecinstitute.com/role-of-cryptography/>
- <http://en.wikibooks.org/wiki/Cryptography>
- <http://www.moserware.com/2009/06/first-few-milliseconds-of-https.html>
- http://www.di-mgt.com.au/rsa_alg.html#simpleexample

Module-1

(Overview of eLearning and IT Enabled Services) Primer on Information Technology, IS Infrastructure and Emerging Technologies

TABLE OF CONTENTS

MODULE 1: PRIMER ON INFORMATION TECHNOLOGY, IS INFRASTRUCTURE AND EMERGING TECHNOLOGIES (6%)-Facilitated E-Learning	231
SECTION 1: OVERVIEW	231
Objective:	231
Task Statements.....	231
Knowledge Statements (Knowledge of)	231
Relationship between Task and knowledge statements	231
Knowledge Statement Reference Guide	232
SECTION 2: CONTENTS	233
Chapter 1: Overview of E-Learning and FAQs	233
Part 1: Overview of E-Learning.....	233
1.1 Introduction.....	233
1.2 Components of IT Infrastructure	233
1.2.1 Hardware	233
1.2.2 Software	234
1.2.3 Database Management Systems	235
1.3 Deployment of IT Infrastructure.....	235
1.4 Computer Networks	236
1.5 Network Standards.....	236
1.6 IP Networks	237
1.7 Securing Networks.....	238
1.7.1 Firewalls.....	238
1.7.2 Personal Firewalls	238
1.7.3 Intrusion Detection Systems (IDS).....	239
1.8 Cryptography	239
Cryptographic Applications	240
1.9 Summary.....	240
Part 2: FAQs of E-Learning.....	241
1. What is Hardware?.....	241

2. What is Cache Memory?	241
3. What is Virtual Memory?.....	242
4. What is Capacity planning?	242
5. What is Operating System?.....	242
6. What are Kernel and Shell?	243
7. What is a Database Management System?	243
8. What is a Relational Database Management System?	244
9. What is Hardening of system?	244
10. What is Bus Topology?	245
11. What is Client Server Architecture?	245
12. What is a Router?	245
13. What is a Network Protocol?	246
14. What is a Physical Address?	246
15. What is TCP/IP?	246
16. What is an IP Address?.....	247
17. Which is the fastest firewall?.....	247
18. Which type of firewall provides best security for data centres?	248
19. What is an IDS?	249
20. What is Cryptography?	250
21. What is a digital signature?	250
22. Who are Certifying Authorities?	250
23. What is a CRL?	251
24. What is SSL/TLS?	251
25. What is S/MIME?	251
Chapter 2: IT Enabled Services and Emerging Technologies	253
Part 1: IT Assurance Services and Role of CAs in BPO-KPO.....	253
Learning Objectives.....	253
1.1 Introduction.....	253
1.2 Opportunities for CAs.....	254

1.3	IT Consulting and Assurance Services by CAs	255
1.3.1	Using COBIT for providing IT-enabled services.....	255
1.	Set and maintain the IT Governance Framework.....	255
2.	Define IT Strategy Planning	256
3.	Manage Risk	256
4.	Review IT Security Management.....	257
5.	Compliance with external requirements	257
6.	Manage Continuity	257
1.4	Business Process Outsourcing	258
1.4.1	Knowledge Processing Outsourcing	258
1.4.2	Medical Transcription	259
1.4.3	Legal Transcription.....	259
1.4.4	Data Entry and data processing	259
1.4.5	IT Help-desk support.....	260
1.4.6	Application development.....	260
1.4.7	Risks and Controls of outsourced services	260
	Risks	260
	Controls	261
1.5	Using global best practices	261
1.5.1	Compliance with external requirements:.....	261
1.5.2	Managing Business Continuity	262
1.6	Summary.....	263
1.7	References	263
1.8	Questions	263
1.9	Answers	264
	Part 2: Emerging Technologies: BI, Data Warehouse, ERP and E-Commerce.....	265
	Learning Objectives.....	265
2.1	Introduction.....	265
2.2	Business Intelligence	265
2.2.1	Key BI tools and techniques.....	266

2.3	Data Warehouse	267
2.3.1	Data Mart.....	267
2.3.2	Need for a Data Warehouse.....	268
2.3.3	Risks and Controls Associated with Data Warehouse	269
	Controls Related To Data Warehouse.....	270
2.4	Data Mining	270
2.4.1	Practical Applications	271
2.5	Enterprise Resource Planning (ERP).....	271
2.5.1	Benefits of ERP:	272
2.5.2	Challenges of ERP	272
2.5.3	Security concerns in ERP	273
2.5.4	Opportunities for CAs in ERP	273
	CAs role during pre-implementation	274
	CAs role during implementation	274
	CAs role during post implementation	275
2.6	E-Commerce.....	276
2.6.1	E-Commerce Models	276
2.6.2	Components of E-Commerce.....	277
2.6.3	Electronic Funds Transfer	277
2.6.4	Risk in E-Commerce	278
	Controls in E-Commerce	278
	CAs role in E-Commerce.....	278
2.7	Summary.....	278
2.8	References	279
2.9	Questions	279
2.10	Answers	280
Chapter 3: Overview of Cloud Computing and Mobile Clouding: Challenges and Opportunities for CAs		281
Part 1: Cloud and Mobile Computing.....		281
Learning Objectives.....		281

1.1	Introduction.....	281
1.2	Cloud Computing	282
1.2.1	Understanding Cloud Computing.....	282
1.2.2	Characteristics of Cloud Computing	282
1.2.3	Features of Cloud Computing	282
1.2.4	Types of Cloud Computing.....	283
1.2.5	Cloud Service Models.....	283
1.2.6	Benefits and risks in Cloud Computing.....	284
	Benefits.....	284
	Risks	285
1.2.7	Impact of Cloud Computing on CAs	285
	Assurance Services in Cloud Computing	285
	Consulting In Cloud Computing	286
1.3	Mobile Computing.....	287
1.3.1	Technology Components.....	287
	1. Mobile communication.....	287
	2. Mobile hardware	287
	3. Mobile software.....	287
1.3.2	Advantages and Security Concerns of Mobile Computing.....	288
	Advantages of Mobile Computing	288
	Security Issues in Mobile Computing.....	288
	Controls in Mobile Computing	288
1.3.3	Opportunities for CAs	289
	Using Mobile computing in CA firm:.....	289
	Consulting on mobile technology implementation:	289
	Assurance services on Mobile technology implementation.....	289
1.4	Summary.....	290
1.5	References	290
1.6	Questions	290
1.7	Answers	291

Part 2: Emerging Technologies: BYOD, XML-XBRL and Social Media	293
Learning Objectives.....	293
2.1 Introduction.....	293
2.2 Bring Your Own Device (BYOD).....	293
2.2.1 Advantages of BYOD.....	293
2.2.2 Security Concerns of BYOD	294
2.2.3 Controls Relating To BYOD	294
2.2.4 Opportunities for CAs.....	295
2.3 XML-XBRL	295
2.3.1 XML.....	295
What is XML?	295
Why to use XML?.....	296
How is XML used?	296
Where is XML used?	296
Who is using XML?	297
Risks of using XML	297
Controls in XML.....	297
2.3.2 XBRL	297
Use of XBRL in financial sector.....	298
Advantages of XBRL	298
How is XBRL used?	299
Risks in XBRL	300
Controls in XBRL.....	300
Impact and avenues for CAs	300
2.4 Use of Social Media	301
2.4.1 Risks and Security Concerns in Use of Social Media.....	301
2.4.2 Mitigating Security Concerns	302
2.4.3 Opportunities for CAs	302
2.5 Geolocation.....	303
2.5.1 Benefits of Geolocation.....	304

2.5.2 Risks and security of Geolocation	304
2.5 Summary.....	305
2.6 References	305
2.7 Questions	305
2.8 Answers	306
Chapter 4: Overview of Business Information Systems and Risk and Controls in Newer Technologies	307
Part 1: Business Information Systems.....	307
Learning Objectives.....	307
1.1 Introduction.....	307
1.2 Artificial Intelligence	308
1.2.1 Expert Systems	309
The Brain Computer Interface	309
1.3 Transaction Processing Systems (TPS).....	309
Transaction Processing Methods.....	310
1.4 Decision Support Systems	311
DSS Characteristics	312
DSS advantages	312
DSS Implementation.....	313
Capabilities of DSS	313
DSS Components	313
Challenges and Risk Factors in DSS.....	313
1.5 Executive Support Systems (ESS)	314
Characteristics of ESS	315
Advantages.....	316
Disadvantages	316
1.6 Big Data.....	316
Why to use Big Data?	317
Where is Big Data used?	317
How does Big Data work?	318

Challenges with Big Data	318
Risks with Big Data	319
Controls with Big Data	319
1.7 Summary.....	320
1.8 References	320
1.9 Questions	320
1.10 Answers	321
Part 2: Emerging Technologies: Risks, Control and Audit	323
Learning Objectives.....	323
2.1 Introduction.....	323
2.2 Green IT.....	323
How to implement Green IT?	324
Using Technology to help solve environmental issues	325
CAs role in Green IT	325
2.3 Web 2.0.....	325
Features of web 2.0	326
Use of Web 2.0	326
Security concerns in Web 2.0	327
Controls in Web 2.0	327
2.4 Some more emerging Technology Trends.....	327
The Internet of Everything: Web of Everything	327
3-D Printing.....	328
Smart Machines	328
2.5 Risks, Controls and assurance in emerging technology	328
Role of CAs in Governance and management of emerging technology:	329
Human Resource Management	330
Security	330
Compliance.....	330
2.6 Summary.....	331
2.7 References	331

2.9	Questions	331
2.10	Answers	332

MODULE 1: PRIMER ON INFORMATION TECHNOLOGY, IS INFRASTRUCTURE AND EMERGING TECHNOLOGIES (6%)-FACILITATED E-LEARNING

SECTION 1: OVERVIEW

Objective:

Demonstrate understanding of functioning of key components of existing and emerging Information Technologies and their practical deployment.

Task Statements

1.6 Consider the impact of deployment of key existing and emerging technologies such as: XML, BURL, Cloud computing, Geo Location, Mobile computing, Social media, Bring Your Own Device (BYOD), Business Intelligence (BI), Big Data, Network Technologies – Web Services, Web 2.0, Data warehouse, Data Mining, Data Mart, Decision Support Systems (DSS), Executive Support Systems (ESS), Artificial Intelligence (AI), Electronic Funds Transfer (EFT), Electronic Transactions and Green IT.

Knowledge Statements (Knowledge of)

1.8 Functioning and impact of key emerging technologies such as: XML, XBRL, Cloud computing, Geo Location, Mobile computing, Social media, BYOD, BI, Big Data, Network Technologies – web services, Web 2.0, Data warehouse, Data Mining, Data Mart, DSS, ESS, AI, EFT, Electronic Transactions and Green IT

Relationship between Task and knowledge statements

The task statements are what the DISA Candidate is expected to know how to perform. The knowledge statements delineate each of the areas in which a DISA candidate must have a good understanding in order to perform the tasks. The task and knowledge statements are mapped in the chart below. Please note that although there is often overlap, each task statement will generally map to several knowledge statements.

Task Statements	Knowledge Statements
1.6 Consider the impact of deployment of key existing and emerging technologies such as: XML, XBRL, Cloud computing, Geo Location, Mobile	1.8 Functioning and impact of key emerging technologies such as: XML, XBRL, Cloud computing, Geo Location, Mobile

computing, Social media, Bring Your Own Device (BYOD), Business Intelligence (BI), Big Data, Network Technologies – web services, Web 2.0, Data warehouse, Data Mining, Data Mart, Decision Support Systems (DSS), Executive Support Systems (ESS), Artificial Intelligence (AI), Electronic Funds Transfer (EFT), Electronic Transactions, Green IT etc.	computing, Social media, BYOD, BI, Big Data, Network Technologies – web services, Web 2.0, Data warehouse, Data Mining, Data Mart, DSS, ESS, AI, EFT, Electronic Transactions, Green IT etc.

Knowledge Statement Reference Guide

Each knowledge statement is explained in terms of underlying concepts and relevance of the knowledge statement to the DISA Candidate. It is essential that the candidate understand these concepts. The knowledge statements are what the IS Auditor must know in order to accomplish the tasks. Consequently, only the knowledge statements are detailed in this section. The sections identified in the matrices are described in greater detail in the various chapters of this module.

Knowledge area	Reference
1.8 XML, XBRL, Cloud computing, Geo Location, Mobile computing, Social media, BYOD, BI, Big Data, Network Technologies – web services, Web 2.0, Data warehouse, Data Mining, Data Mart, DSS, ESS, AI, EFT, Electronic Transactions, Green IT, etc.	Chapters 2 to 4

SECTION 2: CONTENTS

CHAPTER 1: OVERVIEW OF E-LEARNING AND FAQS

PART 1: OVERVIEW OF E-LEARNING

1.1 Introduction

The eLearning module covered 12% and is expected to have been completed before studying this section of facilitated eLearning. The objective of this section is to ensure that DISA can “**demonstrate understanding of functioning of key components of existing and emerging Information Technologies and their practical deployment**”. This section has 4 chapters with each chapter divided into 2 parts. The first part of the first chapter covers overview of eLearning and the second part covers FAQs related to eLearning. The objective of this chapter is to supplement the self-study of eLearning contents and help clarify any doubts on any of these topics. The chapters 2 to 4 cover various topics relating to existing and emerging technology which have critical impact on chartered accountants. The coverage of this module is 6% and will be covered in one day of classroom teaching. The objective of this section is to provide good understanding of Information Technology concepts which is very essential for providing consulting and assurance services in IT driven business processes.

1.2 Components of IT Infrastructure

1.2.1 Hardware

Information technology is an integral part of a modern enterprise. For any enterprise to survive and grow adoption of Information Systems (IS) is essential. The basic infrastructure of Information Systems is provided by Information Technology components such as hardware, system software, Database Management systems (DBMS), networking, application Software and office automation software.

Hardware is one of the most important components of IT. This includes input, output, processing and storage devices. Input and output devices also known as peripherals help in input and output functions, CPU or Central Processing Unit comprising of CU, ALU and registers aid in processing of computer instructions catering to the needs of the users. Programs and data can be stored on storage devices. Secondary storage differs from primary storage in that it is not directly accessible by the CPU. It is important to understand hardware since it performs the important role of managing capacities for effective and efficient working of an enterprise. The monitoring of computing capacity is also essential to ensure that the business requirements are appropriately met. Capacity planning

also ensures that the expansion or reduction of resources takes place in tune with the overall organisational growth or reduction. Hardware asset management is an important function in any organisation using hardware for meeting its goals. It includes management of all the phases such as hardware asset acquisition, hardware maintenance, hardware monitoring and retirement.

1.2.2 Software

Computer hardware constitutes the physical components. It works based on the instruction input given by the users and other programs. Such a set of instruction input is actually its software. The term software in its broad sense refers to the program that the machine executes. Software is the intangible portion whereas hardware is the tangible portion, something we can touch and see. The cost and complexity of software have been increasing over the years and it is critical to effectively manage this as it is both a major investment and major expenditure. Two important types of software are system software and application software. System software includes both operating systems and utility programs. System software controls how various technology tools work with application software. System software is a collection of computer programs used in design, processing and control of application software. System software coordinates instructions between applications and hardware.

Operating system (OS) is one of the important system software that controls how hardware devices work together and interfaces with applications software. Operating system is a set of programs implemented in software, hardware and firmware which permits sharing and use of resources. It enables users to interact with the machine and takes care of technical aspects of a computer's operation. Some important functions of OS are

- Processor management
- Memory management
- Device management
- File Management
- Secondary storage management
- Networking
- Application programme interface
- User interfaces with system

Utility Software provides additional functionality to operating systems. Application software fulfils the specific information processing needs of an organisation. Software is crucial for the success of organisations and hence has to be effectively managed. Operating systems are secured through access controls, hardening of systems and application of patches. Understanding software helps us in optimally managing our software assets through their lifecycle. Software acquisition procedures, licensing, version controls and digital rights management are some important issues which have to be considered.

1.2.3 Database Management Systems

Any organisation has to manage the important resource, information. At the very heart of most of management information systems are databases and database management systems. A database maintains information about various entities and a database management system (DBMS) is software through which users and application programs interact with a database. Databases and DBMS is the foundation of Information Economy. DBMS is a software system for creation and control of a database and manipulation of the data in the database. It provides the facility to create and maintain a well-organized database. Applications access the DBMS, which then accesses the data. The advantages of DBMS are

- Permitting data sharing
- Minimizing data redundancy
- Maintaining data integrity
- Program and file consistency
- User-friendliness
- Improved security
- Achieving program/data independence
- Faster application development

A database should be designed to store all data relevant to business to facilitate quick and easy modifications. The Relational Database Model is one of the most widely used models and is very simple and elegant. A relational database is a collection of one or more relations, where each relation is a table with rows and columns which is a logical equivalent of files. It permits the use of simple, high-level languages to query the data. Since databases allow access to one of the most critical resource of an organisation, i.e. data, the controls in it are implemented through:

- Database roles and permissions- for segregation of duties
- Concurrency control
- Views
- Stored procedures
- Triggers

DBMS is crucial for any organisation and it has to be controlled, monitored and assessed.

1.3 Deployment of IT Infrastructure

After making an IT plan it is imperative to implement the plan, the term which is used more often for this implementation is “Deployment”. Deployment in this background involves having the hardware and software up and running that includes Installation, Configuration, testing, necessary customisations, modifications and running. Some approaches like hardening of systems and configuration management are important concepts relating to deployment of IS infrastructure.

Configuration Management is one such approach which assists in control of IS assets. Configuration Management refers to relative management of parts or elements of IT components. It covers the identification of all significant components within the IT Infrastructure and recording the details of these components in the Configuration Management Database. The Configuration Management system also records relationships between these components. It provides comprehensive information about all components in the infrastructure that enable all other processes to function more effectively and efficiently.

1.4 Computer Networks

Effective and efficient communication is very vital to the management in achieving its objectives. This communication is facilitated with communication networks. Computer network is a collection of computers (servers / nodes), communication medium, software that help them to communicate and the transmission methods used in such communication, software and communication protocols. Where at least one process in one device is able to send/receive data to/from at least one process residing in another device, then the two devices are said to be in a network. A network is a group of devices connected to each other. Each component, namely the computer, printer, etc. in a computer network is called a node. Computer networks are used for exchange of data among different computers and also to share the resources.

These networks can be categorized as LAN, WANs and MANs. To have these networks up and running network devices have to be connected through some kind of media and there has to be some arrangement or physical layout of computers, cables, and other components on the network which are called topologies. Some prominent topologies are:

- Bus Topology
- Star topology
- Ring topology
- Mesh topology

Physical topology refers to the placement of the network's various components, including device location and cable installation, while logical topology shows how data flows within a network, regardless of its physical design. Knowledge of these technologies helps us in selecting a suitable Network Topology to achieve organisational objectives.

1.5 Network Standards

Different networks could have different technologies, but when we have to network these networks; problem is compounded. Understanding of these complicated systems was made easier by splitting the communication process to small portions via a reference model called OSI. The Open Systems Interconnection (OSI) model enables easy integration of various technologies and provides solutions for managing the Internetworking environment. The Open System Interconnection (OSI) Reference Model describes the concepts involved when the message or data or instruction from the sender's

computer or device moves over a range of network environments and reaches the receiver's computer or device, as the sender sent it.

A practical model or more appropriate a suite of specific network protocols is TCP/IP, around which Internet has been built. The practical model or the protocol suite which comes into play in data communication between Devices on a network is TCP/IP. TCP/IP is a set of protocols developed to allow cooperating computers to share resources across the networks. It establishes the standards and rules by which messages are sent through the networks. This model splits the job of moving information between networked computers into five smaller stages called layers; in each of these phases or layers some tasks are done. These tasks are based on certain standards or rules called protocols. TCP/IP protocol suite is a bundle of protocols that are segmented into five layers.

5. Application Layer
4. Transport layer
3. Internetworking Layer
2. Data link layer
1. Physical layer

1.6 IP Networks

IP Networks is the main strength behind Internet. An IP network is a communication network that uses Internet Protocol (IP) to send and receive messages between one or more computers. An IP network is implemented in Internet networks, local area networks (LAN) and enterprise networks. All hosts or network nodes must be configured with the TCP/IP suite and must have an IP address. A logical address is given to all hosts connected to Internet and this logical address is called Internet Protocol Address (IP Address). IP Address (IPv4) is an address which is 32-bits in length written in form of 4 Octets or Bytes separated by a dot. Example: xxx.xxx.xxx.xxx or 117.149.29.234. There are 5 Classes of IP addresses in IPv4 Class A to Class E. IP address contains information of three fields: class type, netid, and hostid.

Every IP address that is exposed to the public Internet is unique and is called Public IP Address. In contrast, IP addresses within a local network can use the same private addresses. IP addresses could again be Static or dynamic IP addresses. Ports are a 16 bit number assigned to user sessions and server applications in an IP network. Domain Name Systems help in mapping generic names of sites, like www.yahoo.com into IP addresses. Understanding of these concepts is essential today since networks like Internet are being used extensively and no enterprise can hope to exist without networks.

1.7 Securing Networks

1.7.1 Firewalls

Firewalls are an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet. Firewall may be a hardware device or a software program running on a secure host computer, or a combination of hardware and software deployed at the perimeter of the network. It enforces the security policy between an organisation's secured network and the unsecured environment and works for both inbound and outbound traffic.

The primary functions of a firewall are:

- Manage and control network traffic
- Authenticate access
- Act as an intermediary
- Protect resources
- Record and report on events

Firewalls could be based on hardware or software and they work as per following configurations:

- Packet filtering firewall
- Stateful inspection packet filtering firewall
- Circuit level firewall
- Application level firewall

For a firewall to be able to successfully protect resources, it is critical to implement a design that lends itself to protecting those resources in the most efficient manner. Although a single firewall will do an adequate job of protecting most resources, certain high security environments may warrant using multi-firewall architecture to minimize exposure and risk. From a simple packet filtering to the screened sub-netting implementations, there are various implementation strategies, as follows,

- Single homed firewalls
- Dual Homed firewalls
- Screened subnet firewalls

Like any other security device firewalls have to be properly configured and monitored.

1.7.2 Personal Firewalls

Personal firewalls are software installed in a user's computer that offers protection against unwanted intrusion and attacks coming from the Internet. A personal firewall controls network traffic to and from a computer, permitting or denying communications based on a security policy. Personal firewalls are available from numerous security vendors, and many of the operating systems include their own

Firewall. In addition to blocking unwanted incoming traffic, these firewalls can be configured to block specific types of outgoing traffic as well.

1.7.3 Intrusion Detection Systems (IDS)

IDS monitors network traffic and host logs for signs of intrusion and by providing Alerts bring potential intrusions to the attention of administrators. It only monitors and lets us know when an event has happened, but does not itself react. It has no ability to prevent any intrusions. There are broadly two types of IDS, network based (NIDS) and host based (HIDS) intrusion detection systems. Detection methods, that an IDS uses, could be Signature Based or Statistical Anomaly Based (Behaviour Based) techniques. These concepts are important to understand from the perspective of securing our networks.

1.8 Cryptography

Cryptography has gained prominence because of the need to safeguard information from falling into wrong hands. It provides solutions to problems related to protection of data and identity with regard to data in transit. Some of the issues which have to be addressed for all communications taking place over network relate to:

- Confidentiality
- Integrity
- Authentication
- Non-repudiation

Cryptography helps in addressing confidentiality related issues. Cryptography when used as an element of PKI also addresses Integrity, Authentication and non-repudiation related issues. There are in general, three types of cryptographic schemes to accomplish these goals:

- Secret Key or Symmetric Cryptography (SKC)
- Public Key or Asymmetric Cryptography (PKC)
- Message Hash Functions

PKI is a comprehensive system that provides public-key encryption and digital signature services to ensure confidentiality, access control, data integrity, authentication and non-repudiation. The basic purpose of PKI is to help in maintaining the attributes of trust in any electronic transaction. PKI includes the following elements:

- Public/private key pair
- Digital certificate
- Certifying authority

Cryptographic Applications

Cryptographic systems are techniques which use one or more forms of cryptography and/or PKI to secure electronic transmissions from threats relating to confidentiality, integrity, authentication and non-repudiation.

Some cryptographic applications are:

- **SSL/TLS** are essentially protocols that provide a secure channel between two machines operating over the Internet or an internal network.

HTTPS allows secure ecommerce transactions, such as online banking. HTTPS provides authentication of the web site and associated web server that one is communicating with. It also provides bidirectional encryption of communications between a client and server.

- **IPsec** is useful for implementing virtual private networks and for remote user access through dial-up connection to private networks.
- **S/MIME** is a secure method of sending e-mail and attachments that uses the RSA encryption system.

Enterprise networks are subject to a number of risks in terms of loss of privacy, confidentiality, integrity, availability and breaches of statutory or regulatory compliances. These risks have to be controlled. To help in building these controls we have to understand the above concepts relating to network security.

1.9 Summary

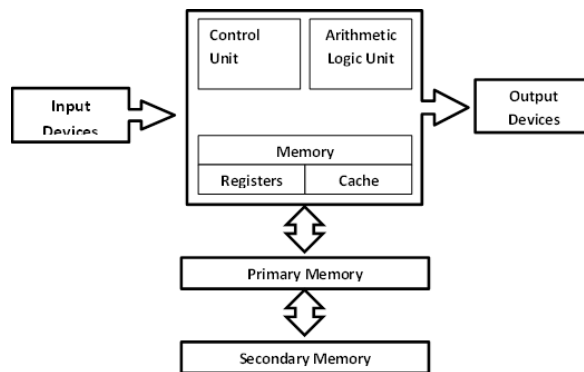
Understanding Information Technology areas is important for us to use in our working as well as providing consulting and assurance services in IT driven business processes. We have provided an overview of Information Technology Infrastructure, introduction to networks and securing networks. The key concepts covered in chapter 1 to 3 of elearning have been summarised in this chapter.

PART 2: FAQs OF E-LEARNING

Information Technology is an interesting but challenging subject. To demystify IT, answers are provided to some of the most critical FAQs relating to IT.

1. What is Hardware?

Hardware is the tangible portion of our computer systems, something we can touch and see and consists of devices that perform the functions of input, processing, data storage and output activities of the computer.



It consists of Computer peripherals (Input and Output Devices); processing devices include computer chips that contain the central processing unit and main memory, storage devices in which programs and data can be stored.

2. What is Cache Memory?

Cache memory is extremely fast memory that is built into a computer's central processing unit (CPU), or located next to it on a separate chip. The CPU uses cache memory to store instructions that are repeatedly required to run programs, improving overall system speed. The advantage of cache memory is that the CPU does not have to use the motherboard's system bus for data transfer.

There is a huge speed difference between Registers and Primary Memory, to bridge these speed differences we have cache memory. Cache (*Pronounced kash*) is a smaller, faster memory which stores copies of the data from the most frequently used main memory locations and Processor/Registers can access it more rapidly than main memory.

Cache memory is something like, we record frequently used telephone numbers in our mobile which we can access quickly otherwise we have to go to telephone directory which takes a longer time. Cache memory works on the same principle frequently used data is

stored in easily accessible cache memory instead of slower memory like RAM. Because, there is less data in cache, processor can access it more quickly.

3. What is Virtual Memory?

Virtual Memory is in fact not a separate device but an imaginary memory area supported by some operating systems (for example, Windows) in conjunction with the hardware. If a computer lacks the random access memory (RAM) needed to run a program or operation, Windows uses virtual memory to compensate. Virtual memory combines computer's RAM with temporary space on the hard disk. When RAM runs low, the control unit moves data from RAM to a space called a paging file on the hard disk. Moving data to and from the paging file frees up RAM to complete its work. Thus, Virtual memory is an allocation of hard disk space to help RAM. With virtual memory, the computer can look for areas of RAM that have not been used recently and copy them onto the hard disk. This frees up space in RAM to load the new applications

4. What is Capacity planning?

Capacity Planning is planning and monitoring of the computer resources to ensure that the available resources are being used efficiently and effectively, in terms of

- CPU utilization
- Computer Storage Utilization
- Telecommunication and Wide Area Network bandwidth utilization
- Terminal utilization
- I/O channel utilization etc.

Like every other investment in an organisation, IT investment too has to be justified on the basis of Returns on Investment (ROI). The capacity of IT resources required, such as processor power, CPU clock speed, hard disk capacity and number of terminals have to be planned meticulously with business need in mind.

5. What is Operating System?

Operating system is a set of programs implemented in software, hardware and firmware that permits sharing and use of resources. It is a set of programs which acts as intermediary agent between the user and the computer hardware. It controls and manages the computer hardware resources among various processes. Also called a Resource Manager, an Operating System helps in the efficient management of the important resources of RAM, CPU, and various I/O devices (which include secondary storage devices also) and the information that is held in the machine.

Functions of operating system are:

- Processor management
- Memory management
- Device management
- File Management
- Secondary storage management
- Networking
- Application Programme Interface
- User Interfaces with system

6. What are Kernel and Shell?

Operating System is like Glue which holds a computer together. On one side of operating system is Hardware and on other side is Application. We can primarily divide Operating system into two layers.

- Kernel Layer
 - Controls Access to Hardware
 - Schedules System resources, Memory, CPU etc.
 - Enforces Security to System Resources
 - Responds to Service Calls(How program accesses services from OS)
e.g. Accessing Hard disk, let's say that a program wants to access hard disk, it will call Kernel of OS for the same and kernel will facilitate it.
- Shell Layer
 - Surrounds kernel and provides Interface for Applications

7. What is a Database Management System?

Data Base Management Systems are software that aid in organizing, controlling and using the data needed by the application programmes. A Database Management System is a software system for creation and control of a database and manipulation of the data in the database. They provide the facility to create and maintain a well-organized database. Applications access the DBMS, which then accesses the data. Advantages of DBMS are

- Permitting Data Sharing
- Minimizing Data Redundancy
- Data integrity can be maintained
- Program and file consistency
- User-friendliness
- Improved security
- Achieving program/data independence
- Faster application development

Disadvantages are:

- Expensive
- Security is an issue: In the absence of proper safeguards in place; it may be possible for some unauthorized users to access the database.
- Single point of failure

8. What is a Relational Database Management System?

The Relational Database Model is one of the most widely used DBMS models, and is very simple and elegant. A relational database is a collection of one or more relations, where each relation is a table with rows and columns which is a logical equivalent of files. It permits the use of simple, high-level languages to query the data. This model represents the database as a collection of Relations and is governed by the following rules:

- Data is represented in a two-dimensional table, in rows and columns.
- Columns describe the attributes.
- Each column in the table has a unique name.
- All the entries in any column are of the same type or same domain.
- Each column has a domain, a set of possible values that can appear in that column.
- A row in the table is called Tuple.
- Ordering of rows and columns is insignificant.
- Duplicate rows are not allowed.
- All data items stored in the columns are atomic in nature, that is, they cannot be split further without loss of information.
- In many tables, there is a column called the Key Column whose value is unique and cannot be null.

9. What is Hardening of system?

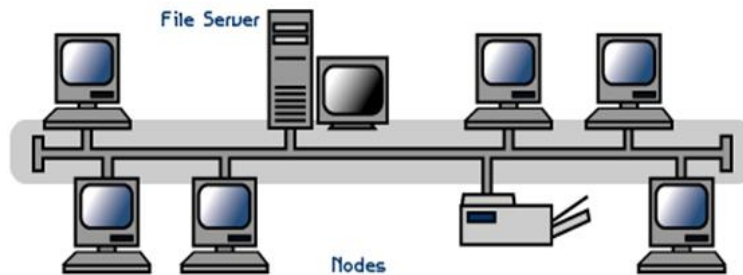
Hardening of systems is the process of securely configuring computer systems, to eliminate as many security risks as possible. There are many default settings in systems which introduce much vulnerability. Moreover, default settings may make operations easier but expose system to vulnerabilities which could compromise the system.

Hardening of system may involve, among other measures, applying patches, service packs and hotfixes; disabling unnecessary services; closing open network ports; Configuring event Log Settings.; Operating systems contain some Privileged Administrator, SuperUser or Root Accounts which have ability to access any information and Change it. Such Ids should be suitably controlled with strong passwords and should be used only for reconfiguring and software updating; configuring registry permissions etc.

10. What is Bus Topology?

The simplest topologies and most common method of networking computers is Bus Topology.

The bus topology computers are connected on a single backbone cable. Setting up a bus topology is quite easy. Bus topology can be easily extended.



The cable runs from device to device by using “tee” connectors that plug into the network adapter cards. Terminator is used at the end to stop the signal from bouncing. A device wishing to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message. Because only one computer at a time can send data on a bus network, the number of computers attached to the bus will affect network performance.

11. What is Client Server Architecture?

The Client-Server architecture separates an application into at least two processes. One process plays the role of the client, the other plays the role of the server. In this architecture, the client process requests services from server process. Client also shares the processing load of the server. Hence, the application also has to be designed to work in C/S mode.

This model is not about how computers or nodes are connected but more about processes or computational logic being split, i.e. there are Client processes which typically request for information and there are server processes which take request for information gather that information and send it to client. Thus it is not about hardware it is about Applications and their processes.

This is the prominent model used in Internet.

12. What is a Router?

Routers are networking devices used to extend or segment networks by forwarding packets from one logical network to another. A router can be a dedicated hardware device or a computer system with more than one network interface and the appropriate routing

software. Routers contain internal tables of information called routing tables that keep track of all known network addresses and possible paths throughout the Internetwork, along with number of hops of reaching each network. Routers use IP addresses for routing.

When a router receives a packet of data, it reads the header of the packet to determine the destination address. Once it has determined the address, it looks in its routing table to determine whether it knows how to reach the destination and, if it does, it forwards the packet to the next hop on the route.

13. What is a Network Protocol?

A networking protocol is defined as a set of rules that governs data communication over a network for:

- what is communicated,
- how it is communicated and
- when it is communicated

The key elements of protocol are:

- **Syntax:** Represents what is communicated. In simple terms it means which portion of packet is address and which is content. As an analogy, in a post card it is pre-defined which part will carry address and which part the content.
- **Semantics:** Represent how it is communicated. It means each section of bits, how a particular pattern is to be interpreted, and based on that, what action to be taken. In simple terms it could represent even in address which portion is sender's address and which is receiver's address
- **Timing:** Represents when it is communicated. It indicates when the data is to be transmitted and how fast it can be sent.

14. What is a Physical Address?

Each NIC Card has a unique hard coded 48 Bit number which is called MAC Address, or the physical address. It is generally of the type 40-2C-F4-0B-24-9E, where it is being represented in hexadecimal and each hexadecimal is represented with 4 bits thus a 48 Bit address. We can see MAC addresses of our computer by command *C:\Ipconfig /all* in command prompt mode. Each device on the network must have a physical address and is used in forwarding packets within a LAN.

15. What is TCP/IP?

TCP/IP (Transmission Control Protocol/Internet Protocol) is a Suite of communication protocol. It is a practical model or the protocol suite which comes into play in data communication between Devices on a network. The Internet's technological success depends on its principal communication tools, the Transmission Control Protocol (TCP) and

the Internet Protocol (IP), generally known as TCP/IP. TCP/IP is a set of protocols developed to allow cooperating computers to share resources across the networks. It establishes the standards and rules by which messages are sent through the networks.

The model divides the tasks involved with moving information between networked computers into five smaller, more manageable task groups. A task or group of tasks is then assigned to each of the five layers. Each layer is reasonably self-contained so that the tasks assigned to it can be implemented independently. TCP/IP protocol suite is a bundle of protocols that are segmented into five layers.

5. Application Layer-Provides service to user applications
4. Transport layer- Provides end to end data delivery services
3. Internet Layer-Routing of data
2. Data link layer-Routines for accessing physical network
1. Physical layer-Deals in 0s and 1s and voltages

16. What is an IP Address?

Internet Protocol has the responsibility of identification of hosts based upon their logical addresses and routing of data between these hosts over the underlying network. For Identification of Hosts, Internet Protocol Addressing Scheme gives the address of a device attached to an IP network (TCP/IP network).

Each client, server and network device is assigned an IP address, and every IP packet traversing an IP network contains a source IP address and a destination IP address. IP Address (IPv4) is an address which is 32-bits in length written in form of 4 Octets or Bytes separated by a dot, e.g. xxx.xxx.xxx.xxx or 117.149.29.234. IP address contains information of three fields: class type, netid, and hostid. There are 5 Classes of IP addresses in IPv4

- **Class A:** Contains one Octet for NetId and three octets for HostId. It has largest No. of Hosts.
- **Class B:** Contains two Octets for NetId and two octets for HostId.
- **Class C:** Contains three Octets for NetId and one octets for HostId. Provides largest No. of Networks.
- **Class D:** Used for multicasting
- **Class E:** Reserved for research.

17. Which is the fastest firewall?

Packet Filtering Firewall works the most fast as it takes filtering action on the basis of source, destination and the port addresses only, and does not examine packets any further.

Packet Filtering Firewall has the benefit of speed and is the simplest firewall, and is usually implemented on a screening router deployed between the private network and the public network. The screening router examines the header of every packet of data traveling between the Internet and the corporate network. Packet filtering firewalls work at the network layer of the OSI model, or the Internet layer of TCP/IP model. The header of a packet would contain:

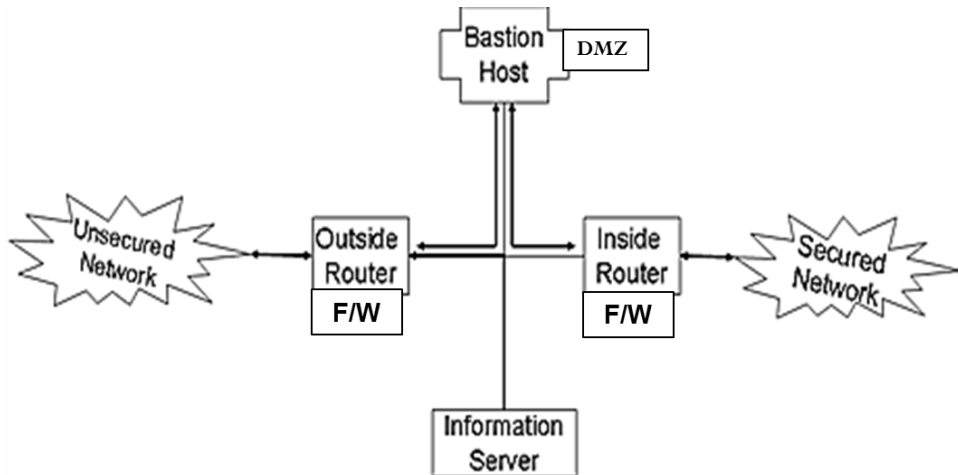
- Type of packet i.e. TCP, UDP, ICMP, IP SEC
- IP Address of Source
- Port Number of Source
- IP Address of Destination
- Port Number of Destination

Firewall rule could be based on any of these.

In case, the rule is matched, and the rule permits, the packet is passed to the next server/device as per the information in the Routing Table of the screening router. If match is found but the rule disallows, the packet is dropped. However, if match is not found, the action to forward or drop the packet is taken as per the default parameter. This firewall is not very costly and has low impact on network performance.

18. Which type of firewall provides best security for data centres?

The Screened Subnet Firewall (DMZ) configuration is the most secured environment. It has two packet-filtering routers, one between the bastion host and the Internet and the other between the bastion host and the internal network, creating an isolated sub-net. For all incoming traffic, the outside router (the router facing the Internet) directs all the packets to the bastion host. The bastion host together with the firewall does preliminary filtering and if the packet passes the test, directs the packet to the less secure or DMZ, the demilitarized zone. However, where the packet needs to travel into the secure network, which is configured as a separate segment, the inside router along with the second firewall provides a second line of defence, managing DMZ access to the private network by accepting only traffic originating from the bastion host.



In a screened sub-net firewall, the internal network (the private segment) is highly secured. The external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity. An intruder must penetrate three separate devices - the outside router, the bastion host, and the inside router to infiltrate the private network.

19. What is an IDS?

Intrusion Detection Systems (IDS), as the name suggests is a detective control. IDS monitors network traffic and host logs for signs of intrusion and by providing Alerts bring potential intrusions to the attention of administrators. It only monitors and lets us know when an event has happened, but does not itself reacts. IDS can detect network scans, packet-spoofing, Denial of Service (DoS), unauthorized attempts to connect to services and improper activity on a system. There are broadly two types of IDS:

- **Network Intrusion Detection Systems (NIDS):** NIDS are placed at various choke points, i.e. Routers, Switches etc. within the network and they monitor all traffic to and from devices on the network.
- **Host Intrusion Detection Systems HIDS:** HIDS are implemented on individual hosts or devices on the network. It monitors all packets to and from the host only and alerts the administrator if suspicious activity is detected

Detection methods which IDS can use could be:

- **Signature:** Based on past history.
- **Statistical Anomaly:** Based on behaviour.

20. What is Cryptography?

Cryptography is the art of protecting information by transforming it into unintelligible form and the process is called encryption. Many schemes used for encryption constitute the area of Cryptography. These are called Cryptographic Systems or Ciphers. Cryptography helps in addressing confidentiality related issues. Cryptography when used as an element of PKI also addresses Integrity, Authentication and non-repudiation related issues. The basic elements of messages and encryption are:

- Any message that is intelligible is termed plaintext, also called as Cleartext.
- Encryption is the process of converting the given plaintext into a scrambled form.
- The encrypted message that is unintelligible is called Ciphertext.
- The process of turning cipher text back into plaintext is called Decryption.

To convert any plaintext into ciphertext we need an Algorithm (in plain speak some mathematical formula or function) and Keys. There are, in general, three types of cryptographic schemes to accomplish these goals:

- **Secret Key or Symmetric Cryptography:** Uses a single key for both encryption and decryption.
- **Public Key or Asymmetric Cryptography:** Uses one key for encryption and another for decryption.
- **Message Hash Functions:** Uses a mathematical transformation to irreversibly information. It is a one way function and from the Message Hash (also called Message Digest). This ensures integrity of transmitted data.

21. What is a digital signature?

Digital Signature may be defined as a data string dependent on some secret known only to the signer, and additionally, on the content of the message. The process involves use of Asymmetric Keys and Hash. A digital signature serves the purpose of:

- Authentication (establishing the identity of the person who has signed it);
- Integrity (that the document that has been signed is unchanged); and
- Non-repudiation (that the person who has signed it can't deny it later).

22. Who are Certifying Authorities?

Certifying Authorities are Trusted Third Parties (TTP) to verify and vouch for the identities of entities in the electronic environment. The trust in the CA is the foundation of trust in the certificate as a valid credential. In India, the IT Act (Information Technology Act) provides for the Controller of Certifying Authorities (CCA), the body under Ministry of Communications and Information Technology to license and regulate the working of Certifying Authorities and also to ensure that none of the provisions of the IT Act are

violated. The primary role of Certifying authority is to digitally sign and publish the public key bound to a given user. Certifying Authority does this using its own private key. This brings a chain of trust i.e. trust in user's key relies on the trust in CA's Key.

23. What is a CRL?

Certificate Revocation List (CRL) is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked, and therefore entities presenting those certificates should no longer be trusted. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. The CRL file is itself signed by the CA to prevent tampering. The CRL is always issued by the CA that issues the corresponding certificates. When a potential user attempts to access a server, the server allows or denies access based on the CRL entry for that particular user.

24. What is SSL/TLS?

The Secure Socket Layer (SSL) and Transport Layer Security (TLS) are the most widely deployed security protocols used today. SSL/TLS are essentially protocols that provide a secure channel between two machines operating over the Internet or an internal network. In today's Internet focused world, the SSL protocol is used when a web browser has to be securely connect to a web server over the inherently insecure Internet. SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. Almost any service on the Internet can be protected with SSL. SSL is being used for

- Secure online credit card transactions.
- Secure system logins and any sensitive information exchanged online e.g. secure Internet Banking session
- Secure cloud-based computing platforms.
- Securing the connection between E-mail Client and E-mail Server.
- Secure transfer of files over https and FTP(s) services.
- Secure intranet based traffic such as internal networks, file sharing, extranets, and database connections.

25. What is S/MIME?

S/MIME refers to Secure Multi-Purpose Internet Mail Extensions. Email message suffers various security issues, we cannot be sure that the sender is who they claim to be; or that the message text has not been tampered with. Email text itself is not generally encrypted, meaning that if someone hacks access to our inbox, they can view our messages. S/MIME is a secure method of sending e-mail and attachments that uses the RSA encryption

system. The standard is based on public-key cryptography. In this specification, an individual user owns a digital certificate which contains a public key and a private key. The private key is held only by its owner; the public key is shared with contacts. With the keys in place, we can use our email client to attach a digital signature to outgoing emails, or to encrypt the content of an email, or both.

CHAPTER 2: IT ENABLED SERVICES AND EMERGING TECHNOLOGIES

PART 1: IT ASSURANCE SERVICES AND ROLE OF CAS IN BPO-KPO

Learning Objectives

- To understand the need for CAs to embrace IT
- To understand opportunities for CAs in IT enabled services
- To gain an understanding of using best practice frameworks
- To gain an overview of IT enabled services like BPO
- To understand how to use best practices for providing assurance and consulting services

1.1 Introduction

Information Technology has pervaded most of the aspects of every organisations be it an SME (Small and Medium Enterprises) or a huge organisation. Adoption of Information Technology carries its own threats, but the nature of threats could be different for SMEs or Large Enterprises. The threats to SME relate more to size and limited manpower. Some of the threats could be in the form of:

- Breakdown/failure of IT infrastructure: Hardware, network, system software, application software, etc.
- Loss or theft of IT resources including data impacting business due to lack of awareness of the need for IT security and low level of controls.
- Lack of adequate security affecting the confidentiality, integrity and availability of IT resources.
- Dependence on few personnel on managing IT, dependency on IT vendors and lack of skilled manpower due to lack of processes, policies, procedures, standards and guidelines.
- Lack of independent assurance of the status of IT security and controls

In case of large enterprises they could be more in the nature of:

- Breach of security due to hacking resulting in non-availability of IT resources
- Breakdown of IT infrastructure due to inadequate business continuity plans
- Lack of adequate risk management strategy and remedial measures
- Over dependency on key personnel
- Lack of appropriate clauses in SLA resulting in enterprises being at mercy of IT vendors

Chartered Accountants have to embrace IT as IT is a key enabler in enterprises of all sizes and this is so even in enterprises providing services. CA firms are impacted by IT in two ways:

- By automation of their client's operations resulting in client's data being digital; and
- CA firms have to use IT in their own offices to provide services.

1.2 Opportunities for CAs

For Chartered Accountants there exist opportunities in Auditing and Assurance as well as consulting areas. Chartered Accountants with their expertise in data and in depth understanding of systems and process functions are uniquely suited for providing consulting in control implementation of IT enabled services as well as review of the same. IT by default rather than by design has become critically relevant for CA firms.

Technology deployment by design from a strategic perspective by CA firms could act as catalyst of growth and key differentiator to not only provide current service offerings to existing clients but also develop innovative delivery capabilities for new service offerings to existing /new clients. This can empower CA firms to stay ahead of the curve by enhancing capabilities to not only transform the way current services are provided but also provide IT enabled services in the areas of IT governance, risk, compliance assurance, consulting and implementation. For this transition to happen, it is important to determine how IT would be used by the enterprise and to invest in IT from a long-term perspective and after a well thought out assessment of the firm's needs. This will ensure that right technology and tools are available for use by the firm's staff. However, to develop their capabilities and technological infrastructure, the CA firms will have to do an assessment of the following:

- **Identifying areas of specialization:** It is important that the gaps between the current situation and the future needs are assessed and areas of specialisation planned.
- **IT skills and competencies:** The firm should inventorise its IT assets both in terms of skill levels and resources and plan on path required to reach its requirements.
- **Assessing the existing and future applications:** The evaluation of existing service delivery mechanism and other related procedures has to be carried out from the automation perspective. The firm should assess whether its processes and the software applications being used, are in tune with the future IT strategy or not.
- **Determining type of technology infrastructure required:** Identification of development areas of IT to ensure its appropriateness for future, is essential. Considering the technological changes, a firm should carefully assess its budgets and resource plans to serve both the present and future clients.
- **Service delivery:** The CA firm has to assess the way it provides and delivers its services and the internal processes adopted by it, to develop new methodologies and ways to deliver services, to tune up with the capabilities of the implemented IT.
- **IT culture and training:** To develop and implement an IT solution, the firm not only requires investment in the technology but also has to ensure the automation of key processes and provide training to all the staff as per requirements, to imbibe the right IT culture.
- **Right Migration Plan:** Investing in the right technology solution is the most critical decision to make. Reviewing the current technology and application infrastructure and then

identifying the gaps for future requirements and then implementing the migration plan makes it a very critical decision.

Apart from adopting IT for their own office, CAs will have myriad challenges and opportunities in the area of Information Technology. Once CA has a good understanding of IT and related processes, they can provide assurance and consulting services to clients as well as other enterprises in many different sectors and industries. CAs can also help their clients in various areas such as:

- Meet the challenges in adoption of emerging technologies and computing models, like, cloud computing, BYOD, Social Media Usage, Big Data etc.
- Mitigation of risks in BPO-KPO and related areas.
- Use of BI using Data Warehouses, Data Mining, Data Marts, DSS, ESS, AI, etc.
- Adoption of ERP, E-Commerce etc.

1.3 IT Consulting and Assurance Services by CAs

CAs could use global best practices for Consulting and Assurance in IT enabled services. COBIT 5 is one such framework which could be used to provide standardised approach to enable auditors to provide different types of IT enabled services. These processes have detailed management practices, input-output matrix, RACI (Responsible, Accountable, Consulted and Informed) chart and activities which can be used as a benchmark and customised for scoping assignments as required. The contents from each of these processes or a combination of selected processes as relevant can be referred and adapted for preparing the proposal. This could then become the starting point for discussing the scope and objectives of assurance/consulting assignment. Once the scope is agreed upon, the extracted contents from these processes can be customised and used as a benchmark for providing the required services. CAs using their cross functional and in depth knowledge can help an organisation implement Governance framework or help an organisation develop IT strategy for itself or provide assurance services in these areas.

1.3.1 Using COBIT for providing IT-enabled services

CAs can use and adopt the best practices framework such as COBIT to provide various IT-enabled services. Some of the services in terms of scope and objectives derived from COBIT are given with sample scope, objectives and areas of review. These can be updated and expanded as per requirements of the assignment.

1. Set and maintain the IT Governance Framework

Scope: Analyse and articulate the requirements for the governance of enterprise IT, and put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.

Objective: Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT---related decisions are made in line with the enterprise's strategies and objectives, IT---related processes are overseen effectively and transparently, compliance with legal and regulatory requirements are confirmed, and the governance requirements for board members are met.

Areas of Review

- Evaluate design of enterprise governance of IT.
- Direct the Governance System.
- Monitor the Governance System.

2. Define IT Strategy Planning

Scope: Provide a holistic view of the current IT environment, the future direction, and the initiatives required to migrate to the desired future environment, leveraging upon enterprise architecture building blocks and components to enable nimble, reliable and efficient response to strategic objectives.

Objective: Align strategic IT plans with business objectives and clearly communicate the objectives and associated accountabilities so that these are understood by all, with the strategic options identified, structured and integrated with the business plans.

Areas of review

- Understand enterprise direction.
- Assess the current environment, capabilities and performance.
- Define the target IT capabilities.
- Conduct a gap analysis.
- Define the strategic plan and road map.
- Communicate the IT strategy and direction.

3. Manage Risk

Scope: Continually identify, assess and reduce IT related risks within levels of tolerance set by enterprise executive management.

Objective: Integrate the management of IT related enterprise risk with overall enterprise risk management, and balance the costs and benefits of managing IT related enterprise risks.

Areas of review

- Collect data
- Analyse risk.
- Maintain a risk profile.
- Articulate risk.

- Define a risk management action portfolio
- Respond to risk.

4. Review IT Security Management

Scope: Define, operate and monitor a system for information security management

Objectives: Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels.

Areas of review

- Establish and maintain ISMS (Information Security Management System).
- Define and manage an information security risk treatment plan.
- Maintain and review the ISMS.

5. Compliance with external requirements

Scope: Evaluate that IT processes and IT--supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with and that the IT compliance integrates with overall enterprise compliance.

Objectives: Ensure that the enterprise is compliant with all applicable external requirements.

Areas to review

- Identify external compliance requirements
- Optimise response to external requirements
- Confirm external compliance
- Obtain assurance to external compliance

6. Manage Continuity

Scope: Establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operations of critical business processes and required IT services and maintain availability of information at a level acceptable to the enterprise.

Objectives: Continue critical business operations and maintain availability of information at a level acceptable to the enterprise in the event of a significant disruption.

Areas to review

- Define the business continuity policy, objectives and scope.
- Maintain a continuity strategy.

- Develop and implement a business continuity response.
- Exercise, test and review the business continuity plan
- Review, maintain and improve the continuity plan.
- Conduct continuity plan training
- Manage backup arrangements
- Conduct post-resumption review.

1.4 Business Process Outsourcing

A Chartered Accountant could play a significant role in areas like outsourcing, cloud services, mobile computing, BPO/KPO, SLA, report validations etc. Let us understand the relevance of these in areas of BPO/KPO. Every modern organisation is dependent upon various operations that would enhance the productivity of the organisation. Outsourcing of various activities/services by an organisation takes advantage of core competences of service providers in these areas, so that the organisation can concentrate on its core business. Many of the IT enabled companies, a big chunk of which are Indian companies today provide a lot of outsourcing solutions/services. BPOs usually deal with fringe business activities such as customer care, finance and HR. The basic purpose is to cut on costs, and the functions outsourced do not have much value add to the organisation. Some of the activities which are outsourced are cheque clearing, ATM cash replenishment, account opening forms and Adhaar Card enrolment. Some of the IT Enabled business processes could be:

1.4.1 Knowledge Processing Outsourcing

Knowledge Process Outsourcing (KPO) is a subset of BPO. KPO involves outsourcing of core functions which may or may not give cost benefit to the organisation but helps in value addition. These processes are usually more specialized and knowledge based as compared to BPOs, and includes services related to R&D, Capital and insurance market services, legal services, biotechnology, animation and design, etc. KPO is application of specialized domain pertinent knowledge of a high level and is the high end of BPO. This may include,

- Risk Management: The process includes services like monitoring the risk factor of various investments, looking after the returns, looking after at the viability of projects a company undertakes. It also includes making quarterly reports of investments and sending it to the company.
- Claims Processing: The process includes checking of documents supporting the claim and storing online data of claims.
- Consultation on accounting and tax implications of significant agreements and transactions helping in SEC Reporting, Mergers and Acquisitions, Private Placement Memorandum.

1.4.2 Medical Transcription

Medical transcription is the process of converting voice-recorded reports into text. A medical transcriptionist listens to a recorded medical report. While listening, they type out the report. The medical reports are dictated (into Dictaphones) by physicians and other medical personnel. Clinical health systems and hospitals often reduce costs and increase efficiency by outsourcing tasks such as transcription and billing rather than assigning to doctors or physician who are overqualified for these duties.

Outsourcing medical transcription gives the responsibility to more dedicated professionals (transcribers) in countries like India and other Asian countries, which leaves doctors to focus on core medical practice and procedures leading to better patient care. India incidentally has been a big beneficiary in this outsourced work, Medical transcribers and solution providers in India allow global healthcare practitioners, clinics and hospital deliver best results in medicine by performing transcription, editing / QA support through IT enabled processes.

1.4.3 Legal Transcription

Legal transcription Similar to medical transcription but involves converting audio dictation by legal professionals and other recordings from legal cases into the printed word. Solicitors, attorneys and legal professionals use the services of legal transcriptionists to assist them in transcribing meetings memorandums, correspondence and court documents. Legal transcription is also used for recording court proceeding and interviews of witnesses. At a higher end, even preparation of legal cases are also outsourced which come in category of knowledge process outsourcing.

1.4.4 Data Entry and data processing

Data entry in the area of accounting and many other business processes is increasingly being outsourced because of cost effectiveness. India is again a big data entry outsourcing hub, since we have a comprehensive range of quality of manpower with professionals in their desirable fields. This enables low cost data entry services with timeliness and high volume of data-entry operations possible along with data processing and analytics. Example of some these areas are outlined here.

- **Taxation / Financial Accounting Outsourcing:** India is known for having both cost as well as technical advantages when it comes to outsourcing IT services and processes. India has emerged as one of the most preferred country for outsourcing various services globally. These include supply chain management, sales, marketing, customer care, human resource besides financial services and E-Accounting services such as:
 - **Accounts Payable:** The process helps client to track payments originating across different locations and in different currencies. It helps to efficiently settle payment issues with vendors.

- **Accounts Receivable Management:** The process includes managing as well as tracking the client's receivables in different locations. It also helps to manage the limit of credit extended by the client.
- **Tax Processing:** The process includes keeping proper tax data and auditing it and also maintenance of various documents and forms relating to taxation.
- **Cash Management:** The process includes checking the cash flow statement of the company. It also includes checking the liquidity of the company, managing current assets like cash, inventories, bills payable and receivables etc.

1.4.5 IT Help-desk support

IT help desk is a resource which provides a kind of single point of contact service to end users for all kinds of IT support. Their purpose is to trouble shoot problems and provide guidance on the technologies powering the business. For End User there are endless IT challenges to deal with on a daily basis. IT help desk facilitates all these challenges and provide a one point support for all of these. These days a help desk generally manages its requests for support through the use of software such as issue tracking systems. This software allows helpdesk to keep a track of users' requests, sort user requests with the help of a unique number, and can frequently classify problems by user, computer program, or similar categories.

1.4.6 Application development

Outsourcing Application Development allows the organisation to focus on its core competencies and at the same time take the benefit of core competency of vendor. Application Development services are also being catered by a large number of Indian companies, who are developing applications and solutions for a large number of overseas clients.

1.4.7 Risks and Controls of outsourced services

Risks

If we consider all the above areas of BPO, there are some common risks or security concerns:

- **Privacy and Confidentiality-** Disclosure of information related to overseas customer could lead to privacy and confidentiality issues which could create a liability.
- **Attrition of staff-**A high turnover rate has an indirect impact on the client organisation because it forces it to increase time spent on knowledge transfer and training new individuals.
- **Legal Compliances-** Vendors are liable for lot of compliances under several laws of India as well as of outsourcing country. For example medical transcription vendor liability has become important in light of HIPAA privacy and security regulations, which place an obligation on covered healthcare providers to ensure that their vendors safeguard confidentiality.

- **Timeliness**-In most of outsourcing Time is of essence and the service level agreements normally provide for Turn Around Time (TAT) which has to be adhered to.
- **Providing service in disaster**- Most of SLAs also provide for clauses relating to provision of services in disaster also.
- **Complying with SLAs**-SLAs could provide for imposition of fee claw back in case of poor service. SLAs also provide for organisations to have in place a risk management program.

Controls

The security concerns can be mitigated by implemented appropriate controls. CAs as IS Auditors can understand the relevant security concerns and confirm whether appropriate controls have been implemented to address these risks, identify areas of control weaknesses and provide recommendations for risk mitigation.

- Access Controls- Have Information security management systems in place with secure practices like each employee required to have a secure password; Voice files and data files maintained in a secure data safe; Security during transmission using VPNs etc.
- HR Controls- Proper background checks, employee bonding
- Good Processes-Have documented processes and quality management systems
- Quality Assurance-Have quality assurance processes in place.
- Compliance Management- Have a system of legal compliances in place and regular review of the same.
- Contingency and Backup Plans- Have contingency and BCP in place

1.5 Using global best practices

1.5.1 Compliance with external requirements:

An Indian BPO service provider, located in India, is duty bound to comply with the various provisions of Indian laws which impact the outsourcing industry. There are numerous Indian legislations which Indian BPOs have to comply with apart from International legislations of the outsourcing country. For example: SOX or HIPAA of USA and PCI DSS or Basel Framework applicable to banking companies. CA can use the best guidance practice available in COBIT relating to: Process MEA03 Compliance with External requirements discussed earlier to ensure such regulatory compliances. COBIT also provides step by step approach for providing assurance of such areas.

For example, in case of regulatory compliances, the steps could be:

- Identify external compliance requirements.
- Optimise response to external requirements.
- Confirm external compliance.
- Obtain assurance external compliance.

Module 1: Facilitating e-Learning

For Example, there are compliance requirements under the Information Technology Act which are applicable for any BPO-KPO. The specific areas of compliance which could be reviewed by the IS Auditor are:

Section 43 A

- Are various components of “sensitive personal data or information” vis-à-vis users/customers defined by the enterprise?
- Does the enterprise have a security policy?
- Is the security policy documented?

Section 67C

- Does the enterprise have an electronic record preservation and retention policy?

Section 69B

- Has the enterprise adopted/established appropriate policy, procedures and safeguards for monitoring and collecting traffic data or information?
- Are these documented?

Section 70B

- Does the enterprise have appropriate documented procedure to comply with the requests of CERT-IN regarding cyber security incidents?

Section 72A

- Does the enterprise have an adequate privacy policy?
- Whether the enterprise has provided for opt-in/opt-out clause in the privacy policy?

General

- Has the enterprise appointed designated officer/nodal officer/computer-in-charge to comply with the directions of competent authority/agency under various provisions of the Act? Whether details of such designated officer/nodal officer readily available online (at its website)?

1.5.2 Managing Business Continuity

Most of SLAs (Service Level Agreements) of BPOs provide for provision of services during disaster also. CAs as IS Auditors can use the best practices provided in the COBIT management process: DSS04 Manage Continuity to provide assurance in this area by assessing.

- Whether the organisation has a defined business continuity policy, with clear objectives and scope.
- Whether organisation maintains a continuity strategy.

- Whether the organisation has developed and implemented a business continuity response plan.
- Whether the organisation exercises, tests and reviews the business continuity plan.
- Whether the organisation reviews, maintains and improves the continuity plan.
- Whether the organisation conducts continuity plan training.
- Whether the organisation manages backup arrangements.
- Whether the organisation conducts post-resumption reviews.

Apart from providing assurance services, a Chartered Accountant could also help a BOP –KPO to manage continuity by providing consulting in the above areas.

1.6 Summary

IT is a big enabler and a CA should understand IT for use in their own practice as well as for helping their clients implement and develop IT enabled processes. CAs can use best practices framework such as COBIT for providing Assurance and Consulting services. IT has been a big enabling factor in BPO in medical transcription, legal transcription and data entry processing areas. There are, however, risks in these areas which have to be mitigated. CAs because of their understanding of IT risks, security and controls can provide assurance or consulting on mitigation of these risks and thus provide value addition to their clients.

1.7 References

1. www.isaca.org/cobit
2. www.gartner.com
3. http://www.sourcimag.com/content/what_is_bpo.asp
4. <http://searchsecurity.techtarget.in/definition/knowledge-process-outsourcing-KPO>
5. http://www.cio.com/article/40380/Outsourcing_Definition_and_Solutions

1.8 Questions

1. Why do Chartered Accountants need to embrace IT?
 - A. IT is a trendy thing
 - B. IT is a buzzword
 - C. IT is a key enabler in Enterprises
 - D. IT is interesting
2. Which of the following is an advantage of Outsourced services?
 - A. Privacy and confidentiality
 - B. Attrition of staff
 - C. Cost cutting

Module 1: Facilitating e-Learning

D. Legal compliances

3. While auditing an Outsourced agreement, an IS auditor would be most concerned with:

- A. The commercial terms of outsourcing arrangement
- B. The continuity of operations in case of failure of service provider
- C. The location from which services are provided
- D. The loss of in-house IT competencies

4. Embracing IT will enable Auditors to provide Consulting and Assurance services in the areas of:

- A. IT Risk Management
- B. IT Strategic Planning
- C. IT Security Management
- D. All the above.

5. An IS Auditor auditing the on-line transaction processing system of an organization outsourced to a third party will be most concerned that

- A. Transactions are authorized by the outsourced agency.
- B. Transaction log is not printed on daily basis.
- C. Organization does not have adequate trained IT personnel.
- D. The third party is providing outsourced services to other clients also.

1.9 Answers

1	C
2	C
3	B
4	D
5	A

PART 2: EMERGING TECHNOLOGIES: BI, DATA WAREHOUSE, ERP AND E-COMMERCE

Learning Objectives

- To gain an overview of BI and Data Analytics
- To gain an overview of Data Warehouse and Data Mining
- To gain an overview of ERP
- To gain an overview of E-Commerce and E-Governance

2.1 Introduction

With today's modern IT systems, organisations are collecting ever increasing volumes of data from various sources, ERP systems, CRM, websites and all, but this data is not in a form which could be useful for decision making, Business intelligence (BI) offers organisations the ability to gain valuable insight that can lead to effective decision making. Data warehouses and data mining are some of the components of Business Intelligence. Organisations have to work smarter, not just harder. With ERP organisations can become more strategic - and more profitable - by applying their resources more efficiently to serving and developing customers. For increasing revenues for an organisation, there is no better alternative than to have an online presence. Most of the companies are introducing e-commerce alternatives to their existing brick and mortar model of business. All these areas where IT is an enabler has to be understood by Chartered Accountants so as to not only keep pace with the latest in IT but also to provide assurance and consulting services in these areas.

2.2 Business Intelligence

Business intelligence (BI) is the use of computing technologies for the identification, discovery and analysis of business data - like sales revenue, products, costs and incomes. BI technologies provide current, historical and predictive views of internally structured data for products and departments by establishing more effective decision-making and strategic operational insights through functions like online analytical processing (OLAP), reporting, predictive analytics, data/text mining, benchmarking and Business Performance Management (BPM). These technologies and functions are often referred to as information management.

Organisations to run optimally need data which comes to them from a growing number of applications (e.g. ERP, e-commerce, CRM, SCM etc.) creating a new data management challenge: that is the effective way of integrating enterprise applications in real time. To learn from the past and forecast the future, many companies are adopting Business Intelligence (BI) tools and systems. Companies

have understood the importance of enforcing achievements of the goals defined by their business strategies through business intelligence concepts.

There are many definitions of BI but the most apt one is: “BI is essentially timely, accurate, high-value, and actionable business insights, and the work processes and technologies used to obtain them”. The business determines the “what”; BI enables the “how”. A practical example is the retailer who wishes to know what time of day particular groceries are purchased and in which combinations, for example. This knowledge makes possible for it to lay out supermarkets to better match consumer buying patterns. Business Intelligence is about making effective business decisions. Business Intelligence is the process by which an organisation manages large amounts of data, extracting pertinent information, and turning that information into knowledge upon which actions can be taken. It is a broad category of application programs and technologies for gathering, storing, analysing, and providing access to data to help enterprise users make better business decisions.

Any organisation that plans to get into a better competitive position has to share and analyse business information between multiple interested parties using BI. There are many different users who can benefit from business intelligence.

- Executives
- Business Decision Makers
- Information Workers
- Line Workers
- Analysts

BI enables organisations to make well informed business decisions and gain competitive advantage. BI enables organisations to use information to quickly and constantly respond to changes. The benefits of BI are improved performance based upon timely and accurate information; Information is based on facts not guesses, helps in expedited decision making. BI is derived by appropriate analysis of data stored in data warehouses and data marts.

Data warehousing (or data mart) system is the backend, or the infrastructural, component for achieving business intelligence. Business intelligence also includes the insight gained from doing data mining analysis, as well as unstructured data (thus the need for content management systems).

2.2.1 Key BI tools and techniques

Simple reporting and querying: This involves using the data warehouse to get response to the query: “Tell me what happened.” The objective of a BI implementation is to turn operational data into meaningful knowledge.

Business analysis: This involves using the data to get response to the query: “Tell me what happened and why.” Business analysis refers to presenting visualising data in a multidimensional manner.

Dashboards: This involves using the information gathered from the data warehouse and making it available to users as snapshots of many different things with the objective of getting response to the query: “Tell me a lot of things, but without too much effort”.

Scorecards: This involves providing a visual representation of the enterprise strategy by taking critical metrics and mapping them to strategic goals throughout the enterprise. Scorecards distil information into a small number of metrics and targets and provide users with an at-a-glance perspective of information.

Data mining or statistical analysis: This involves using statistical, artificial intelligence, and related techniques to mine through large volumes of data and providing knowledge without users even having to ask specific questions.

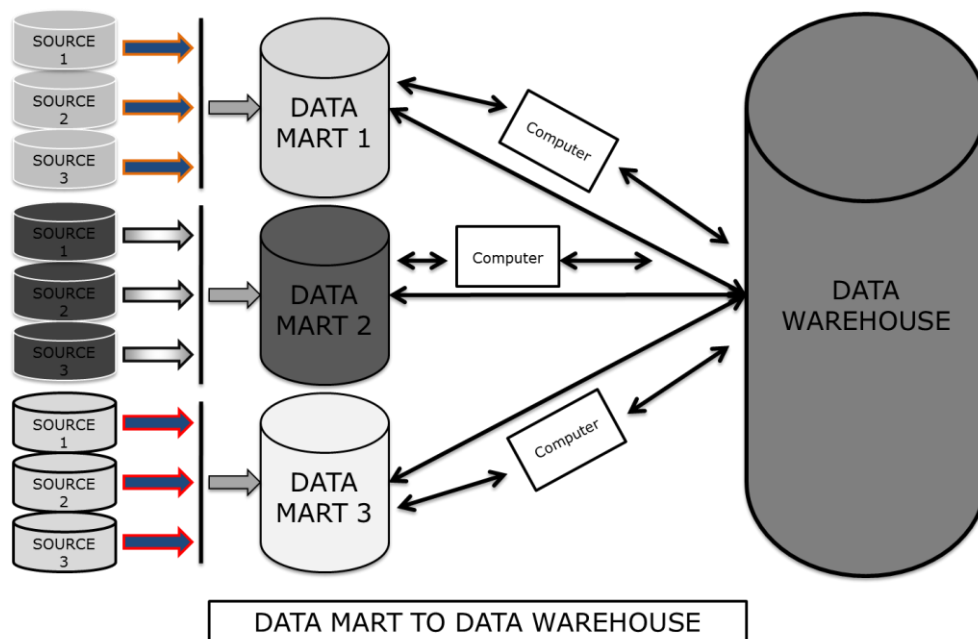
2.3 Data Warehouse

A data warehouse is an analytically oriented, integrated, time-variant, and non-volatile collection of data that supports decision making processes. Time-variant since horizon is longer and it provides information from historical perspective (last 5-10 years) and Non-volatile since it is separate from operational data and operational update of data doesn't occur in Data Warehouse (DW).

Data warehousing provides perfect architecture to combine all the data dispersed throughout the enterprise in different applications in a variety of formats, on a range of hardware, which could be anywhere to be cleaned up, summarized, converted and integrated into one common format and available centrally for further processing. The concept of data warehousing is pretty easy to understand—to create a central location and permanent storage space for the various data sources needed to support a company's analysis, reporting and other BI functions. The sources of data warehouse are the On-line Transaction Processing Systems (OLTPs) and the external resources. To be fresh and accurate DW requires regular updating that should be fast, efficient, automated and includes deletion of the old data.

2.3.1 Data Mart

A subset of a data warehouse is a Data Mart. Small and medium sized businesses and departments within larger companies use this concept. Data for a single aspect of business is stored in a data mart. A data mart can contain more detailed data than a warehouse. As it stores less data than a warehouse, it requires less powerful hardware with a smaller secondary storage device.



The organisation, as per its requirements and the technological architecture, may first build a Data Warehouse and then create its sub-sets; the Data Marts or it may consolidate its data marts to create an enterprise-wide Data Warehouse.

2.3.2 Need for a Data Warehouse

Data in disparate systems makes it difficult to analyse. Data Warehouse provides a solution to these problems and the analysis of data in DW can help in answering questions based on historical operations, aiding decisions, questions like:

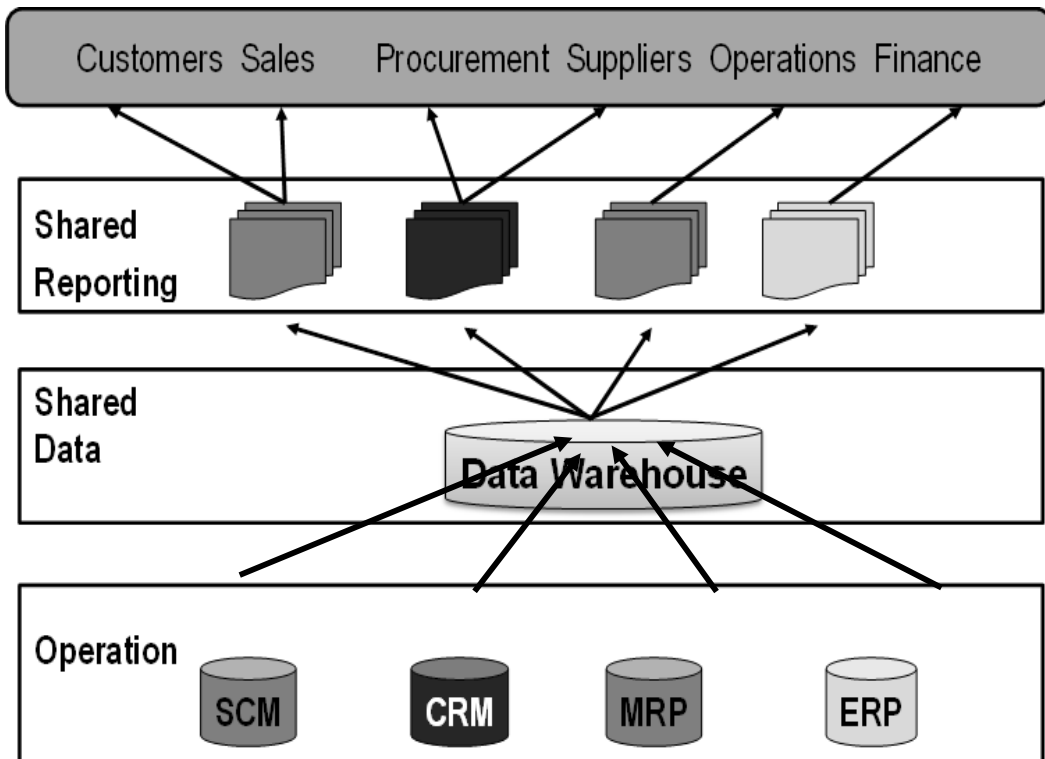
- What were the best selling products last Week/Quarter?
- What is the relationship between sales and returns? What is the return rate by supplier? Why are returns so high for XYZ?
- How do inventory levels compare with sales by product by warehouse?

Advantages of Data warehouse are:

- It delivers enhanced business intelligence.
- Saves time obviating the need to extract data from various sources.
- It enhances data quality and consistency- A data warehouse implementation includes the conversion of data from numerous source systems into a common format.
- Provides historical intelligence.

Data from different systems is moved to a dedicated server that houses a data warehouse. When it is moved it is cleansed, formatted, validated, reorganized, summarized, and supplemented with data

from many other sources. An Extract, Transform, and Load (ETL) software tool is used to obtain data from each appropriate source, including whatever ERP systems are in use. ETL tools read data from each source application edit it, assign easy-to-understand names to each field, and then organize the data in a way that facilitates analysis. A key aspect of the reorganisation process is the creation of areas within the warehouse that are referred to as data marts. In most cases, individual data marts contain data from a single subject area. This resulting data warehouse becomes the main source of information for report generation and analysis via reporting tools that can be used for such things as ad-hoc queries, canned reports, and dashboards.



2.3.3 Risks and Controls Associated with Data Warehouse

Risks associated with data Warehouse are:

- Data corruption or lack of data within the organisation source systems.
- Data Migration routine fails to move data to the Warehouse.
- Data Cleansing routine fails to resolve data inconsistencies.
- Data Transformation routine has incorrect transformation rules.
- Data Loading routine fails or is not constructed properly.
- Complexity of source data structure.

- Data Security might be a huge concern, especially if the data is accessible over an open network such as the Internet. Users will not want their competitor to view, hack, or destroy their data.

Controls Related To Data Warehouse

Controls to mitigate the risks could both be preventive and detective in nature.

Preventive Controls

- Identify and understand where the data is located and what data is to be moved.
- When in doubt, leave it out until we know what to do with the data.
- Deploy software tools that migrate, cleanse and transform data.
- Validate transformation rules with user community.
- Use Firewalls, encryption and other security measures to restrict access to data.

Detective controls

Detective controls involve reconciling data to determine the accuracy and completeness of information.

- Quality of Data could be reconciled by assessing control totals on selected data elements.
- Quantity of Data through quantifying number of records loaded.
- Complete Reconciliation is performed at the completion of every load process.
- Stage Reconciliation is performed after each data process stage flow. Handled when complete reconciliation is not feasible due to number of source systems in operation or complexity in data cleansing or transformation rules.

2.4 Data Mining

Data Mining is the **automated extraction of hidden predictive information** from large databases. Data Mining involves data analysis for discovering useful patterns that are “hidden” in large volume of diverse data. For Example: Market segmentation – to identify common characteristics of customers who buy same products.

It is an information analysis tool that automatically discovers patterns and relationships in a data warehouse. It examines mountains of data to find some valuable information. To evaluate proposed business strategies it extracts patterns, trends and rules from data warehouses. A form of data mining that combines historical data with future assumptions to predict outcomes of events is known as Predictive analyses. A company’s customer list and a year’s sales data can be analysed to find new market segments.

Data Mining looks at:

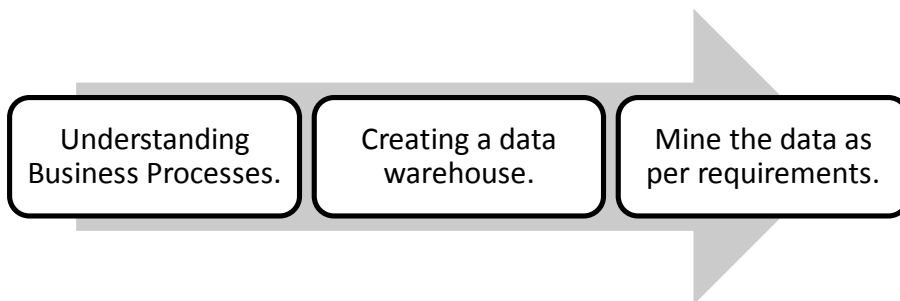
- Patterns in granular data.
- Patterns in summarized data.
- Patterns in summaries along various dimensions.
- Relation of summarized patterns to each other and to granular data.
- Looking at the database from different viewpoints – through slicing and dicing.

Output should be able to give

- Prediction of trends and behavior.
- Discovery of unknown patterns.

2.4.1 Practical Applications

1. Banking and Financial Services for Risk analysis, Channel Utilization and Retention, Segmentation, Prospecting and Acquisition.
2. Retail and Packaged Goods for determining Market share segment wise and other different criteria, demographics, ethnicity, culture, economics, etc. Factors influencing the effectiveness of advertising.
3. Right Time Direct Marketing for segmenting the market into meaningful clusters and segments
4. Internet Web Log Access Analysis to determine who is visiting and their profile



Data Mining

2.5 Enterprise Resource Planning (ERP)

Prior to the concept of ERP systems, every department within an organisation had its own customized computer applications. ERP or Enterprise Resource Planning is a system designed to integrate management information within an entire organisation, including departments such as finance, accounting, manufacturing, sales, and customer relationship management. ERP is implemented via a software application aligned with pre-existing business practices. This configuration allows access to real-time data and equips users with the information to manage

internal and external business functions. ERP is a set of integrated programs managing the vital operations of the company, for a global organisation. It supports many legal entities, languages and currencies.

The advantage of ERP is the fact that people in different departments can all see the same information, and update relevant information. The benefit of ERP is to optimise its resource utilization and also enable seamless availability of information across all users. It integrates the Entire Enterprise from Supplier or Vendor to Customer covering every aspect like financials, accounting, manufacturing, HR, etc. ERP helps organisations to respond to customer requests for information, products or services in the most efficient way. As ERP integrates order, manufacturing and delivery data, the manufacturing is better informed about what the customer has ordered, procuring exactly the right amount of components/material, staging production and minimizing the idle holding time for each component or finished product in the inventory.

2.5.1 Benefits of ERP:

- **Improved data access:** Data integration facilitates operational decision making that provides greater customer service and support, strengthen customer and supplier relationships, and generate new business opportunities.
- **Elimination of Legacy Systems:** ERP system enables an organisation to eliminate dozens or even hundreds of separate systems and replace them with a single, integrated set of applications for the entire enterprise.
- **Improvement of work processes:** The individual application modules included in the ERP system support practices that are most efficient and effective to complete a business process.
- **Upgrade of technology infrastructure:** Implementation of an ERP system provides an opportunity to upgrade the IT such as hardware, operating systems and databases that the organisation uses.
- **Standardized business processes and improved Compliance:** ERP could enforce industry best practices and thus organisations can enforce compliance related to different regulations.
- **Reduced operating costs:** Improved information availability reduces operating costs.

2.5.2 Challenges of ERP

- **Expense and time in implementation:** Implementing ERP involves time and money. Firms spend two to five years and millions of dollars to successfully implement an ERP system.
- **Difficulty in implementing changes:** In some cases, a company has to change its operations to conform to the new work process. These changes can be so drastic to long time employees that they retire or quit rather to adapt to the change.
- **Difficulty in integrating with other systems:** Companies find it difficult to link ERP systems with their B2B or B2C systems that communicate with suppliers, customers, distributors and other business partners.

- **Risks in using one vendor:** After a company has adopted an ERP system, the vendor has less incentive to listen and respond to customer concerns.
- **Information Integration-Selection and configuration of ERP Package:** If enterprises are not careful in implementing an ERP package, the dream of information integration can turn into a nightmare.
- **Weaker Controls:** In its endeavor to implement ERP fast and bring about efficiencies in business processes, organisations may miss out on some of the critical controls which were otherwise implemented in legacy systems.

2.5.3 Security concerns in ERP

The primary security concerns in using ERP are:

- Ensuring security, Confidentiality, Integrity and Availability of information is a matter of key importance as ERP has central repository of information of the organisation and is highly dependent on this information for all its critical processes.
- ERP uses high level of technology and greater the technology, higher is the risk.
- ERP is complex and complexity is anathema to security.
- Multiple users have access, high risk associated with unauthorized access and data leak
- Materiality associated with control environment due to complexity, the ERP Software security features have to be configured as per enterprise's requirements.

These security concerns can be addressed with proper access control planning using access control matrix based on data classification, Control over business processes must be emphasised, Strong change control must be implemented and regular reviewed through audit.

2.5.4 Opportunities for CAs in ERP

The chances that CAs will be on an ERP-related project in their capacity as consultants or employees are very high. CAs could facilitate their clients or employers in the areas of vendor selection or conduct business process mapping. CAs may be involved in gathering business requirements in conducting user trainings. CAs will be using ERP if they are working for any of the big CA firms or an IT consultancy firms or they could be having their own firms offering services in this niche area. The ERP projects are longer in duration and very process oriented. CAs may be involved in an ERP project in following areas:

- Assist in selection.
- Assist in configuration and effective implementation.
- Provide consulting or training in an ongoing implementation.
- Conduct post implementation review from perspective of optimization or security.

CAs role during pre-implementation

Financial information system is the core which supports decision making and monitoring, CAs can act as functional experts as they have comprehensive idea of the fundamental business transactions and their flow. CAs with their business domain knowledge are very well conversant with the processing of transactions in their totality from the moment of origination to their destination. CAs can take an objective view of the transaction flow of enterprises and based on the practices available in the ERP package suggest the flows which are best suited for the enterprise. CAs can also facilitate in selection of ERP and configuration of specific requirements by taking a macro view of the information requirements of the enterprise both from the managerial and compliance perspective. CAs are highly skilled in the areas risks, controls and security of information systems and this coupled with the knowledge of internal controls makes them the ideal candidate to assist in providing consulting or evaluating the adequacy and appropriateness of controls for organisation implementing an ERP package. CAs could help in pre-implementation through:

- Gaining an understanding of the business processes.
- Reviewing the business areas and processes.
- Defining the criticality of business areas and assign appropriate priority for preparing a project plan for implementation.
- Gaining an understanding of the processes of ERP Package.
- Finalising ideas for re-design and streamlining of processes as feasible.
- Setting up the configuration tables (parameters) as per the requirements.
- Involvement in implementation process of the ERP package at various stages.

CAs role during implementation

CAs being a control expert can provide consulting services during implementation in areas of:

- Access security
- Data conversion
- Automated interfaces
- Change control
- Development of procedures and implementation of control reports
 - Analysing current MIS Reports generated
 - Examining Report features available in ERP
 - Identifying Standard Reports available in ERP
 - Customization of reports required
 - Cost benefit analysis of such customisation
 - Identifying Users of such reports
 - Reports required for monitoring and control
 - Mandatory reports required for compliance
- Interaction with functional owners and training the users.

CAs role during post implementation

Role of CA during post implementation has two major perspectives:

- **Optimisation:** Has ERP increased the effectiveness of operations and brought in value addition and
- **Security:** With the key question: Is Confidentiality, Integrity and Availability of information secure enough?

Post Implementation review is essential since implementing an ERP package as per the plan is a major achievement but evaluation of how effective the implementation is also essential. The methodologies envisaged at the time of planning to implementation to the present might have changed. As ERP Package implementation is a major investment decision, there would be a need to conduct cost benefit analysis. Further, with the changes in roles and responsibilities of employees as some of the jobs may have become redundant and some new ones may have been created, the desired access profiles may require a change. These would require a proper review by the auditors.

Sample areas of review:

- Legal considerations
- Review of Chart of accounts
- Closing the day, month or year or posting period
- Review of important financial reports
- Review of changes in GL Master records
- Automatic postings, account assignments and reconciliation accounts
- Review of default values in account master records
- Data entry controls
- Tax management
- Archiving of documents
- Audit Trails and exception reports
- System update rules and User defined update rules
- Posting keys
- Authorisations

Apart from the avenues of consulting and reviewing ERP implementation, CAs working as financial or internal Auditors have to understand ERP because this is where the transactional data is buried. If the organisation wants to know how many products were sold, how many new customers were signed up, how many deliveries were made, or how many employees were fired, the information is probably in the ERP. For all this a CA would be needing data from ERP systems and knowledge of ERP will help a lot.

2.6 E-Commerce

The conduct of business activities electronically using Internet based technologies is generally referred as E-Commerce. E-commerce has vast potential to change the way business is conducted. E-commerce as a general model uses technology to enhance the commercial transaction processes among a company, its customers and business partners. Internet is the enabling technology and usually revolves around multi-media, web browsers, company networks etc. The business activities that are paper based time consuming and inconvenient for customers are strong candidates for conversion to e-commerce. Examples of E-Commerce could be like:

- Online Railway and Air travel booking
- Purchase of goods from sellers using Internet
- Reserving a hotel room on the Internet
- Ordering a computer using the seller's interactive telephone system
- Transferring funds online using Internet banking

E-commerce transactions over the Internet include

- Formation of Contracts
- Delivery of Information and Services
- Delivery of Content

With the advent of e-Commerce, the traditional sources of competitive advantage will be supplanted, power and control will shift from suppliers to customers, global markets will become accessible to all comers and the traditional role of middlemen will be undermined.

2.6.1 E-Commerce Models

Business to business: It is a subset of e-commerce in which all the participants are organisations.

Business to consumer: It is a form of e-commerce in which customers deal directly with an organisation and avoid intermediaries.

Consumer to consumer: It is a subset of e-commerce that involves consumers selling directly to other consumers.

E-Government: It is the use of information and communications technology to simplify the sharing of information, speed formerly paper based processes and improve the relationship between citizens and government.

E-Governance: It refers to the development, deployment and enforcement of the policies, laws and regulations necessary to support the functioning of a knowledge society as well as of e-Government.

The strategic objective of e-Governance is to support and simplify governance for government, citizens and businesses. The use of Information and Communications Technology (ICT) can connect all three parties and support processes and activities. Other objectives are to make government

administration more transparent, speedy and accountable, while addressing the society's needs and expectations through efficient public services and effective interaction between the people, businesses and government. E-Governance facilitates better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. By employing online transactions, government processes become more streamlined, efficient and less dependent on human interaction. Also the cost of processing transactions is reduced online, resulting in great savings.

2.6.2 Components of E-Commerce

- Supporting infrastructure
 - IT manpower
 - Public network and service providers
 - Public Key Infrastructure
 - Regulatory and legal framework
 - Electronic Fund Transfer
- Electronic business processes (how business is conducted)
- Electronic commerce transactions (buying and selling)
- Strong Logistic arrangements where physical delivery of goods is involved.

2.6.3 Electronic Funds Transfer

A major component of the e-commerce infrastructure is the Electronic payment system. EFT is the exchange of money via telecommunications without currency actually changing hands. It refers to any financial transaction that transfers a sum of money from one account to another electronically. With an EFT transaction, sensitive information is sent via telecommunication to the business or organisation with which we are making the transaction. This is a risk prone area with hackers who try to steal the customer's account information as it travels on unsecured networks, or manipulation of information travelling on networks. Risks could also be in terms of identity of the websites or individual.

Current e-commerce technology relies on user identification and encryption to safeguard business transactions. Payments are made in a variety of ways, including electronic cash, electronic wallets, and smart/credit/charge/debit cards. Authentication technologies are used by organisations to confirm the identity of a user requesting access to information or assets. A digital certificate as an attachment to an e-mail message or data embedded in a web site verifies the identity of a sender or web site. The EFT uses a switching solution which is software that normally runs on a front-end system that handles the physical ATM and EFTPOS terminal devices, interfaces to the bank host system and provides 24x7 operations, with stand-in processing where required. This type of software normally also interfaces with National and International switches for ATM sharing arrangements, and can provide authorization interfaces to international card schemes such as Visa and MasterCard. In a 'typical' implementation, it will also manage card issue, PIN validation and so on as well.

Increasingly, this class of system is being enabled for e-Commerce support, and provision of other 24x7 services. The software is normally a packaged solution in most institutions.

2.6.4 Risk in E-Commerce

- Web merchants may be bogus.
- Customers may be fictitious.
- Electronic documents on the Web may not be authentic.
- Trading partners may deny that they were a party to the transaction.
- Transactions may be intercepted, tampered with or replayed.
- Digital signatures and electronic records may not be recognized as evidence in courts of law.
- Transactions may be hard to substantiate causing problem of accounting recognition.
- Audit trails may be insufficient or modified through hacking.

Most of the risks above relate to

- Authentication
- Integrity
- Non repudiation
- Confidentiality

Controls in E-Commerce

- Technical security measures e.g. Network Controls with firewalls, IDS etc.
- Use of Digital Signatures and Encryption could help mitigate the risks
- Third party assurance certification provides confidence and basic faith in entire E-Commerce process.

CAs role in E-Commerce

Chartered Accountants could play an active role in assisting clients in

- Assessing or assisting in implementing e-Commerce as relevant with appropriate security
- Setting up or reviewing Assurance policies
- E-Enabling and facilitating business operations through e-Commerce
- Review of back-up arrangements and procedures for continuity of operations

2.7 Summary

Business Intelligence is imperative to growth in any business. Ability to convert mountains of data to information is what separates winners from losers, BI is a tool to enable this conversion to information aiding in decision making. Important enablers for BI are Data warehouse and Data Mining. ERP has become an essential component of any business for seamless flow of information to users. E-commerce is the lubricant which is oiling revenue growth in every business. Chartered Accountants

have to understand these concepts so that they can play a proactive role in these areas. Understanding how these technologies works, their risks, security and controls opens out new avenues for CAs for providing IT enabled services.

2.8 References

- <http://businessintelligence.com/>
- http://www.cio.com/article/40296/Business_Intelligence_Definition_and_Solutions
- <http://cacm.acm.org/magazines/2011/8/114953-an-overview-of-business-intelligence-technology/fulltext>
- http://www.cio.com/article/40323/ERP_Definition_and_Solutions
- <http://www.ecommercetimes.com/>
- <http://money.howstuffworks.com/ecommerce.htm>

2.9 Questions

1. Which of the following is the primary goal of data mining?
 - A. To create a new data warehouse
 - B. To create data marts
 - C. To eliminate need to understand business
 - D. To discover useful patterns in large volume of diverse data
2. Which of the following is a Data Warehouse?
 - A. A system that is used to run the business in real time and is based on historical data
 - B. A system that is used to run the business in real time and is based on current data
 - C. A system that is used to support decision making and is based on historical data
 - D. A system that is used to support decision making and is based on current data
3. Which of the following is a tool that helps in predicting future trends & behaviors, allowing business managers to make proactive, knowledge driven decisions?
 - A. Data warehouse
 - B. Data mining
 - C. Data marts
 - D. Data Dictionary
4. Which of the following is incorrect?
 - A. Data mart contains more detailed data than DW.
 - B. Data Marts are used only by large Companies.
 - C. Data mart requires less powerful Hardware than DW.

Module 1: Facilitating e-Learning

- D. Data for a single aspect of business is stored in Data mart.
5. Which of the following is a challenge in ERP?
- A. Improved Data Access
 - B. Improvement in work processes.
 - C. Standardized Business processes.
 - D. Selection and configuration of ERP package
6. E-commerce refers to:
- A. any electronic communication between a Company and its shareholders
 - B. organization using electronic media to link to its employees
 - C. conduct of business activities over computer networks electronically.
 - D. use of electronic communications for all business processes.

2.10 Answers

- 1 D
- 2 C
- 3 B
- 4 B
- 5 D
- 6 C

CHAPTER 3: OVERVIEW OF CLOUD COMPUTING AND MOBILE CLOUDING: CHALLENGES AND OPPORTUNITIES FOR CAS

PART 1: CLOUD AND MOBILE COMPUTING

Learning Objectives

- To gain an overview of Cloud Computing
- To gain an overview of Mobile Computing
- To Understand risks and controls in Cloud and Mobile Computing
- To gain an overview of opportunities for CAs in Cloud and Mobile computing

1.1 Introduction

Using and embracing technology is not an option but mandatory for Chartered Accountants to perform their jobs effectively and efficiently. Chartered Accountants in their roles as consultants or auditors have to deal with Data/ Information for analysis and decision making. This data could be coming from computer systems of client which are now-a-days rapidly shifting to the Cloud. Cloud computing has its inherent business benefits but it also has its own risk, security and control issues. As Chartered Accountants we have to ensure that these inherent risks have been properly mitigated by implementing the right level of security and controls. Cloud computing exposes organisations and those who provide assurance on data which is processed and available on the cloud. These are new challenges which need to be addressed but at the same time these challenges also provide new opportunities. The biggest challenge is the inherent risks involved and the impact it has on services offered. The opportunity is that Chartered Accounts could provide consulting and assurance services to clients in the areas of Cloud Computing. Chartered Accountants have to understand concepts of cloud computing, service offerings, deployment models and the related risks and controls from two perspectives:

1. Impact on services provided to clients by accessing relevant data at clients offices or remotely;
2. Impact on how services are/ will be provided within their own offices using cloud computing.

Another emerging technology trend which has changed the way a Chartered Accountant works is Mobile Computing. Today a CA is using Smartphone, Tablet with Internet connectivity for personal uses, but there is an urgent need to expand it so that the same could be used for its professional purposes. A network of mobile devices could be given to staff for efficient execution of work, but at the same time a more mobile work force requires new levels of security and security administration. Apart from that many organisations have started offering mobile based computing like banks who

adopt multi-delivery channels in response to customer demands for greater convenience and lower costs. The wireless channel has seen growing acceptance in the retail payments. Yet another big adoption has come from E-Commerce sites, most of whom have launched their mobile applications. All these areas of Mobile computing have their fair share of risks and security concerns. Chartered Accountants as control expert can offer consulting and assurance services to these organisations to help mitigate these risks.

1.2 Cloud Computing

1.2.1 Understanding Cloud Computing

Cloud computing is a model for enabling, on demand networked access to a shared pool of computing resources - network/ bandwidth, servers, storage, applications, services etc. Cloud computing refers to computing power in all its totality or specified components (infrastructure, platform or service) being offered in the cloud as a utility to users, to be paid by the meter on consumption basis. As Internet connection's speeds increase and wireless Internet access broadens, more computing activities are being delivered on the Internet.

In the Cloud Architecture, the front end includes the client's computer (or computer network) and the Client application required to access the cloud computing system. This could be a Web browser or unique applications that provide network access to clients.

On the back end of the system are the various computers, servers and data storage systems that create the "cloud" of computing services. In theory, a cloud computing system could include practically any computer program we can imagine, from data processing to video games. Usually, each application will have its own dedicated server. Any mid-sized business like cooperative banks, Regional Rural Banks or any Marketing company would be benefited by cloud services as their needs could be met by services offered by the Cloud Service providers.

1.2.2 Characteristics of Cloud Computing

1. **On-demand self-service:** Automatic provisioning of computing capabilities as needed,
2. **Network Access:** Network should be accessible anywhere by any device - PC/laptop, PDA, smart phone.
3. **Resource Pooling:** Serving multiple clients using multi-tenant model with different physical and virtual resources
4. **Rapid Elasticity:** Capabilities to meet clients' increasing requirements at any time.
5. **Measured Services:** Capability to monitor resource usage for each process and client.

1.2.3 Features of Cloud Computing

Cloud computing typically entails the following important features:

1. **High Scalability:** Enables servicing of business requirements for larger audiences.
2. **Agility:** Works in 'distributed mode' environment. Shares resources among users and tasks, while improving efficiency and responsiveness.
3. **High Availability and Reliability:** Chances of infrastructure failure are minimal.
4. **Multi-sharing:** Multiple users and applications can work more efficiently with cost reductions by sharing common infrastructure.
5. **Virtualisation:** Allows servers and storage devices to increasingly share and utilize applications.

1.2.4 Types of Cloud Computing

The Cloud Computing Environment can consist of multiple types deployment models such as:

Public Cloud: Refers to service providers that offer their cloud based services to the general public.

Private Cloud: Refers to use of cloud computing concepts use within the confines of a private network. Some businesses like private cloud computing because it provides more control over infrastructure and security than public cloud computing.

Hybrid Cloud: Businesses may decide to combine public cloud and private cloud services to create a hybrid cloud.

Community Cloud: Several businesses share cloud computing resources.

1.2.5 Cloud Service Models

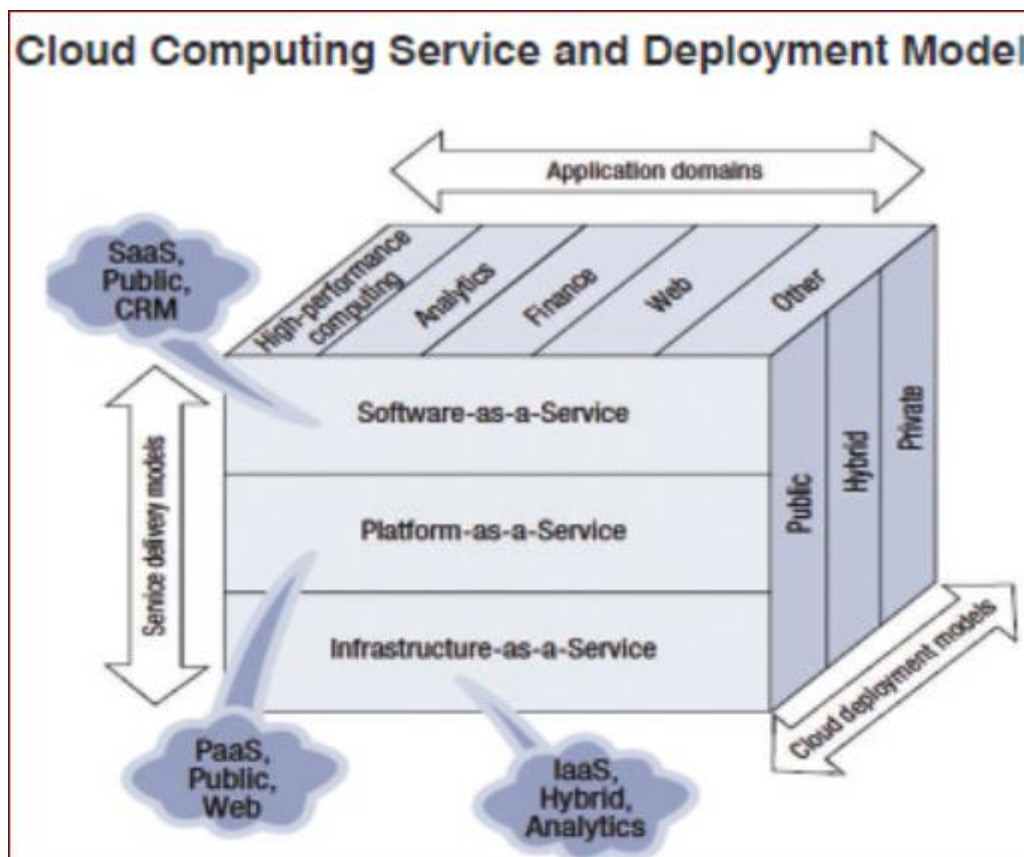
There are three dominant cloud computing models:

1. Infrastructure as a Service (IaaS)
2. Software as a Service (SaaS)
3. Platform as a Service (PaaS).

Infrastructure as a Service (IaaS): This has the capability to provision processing, storage, networks and other fundamental computing resources that offer the customer the ability to deploy and run arbitrary software, which can include operating systems and applications. Users are not required to manage the infrastructure as they do not possess the ownership of the underlying Cloud infrastructure.

Software as a Service (SaaS): This provides the capability to use the provider's applications that run on the cloud infrastructure. The applications are accessible from various client devices. Users are freed from the possession and maintenance issues of software and hardware.

Platform as a Service (PaaS): This provides the user organisation's application developers access the hardware and operating system platform allowing them to simply code and deploy applications on the platform without directly interacting with the underlying infrastructure.



Source: <https://cloudsecurityalliance.org>

1.2.6 Benefits and risks in Cloud Computing

Though cloud computing offers a lot of advantages to the organisation, yet there are a lot of associated risks. The benefits and risks are outlined below:

Benefits

- Gain competitive advantage.
- Reach new markets.
- Improve existing products and services.

- Retain existing customers.
- Increase productivity.
- Contain cost.
- Develop products or services that could not be possible without cloud services.
- Break geographic barriers.

Risks

- Greater dependency on third parties, wherever third party services used.
- Computing services do fail, leaving users unable to access programs or data.
- Computing services can lose customer data.
- Increased complexity of compliance with laws and regulations.
- The dynamic nature of cloud computing may result in confusion as to where information actually resides. When information retrieval is required, this may create delays.
- Due to the dynamic nature of the cloud, information may not immediately be located in the event of a disaster.

1.2.7 Impact of Cloud Computing on CAs

Cloud computing is the new way to do business in our profession. There is absolutely nothing mystical or overly complicated about this model. Technology has and continues to change the way we function within our practices. Think about the changes that we have witnessed over the past 15 years — e-mailing, document management, electronic filing, dual monitors, the scanning of source documents, the proliferation of mobile computing technologies and use of smaller, more powerful handheld devices, as well as the use of social networking as a new way to interact with prospective and existing clients and employees, and other professionals. The opportunities lie in the areas of assurance, consulting and implementation.

Assurance Services in Cloud Computing

In the realm of assurance services, the auditor is required to assess,

- How much security is enough?
- Criticality of the application being sent to the cloud.
- Outsourcer's experience with SLA and vendor management
- Does the present security model have to be altered?
- Cloud vendor's policy on vulnerability management – reporting (beyond basic 'Contact Us' links), commitment to following up, promptly responding to reports etc.
- Is there an independent auditor's report?

Module 1: Facilitating e-Learning

- What is the impact on the auditor when client has used cloud computing and the data to be audited is with the cloud service provider?
- How will the auditor access and audit this data?
- What is the impact on compliances?
- What is the impact on security?
- Who is responsible for security of data?
- Who owns the data?
- Where does the data reside?
- What business continuity and disaster recovery measures are in place in the cloud infrastructure? Does the cloud provider have a backup in place?
- How do I audit or evaluate security controls placed on the cloud-based infrastructure?

Consulting In Cloud Computing

A Chartered Accountant can provide consulting to clients in the areas of Cloud Computing and can even help a client move to cloud. Following are the steps involved in moving to cloud where a Chartered Accountant can provide consulting service at perhaps every step.

1. Understand the mission.
2. Identify the culture.
3. Determine the value.
4. Understand your data.
5. Understand your services.
6. Understand your processes.
7. Understand the cloud resources.
8. Identify candidate data.
9. Identify candidate services
10. Identify candidate processes.
11. **Create a governance strategy.**
12. **Create a security strategy.**
13. Bind candidate services to data and processes.
14. Relocate services, processes, and information.

15. **Implement security.**
16. **Implement governance.**
17. Implement operations

1.3 Mobile Computing

1.3.1 Technology Components

Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link. Mobile computing is not just about using mobile phones but it is about computing on the move using wireless connectivity. Mobile computing is enabled by use of mobile devices (portable and hand held computing devices) such as PDA, laptops, mobile phones, MP3 players, digital cameras, tablet PC and Palmtops on a wireless network. The key components of mobile computing are:

1. Mobile communication
2. Mobile hardware
3. Mobile software

1. Mobile communication

Mobile communication refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. This would include devices such as Protocols, Services, Bandwidth, and Portals necessary to facilitate and support the stated services. The data format is also defined at this stage. This ensures that there is no collision with other existing systems offering the same services.

2. Mobile hardware

Mobile hardware includes mobile devices or device components that receive or access the service of mobility. They would range from Portable laptops, Smartphones, Tablet PC's, Personal Digital Assistants. These devices use an existing and established network to operate on. In most cases, it would be a wireless network. At the back end, there are various servers like Application Servers, Database Servers and Servers with wireless support, WAP gateway, a Communications Server and/or MCSS (Mobile communications server switch) or a wireless gateway embedded in wireless carrier's network (this server provides communications functionality to allow the handheld device to communicate with the Internet or Intranet infrastructure).

3. Mobile software

Mobile software is the actual program that runs on the mobile hardware. It deals with the characteristics and requirements of mobile applications. It is the operating system of that appliance. It's the essential component that makes the mobile device operate. Mobile applications popularly

called Apps are being developed by organisations for use by customers but these apps could represent risks, in terms of flow of data as well as personal identification risks, introduction of malware and access to personal information of mobile owner.

1.3.2 Advantages and Security Concerns of Mobile Computing

Advantages of Mobile Computing

- **Location flexibility:** Mobile Computing enables user to work from anywhere as long as there is a connection established. A user can work without being in a fixed position.
- **Saves time:** Time reduced as there is no travel required from different locations such as office and back.
- **Enhanced productivity:** Employees can work efficiently and effectively from any location they are comfortable with and at any time they want.
- **Ease of research:** Research is made easier, since users in the field searching for facts can feed data back to the system.
- **Entertainment-** Video and audio recordings can be streamed on the go using mobile computing. It makes it easy to access a wide variety of movies, educational and informative material.

Security Issues in Mobile Computing

Following are some of the major security issues in Mobile Computing:

- It is not easy to monitor the proper usage. Improper and unethical practices such as hacking, industrial espionage, pirating, online fraud and malicious destruction are some problems experienced due to mobile computing.
- The problem of identity theft is very difficult to contain or eradicate.
- Unauthorized access to data and information by hackers.
- Physical damage to devices, data corruption, data leakage, interception of calls and possible exposure of sensitive information.
- Lost devices or unauthorized access to unsecured devices allows exposure of sensitive data, resulting in loss to the enterprise, customers or employees.
- Mobile Apps could also represent a big security risk

Controls in Mobile Computing

Some of the practices to mitigate these security concerns are:

- Developing and implementing a Mobile computing security policy.
- Use of encryption technology such as virtual private networks.
- Use of power-on passwords.
- Use of encryption for stored information.
- Installing security software.

- Educating the users on proper mobile computing ethics.
- Enforcing proper access rights and permissions.
- Auditing mobile security policy and implementation.

1.3.3 Opportunities for CAs

As with any IT, CAs have to understand mobile computing technology from three perspectives:

- Using Mobile computing within a CA firm.
- Provide consulting services on mobile computing for clients.
- Provide assurance services on mobile computing for clients.

Using Mobile computing in CA firm:

Mobile computing can be used by CAs in their own offices for enhancing overall efficiency and effectiveness of services rendered by the firm. However, implementation has to be based on the overall IT Strategic plan of the firm and should take into consideration the current technology deployed, organisation structure, technical competency of the staff, services offered currently and planned in the future, client profile, usage of technology by clients, cost benefit analysis, etc. A detailed project plan with specific milestones and timelines has to be prepared and implemented considering all the above factors rather than just buying mobile devices with connectivity.

Consulting on mobile technology implementation:

The areas where Chartered Accountants can add value and provide consultancy services are:

1. Business strategy/business process transformation.
2. Risk Assessment, risk mitigating strategy and security at different layers of technology.
3. Designing security policy for the enterprise.
4. Access controls at different layers of technology and for devices/employees.
5. Application and business process controls to be implemented.
6. Training to users on risks, security and controls.

Assurance services on Mobile technology implementation

Some of the areas where auditors can have a significant role in providing assurance services:

1. Information systems audit of all/any aspect of security policy, business continuity, environmental access, physical access, logical access and application security.
2. Compliance with enterprise policies, procedures, standards and practices as relevant.
3. Physical verification or confirmation of usage of mobile devices.
4. Compliance with regulations as applicable.
5. Network security, Database security and Penetration testing as required.

1.4 Summary

Accelerated adoption of emerging technologies like Cloud Computing and Mobile Computing has provided a lot of advantages to organisations. However; at the same time the technology implementation has inherent risks which have to be properly understood and mitigated. Chartered accountants have to understand the inherent risks in these technologies so that these could be considered while auditing. An understanding of these technologies will also open new opportunities to the Chartered Accountants in providing related assurance and consulting Services.

1.5 References

- www.isaca.org/cloud
- www.cloudconnectevent.in
- www.cloudsecurityalliance.org/
- www.csrc.nist.gov/groups/SNS/cloud-computing/
- www.opencloudconsortium.org/
- www.opencloudmanifesto.org/
- www.cloud-standards.org/wiki/
- www.searchcloudcomputing.techtarget.com/
- www.cloudcomputing.sys-con.com/
- www.cloudsecurity.org/
- www.cloudaudit.org/

1.6 Questions

1. Which of the following is not a service model for cloud?
 - A. IaaS (Infrastructure as a service)
 - B. Paas (Platform as a Service)
 - C. SaaS (Software as a Service)
 - D. DaaS (Display as a Service)
2. Which of the following would not be a reason to move to cloud computing?
 - A. Agility
 - B. Scalability
 - C. Security
 - D. Resource Pooling
3. Which of the following is not a benefit of cloud computing?
 - A. Vendor lock in

- B. Ability to access the application & data from anywhere
- C. Reduce Hardware Costs
- D. Reduce need for physical space

4. Which of the following is not an advantage of Mobile Computing?

- A. Saves time
- B. Entertainment
- C. Health hazard
- D. Location flexibility

1.7 Answers

- 1 D
- 2 C
- 3 A
- 4 C

PART 2: EMERGING TECHNOLOGIES: BYOD, XML-XBRL AND SOCIAL MEDIA

Learning Objectives

- To gain an overview of BYOD
- To gain an overview of XML and XBRL
- To gain an overview of use of Social Media

2.1 Introduction

IT environment is continually evolving and growing. The growing trend in this direction is BYOD (Bring your own Device) and now even BYOT (Bring your own Technology) where employees are encouraged to use their hand-held devices for organisation's business. A common term sometimes used is BYODT. Use of XML and XBRL has changed the way of corporate reporting and enhances the distribution and usability of existing financial statement information. Another technology trend that has brought a whole revolution is the use of Social Media. Social media has become a big booster to any business. Whereas all these provide advances in technology at the same time, the potential risks associated with these cannot be ignored. Chartered Accountants have to know about these technologies works, their risks, security and controls and impact on assurance. This understanding can help CAs in using these technologies as relevant not only in their own offices and professional practice but also to provide consulting and assurance services to organisations in these emerging area.

2.2 Bring Your Own Device (BYOD)

BYOD refers to that policy of an organisation that allows its employees to use a preferred computing device like a laptop or a smart phone. It allows employees to use personal devices to connect to the corporate network for information. The workspaces are made flexible that allows employees to work beyond the required hours. It has reduced IT costs for organisations because a onetime investment is made by the organisation that enables employees to buy and maintain their devices. However, it also means surrendering all control over the end-user device. Service delivery, data protection and providing support and services when user device is not working are some of the challenges. If not properly controlled the device may become conduit for a serious data security breach.

2.2.1 Advantages of BYOD

BYOD implementation has many advantages. These are:

- **Happy Employees:** Employees love to use their own devices when at work. This also reduces the number of devices an employee has to carry; otherwise he would be carrying his personal as well as Organisation provided devices.
- **Lower IT Budgets:** Could involve financial savings to the Organisation since employees would be using the devices they already possess thus reducing the outlay of the Organisation in providing devices to employees.
- **IT reduced support requirement:** IT Department does not have to provide end user support and maintenance for all these devices resulting in cost savings.
- **Early adoption of new technologies:** Employees are generally proactive in adoption of new technologies. Their early adoption of technologies also results in enhanced productivity of employees leading to overall growth of business.
- **Increased Employee efficiency:** Employees using their own devices are adept at these and are familiar with these devices. The efficiency of employees is more whereas in Organisation provided devices employees have to learn and there is a learning curve involved.

2.2.2 Security Concerns of BYOD

- **Security Administration Issues:** The device may have been built on relatively nascent, consumer focussed platform that does not provide the underlying management controls of the organisation. Allowing employees to bring their own devices has to be aligned with the Security Governance and security policies.
- **Ownership of Data and Regulatory compliance issues:** Private and corporate data is on the same device could raise ownership issues. Much regulatory compliance would become difficult for corporates to follow.
- **Confidentiality and Privacy issues:** This would be a huge challenge for the Organisation, protecting the data on devices not owned by it. Many organisations having sensitive data, this could be the toughest challenge. If the device is connected to the network of the organisation without appropriate controls having been put in place, this could lead to unauthorized access to the whole network.
- **Compatibility issues:** Since employees will be having diverse devices, there will not be a uniformity and whole lot of compatibility issues could arise. Applications on devices also could be different leading to incompatibilities
- **Reluctance of employees:** Not all employees could be comfortable with using their own devices for office work.

2.2.3 Controls Relating To BYOD

Effective implementation of controls to mitigate these risks could be:

- **Establishing a BYOD Governance framework:** A strategy for BYOD usage could be framed taking into account Network access Controls, Device Management controls, Application Security management controls.

- **Security Policy:** A well-defined security policy specifying the rules for use and organisations expectations regarding security should be there clearly specifying the security requirements like security tool to be mandatorily installed or prohibiting download of black listed applications or encryption of data. Policy may specify that only approved and duly authorized devices that are known to have appropriate security controls are used.
- **Appropriate Use Policy:** The employees may be required to sign an AUP that specifies organisation's expectations of employee responsibilities.
- **Network Security:** Secure access to corporate networks could be ensured using VPNs.
- **Segregation of Personal and Corporate Data:** Data classification should be followed to determine the kind of data which can be stored on personal devices. Important data of Organisation could be in a separate container with encryption, apart from providing protection this also makes it easy to wipe corporate data when an employee leaves the organisation or the device is stolen, where data could be wiped remotely.
- **Secure Remote Support:** Organisations may deploy remote Support Solutions that facilitates remote configuration and control of the device from Help Desk. They also provide access and activity logs for monitoring.
- **Regular Audits:** All the BYOD Devices should be subject to audits to determine adherence to Security policies and determining the kind on data residing on those devices.

2.2.4 Opportunities for CAs

Due to significant risks involved in BYOD adoption, Chartered Accountants being control experts can provide assurance or consulting services in formulating right type of policies, implementing governance framework and implementing right level of security using best practices as appropriate.

2.3 XML-XBRL

2.3.1 XML

What is XML?

World Wide Web Consortium (W3C) has defined XML as follows: "XML is a set of rules, guidelines, conventions, whatever you want to call them, for designing text formats for such data, in a way that produces files that are easy to generate and read (by a computer), that are unambiguous, and that avoid common pitfalls, such as lack of extensibility, lack of support for internationalization or localization, and platform-dependency."

XML was initially developed by the World Wide Web Consortium (W3C). XML is universally accepted method of exchanging information. XML stands for **eXtensible Markup Language**. It is a markup language just like HTML. XML is a platform-independent, self-describing, expandable, standard data exchange format. XML was designed to describe data and to carry data, it does not do anything, it

is created to structure, store, and to send information. XML uses self-Descriptive XML Schema or Data Type Definition (DTD) to describe Data.

It is much more powerful than HTML (Hypertext Markup Language). HTML is a page description language and is used for specifying how text, graphics, videos and sound are placed on a web page document. Whereas HTML describes how data should be presented in the form of web pages, XML performs presentation, communication and storage of data. In XML, tags represent a price, a date or a PIN code for example. XML makes it possible for computers to manipulate and interpret data automatically and perform operations on the data without human intervention.

In HTML Tags are predefined, whereas in XML Tags are not predefined; we must define our own tags. The XML tag teaches the receiving program how to read the data. For example `<DATE>March 31, 2014</DATE>` i.e. it describes information not presentation and tags `<Date>` has been defined by us. With XML, data can be stored outside an HTML in another file or can also be stored inside HTML.

Why to use XML?

Computer systems and databases may contain data in incompatible formats. The challenge is how to make these systems interoperable so that they can exchange data. This exchange of data is facilitated by XML, since XML helps create data so that it can be read by different applications. XML enables new levels of interoperability as it is portable, vendor neutral and is also in an easily readable format which is supported by all major software products. XML provides a standard format for data exchange, enabling web services to pass data from one process to another.

How is XML used?

An example of how XML is used is given below:

```
<Account>
<AccountID>123456</Name>
<Name>Travelling Expenses</Name>
<Group>Expenses<Group>
<Opening Balance>2344.00</ Opening Balance >
<Type>Dr</Type>
</Account>
```

It gives meaning to raw data by describing information through use of tags.

Where is XML used?

Today XML is being used to exchange financial information, business information, and Industry information. It is being used in many B2B (Business to Business) applications. Many Web Services

rely upon integrated software solutions. All these are using XML for data interchange amongst the applications.

Who is using XML?

XML is being used by:

- Software developers use XML as the core technology for new products to derive advantages of interoperability. Microsoft has made MS Excel 2007 onwards XML based so that data can be shared by different applications.
- Database developers build XML support into their products, since XML data is structured in such a way that allows machines to read it and make it accessible to the database.
- Organisation may have different application for different processes within the organisation. To enable them to share data, XML is used thus tying inter and intra organisation processes together.

Risks of using XML

The ease of viewing and editing text produces risks related to confidentiality and integrity. The XML specification does not provide mechanisms to enforce standard data formats; thus XML lacks inherent security and does not provide any means of validation, confidentiality or Integrity. XML could be cause of denial of service attack through means where XML causes machine to use lot of memory and processing, ultimately hanging the system.

Controls in XML

Controls in XML could be

- For validation, external validation utilities can be used.
- Encryption could be used to ensure confidentiality.
- Security through SSL has to be ensured whenever transmitting XML data over unsecured networks.
- The applications receiving XML may have validations to prevent XML DOS attacks.

2.3.2 XBRL

XBRL (eXtensible Business Reporting Language) is a freely available and global standard for exchanging business information. XBRL allows the expression of semantic meaning commonly required in business reporting. The language is XML-based and uses the XML syntax and related XML technologies such as XML Schema. One use of XBRL is to define and exchange financial information, such as a financial statement. The XBRL Specification is developed and published by XBRL International.

XBRL is a standards-based way to communicate and exchange business information between business systems. It offers major benefits at all stages of business reporting and analysis. XBRL is being used across a wide range of sectors, including securities regulation, banking, insurance, data aggregators and taxation, as well as for non-financial reporting such as carbon disclosure, sustainability efforts and risk reporting.

Tags for XML are most of the times defined by industry consortiums. These industry's standard tags are commonly referred to as taxonomy. Taxonomies are similar to dictionaries; they are long lists of agreed-upon definitions for all the terms used in specific types of business reports. Each definition has a "tag" that can be read and used by computers. One such standard taxonomy for business reporting is defined by XBRL. XBRL is "extensible," meaning local users can extend XBRL taxonomies to satisfy their own needs.

Use of XBRL in financial sector

XBRL is flexible and is intended to support all current aspects of reporting in different countries and industries. Its extensible nature means that it can be adjusted to meet particular business requirements, even at the individual organisation level. With different financial statements speaking different languages, there will always be an inefficient analysis of financial information leading to ineffective communication to investors and stakeholders. With enabling of XBRL, documents can be prepared efficiently, exchanged reliably, published easily, analysed quickly and retrieved by investors simply to enable smarter investments.

Advantages of XBRL

The advantages of XBRL data over conventional forms of data are:

- Standard - XBRL is a standard that has been accepted and adopted the world over thus reducing inconsistencies in terminologies and data formatting.
- Accuracy - XBRL provides highly accurate data as the data can be both calculated and verified.
- Speed - XBRL allows much faster and real-time preparation of reports and at the same time allows efficient, accurate and relevant ways to search data.
- Reusable - XBRL data once entered can be reused to represent the same data in multiple ways and multiple formats.
- Platform Independent - XBRL is an open standard and hence platform independent, this allows the data to be exchanged and transferred with ease.
- Region Independent - XBRL allows the presentation and exchange of data in many different languages.

It also helps in reducing cost of analysing and reporting financial information and helps in corporate decision making. Today by submission of financial information in XBRL to bank, bank will take a

lesser time to analyse information and quickly sanction loans to the corporates. A Large Multi-national Corporation using XBRL can quickly publish the financial statements of numerous subsidiaries in different countries, with different languages, using different GAAPs on different computer systems.

How is XBRL used?

XBRL makes the data readable, with the help of two documents – Taxonomy and instance document. Taxonomy defines the elements and their relationships based on the regulatory requirements. Using the taxonomy prescribed by the regulators, companies have to map their reports, and generate a valid XBRL instance document. The process of mapping means matching the concepts as reported by the company to the corresponding element in the taxonomy. In addition to assigning XBRL tag from taxonomy, information like unit of measurement, period of data, scale of reporting etc., has to be included in the instance document. An XBRL instance document is a business report in an electronic format created according to the rules of XBRL. Let's say we have the data in table as given here:

Company	Financial Statement	Line Item	Label	Year	Value
ABC Ltd.	Balance Sheet	Current Assets. Cash and Cash Equivalents	CurrentAssets. CashandCashEquivalents	2012	98765432
ABC Ltd.	Balance Sheet	Current Assets. Cash and Cash Equivalents	CurrentAssets. CashandCashEquivalents	2013	99887766

In XBRL the same would be mapped as follows:

```
<group>
```

```
<group type="CurrentAssets.CashandCashEquivalents">
```

<item period="2012">Rs. 98765432</item>

<item period="2013">Rs. 99887766</item>

</group>

Risks in XBRL

Apart from risks related to XML discussed above, some specific risks of XBRL are:

- Creation and implementation of taxonomies incorrectly.
- Errors in Mapping - Inaccurate mapping of business information to tags and the use of inappropriate taxonomies (i.e., XBRL dictionaries that define the specific tags for individual items of data). This can mean that the data retrieved represents invalid and inaccurate transactions.
- As the XBRL documents may include internal and external links to the organisation; hackers may try to change those links or the linked files.

Controls in XBRL

- Evaluation of algorithms used to Tag XBRL data and an effective internal control structure to ensure accurate tagging.
- Enforcing Change Management Process for XBRL process.
- Hacking and related risks could be mitigated by implementation of appropriate firewall encryptions.

Impact and avenues for CAs

Chartered Accountants spend a lot of time importing data from corporate financial applications to their spreadsheets and allied Data Analysis Software, making the whole thing inefficient. XBRL can help reduce time spent manually preparing information for analysis; further data quality can also be improved through fully automated information exchanges among disparate software applications. Once CAs can electronically receive, validate and send standardized information, they can quickly analyse and confidently redistribute it to managers, stakeholders and others for use in better informed decision making.

Being well versed with the benefits and control issues is of special importance to auditors, as more and more countries are mandating the use of XBRL. The opportunities for CAs are in the area of Assurance Services to organisations, by:

- Developing controls framework tailored to the organisation's specific implementation.
- Assessing the quality of XBRL submission and evaluating the supporting XBRL business processes.
- Evaluating the effectiveness of firewall security controls for prevention of hacking attempts.

2.4 Use of Social Media

Social media is a blur of tweets, shares and content. It has pervaded every aspect of life of individuals and now impacting bottom-line of organisations also. Tech target defines “Social media is the collective of online communications channels dedicated to community-based input, interaction, content-sharing and collaboration. Websites and applications dedicated to forums, microblogging, social networking, social bookmarking, social curation, and wikis are among the different types of social media.” Some of the examples are Facebook, Twitter (microblogging), LinkedIn (social networking), Pinterest (social curation i.e. ***filtering of information and links in a socially enhanced way around a specific theme***).

In Social Media, content is supplied and managed by user through the use of tools and platforms supplied by social media sites. Use of social media by people and organisations is increasing rapidly and the potential benefits of a successful social media strategy are significant. Organisations as well as individuals can create online presence easily and economically, since social media technologies have significantly reduced the cost of content creation and dissemination to a small or a very large audience in virtually real time. Most of the businesses are changing their strategy of marketing through social media, this change has stemmed from the speed at which information travels in the social media arena. Social media provides an opportunity for businesses, giving them a personalized platform to connect with their customers. By using social media as a way to advertise, the organisation can speak directly to the consumer in an arena they are comfortable with. Social media allows businesses to connect with customers while shaping their perceptions of products and services.

2.4.1 Risks and Security Concerns in Use of Social Media

Many enterprises have adopted social media tools which require no further IT investments and are quick to implement, often these adoptions carry risks such as breach of privacy, fear of legal action, developing a negative reputation and lack of control. These carry a huge risk in terms of enterprise security. Risks could arise from use of social media for client communication or from use of social media by employees on organisation networks or organisation devices.

Risks and security concerns also exist in the content put up on social media. The content put on social media could have security concerns relating to privacy and confidentiality and may also have implications in breach of regulations. For highly regulated sectors like finance, insurance and banking social media can be a legal minefield. As an example, on March 7, 2010, Gene Morphis, Chief Financial Officer (CFO) for fashion retailer Francesca’s Holding Corp., tweeted from his personal Twitter account (@theoldcfo): “Board meeting. Good numbers=Happy board.” — two days before the actual numbers were released. Morphis’ 238 Twitter followers were privy to insider information which is an SEC breach. He was fired shortly thereafter for the offense of “improperly communicating organisation information through social media.”

2.4.2 Mitigating Security Concerns

The combination of the right policy and the right technology can mitigate the security concerns and make organisations compliant. These are explained below:

- **Social Media Policy:** The firm must have a social media policy specifying how there will be interaction between organisation and the world through social media. These policies should consider technology as well as regulatory compliance requirements.
- **Training of People:** Employees should be trained on a regular basis on the benefits, opportunities and risks relating to use of social media. Employees have to be educated about the dangers and common pitfalls in the use of social media and how to prevent them, as also acceptable use policy regarding the kind of material that could be posted on social media sites and their use.
- **Pre-approval and vetting of content before uploading:** There should be a system of pre-approval of content like profiles before posting on sites like Facebook and LinkedIn. Interactive content must be supervised both from an official account or an employee's own personal account relating to business.
- **Provision for regulatory compliances:** Many companies having presence in US and other Countries could be subject to legal compliances relating to those countries. Regulations in some countries provide for archival of business communication of social media for some periods which has to be adhered to. (Some technical tools are available which often integrate with existing email compliance solutions, can automatically capture social content from both desktops and mobile devices, storing it securely on cloud-based servers).
- **Technical Controls:** Some tools like enterprise social media management systems, allow firms to assign limited permissions to certain employees. Limited users are free to draft tweets and updates, which are then fed into approval queues for manager review. Organisations could also enable web content filtering, which can block all access or allow limited access. Use of Antivirus and Operating system security can provide protection against malware downloads and hacking.

2.4.3 Opportunities for CAs

Use of social media has changed the way an organisation functions today as new products are being launched on social media. This could have an important implication for Chartered Accountants in three areas:

- Using Social media for their own professional development.
- Using the power of social media for clients and providing services in development of social media governance and strategy.
- Providing assurance services in reviewing client's strategy for risk mitigation in use of social media.

Some of the sample areas to consider which could be basis of providing consulting or assurance services from two different perspectives

(1) In respect of an organisation which is using social media for its business,

- Does the organisation strategy outline short, medium and long term goals relating to Social media and how these will be accomplished?
- Has the organisation assessed the different social media channels or Social Collaboration Platforms available and made an informed decision about which channel to focus on platform to adopt?
- Does the organisation's policy fit into organisation's culture and can employees understand it?
- Has the organisation ensured that employees understand the needs of the organisation in relation to social media?
- Has the organisation implemented the controls and are they effective?
- Have regulatory and legislative requirements been assessed and considered in internal policies and procedures?
- Has the organisation set out data classification criteria and are there controls established to ensure adherence?
- Have roles and responsibilities been defined and communicated?
- How does the organisation manage its data?
- Does the organisation have a detailed plan in place to deal with crisis related to social media?
- Does the plan identify responsible persons?
- Does it include timescales?

(2) In respect of all other organisations, assess the need to control access by its employees to social media.

- Does the organisation policy address employees' use of social media?
- How the organisation has trained the employees to use social media responsibly?
- Does the organisation have a plan in place to deal with crisis created by employee use of social media?
- How does the organisation monitor to what is happening in social media outside of its own channels?

2.5 Geolocation

Geolocation refers to the technology that uses data acquired from an individual's computer or mobile device (any type of radio or network-connection-enabled device) to identify or describe his/her actual physical location. This is one of the most popular usage of the current development of IT. This involves identification of the real-world geographic location of an object, such as a radar, mobile phone or an Internet-connected computer terminal. Geolocation is closely related to the use of positioning systems but can be distinguished from it by a greater emphasis on determining a meaningful location (e.g. a street address) rather than just a set of geographic coordinates.

2.5.1 Benefits of Geolocation

ISACA has published a white paper on “Geo Location: Risk, Issues and Strategies” which has outlined the business benefits and risks of Geolocation and how to implement the right level of governance and control. Mobile Geolocation services have become pervasive in the “always connected” world. They have introduced innovative, profitable and functional services and applications. With location technology, a user’s experience can be uniquely personalized, which appeals to marketers, retailers, government entities, law enforcement, lawyers but it also attracts many criminals. Geo location has far-reaching benefits and are being leveraged by all types of enterprises such as manufacturing, retail sales, financial services, insurance, transportation, utilities and governments. Some of the key business benefits are:

- In advertising, use of designated market areas (DMA) and demographic data
- Know your customer (KYC), e.g., better understanding of customer requirements and expectations for products and services and benefits accruing from targeted sales
- Delivery and asset management, e.g., truck location and manifest status
- Content customization and delivery, such as movies on demand
- Fine-grained management of Internet commerce activities and interests
- Optimal request routing
- Cloud balancing
- Fraud detection and prevention using IP location technology in conjunction with fraud profile data
- Real-time incident management through Geolocation enrichment of logs and other IT data

2.5.2 Risks and security of Geolocation

Although there are many benefits, the services of Geolocation also increases risk to the user, the service providers and those who utilize the data collected by the service providers. When a user utilizes an application and its services, there may be multiple data controllers: the service provider, wireless access points and/or developers. Multiple data controllers force users to accede control of the systems that determine and store their location and other personal information. Consequently, users usually cannot identify the source and ownership of data collection. This raises several questions of concern for the user, such as how their location data are being used, with whom the data will be shared, whether there will be onward transfer of the data, and the timeline for data retention and destruction.

As the rise in the use of location-aware apps and geo-marketing continue, concerns keep on growing around online privacy and specifically, business practices around the collection and use of the PII data. As the user group grows, continually utilizing new features and creative applications on their smartphones and other mobile devices, the prospect of criminal attacks becomes even more probable and a major cause of concern. The amount and the nature of individual and corporate

information available to potential hackers would allow targeted attacks that are difficult to prevent, detect and manage. From social engineering arises the risk of a user being subjected to location-based spamming. IP Geolocation attacks can occur in two ways:

- It identifies the physical location of an organization's hosted e-mail. The spammer uses this information to plan a targeted attack that will overload the enterprise's servers, causing usage issues.
- Spamming attacks to an individual's e-mail or mobile device are targeted and are, therefore, highly effective at soliciting a response acknowledgment from the victim.

Enterprise needs to understand the benefits and risks of Geolocation and harness the power of this technology but ensure that proper controls are implemented. The information Technology Act 2000 as amended in 2008 provides guidelines and stipulations on maintaining privacy of personal and sensitive information. Geo Location involves collection of personal information of the users. Hence, appropriate controls have to be implemented to ensure risks are identified and mitigated.

2.5 Summary

Emerging Technology trends such as BYOD are revolutionising the way organisations work and could have implications in terms of risks and security concerns which have to be mitigated. XML and XBRL have made sharing of data among different applications easy and efficient. Use of social media provides unprecedented growth opportunities for any organisation but the use has to be controlled through appropriate security and controls so that benefits can be realised. Geo Location provides immense benefits to organisations but has its inherent risks which need to be mitigated by implementing the right level of controls. CAs with good understanding of these emerging technologies in terms of features, benefits, risks and controls can provide innovative IT enabled services of consulting, implementation and assurance services in all these emerging areas.

2.6 References

- <http://www.xml.com/>
- www.webdeveloper.com/xml/
- <http://www.ucc.ie/xml/>
- <http://www.xbrl.org/>
- <http://www.microsoft.com/msft/XBRL/FinancialXBRLwp.htm>
- <http://blogs.hbr.org/2012/12/how-not-to-unwittingly-reveal/>
- www.isaca.org/socialmedia.

2.7 Questions

1. Which of the following is not a concern of BYOD?

Module 1: Facilitating e-Learning

- A. Reluctance of Employees
 - B. Compatibility issues
 - C. Reduced IT support requirement
 - D. Security Administration issues
2. Which of the following facilitates data exchange and defining of tags?
- A. HTML
 - B. Social Media
 - C. BYOD
 - D. XML
3. In which of the following, is content managed & supplied by user?
- A. XBRL
 - B. XML
 - C. BYOD
 - D. Social Media
4. Social Media benefits both users and marketers because:
- A. it leads to an increase in Internet traffic.
 - B. through use of social media marketers will have a more robust online presence.
 - C. marketers will have monopoly over users.
 - D. users will have less influence over the marketplace.
5. Which of the following is not an advantage of XBRL?
- A. Accuracy
 - B. Speed
 - C. Reusability
 - D. Taxonomies are always accurate

2.8 Answers

- 1 C
- 2 D
- 3 D
- 4 B
- 5 D

CHAPTER 4: OVERVIEW OF BUSINESS INFORMATION SYSTEMS AND RISK AND CONTROLS IN NEWER TECHNOLOGIES

PART 1: BUSINESS INFORMATION SYSTEMS

Learning Objectives

- To gain an overview of Artificial Intelligence
- To gain an overview of Transaction Processing Systems
- To gain an overview of Decision Support Systems
- To gain an overview of Executive Support Systems

1.1 Introduction

Businesses are growing at a phenomenal rate, more information a business acquires more difficult it becomes to take decisions. The amount of information people must understand is growing at an exponential rate, with such massive information taking a decision is a big challenge, without using some information system. There is also a growing need to take decisions quickly, since time is of the essence here. This has necessitated use of sophisticated analysis techniques using information systems. Business Information Systems work on business information to lend an insight into important business problems and opportunities. Three common types of business information systems used are:

1. Transaction Processing Systems provide an answer to structured problems and doing routine transactional jobs.
2. Decision support Systems provide answers to semi structured problems answering the question "Are we doing the right Things".
3. Executive Support Systems deal with unstructured problems and provide support to the Executive Management in planning Strategy and vision.

Executive Support Systems	• Executives
Decision Support Systems	• Managers
Transaction Processing Systems	• Analysts, Operations

Business information systems are starting to take advantage of artificial intelligence to help executives make strategic decisions. Computers were meant and used for repetitive tasks but with the advent of Artificial Intelligence we are coming to an era where computers would be using

cognitive behaviour and displaying human traits of problem solving. Business Information systems are essential to organisations' success. Huge amounts of data getting generated from different systems when amassed has given rise to the concept of Big Data, which is being used by organisations to come up with ground breaking insights into business operations.

1.2 Artificial Intelligence

Stanford University Computer Science professor John McCarthy coined the phrase in 1956 to mean "the science and engineering of making intelligent machines." AAAI (Association for the Advancement of Artificial Intelligence) defines Artificial Intelligence as "the scientific understanding of the mechanisms underlying thought and intelligent behaviour and their embodiment in machines." Artificial Intelligence (AI) refers to a term that describes computers with the ability to mimic or duplicate the functions of the human brain. Advances in AI have led to systems that can recognize complex patterns.

Artificial Intelligence systems include the people, procedures, hardware, software, data and knowledge needed to develop computer systems and machines that demonstrate characteristics of intelligence. AI can be used by most industries and applications. Researchers, scientists and experts on how human beings think and behave in a given situation are often involved in developing these systems. Computers are best suited to perform simple but monotonous tasks efficiently and reliably, performing mechanical computations, using fixed programmed rules. Wherever complex problems arise, which need understanding specific situations, and adapting to new situations, computers fail. Artificial Intelligence aims to impart computer problem solving skills based on abstract thought, high-level deliberative reasoning and pattern recognition.

Artificial intelligence works with the help of Artificial Neurons (Artificial Neural Network) and scientific theorems (If-Then Statements, Logics). Despite advances which have happened in AI area not all human intelligence traits can be captured in Computer. AI is more focussing on limited Domain specific applications. That is the reason there are many different approaches to AI, one could be more suited than others in a specific circumstance. Artificial Intelligence is split into many branches, like neural networks, fuzzy logic, speech recognitions, translation, robotics etc. Some of the daily use commercial applications like MSWord have some element of AI built in, when we have keyed-in only a few letters of a word, it simply pops up the suggested complete words, to choose from. Also it keeps on updating its database of the words which the user has used. This is one of the simplest examples that explain the basic concept of AI. At a very simple level, Speech recognition software in our Smartphones also uses some components of AI. Another application of AI is Smile detector or automatic face detector in our Cameras.

The potential applications of Artificial Intelligence are many. AI has been used in a wide range of fields including medical diagnosis, stock trading, robot control, law, remote sensing, scientific discovery, military for autonomous control and target identification, to the entertainment industry for computer games and robotic pets. Other users could be big organisations with huge amounts of

information such as hospitals, banks and insurances, which can use AI to predict customer behaviour and detect trends.

1.2.1 Expert Systems

In the field of AI one of the biggest deployments is of Expert Systems. An expert system is computer software that embodies a significant portion of the specialised knowledge of a human expert in a specific, narrow domain, and emulates the decision-making ability of the human expert. The technology is based on the premise that what makes a person an expert is years of experience that enables him to recognize certain patterns in a problem as being similar to patterns he has seen previously. Most expert systems reflect expertise from many humans and can therefore perform better analysis than any single expert.

Another area of AI and expert system usage is embedded systems where precision is required and chances of human error have to be reduced. For example: automated processes in Atomic plant operations, Space operations, etc. Typically, the system includes a knowledge base containing various accumulated experiences and a set of rules for applying the knowledge base to each particular situation. There is no flexibility. Expert Systems are used for Structured Logic only, like if-then-else approach. A rule consists of two parts: condition (antecedent) part and conclusion (action, consequent) part, i.e.: IF (conditions) THEN (actions)

- Antecedent part of the rule describes the facts or conditions that must exist for the rule to fire
- Consequent describes
 - the facts that will be established, or
 - the action that will be taken or conclusion that will be made

Expert systems are the most commonly used form of AI in areas such as Medical Expert systems.

The Brain Computer Interface

Developing a link between the human brain and the computer is another exciting area that touches all aspects of artificial intelligence. The idea is to directly connect the human brain to a computer and have human thought control computer activities. The new systems use a special helmet that can measure and transmit brain activity to a computer. For humans intelligence is no more than taking a right decision at right time and for machines Artificial Intelligence is no more than making the right decision at right time.

1.3 Transaction Processing Systems (TPS)

A transaction processing system is a computerized system that performs and records the daily routine transactions necessary to conduct the business, and serve the operational level of the organisation. The transaction is the activity that changes stored data; examples of such an activity

would be using a credit card, making a reservation or making cash withdrawal at an ATM. TPS capture and process the detailed data necessary to update records about the fundamental business operations of the organisation. These systems include order entry, inventory control, payroll, accounts payable, accounts receivable and the general ledger and few others. The inputs to these systems are basic business transactions. The processing includes data collection, data editing, data correction, data manipulation, data storage and document production. A TPS also provides valuable input to management information systems, decision support systems and knowledge management systems. The transaction processing system (TPS) is the most basic part of the MIS, gathering and organizing basic business transactions; this component of the MIS does not involve decision-making and serves the supervisory level of management.

TPS are often so central to the business that a failure of a TPS for a few hours may have a disastrous impact on the business of the organisation and those firms linked to it. For example ATM failure, POS failure, Customer order capturing is first point of contact with customer and critical for any business. The data captured and stored by a TPS serves two purposes:

1. It assists day-to-day, routine operations by providing data to parts of the organisation who need them.
2. It also provides data to Management Information System and produce performance reports about the effectiveness and efficiency of the operations. The large volumes of data captured by TPS can be used as a historical reference for forecasting, identifying trends, and measuring performance.

Transaction Processing Methods

- **Batch Processing Systems:** It is a form of data processing whereby business transactions are accumulated over a period of time and prepared for processing as a single unit or batch. Transactions are accumulated for the length of time needed to meet the needs of the users of that system.
- **Online Transaction Processing (OLTP):** It is a form of data processing where each transaction is processed immediately, without the delay of accumulating transactions into a batch. Consequently, at any time, the data in an online system reflects the current status. This type of processing is essential for businesses that require access to current data such as airlines, ticket agencies and stock investment firms.

TPS are life blood of any organisation because that is where data capturing starts. TPS involves:

- Large amounts of input/output
- Large number of users
- Huge storage requirements
- Low computational complexity
- Fast input/output as well as processing capabilities
- A high degree of concern for potential security related problems
- A high degree of concern for reliability and fault tolerance.

There are four characteristics that all transaction processing systems should have:

1. **Rapid response:** Quicker the response the happier the customer and the more revenue that can be collected.
2. **Reliability:** Information system involves recording transactions which all boil down to money. Any mistakes here can have serious consequences for organisations bottom line, customer satisfaction, etc.
3. **Inflexibility:** Recording of transaction is as per predetermined rules. It must be performed the same way every time. If any step is altered it becomes more likely that a mistake may be made. With computers it must be rigidly adhered to.
4. **Controlled processing:** There must be procedures in place to check that everything and everyone is doing the right thing. At the computers end, is something called a transaction processing monitor to ensure that everything is right with the TPS but there must also be human controls to ensure that everyone is doing the right thing

A customer's satisfaction with an organisation is composed of two factors,

1. The satisfaction with the Product (service) acquired-its functionality and quality
2. The satisfaction with the process involved in acquiring the product or service.

The latter is a function of the effectiveness and efficiency of the organisation's TPS. Imagine a long Queue at ATM or a big queue at cash counter of a mall. TPS is often the system with which the customer interacts so it is important to any organisation to have an efficient TPS. Managers depend upon TPS to monitor the status of internal operations. TPS are also a major source of input for other systems, like a pay-roll system will supply input to the GL system that is responsible for P & L and Income statements of the organisation. It also provides employee payment details for pension, insurance and gratuity to the HR System and employee payments data to the Tax Authorities.

1.4 Decision Support Systems

Users in an organisation need information to help them make decisions. Decision making is the process of developing and analysing alternatives to make a decision - a choice from the available alternatives. Most decisions are made in response to a problem. A sales manager, for example, may be required to determine how high to set yearly sales quotas based on increased sales and lowered product costs. Decision Support systems help provides information to support such decisions.

Whatis.com defines DSS as "A decision support system (DSS) is a computer program application that analyses business data and presents it so that users can make business decisions more easily." A decision support system (DSS) is thus a computer-based information system that supports business or organisational decision-making activities. DSSs serve the management, operations, and planning levels of an organisation and help to make decisions, which may be rapidly changing and not easily specified in advance. DSSs include knowledge-based systems. A properly designed DSS is an interactive software-based system intended to help decision makers compile useful information

from a combination of raw data, documents, personal knowledge, or business models to identify and solve problems and make decisions.

A decision support system (DSS) is an organised collection of people, procedures, software, databases and devices used to help make decisions that solve problems. The focus of a DSS is on decision-making effectiveness when faced with unstructured or semi-structured business problems. They offer the potential to generate higher profits, lower costs and better products and services.

DSS Characteristics

A DSS can have the following characteristics:

- Provides quick access to information.
- Capability to handle huge amount of data from varied sources.
- Provide report and presentation flexibility.
- Offer both textual and graphical orientation.
- Provide complex, sophisticated analyses and comparisons using advanced software packages.
- Perform simulation analysis—the ability to duplicate the features of a real system, where probability or uncertainty is involved.

DSS advantages

Advantages of DSS are:

- Enhance decision-making effectiveness
- Gain a competitive advantage
- Improve communication among decision-makers
- Increase data accuracy and data sharing
- Increase decision-maker satisfaction
- Increase organisational control
- Promote decision-maker learning
- Reduce cycle time
- Reduce decision process costs

DSS are especially valuable in situations in which the amount of data is prohibitive for the perception of an unaided human decision maker and in which precision is important. Decision support systems can aid users by integrating various sources of information, providing intelligent access to relevant knowledge, and aiding the process of structuring decisions. They can also support choice among well-defined alternatives and build on formal approaches, such as the methods of engineering economics, operations research, statistics, and decision theory.

DSS Implementation

There are endless possibilities of implementation of DSS:

- Examples could be a bank loan officer verifying the credit of a loan applicant or an engineering firm that has bids on several projects and wants to know if they can be competitive with their costs.
- DSS is extensively used in business and management. Executive dashboard and other business performance software allow faster decision making, identification of negative trends, and better allocation of business resources

Capabilities of DSS

- DSS helps in different phases of problem-solving.
- DSS could be an Ad-hoc DSS i.e. it is concerned with decisions which don't have to be repeated like 'Should the organisation build a new plant in a Tax free Zone'. This is a one-time decision, on the other hand a DSS could be used at regular frequencies like DSS for investment decisions or product optimisation.
- DSS could support Semi-structured or unstructured problems.
- DSS could provide decision help to managers at all levels right from operational to strategic.

DSS Components

DSS has primarily three components:

1. The Database: The Database Management Systems allows managers and decision makers to perform qualitative analysis on the company's vast stores of data in warehouses, data marts and databases.
2. The Model Base: A model-driven DSS primarily performs mathematical or quantitative analysis. The model base allows managers and decision makers to perform quantitative analysis on internal and external data.
3. The User Interface or Dialogue Manager: It allows users to interact with the DSS to obtain information. It assists with all aspects of communications between the user and the hardware and software that constitute the DSS.

Challenges and Risk Factors in DSS

Some of the challenges in implementation of DSS are

- **Monetary cost:** The decision support system requires investing in information system to collect data from many sources and analyse them to support the decision making.
- **Transfer of power:** Building Decision Support System, especially knowledge-driven Decision Support System, may be perceived as transferring decision authority to a software program.

- **Obscuring responsibility:** The computer does not make a "bad" decision, people do. Unfortunately some people may deflect personal responsibility to a Decision Support System.
- **Status reduction:** Some managers argue using a Decision Support System will diminish their status and force them to do clerical work.
- **Information overload:** Too much information is a major problem for people and many Decision Support Systems increase the information load.

The Risk factors in DSS relate to DSS dependence on repositories, knowledge management, mis-interpretation of organisational datasets.

- **Dependence on data repositories:** One of the critical architecture components of DSS is the knowledge base. The knowledge base depends on a centralized data repository as well as external systems also, like the current stock prices or product prices of competitors. The fact that DSS depends on good quality data repository reinforces the need for standardized data representation, storage, and retrieval that can be centrally managed in the knowledge base repositories. Lack of good data warehouse could have significant impact on the quality of advices emanating from DSS. Data mining algorithms require good quality data repositories to be able to extract knowledge to support decision-making.
- **Knowledge Management:** DSS depend on appropriate implementation of knowledge management. Knowledge is organized and transformed combination of information, assimilated with a set of rules, procedures and operations learnt through experience and practice. The risk is if rules or the data on which rules are applied are wrong, it could lead to poor quality Knowledge leading to disastrous results. It becomes imperative that proper Knowledge management is adopted.
- **Misinterpretation of Datasets:** Inconsistencies in data coding and extraction of poor quality data could lead to misinterpretation of data sets.

The controls to address these risks is auditing the DSS systems, review the decision rules and data mining algorithms, including data warehouses/ repositories.

1.5 Executive Support Systems (ESS)

Executives need information to help them assess their organisation's success and the performance of individuals critical to the success. They also need information to support top-level decisions on:

- Should we spin-off a marginally profitable subsidiary?
- Should we open another manufacturing plant?
- How much long term debt can we afford to risk?

ESS intended to be used by the senior managers directly to provide support to non-programmed decisions in strategic management. These information are often external, unstructured and even uncertain. Exact scope and context of such information is often not known beforehand. Most Executives have a concept of how their business works, they have a feel for what is important, and

they know what to look at to see how well or how badly the business is going. An ESS is a computer-based working model used to express, to quantify and to analyse those business concepts.

ESS acts as a Dashboard which alerts an executive when KPIs (Key Performance Indicators) indicate that action should be taken. ESS helps in measuring organisation's performance against the changes in the external environment, based on:

- Market intelligence
- Investment intelligence
- Technology intelligence

The Intelligence information could be from myriad sources:

- External databases
- Technology reports like patent records etc.
- Technical reports from consultants
- Market reports
- Confidential information about competitors
- Speculative information like market conditions
- Government policies
- Financial reports and information

An ESS is a specialized DSS that includes all hardware, software, data, procedures and people used to assist senior-level executives within the organisation. ESS is part of the decision support field. ESS and DSS are two different but complementary applications and indeed complement each other. ESS is used for continuous tracking of information to keep top manager abreast with what is happening. ESS is structured and its major role is to provide information. It is a communication device. DSS is semi or unstructured. It provides analysis capabilities and provides answers to "what if" and "why".

Characteristics of ESS

The characteristics of ESS are:

- Are tailored to individual executives
- Are easy to use
- Contain extensive graphic capabilities
- Provide "drill-down" for quick access to detailed information behind the text, numbers or graphs
- Filter compressed and track critical data.
- Extensive use of data on the organisation's environment (competitors, customers, industry, markets, government, international).
- Support the need for external data, provide linkages to external databases.
- Can help with situations that have a high degree of uncertainty

- Have a future orientation
- Are linked with value-added business processes
- Designed to rapidly provide information for decision made under pressure, that is, timely information is a critical attribute.
- Text and time-series information handling capabilities.
- Provided status access -- rapid access to current information.

Advantages

The advantages of ESS are

- Easy for upper level executive to use
- Ability to analyse trends
- Augmentation of managers' leadership capabilities, enhance personal thinking and decision making
- Enhance organisational competitiveness in the market place
- Increased executive time horizons.
- Better reporting system
- Help improve consensus building and communication
- Improve office automation
- Reduce time for finding information
- Early identification of company performance
- Detail examination of critical success factor

Disadvantages

The disadvantages of ESS are:

- Functions are limited
- Hard to quantify benefits
- Executive may encounter information overload
- Difficult to keep current data
- Excessive cost for small company

1.6 Big Data

Big Data refers to a large collection of data that can span across petabytes or Exabyte containing trillion of records from various sources. Its characteristics are:

- **Variety:** Various sources from where the data of varied genre is getting generated,
- **Value:** Valuable data is always allowed into the system.
- **Volume:** Huge data chunks coming from various sources, and
- **Velocity of data:** Data is being gathered at an enormous speed.

Data being handled has become mindboggling. Google processes more than 24 Petabytes of data every day, 100 hours of video are uploaded to YouTube every minute. The trend to larger data sets is due to the additional information derivable from analysis of a single large set of related data, as compared to separate smaller sets with the same total amount of data allowing correlations to be found to "spot business trends, determine quality of research, prevent diseases, link legal citations, combat crime, and determine real-time roadway traffic conditions." What is considered "big data" varies depending on the capabilities of the organisation managing the set, and on the capabilities of the applications that are traditionally used to process and analyse the data set in its domain.

Using Big Data Technologies we can crunch an incomprehensible amount of information, providing us with valuable insights about the "What" rather than the "Why". As Big Data is a collection of data sets so large and complex that it becomes difficult to process using on-hand database management tools or traditional data processing applications, we need to have specific DBMS and analytical solutions. Sources of Big data could be Word documents, spread sheets, customer databases, on-line portals/corporate websites, Instant Messages, Social Media and News Feeds. More than 90% data of today has been created in the last two years only.

Why to use Big Data?

Real Value of Big Data is enabling the next generation of interactive data analysis with real-time answers.

- **Big Data to Make Better Decisions:** Global companies experienced a 26 percent improvement in performance over the last three years when big data analytics were applied to the decision-making process. (*Economist Intelligence unit study*)
- **Big data allows using messy data:** Even unstructured data can be used for data analysis.
- **Creating transparency:** Simply making big data more easily accessible to relevant stakeholders in a timely manner can create tremendous value.
- **Segmenting populations to customize actions:** Big data allows organisations to create highly specific segmentations and to tailor products and services precisely to meet those needs.
- **Innovating new business models, products, and services:** Big data enables companies to create new products and services, enhance existing ones, and invent entirely new business models.

Where is Big Data used?

The use of Big Data is becoming a crucial way for leading companies to outperform their peers. Big data lets retailers predict trends by combining enterprise data with other relevant information to create predictive models and consumer behaviour patterns. These models can help further analyse buying behaviours to identify the type of customers most likely to buy a specific product offering. Creating customer profiles lets a retailer see which method of contact customers prefer, and predict

which medium they're most likely to use when interacting with a brand or buying a product. Simply by creating customer profiles, a business can tailor its marketing efforts.

Researchers have found a spike in Google search requests for terms like 'flu symptoms' and 'flu treatments' a couple of weeks before there is an increase in flu patients coming to hospital emergency rooms in a region. Analysis of sets of transaction like reward points, warranty policies, which are growing and may hold unforeseen customer information patterns. Huge sets of governmental or publicly available data could help shape the business plans. With more regulation from governments, financial institutions are finding more value in big data programs for compliance checks and audits. Economic times writes "NATGRID, will utilise technologies like Big Data to study and analyse the huge amounts of data from various intelligence and enforcement agencies to help track suspects and prevent such attacks."

How does Big Data work?

How Big Data works depends on the technology used and specifically on what is sought to be achieved through the use of Big Data. Big Data is a concept which is applied to data which does not conform to the normal structure of a traditional database. Big Data consists of different types of technologies which work together to achieve the end goal: extracting value from data that would have been previously considered 'dead'. Some of the key technologies / concepts associated with Big Data are Hadoop, HDFS, NoSQL, Cassandra etc.

Challenges with Big Data

The challenges include capture, curation, storage, search, sharing, transfer, analysis and visualization. Some of the challenges are:

- **Heterogeneity and incompleteness of data:** Even after data cleaning and error correction, some incompleteness and errors in data are likely to remain. This incompleteness and these errors must be managed during data analysis. Doing this correctly is a challenge.
- **Privacy:** The privacy of data is another huge concern, and one that increases in the context of Big Data.
- **Human Collaboration:** In spite of the tremendous advances made in computational analysis, there remain many patterns that humans can easily detect but computer algorithms have a hard time finding; example "Captcha"
- **Shortage of talent:** A significant constraint on realizing value from big data is the shortage of talent, particularly of people with deep expertise in statistics and machine learning, and the managers and analysts who know how to operate companies by using insights from big data.

Risks with Big Data

The key risks associated with Big data are:

- **Privacy:** One of the biggest risks is loss of privacy, with others gathering, storing and using our personal data. Amazon monitors our shopping preferences. Google monitors our browsing habits and searches. Privacy becomes difficult.
- **Penalties based on Inclination:** Law enforcement and regulatory agencies using Big Data could penalize based on tendency even before actual act.
- **Dictatorship of data:** Using Data analyses for everything could create obsessions with data. Big Data predictions used injudiciously could lead to unnecessarily letting it govern our lives.

Controls with Big Data

- **Addressing privacy and security issues:** This will become paramount as more data increasingly travel across boundaries for various purposes. Privacy, in particular, not only requires attention to compliance with laws and regulations, but also is fundamental to an organisation's trust relationships with its customers, business partners, employees, and other stakeholders. Organisations will need policies that comply with privacy laws and any government privacy regulations.
- **Accountability of the users:** Using personal data of individuals could be an effective way to privacy issues. Since in this Big Data world there are plenty of secondary uses of data not envisioned by traditional privacy policy.
- **Enterprise Information Strategy:** To prepare for a big data world, organisations have to develop an integrated data strategy for the entire enterprise. Data models, architectures, and attributes of solutions have to be considered holistically. An effective enterprise data strategy must include interoperable data models, transactional data architecture, integration architecture, analytical architecture, security and compliance, and frontline services. Many organisations require additional investment in IT hardware, software, and services to capture, store, organize, and analyse large datasets. The level of investment varies considerably depending on a company's current state of IT capability and maturity.
- **Proper Data Handling Strategy:** The faster and easier it is to access big data, the greater the risk to all of that valuable information. Organisations must get a proper insight into the performance of their data handling processes to minimise the risks. Service level agreements with clients must be checked and adapted where necessary.
- **End to End Security:** Organisations have to ensure that employees, data, networks, partners and customers are protected end-to-end. To minimise the potential for damage resulting from inaccurate or fraudulent data, organisations have to consider all the data sources they are pulling into their analyses and assess each source for vulnerabilities.
- **Ensure future-proof systems:** This means that not only the right systems, but also the right tools and processes are implemented for big data today and can cope with the inevitable data growth of in the future. Companies have to invest in tools that help ensure their data is accurate, up to date and clean at all times.

- **Logical and physical access security controls:** These are needed to prevent unauthorised access to sensitive and/or valuable data. It is imperative for organisation to keep up-to-date with the latest legislative proposals and use the opportunity to employ data lifecycle best practices.

1.7 Summary

All organisations need business Information systems to manage their information requirements. Artificial Intelligence provides new and innovative ways of handling data akin to Humans. TPS, DSS and ESS are part of traditional Information systems for providing Information to different levels of Management. Big Data provides capability to an organisation to analyse massive amounts of Data. However, any technology has its risks and these risks need to be managed by implementing appropriate controls.

1.8 References

- <http://www.ucs.louisiana.edu/~isb9112/dept/phil341/wisai/WhatisAI.html>.
- <http://aitopics.org/>
- Daniel J. Power, Decision Support Basics, Business Expert Press
- Viktor Mayer-Schonberger , Kenneth Cukier , Big Data, John Murray

1.9 Questions

1. Which of the following system can processes semi-structured problems?
 - A. Expert systems
 - B. DSS
 - C. Artificial Intelligence
 - D. Transaction processing Systems
2. Which of the following refers to a normal operational activity for conduct of business?
 - A. DSS
 - B. Expert Systems
 - C. Artificial Intelligence
 - D. Transaction Processing Systems
3. A technology that manages huge amount of data from diverse sources is called:
 - A. Big Data
 - B. DSS
 - C. Expert Systems
 - D. Transaction Processing Systems

4. A computer program that embodies specialized knowledge in a specific domain is called:
- A. Automatic Processor
 - B. Intelligent planner
 - C. Expert System
 - D. Transaction processing systems
5. Which of the following systems is used to present high-level overview of information as well as the ability to drill down to details for senior managers?
- A. Decision support system
 - B. Executive support system
 - C. Expert support system
 - D. Transaction-processing system

1.10 Answers

- 1 B
- 2 D
- 3 A
- 4 C
- 5 B

PART 2: EMERGING TECHNOLOGIES: RISKS, CONTROL AND AUDIT

Learning Objectives

- To gain an overview of Green IT
- To gain an overview of Web 2.0
- To gain an overview of risk, control and assurance of Emerging Technologies

2.1 Introduction

Until recently, power utilization has generally not been a major concern in the development and implementation of technology components. Internet use and data transfer are ever growing, this growth is associated with enormous energy consumption. Green IT is about acting responsibly and reducing carbon footprint. Web 2.0 technologies are the buzzword which has made web interactive and social media etc. possible. We have to be at forefront of technology to watch new technology trends to reap the benefits. Mitigating risks posed by technology during implementation can unlock the tremendous business value in these technologies. A Chartered Accountant can play a definitive role in helping understand the risk and building controls in implementation of these policies.

2.2 Green IT

Green IT stands for Green Information Technology. Information Technology is essentially the design, implementation and management of computers that both individuals and businesses use. Green IT involves consciously making choices to:

- Minimize the carbon footprint of computer. Carbon footprint is a measure of an organisation's impact on the environment in terms of the amount of greenhouse gases produced (Carbon Di-oxide, methane, Ozone etc.),
- Minimize networking hardware.
- Minimize energy consumption of computer devices during their life cycle.

In a nutshell, "Green" IT is composed of two things:

- Minimising the negative impact of information technology use on the environment.
- Using information technology to help solve environmental issues.

Green technology solutions are hardware-based, software-based or workflow strategies that save energy and/or promote sustainability. The energy savings or degree of sustainability can be quantified in a number of ways, including measuring the organisation's physical footprint, its carbon emissions and the amount of its e-waste.

IT contributes to e-waste and to CO₂ emissions. Reasons to go green are

- **Economic:** Cisco suspended all travel not relating to customers to reduce carbon footprint.
- **Social and environmental:** Landfill issues, huge amount of e-waste, PC with 15" CRT Monitor contains over one kilogram of lead and chemicals including antimony, arsenic, boron, phosphor, nitric acid, hydrofluoric acid, and hydrogen fluoride and uses huge amount of electricity.
- **Technological:** Data centres consume 1.5% total electricity used; a typical desktop computer uses 868 KW of electricity per year.
- **Political:** Legislative and regulatory, like regulatory compliance initiatives around power consumption in some places.

How to implement Green IT?

At an Individual level, it could be as simple as turning off your computer each night or when not in use. Outsourcing the data centre, cloud computing and using co-location facilities are additional ways in which companies realize energy savings and/or sustainability. The true challenge in achieving sustainability lies in seeing beyond annual or even quarterly budgets to institute green IT strategies that will ultimately reduce costs and guarantee long-term power availability. Some of the key principles of Green IT are given here:

- Green IT organisations have ability to implement solutions that address overall green IT goals.
- Green IT management strategy should be established with clear goals such as for power reduction, regulatory compliance, decreased carbon footprint, and operational cost savings.
- Decommissioning unused systems: Systems that are rarely used but draw power should be retired.
- Consolidation: Unused servers should be consolidated.
- Utilization management processes allows computing services to be distributed across available servers.
- Virtualization allows multiple system implementations to be combined onto a single power efficient server while at the same time allowing them to operate "independently" within separate virtual containers.
- Power management schemas allow automatic shutdown and power up processes not only for servers but even personal computers.
- Upgraded Hardware Technology: Modern power efficient systems could be used, use of thin clients to achieve energy efficiency could be there.
- Cloud computing is another approach to gaining IT efficiencies.
- Digitization, automating business processes, purchasing energy-smart software and developing custom software solutions enable energy efficiencies in the business.

Using Technology to help solve environmental issues

Another aspect is using technology to save environment. IT helps us understand how we can fix environmental issues. For example technology can help us achieve things such as climate change modelling. Using energy-smart software like telecommunication and collaboration tools, allow companies to reduce airplane travel and time in the office. For some companies, this software significantly cuts down on the physical footprint of the office space because it makes working from home a viable, productive option.

CAs role in Green IT

CAs can help in Green IT initiatives by assisting in implementing Green IT management strategy, to:

- drive efficiency in the IT organisation by identifying green strategies;
- support and implement green initiatives across the enterprise by finding green technology products and solutions that enable the business plan; and
- act as thought leaders on green technology solutions for the business by conceiving green IT strategies that benefit the business.

Further, by understanding CAs could themselves aid in reducing carbon footprint by using green initiatives in their office. By using collaborative tools CAs can reduce their travel thereby going green. Making use of emails rather than printing can also help save the plants.

2.3 Web 2.0

Tim O'Reilly defined "Web 2.0 is the business revolution in the computer industry caused by the move to the Internet as a platform, and an attempt to understand the rules for success on that new platform." Web 2.0 is the term given to describe a second generation of the World Wide Web that is focused on the ability for people to collaborate and share information online. It is in fact a transition from static HTML Web pages to a more dynamic Web that is more organized and is based on serving Web applications to users. Web 1.0 refers to Websites, e-mail newsletters i.e. one person or organisation pushing content out to many people via websites and e-mail newsletters.

Web 2.0 is the beginning of two-way communication in the online public space like the Blogs, wikis and social networking sites. People can post comments and converse with the organisation in public for all to see. It's one person or organisation publishing content to many on social networking sites who then re-publish your content to their friends, fans, followers, connections, etc. Web has been evolving and is transiting towards Web 3.0 that may be called the third-generation of the Web, which is enabled by the convergence of several key emerging technology trends, like: Mobile Websites, Text Campaigns and Smartphone Apps i.e. it is all of the above except that the Web experience is no longer limited to desktop and laptop computers while remaining stationary in one

place. It's the Internet on the go fuelled by mobile phones and tablets. For Web 3.0, the Mobile websites must be designed to be easily read on mobile devices. Web 3.0 will be much more than Web 2.0.

Web 1.0 sites are content driven and the user has no way to increase their involvement or interact with the interface. Web 2.0 sites move beyond mere posting of content by allowing the user to become part of the process through collaboration. Content management systems became wikis, directories (taxonomy) became tagging. Web 2.0 describes web sites that use technology beyond the static pages of earlier web sites. In Web 2.0 online content is not only created by webmasters but also by the users.

Features of web 2.0

The Web 2.0 phenomenon is important because this collaborative, community approach brings changes to how users behave online and changes in expectations. Key features of web 2.0 are:

- The 'read write web'
- Not just static pages but shareable content
- Forging links between 'nodes' to build networks
- Participation and user generated content
- Collaborative and open

Use of Web 2.0

Web 2.0 is being used today in:

- **Blogging:** Individuals broadcast ideas to like-minded people, Businesses broadcast latest information to stakeholders
- **Forums:** These are online message board around one topic, includes discussions with posts and replies, these form threads which are collections of posts and replies.
- **Wikis:** Collectively share and edit a body of knowledge, it is an ongoing process of creation and collaboration, e.g. Wikipedia
- **Social Networks:** Online communities which share information and connect people with same interest, e.g. LinkedIn
- **Bookmarking:** Users save and share links and add meta-data e.g. Reddit
- **E-commerce:** Connect seller and buyer, they add value by providing service e.g. Amazon, Ebay etc.
- **Syndication:** Make updates come to you using standard formats. Are used to publish frequently updated works, e.g. RSS (Really Simple Syndication) through Google reader
- **Mashup:** Aggregates data from more than one source e.g. Real estate data on Google map.
- **Collaborative Software:** Change the way we work, allow real-time collaboration on documents e.g. Google Docs.

Security concerns in Web 2.0

- Openness-Collaboration and third-party content can be major attack vectors.
- Community based- Exposes valuable personal information that can be used in social engineering attacks or can create physical security risks.
- Collaboration-Blogs and wikis could be quickly compromised to distribute spam and malware.
- Third party content-Weak security may add vulnerabilities to otherwise secure applications.

Controls in Web 2.0

- **Validate all websites:** Using techniques like extended validation, SSL certificates validate websites.
- **Use risk reporting tools:** Such as Google alert.
- **Defend against click jacking:** Click jacking is one of the most dangerous and troubling security problems on the web. In this attack, two layers appear on a site, one visible, one transparent, and users inadvertently interact with the transparent layer that has malicious intent. Login credentials for a bank account, for example, can be captured by the second layer. Using NoScript with ClearClick for the Firefox Web browser, reduce the click jacking risk.
- **Use commercial tools:** Use of commercial to keep malicious content out.
- **Monitoring user behaviours:** Monitor users during use of web 2.0 tools could help identify suspicious behavior and stop exploits.
- **Implement right policies:** Organisation should have policies taking care of Web 2.0 risks.

2.4 Some more emerging Technology Trends

Chartered Accountants have to keep themselves updated with the latest technology trends so as to be able to use them in their own professional practice and also use this knowledge to provide consulting and assurance services to their clients. Gartner has predicted the following latest emerging technology trends.

The Internet of Everything: Web of Everything

Internet of Things is about Internet expanding beyond Computers to everything like cars, refrigerators etc.; i.e. identifiable objects are seamlessly integrated into the information network. The Web of Things takes advantage of mobile devices' and sensors' ability to observe and monitor their environments, increasing the coordination between things in the real world and their counterparts on the Web. It will merge physical world with digital world.

3-D Printing

New 3D printing tools and techniques are empowering everyone from global corporations to do-it-yourselfers to create new devices and realize new concepts more quickly, cheaply, and easily than ever like car parts, batteries, prosthetics, and computer chips. Organisations today are becoming aware of the fact 3D printing is a real, viable and cost-effective means to reduce costs through improved designs, streamlined prototyping and short-run manufacturing.

Smart Machines

Smart Machines will increase machines which are contextually aware, intelligent personal assistants, smart advisors, advanced global industrial systems and public availability of early examples of smart machines.

2.5 Risks, Controls and assurance in emerging technology

It is strategically imperative for any enterprise to adopt emerging new technologies. No organisation is protected from the competitive disruption brought about by wide spread adoption of emerging technologies. Any enterprise in today's world has to embrace technology to conquer the problems it faces. Jack Welch once said, "Willingness to change is strength, even if it means plunging part of the company into total confusion for a while." IT encompasses all aspects of functioning of enterprises from strategy to operations, conception to completion and from ideation to value creation. Business, regulatory and competitive requirements are demanding innovation in technology deployment resulting in changing business models of delivery of services using diverse digital media. Enterprise has to believe in the ability of technology to bring transformative changes to business.

IT is evolving at an accelerating pace and the role of IT is transforming business processes. It is expected that role of IT in enterprises will fundamentally change from being a service provider to IT becoming a Service Broker, aggregator of services and primarily responsible for building, maintaining and sustaining the business relationship by rendering core services to the customer. Enterprises that effectively manage Information technology can expect to gain in one or more of three areas: better customer experiences and engagement, streamlined operations and new lines of business or business models.

IT is a big enabler and organisations routinely invest in technology, but too often feel they get routine results. Technology's promise is not simply to automate processes, but to open routes to new ways of doing business. Many times the results may not be astounding which could be because technology has its own risks which have to be mitigated. One of the primary reasons for organisations not getting the desired results from technology could also be that one: they lack both the management temperament and relevant experience to know how to effectively drive transformation through technology and two: not implementing in a way that enhances the business

value of technology. Implementation of Information technology to harness its power by mitigating the risks is important.

A key requirement of organisations in IT deployment is to ensure that business objectives are achieved and not the mere implementation of latest technology. A key challenge in implementing IT is: higher the technology, greater is the need for controls. CAs with their in-depth knowledge and core competencies in business processes and internal controls coupled with a thorough understanding of emerging technologies are uniquely positioned to provide assurance and consulting services in IT area. CAs have to encash this challenge by updating their competencies and skill-sets to successfully surf the technology wave. Either they may bury their heads in the sand and ignore it, or can find ways to embrace this evolution by making it an important part of their long-term profession model.

Every emerging technology has its own risk; one emerging technology trend which is ubiquitous in its presence today is use of social media. Everyone personally has embraced applications like Facebook that actually encourage to electronically check-in at one's favourite restaurant, at the airport, or at a big game. Whether one understands it or not, this form of social media has become an important part of everybody's daily life. Every enterprise is using innovative uses of social media to catapult it to unimaginable heights. This social media despite providing excellent business value to any enterprise is fraught with security concerns if we implement it. Risks could be in form of:

- Deploying a social media without clear business purpose will fail to deliver expected business value.
- Privacy and confidentiality issues are again a big risk which has to be mitigated in social media deployment.
- Culture mismatch is a risk that this new way of working might not align to an organisation's culture.
- Too much noise: sheer volume of noise on a network can be distracting, with people suddenly contending with a never-ending wall of activity.
- Loss of employee productivity is one of the risks which is a result of improper implementation of social media.
- Compliance and reputational risks also heighten in Social media.

Role of CAs in Governance and management of emerging technology:

CAs could help implement or review implementation of social media by reviewing controls and confirm whether they mitigate the risks posed by technology such as social media, so that enterprise could derive astounding business value out of it:

- A clearly articulated business purpose should be established before embarking on social media.
- A planned business processes to leverage social media should be established.
- Business processes should be aligned with Corporate Policy.

- A proper risk assessment exercise in respect of social media should be conducted.
- A social media policy or guidelines should be formulated to guide employee behaviour in use of social media.
- Policy should not only include use of social media at workplace but also its personal use.
- Guidelines should be established involving legal teams to formulate an approval workflow for outbound content and content rules that flag unacceptable outbound content.
- Guidelines to handle rogue accounts would be required.
- Tracking mechanism to track messages from inception to resolution has to be implemented.

Human Resource Management

- Training and effective community management are essential to use of social media.
- Acceptable behaviour training could help prevent Combustible conversations.
- Appropriate communication channels to be used by customers and escalations have to be decided.
- Information which can be shared also has to be decided and communicated to people.

Security

- Technological measures are required with the ability to treat private messages differently.
- Access Management should be implemented with enterprise-wide, single point password control.
- Technological measures should be integrated with enterprise-wide authentication systems.
- Deployment of tools and platforms that are enterprise-grade security compliant with controls to mitigate risk from malware including incident response in case of any malware incident.
- Technical controls so that browser settings ensure download restrictions, automated content monitoring and filtering.
- Monitoring of other social media for fraudulent or unauthorised use of brand should be done to mitigate reputational risk.

Compliance

- Controls are required to enable documentation of internal conversations about social media situations.
- Controls with ability to archive outbound content as well as inbound content including audit trail of social media activities.

2.6 Summary

The objective of this chapter was to provide an overview of existing and emerging technologies and the role of CAs in understanding the impact of these technologies so that they can provide assurance and consulting services in these areas. IT will keep on evolving with new emerging trends like Web 2.0, Green IT, 3D Printing, Smart Machines etc. Enterprises in India are continuing to invest in IT in a big way to remain globally competitive and adopting new and emerging technological trends. The scope and objectives of assurance do not change with technology but the way controls are reviewed is drastically changed. We have to equip ourselves to emerging technology, choosing to do nothing in the face of a changing marketplace is unacceptable. As Charles Darwin once said, *"In the struggle for survival, the fittest win out at the expense of their rivals because they succeed in adapting themselves best to their environment."* Study, learn, evolve, our success depends on it.

2.7 References

- <http://www.paulgraham.com/web20.html>
- <http://oreilly.com/web2/>
- <http://www.computer.org/portal/web/membership/Top-10-Tech-Trends-in-2014>
- <http://www.gartner.com/newsroom/id/2603623>

2.9 Questions

1. Which of the following is not a Green IT Practice?
 - A. Decommissioning unused systems
 - B. Consolidation of unused systems
 - C. Virtualization
 - D. Using manual instead of electronic records
2. Which of the following is not a reason to adopt Green IT?
 - A. Short term profits
 - B. Economic
 - C. Social and environmental
 - D. Regulatory
3. Which of the following is a characteristic of Web 2.0 applications?
 - A. Multiple users schedule their time to use it one by one
 - B. Focused on the ability for people to collaborate and share information online
 - C. They provide users with content rather than facilitating users to create it

D. Web 2.0 application use only static pages

4. Which of the following is not an use of Web 2.0 applications?

- A. Blogs
- B. Wikis
- C. Personal read only websites
- D. Social Networks

5. Which of the following is not a Security Concern of Web 2.0 application?

- A. Collaboration and third party content
- B. Click jacking
- C. Community based
- D. Extended validation Tools

2.10 Answers

- 1 D
- 2 A
- 3 B
- 4 C
- 5 D

Module-2

Information Systems Assurance Services

TABLE OF CONTENTS

MODULE 2: INFORMATION SYSTEMS ASSURANCE SERVICES	343
SECTION 1: OVERVIEW	343
Objective.....	343
Learning Objectives.....	343
Task Statements.....	343
Knowledge Statements	344
Relationship of Task Statements with Knowledge Statements.....	344
Knowledge Statement Reference Guide	348
SECTION 2: CONTENTS.....	351
Chapter 1: Concepts of IS Audit	351
Learning Objectives.....	351
1.1 Introduction.....	351
1.2 Definitions	352
1.3 Concepts of Audit	353
1.4 Concept of IS Audit and Auditing in a computerized environment	354
1.4.1 Audit in a computerized environment.....	354
1.4.2 IS Audit (Auditing of the computerized environment)	355
1.5 Concept of IT Risk.....	355
1.5.1 IT Risk in the Risk Hierarchy	356
1.5.2 Risk management	357
1.6 Risk Based Auditing	357
1.7 Audit Risk and Materiality.....	358
1.7.1 Audit Risk.....	358
1.7.2 Materiality	359
1.8 Concepts of Internal Control.....	361
Types of Internal Controls	361
Types of IS Controls	362
1.9 Organization of IS Audit Function	363

1.9.1 Infrastructure and organization.....	363
1.9.2 Internal and external audit control framework	364
1.9.3 Quality Assessment and Peer Reviews	364
1.9.4 Standards on Audit Performance	364
1.10 Summary.....	365
1.11 Questions	366
1.12 Answers and Explanations	367
Chapter 2: IS Audit in Phases	369
Learning Objectives.....	369
2.1 Introduction.....	369
2.2 Conducting an IS Audit	370
2.2.1 Setting up of audit objectives	370
2.2.2 Request for Proposal and submitting response	370
Request for proposal (RFP)	370
Response to RFP	372
2.3 Audit Charter and Terms of Engagement.....	373
2.3.1 IS Audit charter.....	373
Contents of the Audit Charter	373
2.3.2 Audit Engagement Letter	374
2.3.3 Communication with Auditee	376
2.3.4 Quality Assurance Process	377
2.4 Audit Scope.....	377
2.5 Audit Planning	378
Risk Assessment in Planning	380
2.6 Objectives of IS Controls	380
2.6.1 Principles of Fiduciary	380
2.6.2 Principles of Quality	381
2.6.3 Principles of Security (CIA).....	381
2.7 Understanding the Auditee Environment.....	383

2.7.1 Business of the Entity	383
2.7.2 Organization Structure	383
2.7.3 IT Infrastructure	384
2.7.4 Regulations, Standards and Frameworks	384
Information Technology Act 2000 (Amended in 2008)	384
Sarbanes Oxley Act, 2002 (SOX)	385
Public Company Accounting Oversight Board (PCAOB)	385
Clause 49 of Listing Agreement on Corporate Governance	385
ISO 27000 Family	386
2.8 Using Standards, guidelines and best practices for IS Audit.....	387
2.8.1 ITAF	387
2.8.2 COBIT 5 Framework: Principles, Enablers, Processes, Assurance	387
Five Principles of COBIT 5	388
Seven enablers of COBIT 5	389
Using COBIT 5 for IS Assurance	390
Evaluating system of internal controls	390
2.9 Risk Assessment.....	391
2.9.1 Guidance on risk assessment by ISACA	391
2.9.2 Risk Management steps	392
Collect Data	392
Analyze Risk.....	393
2.9.3 Risk Assessment procedures and related activities.....	394
2.9.4 Use of Risk Assessment in Audit Planning.....	394
2.10 Governance and Management Controls.....	395
2.10.1 IT General Controls areas	395
Operating System controls	396
Organisational controls	396
Guidelines on segregation of duties.....	398
Management Controls	399
Financial Controls	399

Data management controls	400
Organizational structure controls	401
Data Processing Controls	401
Physical Access Controls	401
Logical Access Controls	401
System development controls	402
Business Continuity Planning Controls.....	402
System maintenance controls	402
Computer Centre security controls	402
Internet and Intranet controls	402
Personal computers controls.....	403
Audit Trails.....	403
2.10.2 Types of IT Application Controls	403
1. Boundary Controls	404
2. Input Controls	404
3. Processing Controls.....	405
4. Data file controls	405
5. Output Controls	405
Scope of IS Audit of Application software	406
Steps for IS Audit of Application software	406
2.11 Creation of Risk Control Matrix	408
2.12 Audit Sampling, Data Analysis and Business Intelligence	409
2.12.1 Audit Sampling	409
2.12.2 Data Analysis	410
2.12.3 Business Intelligence	411
2.12.4 Analytical Review Procedures: CAAT Tools	411
Analytical Review Procedures.....	411
CAATs	411
Functional Capabilities of CAATs.....	412
How to use CAATs?	412

General Uses and Applications of CAATs:	412
Strategies for using CAATs	413
2.13 Compliance Testing	415
2.14 Substantive Testing	416
2.15 Design and Operational effectiveness	416
2.15.1 Design Effectiveness	416
2.15.2 Operational Effectiveness	417
2.16 Audit Evidence: Methods	418
2.16.1 Evaluating audit evidence	418
2.16.2 Types of evidence	419
2.16.3 Types of Audit Evidences	420
2.16.4 Evidence preservation	420
2.16.5 Standards on evidence	421
Standards by ICAI	421
Standards by ISACA	421
Guidance by ISACA on evidence covers following key aspects	421
2.17 Audit Documentation	423
Test working papers	424
Organization of audit working papers	424
Documentation Controls	424
2.18 Using work of another auditor and expert	426
2.19 Evaluation of strengths and Weaknesses: Judging by materiality	428
Judging the materiality of findings	428
2.20 Risk Ranking	429
2.21 Audit Report Structure and contents	430
Audit report structure and contents	431
2.22 Management Implementation of recommendations	432
2.23 Follow up review	433
2.24 Summary	434
2.25 Questions	434

2.26	Answers and Explanations	436
	Chapter 3: IT Enabled Services	439
	Learning Objectives.....	439
3.1	Introduction.....	439
3.2	Classification of Audits	439
3.3	IT Enabled Services	442
3.4	Fraud	443
3.4.1	Fraud Detection.....	443
3.4.2	Cyber fraud Investigation	446
3.4.3	Cyber Forensics: Digital Forensics	448
3.4.4	Fraud investigation tools and techniques	449
3.4.5	Some Case Studies of frauds and lessons	449
	Case Study 1: The WorldCom fraud	449
	Lessons and Tips:	450
	Case Study 2: The \$54 million fraud.....	450
	Lessons and Tips	450
	Case Study 3: The Satyam Fraud.....	450
	Lessons and Tips	451
3.4.6	Overview of lessons learned	451
3.5	Summary.....	451
3.6	References	451
3.7	Questions	451
3.8	Answers and Explanations	453
	SECTION: 3 APPENDIX	457
	Checklists and other related materials.....	457
	Reference material (available in DVD only)	457
	Useful checklists (available in DVD only)	457
	Useful checklists available as soft copy in DVD and in section 3: appendix 1 to 6	457
	Appendix 1: RFP from Bank for IS Audit of Application software	458

Appendix 2: Response to RFP for Logical Access Controls Review of SAP	459
Introduction.....	459
The Client Company (Max Infotech).....	459
IS Assurance and Consulting Firm	459
Background.....	460
Objective of SAP Review	460
Need for SAP review	460
Need for Logical Access Controls Review of SAP	460
Understanding the need	461
Methodology for executing the Assignment	461
Primary Objective	461
Scope and Terms of Reference.....	461
Our Approach/Methodology	462
Audit Approach	462
Structured Methodology	462
Audit plan	463
Audit Program\procedures.....	463
Assignment Team.....	464
Logistic arrangements	464
Infrastructure Required	464
Documentation Required	465
Estimated Timeframe, Deliverables and Fees	465
Deliverables	465
Time Frame.....	465
Fees.....	465
Out of pocket Expenses	465
Appendix 3: Sample IS Audit Finding	466
Logical Access Controls Review of Operating System	466
1. System Users have blank user-id:.....	466

2. PQR Computer is networked to other office computers.....	466
Appendix 4: CAAT Report using SQL.....	468
Sample Results of using CAAT	468
Users available with Invalid employee codes:	468
Past employees having ID in user table	468
Transactions with amount as Null in FA Trans_table	469
Appendix 5: Sample IS Audit Report	469
Objectives of the Assignment.....	469
Proposed Scope of Review/Terms of Reference	469
Our Approach/Methodology	470
Audit Environment.....	470
Audit Reports.....	470
Overall Conclusions	471
Security and Access Controls	471
Business Process Controls	471
Further Action.....	471
Appendix 6: Questionnaire for Providing Assurance services in.....	472
E-Commerce	472

MODULE 2: INFORMATION SYSTEMS ASSURANCE SERVICES SECTION 1: OVERVIEW

Objective

Provide IS assurance or IT Enabled services and perform effective audits in a computerised environment by using relevant standards, guidelines, frameworks and best practices.

Learning Objectives

Provide assurance or consulting services in the areas of Governance, Risk Management, Security, Controls and compliance by using relevant standards, guidelines, frameworks and best practices services.

Task Statements

- 2.1. Develop and implement appropriate risk-based approach as per scope and objective of the assignment.
- 2.2. Adapt and use relevant IT assurance standards, guidelines, frameworks and best practices.
- 2.3. Plan assurance or consulting assignments covering specific steps such as: responding to request for proposal from client, submitting proposal, scoping of audit objectives, performing audit, evaluate findings and reporting, covering the complete life cycle of the assignment.
- 2.4. Document understanding of the enterprise technology deployment, IT organisation structure, technology environment including control architecture so as to analyse and assess IT risks.
- 2.5. Perform assurance or consulting services covering the complete assurance life cycle including scoping, risk assessment, audit planning, audit program, audit procedures, using audit tools, performing audit as per audit objectives, obtaining and evaluating audit evidence identifying key areas of weaknesses, reporting findings, obtaining management response and follow up of implementation.
- 2.6. Use Computer Assisted Audit Techniques, tools and risk assessment techniques including sampling, data analysis, Business Intelligence and Business Analytics.
- 2.7. Distinguish between IS Assurance assignments and auditing in a computerised environment and use the relevant frameworks and best practices for compliance and assurance assignments.
- 2.8. Communicate/Report findings in specific format using standards/best practices as required.
- 2.9. Conduct follow-up reviews or prepare status reports to ensure appropriate actions have been taken by management in a timely manner.
- 2.10. Distinguish key steps and processes of Cyber Frauds investigation and Cyber Forensics.

2.11. Create IS Assurance or consulting function in an enterprise/within CA office by identifying key enablers and resources including identifying required personnel with required competencies and skill sets.

Knowledge Statements

- 2.1. Relevant IT assurance standards, guidelines, frameworks and best practices as per scope and objective of the assignment.
- 2.2. Statements of auditing relating to auditing in a computerised environment.
- 2.3. Different aspects of IS Audit process - audit charter, audit planning, audit universe, risk-based audit approach, IS Audit standards, guidelines, regulations, procedures and audit reporting.
- 2.4. Role and responsibilities of IS Audit function/department and key enablers.
- 2.5. Documenting enterprise, technology deployment, organisation structure, technology environment including control architecture so as to analyse and assess Risks.
- 2.6. Audit Risk management strategy and approach
- 2.7. Assurance or consulting services including scoping, risk assessment, audit planning, audit program, audit procedures, using audit tools, analysis and reporting.
- 2.8. IS Audit process cycle from scoping to reporting
- 2.9. Defining Audit scope and objectives
- 2.10. Preparing request for proposal from client, submitting proposal
- 2.11. Audit documentation, obtaining and evaluating audit evidence
- 2.12. Analysis of evidence, Risk Rating of findings/Control weaknesses, reporting findings, obtaining management response and follow up of implementation.
- 2.13. Types of Internal control and related risks
- 2.14. Analytical procedures, compliance testing and substantive testing
- 2.15. Types of IT enabled services, IS Assurance assignments and auditing in a computerised environment and using the relevant processes and best practices for compliance and assurance assignments.
- 2.16. Cyber Frauds investigation and cybercrimes, specific process relating to Cyber Forensics.
- 2.17. Audit tools and techniques including CAAT, tools and risk assessment techniques including data analysis, Business Intelligence, sampling, Automation of IS Assurance, etc.
- 2.18. Using best practices frameworks such as COBIT, ISO etc.
- 2.19. Key provisions of Information Technology Act and Rules and impact on IS Assurance.
- 2.20. Follow up review

Relationship of Task Statements with Knowledge Statements

Task Statement	Knowledge Statement
2.1. Develop and implement appropriate risk-based approach as per scope and objective of the assignment.	2.1. Relevant IT assurance standards, guidelines, frameworks and best practices as per scope and objective of the assignment.

	2.3. Different aspects of IS Audit process - audit charter, audit planning, audit universe, risk-based audit approach, IS Audit standards, guidelines, regulations, procedures and audit reporting.
	2.6. Audit risk management strategy and approach
	2.7. Assurance or consulting services including scoping, risk assessment, audit planning, audit program, audit procedures, using audit tools, analysis and reporting.
	2.18. Using best practices frameworks such COBIT
	2.19. Key provisions of Information Technology Act and Rules and impact on IS Assurance.
	2.20. Follow up review
2.2 Adapt and use relevant IT assurance standards, guidelines, frameworks and best practices.	2.5. Documenting enterprise, technology deployment, organisation structure, technology environment including control architecture so as to analyses and assess Risks.
	2.7. Assurance or consulting services including scoping, risk assessment, audit planning, audit program, audit procedures, using audit tools, analysis and reporting.
	2.18. Using best practices such as COBIT, ISO, etc.
	2.19. Key provisions of IT Act and Rules and impact on IS Assurance.
2.3. Plan assurance or consulting services covering specific steps such as: responding to request for proposal from client, submitting proposal, scoping of audit objectives, performing audit, evaluate	2.3. Different aspects of IS Audit process - audit charter, audit planning, audit universe, risk-based audit approach, IS Audit standards, guidelines, regulations, procedures and audit reporting.

findings and reporting, covering the complete life cycle of the assignment.	2.4. Role and responsibilities of IS Audit function/department and key enablers.
	2.6. Audit risk management strategy and approach.
	2.7. Assurance or consulting services including scoping, risk assessment, audit planning, audit program, audit procedures, using audit tools, analysis and reporting.
	2.8. IS Audit process cycle from scoping to reporting.
	2.9. Defining audit scope and objectives.
2.4. Document understanding of the enterprise, technology deployment, organisation structure, technology environment including control architecture so as to analyze and assess Risks.	2.5. Documenting enterprise, technology deployment, organisation structure, technology environment including control architecture so as to analyze and assess Risks.
	2.17. Types of Internal control and related risks
2.5. Perform assurance or consulting services covering the complete assurance life cycle including scoping, risk assessment, audit planning, audit program, audit procedures, using audit tools, performing audit as per audit objectives, obtaining and evaluating audit evidence identifying key areas of weaknesses, reporting findings, obtaining management response and follow up of implementation.	2.3 Different aspects of IS Audit process - audit charter, audit planning, audit universe, risk-based audit approach, IS Audit standards, guidelines, regulations, procedures and audit reporting.
	2.4. Role and responsibilities of IS Audit function/department and key enablers.
	2.6. Audit risk management strategy and approach.
	2.7. Assurance or consulting services including scoping, risk assessment, audit planning, audit program, audit procedures, using audit tools, analysis and reporting.
	2.8. IS Audit process cycle from scoping to reporting.
	2.9. Defining audit scope and objectives

2.6. Use Computer Assisted Audit Techniques, tools and risk assessment techniques including data analysis, Business Intelligence, sampling, etc.	2.17 Audit tools and techniques including CAAT, tools and risk assessment techniques including data analysis, Business Intelligence, sampling, Automation of IS Assurance, etc.
2.7 Distinguish between IS Assurance assignments and auditing in a computerised environment and use the relevant frameworks and best practices for compliance and assurance assignments.	2.2 Statements of auditing relating to auditing in a computerised environment.
	2.15. Computer Assisted Audit Techniques, tools and risk assessment techniques including data analysis, Business Intelligence, sampling
	2.20. Follow up review
2.8. Communicate/Report findings in specific formats using standards or best practices as required.	2.12 Analysis of evidence, risk ratings of findings/control weaknesses, report findings, obtaining management response and follow up of implementation.
2.9. Conduct follow-up reviews or prepare status reports to ensure appropriate actions have been taken by management in a timely manner.	2.20. Follow up review
2.10. Distinguish key steps and processes of Cyber Frauds investigation and Cyber Forensics.	2.14. Cyber Frauds investigation and specific process relating to Cyber Forensics
	2.15. Computer Assisted Audit Techniques, tools and risk assessment techniques including data analysis, Business Intelligence, sampling, Automation of IS Assurance, etc.
2.11 Create IS Assurance or consulting function in an enterprise/within CA office by identifying key enablers and resources including identifying required personnel with required competencies and skill sets.	2.3 Different aspects of IS Audit process - audit charter, audit planning, audit universe, risk-based audit approach, IS Audit standards, guidelines, regulations, procedures and audit reporting.
	2.15 Types of IT enabled services, IS Assurance assignments and auditing in a computerised environment and using the relevant processes and best practices for compliance and assurance assignments.

Knowledge Statement Reference Guide

Each knowledge statement is explained in terms of underlying concepts and relevance of the knowledge statement to the DISA Candidate. It is essential that the candidate understand the concepts. The knowledge statements are what the IS Auditor must know in order to accomplish the tasks. Consequently, only the knowledge statements are detailed in this section. The sections identified in the matrices are explained in the following chapters.

2.1 Relevant IT assurance standards, guidelines, frameworks and best practices as per scope and objective of the assignment.

Key Concepts	Reference
IT assurance standards, guidelines, frameworks and best practices	2.8

2.2 Statements of auditing relating to auditing in a computerised environment.

Key Concepts	Reference
Statements of auditing relating to auditing in a computerised environment.	1.3, 1.4 and 2.8

2.3 Different aspects of IS Audit process - audit charter, audit planning, audit universe, risk-based audit approach, IS Audit standards, guidelines, regulations, procedures and audit reporting.

Key Concepts	Reference
IS Audit process - audit charter, audit planning, audit universe, risk-based audit approach, IS Audit standards, guidelines, regulations, procedures and audit reporting	1.6, 2.2, 2.3, 2.5 2.7, 2.8, 29 and 2.21.

2.4 Role and responsibilities of IS Audit function/department and key enablers.

Key Concepts	Reference
Role and responsibilities of IS Audit functions/departments	1.9

2.5 Documenting enterprise, technology deployment, organisation structure, technology environment including control architecture so as to analyse and assess risks.

Key Concepts	Reference
Documenting enterprise, technology deployment, organisation structure, technology environment and control architecture	2.7

2.6 Audit Risk management strategy and approach

Key Concepts	Reference
Audit risk management strategy and approach	1.5, 1.7, 2.9 and 2.12

2.7 Assurance or consulting services including scoping, risk assessment, audit planning, audit program, audit procedures, using audit tools, analysis and reporting.

Key Concepts	Reference
Assurance or consulting services	Chapter 1, 3 and appendix

2.8 IS Audit process cycle from scoping to reporting

Key Concepts	Reference
IS Audit process cycle	2.2 to 2.23

2.9 Defining Audit scope and objectives

Key Concepts	Reference
Audit scope and objectives	2.2 and 2.4

2.10 Preparing request for proposal from client, submitting proposal

Key Concepts	Reference
RFP and submitting proposal	2.2.2

2.11 Audit documentation, obtaining and evaluating audit evidence

Key Concepts	Reference
Audit documentation and evidence	2.16, 2.17, 2.19 and 2.20

2.12 Analysis of evidence, Risk Rating of findings/Control weaknesses, reporting findings, obtaining management response and follow up of implementation.

Key Concepts	Reference
Audit evidence, risk rating, reporting and follow up	2.16, 2.20 to 2.23

2.13 Types of Internal control and related risks

Key Concepts	Reference
Internal controls and related risks	1.5 to 1.8 and 2.9

2.14 Analytical procedures, compliance testing and substantive testing

Key Concepts	Reference
Analytical procedures, compliance testing and substantive testing	2.12.4, 2.13 and 2.14

Module 2

2.15 Types of IT enabled services, IS Assurance assignments and auditing in a computerised environment and using the relevant processes and best practices for compliance and assurance assignments.

Key Concepts	Reference
2.15 Types of IT enabled services, IS Assurance assignments and auditing in a computerised environment and using the relevant processes and best practices for compliance and assurance assignments.	Chapter 3 and appendix

2.16 Cyber Frauds investigation and cybercrimes, specific process relating to Cyber Forensics

Key Concepts	Reference
Cyber Frauds investigation and cybercrimes, specific process relating to Cyber Forensics	3.4

2.17 Audit tools and techniques including CAAT, tools and risk assessment techniques including data analysis, Business Intelligence, sampling, Automation of IS Assurance, etc.

Key Concepts	Reference
Audit tools and techniques, CAAT, tools and risk assessment techniques including data analysis, Business Intelligence, sampling, Automation of IS Assurance, etc.	2.12

2.18 Using best practices frameworks such COBIT, ISO etc.

Key Concepts	Reference
COBIT, ISO	2.7.4 and 2.8

2.19 Key provisions of Information Technology Act and Rules and impact on IS Assurance.

Key Concepts	Reference
IT Act and impact on IS Assurance	2.7.4

2.20 Follow up review

Key Concepts	Reference
Follow up review	2.23

SECTION 2: CONTENTS

CHAPTER 1: CONCEPTS OF IS AUDIT

Learning Objectives

The objective of this chapter is to provide sufficient knowledge about the fundamental concepts of information systems audit. This chapter provides insight into all the key concepts relating to IS audit such as IS Audit methodology, enterprise risk management, risk based auditing, materiality, internal controls and the roles and responsibilities of the IS audit function. A good understanding of these concepts will enable DISAs to plan, perform and provide report on IS Assurance and consulting assignments. The concepts covered are the building blocks for planning, execution and reporting of IS audit which are covered in Chapters 2 and 3.

1.1 Introduction

In the present age of globalization, Information System and the Information Technology (IT) has become a backbone for any organization whether the field of its operation is manufacturing, education, trading, technology, entertainment, etc. Nowadays, the success of any organization is dependent on the information that is generated from the automated information system. IT is used by enterprises for providing greater satisfaction to customers, to access wider range of information, to handle business changes as real time events, and create more efficiency within the enterprise. Further, with the development of automated information systems there has been a simultaneous increase in the threats to the security of information systems which has led to financial losses to the enterprise and most importantly loss of critical information. Hence in the current competitive world, the enterprises strive not only to attain more efficiency and effectiveness of business through implementation of information systems but also secure the information which has become the most valuable asset to the enterprise.

As an IS auditor, the scope of work can vary from assisting the enterprise to select and successfully implement information systems. The engagements can go beyond just implementing some basic IT level security. It is important for organisations to take a holistic perspective and implement security from a governance perspective with involvement of board in direct and monitoring the use of IT for achieving business objectives. Regulatory requirements also demand involvement of senior management in effective decision making in all key aspects of IT security. Senior management look for assurance from IS Auditors on the availability, adequacy and appropriateness of IT controls as implemented and also seek advice on best deployment of IT for achieving business objectives. Hence, the role of the IS auditor has expanded to review not only whether IT is deployed in a safe and secure environment but also to provide advisory services on optimum use of technology to enable organizations to survive and thrive in the competitive environment while complying with regulatory requirements.

1.2 Definitions

Audit: In simple terms audit is an official inspection of an organization's accounts, typically by an independent body. In case of financial audit, audit is an independent examination of financial information of any entity, whether profit oriented or not, and irrespective of its size or legal form with a view to expressing an opinion thereon. In case of IS Audit, the audit encompasses independent review and evaluation of automated information systems, related manual systems and the interfaces between them.

Computer System: Refers to a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions.

Information: As per IT Act 2000, information includes data, text, images, sound, voice, codes, computer programs, software and databases or micro film or computer generated micro fiche. In general data processed in a meaningful context is information. Information has value to user. Information is data that is (1) accurate and timely, (2) specific and organized for a purpose, (3) presented within a context that gives it meaning and relevance, and (4) can lead to an increase in understanding and decrease in uncertainty.

Information Systems (IS): In general is refers to the study of complementary networks of hardware and software, that people and organizations use to collect, filter, and process, create, and distribute data. Specifically in the context of IT, Information systems are the software and hardware systems that support data-intensive applications and includes the design and implementation of languages, data models, process models, algorithms, software and hardware for information systems.

Secure system: It means computer hardware, software, and procedure that:

- (a) Are reasonably secure from unauthorized access and misuse;
- (b) Provide a reasonable level of reliability and correct operation;
- (c) Are reasonably suited to performing the intended functions; and
- (d) Adhere to generally accepted security procedures;

Risk: It is the potential of uncertain event resulting in losing something of value, weighed against the potential to gain something of value. In IT parlance, it can be an uncertain event or something going wrong, which affects enterprise from achieving set objectives. Risk is the potential that a given threat will exploit the vulnerabilities of an asset or a group of asset to cause loss or damage to the assets.

Internal Control: It is a process implemented in an organization to help in achieving specific goals. Internal control include the policies, standards, plans and procedures, and organisational structures designed to provide reasonable assurance that enterprise objectives will be achieved and undesired events will be prevented or detected and corrected.

Business Process: A business process is a collection of related, structured activities or tasks that produce a specific service or product (serve a particular goal) for a particular customer or customers. It often can be visualized with a flowchart as a sequence of activities with interleaving decision points or with a Process Matrix as a sequence of activities with relevance rules based on data in the process.

1.3 Concepts of Audit

The general standards of auditing are applicable to IS Audit also as IS Audit is a type of internal audit or sub-set of the statutory audit. As per the general guidelines on Internal Auditing issued by ICAI, Auditing is defined as a systematic and independent examination of data, statements, records, operations and performances of an enterprise for a stated purpose. In an auditing situation, the IS Auditor perceives and recognizes the propositions before him for examination, collects evidence, evaluates the same and on this basis formulates judgment which is communicated through the report.

Internal auditing is defined an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

SA 200 describes the basic principles of audit and these principles are applicable for IS Audit also and have to be complied with. IS Audit is primarily an internal audit conducted for providing assurance after evaluation of risks and provides report on the implemented controls. Based on such evaluation, the IS Auditor would provide appropriate recommendations for mitigating control weaknesses in IT related areas. **IS Audit may also be carried out by external auditors as part of statutory audit to review internal controls in automated information systems. However, the scope would be bound by the objectives of the applicable regulatory requirements. IS Audit could also be carried out as a part of internal audit or as a specialized audit of IT environment such as: penetration testing, audit of data centre, audit of BCP or review of IT strategy, etc.**

Integrity, Objectivity and Independence: The IS Auditor should be straight forward, honest and sincere in his approach to his professional work. He must be fair and must not allow prejudice or bias to override his objectivity. He should maintain an impartial attitude and appear to be free from any interest which might be regarded whatever its actual effect as being incompatible with integrity and objectivity.

Skill and Competence: The IS audit should be performed and the report prepared with due professional care by persons who have adequate training, experience and competence. This can be acquired through a combination of general education, technical knowledge obtained through study and formal courses concluded by a qualifying examination recognized for this purpose and practical experience under proper supervision.

Confidentiality: The IS Auditor should respect the confidentiality of information acquired during the course of work and should not disclose any such information to a third party without specific authority or unless there is any legal or professional duty to disclose.

Work performed by others: When the IS Auditor delegates work to assistants or uses work performed by other IS Auditors or experts, he will continue to be responsible for forming and expressing his opinion on auditee environment as per the scope and objectives of audit. However, at the same time IS Auditors are entitled to rely on the work performed by others provided they exercise adequate skills and care and are not aware of any reason to believe that they should not have relied. The IS Auditors should carefully direct, supervise and review work delegated to assistants. They should obtain reasonable assurance that work performed by other IS Auditor or experts are adequate and in accordance with set audit objectives.

Documentation: The IS Auditor should have documentary evidence, which is important in providing evidence that the audit was carried out in accordance with IS Auditing standards, guidance and procedures and adhering to the regulatory requirements.

Information systems and internal control: The IS Auditor should gain an understanding of the information systems and related internal controls. They should study and evaluate the operation of those internal controls upon which they wish to rely to determine the nature, timing and extent of other audit procedures.

Audit conclusions and reporting: The IS Auditor should review and assess the conclusions drawn from the audit evidence obtained and from their knowledge of business of the entity as the basis for the expression of their opinion.

1.4 Concept of IS Audit and Auditing in a computerized environment

1.4.1 Audit in a computerized environment

Historically, all kinds of accounting and data processing job was conducted manually which involved preparation of physical records and the auditor had no choice but to conduct audit manually. With the increased use of internet and e-commerce technologies, enterprises are relying more and more on computer systems for much of accounting and all other critical business processes leading to most of the auditee information being available in electronic format rather

than manual format. Hence, the audit approach, audit evidence has moved from physical to digital and it has become imperative for auditors to use computers to audit this digital information.

The overall scope and objectives of audit doesn't change in a computerised environment. However, the use of a computer changes the processing and storage of information and may affect the organization and procedures employed by the organisation to implement adequate and appropriate internal control. Accordingly, the procedures followed by the auditor in their review and evaluation of the: information systems, related internal controls, nature, timing and extent of audit procedures are directly impacted by the computerised information systems environment.

1.4.2 IS Audit (Auditing of the computerized environment)

The IS Audit of an Information System Environment may include one or both of the following:

- Assessment of internal controls within the IS environment to assure validity, reliability, and security of information and information systems.
- Assessment of the efficiency and effectiveness of the IS environment.

The objective of IS audit process is to evaluate the adequacy of internal controls with regard to both specific computer program and the data processing environment as a whole. ISACA defines IS Audit as: "IS audit refers to any audit that encompasses wholly or partly, review and evaluation of automated information processing systems, related non-automated processes and the interfaces between them". Although IS Audit is often mis-understood as a mere technical audit and a domain of IT professionals, it is clear that IS Audit involves evaluating the adequacy and efficiency of internal controls in business processes that are either partly or fully computerized. Hence Audit and control professionals who have expertise in understanding of business processes and internal controls with exposure to information technology risks and controls are considered the most appropriate professionals to conduct most of the information systems audits.

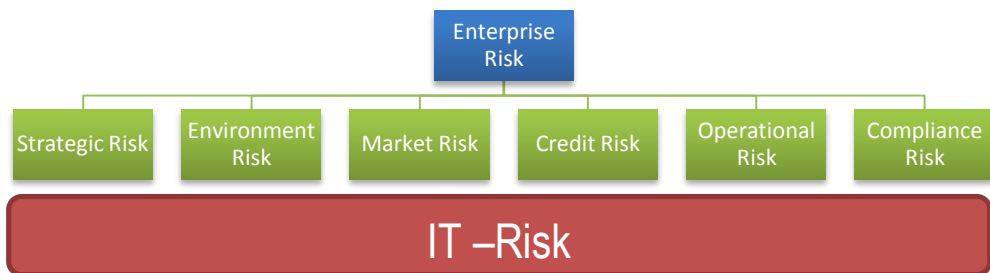
An IS Audit cannot be viewed from a narrow perspective of audit of only automated information processing systems but would include audit of non-automated control processes and interfaces. Therefore, depending on the audit environment, objectives and scope, the audit could involve audit of entire business processes, partially or fully automated, or audit of specified application, technology and related controls. IS Audit is a focused audit about auditing an information systems area whereas Audit in a Computerized Environment is a regular audit engagement performed in process area using the computer. **Please refer to the Technical guide on IS Audit (included as reference material in DVD).**

1.5 Concept of IT Risk

There are numerous changes in IT and its operating environment that emphasizes the need to better manage IT related risks. This has increased the level of dependency of organization on electronic information which are processed by IT systems. These IT systems are now essential to

support critical business processes. Risk is an event which has a potential to impact organization goal and strategy implementation in a negative manner. Another way of defining risk would be Threat exploiting Vulnerabilities.

IT risk has significant impact on the overall business risk as failure of IT could impact the business. IT risk is a component of the overall risk universe of the enterprise, as shown in below figure. Other risks that an enterprise faces include strategic risk, environmental risk, market risk, credit risk, operational risk and compliance risk. In many enterprises, IT-related risk is considered to be a component of operational risk, e.g., in the financial industry in the Basel II framework. However, even strategic risk can have an IT component to it, especially where IT is the key enabler of new business initiatives. The same applies for credit risk, where poor control on IT and IT security can lead to lower credit ratings of organizations. For that reason it is better not to depict IT risk with a hierarchic dependency on one of the other risk categories.



1.5.1 IT Risk in the Risk Hierarchy

Managing the IT risk of the enterprise starts with defining the risk universe; a risk universe describes the overall environment and provides a structure for managing IT risk. The Risk universe:

- Considers the overall business objectives, business processes and their dependencies throughout the enterprise. It describes which IT applications and infrastructure support the business objectives through the provision of IT services. It is worth highlighting that IT risk needs to be seen from an end-to-end business activity perspective, crossing IT function silos (IT operations, project management, application development, disaster recovery, security, etc.).
- Considers the full value chain of the enterprise. This can include not only the enterprise and its subsidiaries/business units, but also clients, suppliers and service providers.
- Considers a full life-cycle of IT related business activities, including transformation programs, investments, projects and operations.
- Includes a logical and workable segmentation of the overall risk environment. This sounds relatively easy but often it is not – the hierarchical organizational of the enterprise business, business processes and supporting IT infrastructure and services often are not aligned, and it is highly probable that different views along different dimensions exist for the overall environment. It is up to the enterprise to determine which view will be the most

meaningful to support the business objectives of the enterprise while considering the potential overlaps and omissions.

- Needs to be reviewed and updated on a regular basis due to the constantly changing internal and external requirements.

1.5.2 Risk management

Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization. Risk can be avoided, reduced, transferred or accepted. An organization can also choose to reject risk by ignoring it, which can be dangerous and should be considered a red flag by the IS Auditor. The counter-measures for mitigating risks are also called controls and these need to be implemented as appropriate. In reviewing an IS environment, the primary focus of the IS Auditor would be to review the risk assessment done by the organisation, assess whether these risks have been mitigated by implementing appropriate controls and the residual risk is knowingly accepted and is within the risk appetite. In case the residual risks after applying the controls exceed the residual risk and have not been approved by the management, report these risks with appropriate remedial measures.

Here onwards, the word risk should be interpreted as IT Risk and Audit would be referred as IS Audit.

1.6 Risk Based Auditing

A risk based audit approach is usually adapted to develop and improve the audit process on a continuous basis so that the focus is on high risk areas and maximum value addition is derived from audit resources deployed. This approach is used to assess risk and to assist an IS Auditor to focus on high risk areas and in making the decision with regards to the sample size to perform either compliance testing and/or substantive testing. It is important to stress that the risk based audit approach efficiently assists the IS Auditor in focusing on the risk areas which are most critical and also in determining the nature and extent of testing.

Within this concept, inherent risk, control risk or detection risk are of major concern for the IS Auditor. In a risk based audit approach, IS Auditors are not just relying on risk; they also are relying on internal and operational controls as well as knowledge of the company or the business. This type of risk assessment decision can help relate the cost-benefit analysis of the control to the known risk, allowing practical choices.

Business risks include concerns about the probable effects of an uncertain event in achieving established business objectives. The nature of these risks maybe financial, regulatory or operational, and may also include risks derived from specific technology deployment. For example,

an airline company is subject to extensive safety regulations and economic changes, both of which impact the continuing operations of the company. In this context, the availability of IT service and its reliability are critical.

By understanding the nature of business, IS Auditors can identify and categorize the types of risk associated with the business and identify the risks applicable to specific situations or audit environment. On the other hand, risk assessment refers to the methodology where risks have been given elaborate weights based on the nature of the business or the significance of the risk and risks are categorized as high, medium or low based on which appropriate decisions are taken by management.

SA 315, the standard for risk identification and assessment requires IS Auditors to assess risk that is part of the business environment and the internal control system. SA 330 requires IS Auditors to review whether management has designed and implemented appropriate risk remediation measures and provide recommendations on the residual risks that have been identified as critical and are not appropriately mitigated. Usually the IS Auditor would provide recommendations for risk remediation as part of the Audit Report.

1.7 Audit Risk and Materiality

1.7.1 Audit Risk

Audit risk: In general, audit risk refers to the risk that an auditor may issue unqualified report due to the auditor's failure to detect material misstatement either due to error or fraud. This risk is composed of inherent risk (IR), control risk (CR) and detection risk (DR). Audit risk can be high, moderate or low depending on the sample size selected by the Auditor. In the context of IS Audit, the meaning of audit risk is still relevant but it would vary depending on the specific scope and objectives of audit.

Inherent risk means overall risk of management which is on account of entity's business operations as a whole. Inherent risk is the susceptibility of information resources or resources controlled by the information system to material theft, destruction, disclosure, unauthorized modification, or other impairment, assuming that there are no related internal controls. Inherent risk is the risk that has natural association. The inherent risk for audit assignment can be project related risks, revenues related risks, and resource related risks. Inherent risk to business can be dependent on nature of business. If the IS Auditor concludes that there is a high likelihood and consequence of risk exposure, ignoring internal controls, the IS Auditor would conclude that the inherent risk is high.

Detection risk is the risk of the IS Auditor when he is not able to detect the inherent risk or the controllable risk. It means higher the level of non-detection by the IS Auditor, higher is the detection risk. Detection risk is the risk that the IS Auditor's substantive procedures will not detect an error

which could be material, individually or in combination with other errors. For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high if the audit logs for the whole period of audit are not available at the time of the audit. Detection risk is a measure of the IS Auditor's assessment of the likelihood that the vulnerability or gaps will not be detected by the IS Auditors. IS Auditor will carry out more detailed audit to detect material vulnerabilities or gaps if the inherent risk and control risk are high. Detection risk primarily refers to the fact that there exists a control weakness that auditor fails to detect.

Control risk is the risk that an error which could occur in an audit area, and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. Control risk is a measure of the IS Auditor's assessment of the likelihood that risk exceed a tolerable level and will not be prevented or detected by the client's internal control system. This assessment includes an assessment of whether a client's internal controls are effective. For example: the enterprise has good system of segregation of duties but two employees could collaborate and still commit fraud.

Assessing inherent, control and detection risk gives the final assessment of the overall Audit Risk i.e. the risk which the IS Auditor is ready to accept in an audit assignment. Audit risk is the product of inherent risk, control risk and detection risk. The extent of audit effort is dictated by the degree of audit risk, the assessment of which is critical to the effectiveness of the audit effort. Amongst the critical factors affecting the audit risk is the appropriate assessment of the control environment. The preliminary review of audit environment enables the IS Auditor to gain understanding of the business, technology and control environment and also gain clarity on the objectives of the audit and scope of audit. Risk assessment allows the IS Auditor to determine the scope of the audit and assess the level of audit risk and error risk.

1.7.2 Materiality

The concept of materiality in the case of financial audit is based on value and volume of the transactions and the relevant error or discrepancy or control weakness detected. In case of regulatory audit, materiality is based on impact of non-compliance and in case of IS Audit, materiality is based on the effect or consequence of the risk in terms of potential loss. Hence, materiality varies based on the scope and objectives of the audit and specific auditee environment. Materiality is an important aspect of the professional judgment of the IS Auditor as he/she has to decide whether the information is material or immaterial. With regards to the materiality of the financial statements, information is regarded as material if it changes the decision of the users of the financial statement i.e. if the misstatement is of a high value and quantity. The IS Auditor should have a good understanding of these audit risks when planning an audit. An audit sample may not detect every potential error in a population. When evaluating internal controls, the IS Auditor should realize that a given system may not detect a minor error. However, that specific error, combined with others, could become material to the overall system.

The concept of materiality requires sound judgment from the IS Auditor. The IS Auditor may detect a small error that could be considered significant at an operational level, but may not be viewed as significant to upper management. Materiality considerations combined with an understanding of audit risk are essential concepts for planning the areas to be audited and the specific test to be performed in the audit. It depends on the IS Auditor to decide whether the information is material for him which means that lower the risk than an IS Auditor is willing to undertake, lower is the level of materiality. In other words, higher the level of materiality, lower is the risk that an IS auditor is willing to take.

For systems and operations not affecting financial transactions, the following are examples of measures that should be considered to assess materiality:

- Criticality of the business processes supported by the system or operation
- Cost of the system or operation (i.e., hardware, software, staff, third-party services, overheads, and a combination of these). E.g. A virus has been detected and cleaned and there was no impact on business or operations. Apparently, this may not be a material risk. However, materiality can be correctly determined only when root cause analysis is done to ascertain the how and from where the virus entered the organisation's information system. The analysis may reveal that there is weakness in control process. Hence although the incident per se is not material but inherent cause of weakness is definitely material as the virus problem can recur and cause harm to the organisation information system. If auditor fails to detect this weakness it might result in detection risk.
 - Potential cost of errors (possibly in terms of lost sales, warranty claims, irrecoverable development costs, cost of publicity required for warnings, rectification costs, health and safety costs, unnecessarily high costs of production, high wastage, etc.)
 - Number of accesses/transactions/inquiries processed per period
 - Nature, timing and extent of reports prepared and files maintained
 - Nature and quantities of materials handled (e.g., where inventory movements are recorded without values)
 - Service level agreement (SLA) requirements and cost of potential penalties
 - Penalties for failure to comply with legal and contractual requirements

SA 320 is the Auditing standard for Audit Materiality. It requires the Auditor to report those items that create an impact on the financial statements and which changes the decision that would be made by the stakeholder. The same concept is applied even when conducting an IS Audit Engagement. The ITAF, 2nd edition issued by ISACA has the following standards on "Materiality" which has to be complied by the IS Auditor.

1204.1 IS audit and assurance professionals shall consider potential weaknesses or absences of controls while planning an engagement, and whether such weaknesses or absences of controls could result in a significant deficiency or a material weakness.

1204.2 IS audit and assurance professionals shall consider audit materiality and its relationship to audit risk while determining the nature, timing and extent of audit procedures.

1204.3 IS audit and assurance professionals shall consider the cumulative effect of minor control deficiencies or weaknesses and whether the absence of controls translates into a significant deficiency or a material weakness.

1204.4 IS audit and assurance professionals shall disclose the following in the report:

- Absence of controls or ineffective controls
- Significance of the control deficiency
- Likelihood of these weaknesses resulting in a significant deficiency or material weakness

1.8 Concepts of Internal Control

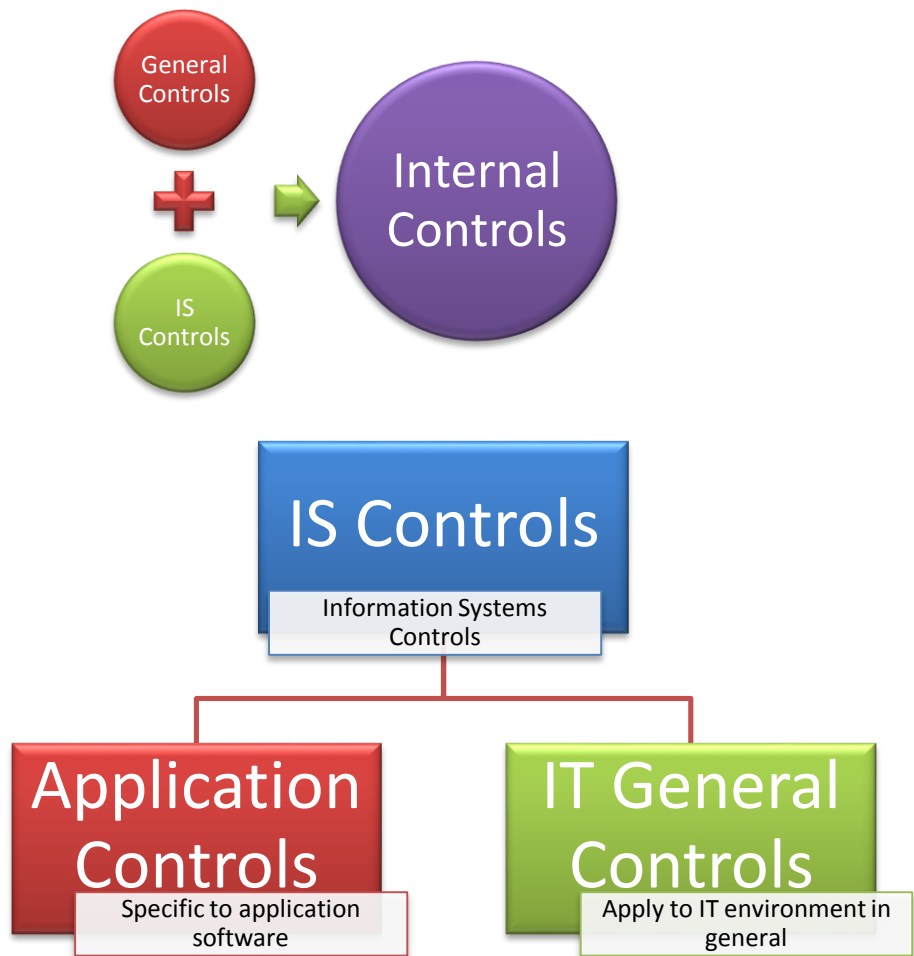
The increasing use of IT in organizations has made it imperative that appropriate information systems are implemented in an organization. IT should cover all key aspects of business process of an enterprise which have an impact on its strategic and competitive advantage for its success. Control is defined by ISACA as: “Control refers to the policies, procedures, practices and organisation structure that are designed to provide reasonable assurance that the business objectives will be achieved and undesired events are prevented or detected and corrected”. This definition of control is applied for all IS Audits. Internal Controls are normally composed of policies, procedures, practices and organizational structures which are implemented to reduce risks in the organisation to an acceptable level. Internal controls are developed to provide reasonable assurance to management that the organization's business objectives will be achieved and risk events will be prevented or detected and corrected.

Internal control activities and supporting processes are either manual or driven by automated computer information resources. Thus, IS audit includes reviewing the implemented systems or providing consultation and evaluating the reliability of operational effectiveness of controls. The objective of controls is to reduce or if possible eliminate the causes of the exposure to potential loss.

Types of Internal Controls

1. **Preventive:** Designed to prevent errors or irregularities from occurring.
2. **Detective:** Designed to detect errors or irregularities that may have occurred.
3. **Corrective:** Designed to correct errors or irregularities that have been detected and report them.

Internal Controls is said to be a mechanism that is established by organizations which is a sum of General Controls and IS Controls. IS controls is said to be a sum of IT Application Controls and IT General Controls. General Controls refers to internal controls that encompass all administrative areas in general including IT implementation whereas application controls are implemented in specific application software. In general, it can be said that IS Controls are controls that are present on the enterprise's IT Infrastructure. IT Infrastructure includes hardware and software.



Types of IS Controls

IS Controls can also be classified in the following manner:

Preventive Controls: Controls that prevents problems before they arise. They monitor both operation and inputs. They attempt to predict potential problems before they occur and make adjustments. They also help in preventing an error, omission or malicious act from occurring.

Detective Controls: Controls that detect and report the occurrence of an error, omission or malicious act.

Corrective Controls: Controls that minimize the impact of a threat. They remedy problems that are discovered by Detective controls. They help in identification of the cause of the problem. They correct errors arising from the problem. They modify the processing systems to minimize future occurrences of the problem.

1.9 Organization of IS Audit Function

The IS audit function should be placed in the organization so as to ensure its objectivity and independence. The appointment of external auditor should also be governed by stipulations for independence and objectivity, which is the foundation for an effective audit function. The composition and constitution of the IS audit function should ideally be decided by the audit committee and should be the prime reporting pointer for the IS Audit function. The role of the IS Audit function is defined by the audit charter which defines the authority, scope and responsibility. The audit charter provides mandate for performing the audit function. Based on the overall guidelines defined in the audit charter, the audit function is created with specific roles and responsibilities.

1.9.1 Infrastructure and organization

IS audit function should be equipped with sufficient resources to discharge its duties efficiently and effectively. An important determinant in the quality of the IS audit function is the quality of human resource that staff the audit function. The skills and competence requirements should be clearly established and as an IS Audit function should collectively possess the skills and knowledge necessary for performing an effective and professional audit. Even in cases where external agencies are engaged, the professional competence and skills of such agencies should be ensured. Continuing Professional Education should be included as part of the IS audit management plan.

Assurance function perspective: It describes what is needed in an enterprise to build and provide assurance function(s). The assurance function perspective describes how each factor contributes to the overall provisioning of assurance, for example:

- Which organizational structures are required to provide assurance (board/audit committee, audit function, etc.)
- Which information items are required to provide assurance (audit universe, audit plan, audit reports, etc.)

The function might require special infrastructure for using CAATs. If so, availability of appropriate tools and infrastructure should be ensured.

ITAF, 2nd edition issued by ISACA provides the following standard regarding independence of IS Auditor.

1002 Organisational Independence

1002.1 The IS audit and assurance function shall be independent of the area or activity being reviewed to permit objective completion of the audit and assurance engagement.

1003 Professional Independence

1003.1 IS audit and assurance professionals shall be independent and objective in both attitude and appearance in all matters related to audit and assurance engagements.

1.9.2 Internal and external audit control framework

The internal and external audit control framework ensures the minimum quality of audits. This forms the basis for the organization to implement the appropriate an audit control framework. Accordingly, policies and procedures for risk assessment, planning, implementation and reporting are to be established. The audit control framework assures the effectiveness and efficiency of operations, reliability of reporting and compliances with laws and regulations. The standards and professional pronouncements should be strictly adhered to, and this should be reflected in the organization and operations of the audit function. Specific guidelines have to be issued to ensure the qualitative work under control environment.

1.9.3 Quality Assessment and Peer Reviews

Quality Assessment ensure that the IS audit function is delivering in line with the best auditing practices and following the professional standards and pronouncements, It also ensures that the IS Audit function is subject to both internal and external quality assessments, peer reviews, certification and accreditation. Though the objective of the internal and external IS audit remains same, the scope and approach might vary. In case of an internal IS audit, the IS Auditor reviews the internal control environment in detail whereas an external IS Auditor takes an overall view of internal control environment and focuses on substantive testing as per the specific scope and objective of the assignment. In case of external audit, the audit engagement letter defines the scope and objectives of individual audit assignment.

1.9.4 Standards on Audit Performance

IS auditors have to comply with the following standards of ITAF, 2nd Edition issued by ISACA.

1004 Reasonable Expectation

1004.1 IS audit and assurance professionals shall have reasonable expectation that the engagement can be completed in accordance with the IS audit and assurance standards and, where required, other appropriate professional or industry standards” or applicable regulations and result in a professional opinion or conclusion.

1004.2 IS audit and assurance professionals shall have reasonable expectation that the scope of the engagement enables conclusion on the subject matter and addresses any restrictions.

1004.3 IS audit and assurance professionals shall have reasonable expectation that management understands its obligations and responsibilities with respect to the provision of appropriate, relevant and timely information required to perform the engagement.

1005 Due Professional Care

1005.1 IS audit and assurance professionals shall exercise due professional care, including observance of applicable professional audit standards, in planning, performing and reporting on the results of engagements.

1006 Proficiency

1006.1 IS audit and assurance professionals, collectively with others assisting with the assignment, shall possess adequate skills and proficiency in conducting IS audit and assurance engagements and be professionally competent to perform the work required.

1006.2 IS audit and assurance professionals, collectively with others assisting with the assignment, shall possess adequate knowledge of the subject matter.

1006.3 IS audit and assurance professionals shall maintain professional competence through appropriate continuing professional education and training.

1007 Assertions

1007.1 IS audit and assurance professionals shall review the assertions against which the subject matter will be assessed to determine that such assertions are capable of being audited and that the assertions are sufficient, valid and relevant.

1008 Criteria

1008.1 IS audit and assurance professionals shall select criteria, against which the subject matter will be assessed, that are objective, complete, relevant, measureable, understandable, widely recognised, authoritative and understood by, or available to, all readers and users of the report.

1008.2 IS audit and assurance professionals shall consider the source of the criteria and focus on those issued by relevant authoritative bodies before accepting lesser-known criteria.

1.10 Summary

This chapter has provided brief overview of the fundamental concepts of Audit, IS audit, risks, controls and internal controls. We have also provided the distinction between audit in an IS environment and audit of a computerized environment. Further, the conceptual understanding of

IT risk and risk based auditing has been provided with an overview of types of audit risks and their categorization as: Inherent Risk, Controllable Risk and Detection Risk. The concept of materiality and internal controls with overview of types of internal controls has been provided. Controls can be classified as: IS Controls and general Controls and IT controls are bifurcated as IT Application Controls which are specific to application software and IT General Controls which pertain to the IT environment in general. The classification of controls as preventive, detective and corrective has been explained. The overall objective of this chapter is to provide an understanding of the key concepts of information systems, audit function, materiality and the attached risk. In the next chapter, we will discuss the practical aspects of how IS Audit is planned, executed and reported.

1.11 Questions

1. Who among the following is responsible for establishing IS Audit function in the organisation?
 - A. Audit Charter
 - B. Audit Governance
 - C. Audit Objectives
 - D. Audit Project Plan
2. Which of the following control classifications identify the cause of a problem and minimize the impact of threat?
 - A. Administrative Controls
 - B. Detective Controls
 - C. Preventive Controls
 - D. Corrective Controls
3. Which of the following is NOT generally considered a category of Audit Risk?
 - A. Detection Risk
 - B. Scoping Risk
 - C. Inherent Risk
 - D. Control Risk
4. Which of the following are most commonly used to mitigate risks discovered by organizations?
 - A. Controls
 - B. Personnel
 - C. Resources
 - D. Threats
5. Which of the following is not a type of internal controls?
 - A. Detective

- B. Corrective
 - C. Preventive
 - D. Administrative
6. What means the rate at which opinion of the IS Auditor would change if he selects a larger sample size?
- A. Audit Risk
 - B. Materiality
 - C. Risk Based Audit
 - D. Controls
7. Which of the following cannot be classified as Audit Risk?
- A. Inherent Risk
 - B. Detection Risk
 - C. Controllable Risk
 - D. Administrative Risk
8. After you enter a purchase order in an on-line system, you get the message, "The request could not be processed due to lack of funds in your budget". This is an example of error?
- A. Detection
 - B. Correction
 - C. Prevention
 - D. Recovery
9. When developing a risk-based audit strategy, an IS auditor should conduct a risk assessment to ensure that:
- A. controls needed to mitigate risks are in place.
 - B. vulnerabilities and threats are identified.
 - C. audit risks are considered.
 - D. a gap analysis is appropriate
10. Reviewing management's long-term strategic plans helps the IS auditor:
- A. Gains an understanding of an organization's goals and objectives.
 - B. Tests the enterprise's internal controls.
 - C. Assess the organization's reliance on information systems.
 - D. Determine the number of audit resources needed.

1.12 Answers and Explanations

1. An audit charter establishes the role of the internal audit function. These are established by the senior management.

2. Corrective Controls classifications identify the cause of a problem and minimize the impact of threat. The Goal of these controls is to identify the root cause of an issue whenever possible and eliminate the potential for that occurring again. The other controls are useful but perform other functions instead.
3. Scoping risk is not generally considered as category of audit risk. The other risk categories are also possible types of risk; however they are not the one that question demand.
4. Controls are most commonly used to mitigate risks discovered by organizations. This is what organizations implement as a result of the risks an organization discovers. Resources and personnel are often expended to implement controls.
5. Administrative is not a type of internal controls. Detective is designed to detect errors or irregularities that may have occurred. Corrective is designed to correct errors or irregularities that have been detected. Preventive is designed to keep errors or irregularities from occurring.
6. Audit risk means the rate at which opinion of the IS Auditor would change if he selects a larger sample size. Audit risk can be high, moderate or low depending on the sample size selected by the IS Auditor. A risk based audit approach is usually adapted to develop and improve the continuous audit process. Materiality means importance of information to the users. It is totally the matter of the professional judgment of the IS Auditor to decide whether the information is material or immaterial.
7. Inherent risk means overall risk of management which is on account of entity's business operations as a whole. Controllable risk is the risk present in internal control system and the enterprise can control this risk completely and eliminate it from the system. Detection risk is the risk of the IS Auditor when he is not able to detect the inherent risk or the controllable risk.
8. To stop or prevent a wrong entry is a function of error prevention. All other options work after an error. Prevention works before an occurring of error.
9. In developing a risk-based audit strategy, the risks and vulnerabilities are understood. This will determine the areas to be audited and the extent of coverage. Understanding whether appropriate controls required to mitigate risks are in place is a resultant effect of an audit. Audit risks are inherent aspects of auditing, are directly related to the audit process and are not relevant to the risk analysis of the environment to be audited. Gap analysis would normally be done to compare the actual state to an expected or desirable state.
10. Strategic planning sets corporate or departmental objectives into motion. Strategic planning is time and project-oriented, but must also address and help determine priorities to meet business needs. Reviewing long-term strategic plans would not achieve the objectives expressed by the other choices.

CHAPTER 2: IS AUDIT IN PHASES

Learning Objectives

This chapter provides detailed insights into the various phases of IS audit. The fundamental concepts which were discussed in earlier chapter are connected to their practical aspects in terms of how to define the audit scope and objectives, gain knowledge of the organisation's business, assessment of risk, IT application controls and IT general controls of the enterprise. Sampling and testing methodologies using CAAT as used by the IS auditor are also discussed. How to develop audit programs and approach and design appropriate tests for compliance and substantive testing for reviewing the design effectiveness and operational effectiveness of the IS systems are explained. The need for IS auditor to obtain sufficient evidence as a part of the audit process which forms critical part of the assurance services as well as use of global best practices as benchmarks for performing and reporting IS audit findings are discussed in this chapter. Please note that organisation and enterprise are used inter-changeably.

2.1 Introduction

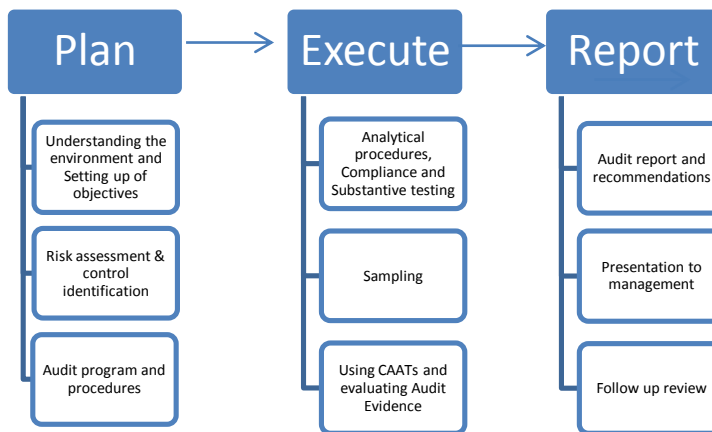
Information systems have become an integral part assurance process. The growth of technology has made IT an indispensable part of our day to day functioning. Organizations value information as the most critical asset. Hence, organisations have become more vulnerable due to potential loss such as theft of information causing loss for the enterprise. There is also the risk that the information may be stolen in fraudulent manner and it can be used by the fraudster for financial gains. Dependency on information and information technology has helped organizations in improving efficiency in customer delivery and also opened up new delivery channels. In order to adapt to these technological advancements organizations have reengineered their processes resulting in new vulnerabilities.

There is critical requirement of enhancing value of information by making it available online but this has to be coupled with right level of security. In the networked world, the fraudster can intrude into the system anytime and from anywhere. It is important that management has systems and processes in place not only to ensure that adequate controls exist and are working effectively but by having an independent evaluation of information systems from IS Audit professionals. The IS auditor has to plan the audit considering the information systems and keeping in mind the scope and objectives of the audit including the auditee environment, regulatory requirements and technology deployment.

The IS Audit phases are summarized in the following diagram.



Conducting an IS Audit



2.2 Conducting an IS Audit

2.2.1 Setting up of audit objectives

Audit objectives refer to the specific goals that must be met by the audit. In contrast, a control objective refers to how an internal control should function. An audit may, and generally does, incorporate several audit objectives. Audit objectives often focus on substantiating that internal controls exist to business risks, and that they function as expected. These audit objectives include assuring compliance with legal and regulatory requirements as well as the confidentiality, integrity, reliability and availability of information and IT Resources. Audit management may give the IS Auditor a general control objective to review and evaluate when performing an audit.

One of the basic purposes of any IS audit is to identify control objectives and the related controls that address these objectives. The objective of an information systems audit (design and operating effectiveness of the internal control system) is to enable the IS Auditor to express an opinion on whether the internal control system set up and operated by the organisation for the purpose of managing risks to the achievement of the objectives was suitably designed and operated effectively in the period. If there are control weaknesses, report these with appropriate recommendations for mitigating these risks by improving controls and thus provide value addition.

2.2.2 Request for Proposal and submitting response

Request for proposal (RFP)

A RFP is a standard solicitation document used by various organisations to compete for contract opportunities. An RFP is most often used to acquire services, although it may be used in some circumstances to acquire goods. A successful RFP process will support the principles of fair, open, and transparent procurement; it will satisfy the business requirements. This guide has been

developed to help organisations successfully navigate the RFP process. Well-prepared RFPs can go a long way to creating effective solutions and programs for business development and associations. With an RFP, proposals are evaluated against multiple criteria such as price, qualifications and experience, and the proposed solution or approach. The best proposal will be awarded the contract and the best proposal may, or may not, have the lowest price. **Please refer to section-3 for format of request for proposal.**

The stages in developing an effective RFP are as follows:

Introduction: This is the first stage in the RFP process where the background of the proposed activity is provided. The potential bidders are provided the need and rationale for publishing the RFP. It may also contain a key summary of the key contents which form the other sections of the document.

Requirements: This is the most important part of the document as it specifies the requirement of the organization. The requirements have to be specified in detail and if the need be the same can be broken down into various subsections depending upon the number of requirements and specifications for e.g.

1. **Size and quality of the service deliverables.**
2. **Technical specification needed for the product.**
3. **Quantity and specific expectations.**

Selection Criteria: In this section the selection criteria of the proposed bidders/ vendors should be specified. The selection would be based on the predefined criteria of deliverables and would be decided by a committee.

Timelines: This section should define of the timelines for submission of bids and the manner in which the same shall be accepted by the organization. This would ensure that not only potential vendors would comply with the timelines but also defines the structure of the bidding document; the vendors who fail to comply with the specifications would get eliminated immediately.

Process: In this section there is a need to explain how the whole process will work from sending the RFP to awarding the contract and starting the work. The commercial terms and conditions shall be mentioned along with the clauses on default and applicable damages for failure to deliver on the requirements as specified in the above section. The specific requirements of skills and competencies of the personnel deployed for the assignment would have to be provided. Further, the approach or methodology to be followed with standard templates of reporting will be requested from the bidders. This will help organisation in evaluating the technical competence of the vendor in executing the assignment by following a standard approach and using best practices framework and practices as applicable.

Request for References: This is an optional content which the organization can insert where the potential bidders/vendors need to furnish one or more references of their clients. The objective is

to evaluate experience of performing similar work and obtain confidence on the capacities of the bidder/vendor for performance.

Point of contact: This forms the concluding section of the RFP, where the organization mentions of a point of contact within the company to not only ensure that one person is assigned to the process but also that the vendors/bidders can connect regarding any queries/clarities on the RFP.

Response to RFP

The response to the RFP should be complete in all respects and assist the evaluators from the organisation to come to a conclusion on technical competencies for executing the services as required. The details provided should lead to a potential awarding of the contract. The stages for responding to an RFP are as follows:

Introduction: In this section the organization introduces itself in brief, the areas of work and specialization to make the client understand the business offerings and areas of specialization that are on offer.

Submission of Technical Bid: The organization has to highlight the detailed response to each requirement of the proposer. The information on the product in the offering, the technical specifications, design specifications and other important details has to be inserted in this section. Here, it can be reflected as to how the product meets the requirements of the proposer.

Price Offering: In this section the price being offered is mentioned. If there exists any discounts, other offers the same has to be mentioned. If there exists, any time frame for the offer the same needs has to be provided.

Commercial Terms: All the commercial terms and conditions of the product, deliveries, warranties, replacements, etc. should be mentioned. If there are any special clauses, these have to be highlighted.

Point of contact: This forms the concluding section of the RFP response, where the organization mentions of a point of contact within the company to connect regarding any queries/clarities on the service offerings.

Request for References: This is an optional content which the organization can insert, if requested by the proposer.

Please refer to section-3 for sample proposal of responding to request for proposal.

2.3 Audit Charter and Terms of Engagement

2.3.1 IS Audit charter

The IS Audit charter is like the constitution for the IS Audit function as it mandates the authority, scope and responsibility of IS Audit in the organisation. The IS Auditor should have a clear mandate to perform the IS audit function as authorized through the audit charter. This mandate is generally documented in an audit charter that should be formally accepted and approved by senior management. Where an audit charter exists for the audit function as a whole, the IS audit mandate should be included in the same.

The IT Auditing Assurance framework has the following standards for audit charter:

1001.1: The IS audit and assurance function shall document the audit function appropriately in an audit charter, indicating purpose, responsibility, authority and accountability.

1001.2: The IS audit and assurance function shall have the audit charter agreed upon and approved at an appropriate level within the enterprise.

Contents of the Audit Charter

The audit charter should clearly address the four aspects of purpose, responsibility, authority and accountability. Aspects to consider are set out in the following sections.

Purpose

- Role
- Aims/goals
- Mission statement
- Scope
- Objectives

Responsibility

- Operating principles
- Independence
- Relationship with external audit
- Auditee requirements
- Critical success factors

Module 2

- Key performance indicators
- Risk assessment
- Other measures of performance

Authority

- Right of access to information, personnel, locations and systems relevant to the performance of audits
- Scope or any limitations of scope
- Functions to be audited
- Auditee expectations
- Organizational structure, including reporting lines to board and senior management
- Grading of IS audit staff

Accountability

- Reporting lines to senior management
- Assignment performance appraisals
- Personnel performance appraisals
- Staffing/career development
- Auditee rights
- Independent quality reviews
- Assessment of compliance with standards
- Benchmarking performance and functions
- Assessment of completion of the audit plan
- Comparison of budget to actual costs
- Agreed actions,
e.g., penalties when either party fails to carry out their responsibilities

2.3.2 Audit Engagement Letter

Purpose

Engagement letters are often used for individual assignments or for setting the scope and objectives of a relationship between external IS audit and an organization.

Content

The engagement letter should clearly address the three aspects of responsibility, authority and accountability. Aspects to consider are set out in the following paragraphs.

Responsibility

- Scope
- Objectives
- Independence
- Risk assessment
- Specific Auditee requirements
- Deliverables

Authority

- Right of access to information, personnel, locations and systems relevant to the performance of the assignment
- Scope or any limitations of scope
- Evidence of agreement to the terms and conditions of the engagement

Accountability

- Intended recipients of reports
- Auditee rights
- Quality reviews
- Agreed completion dates
- Agreed budgets/fees if available

The standards of auditing (SA) 210 Agreeing the terms of Audit Engagements requires the auditor and the client to agree on the terms of engagement and document them in the audit engagement letter. It requires that the engagement letter be renewed if necessary before the commencement of the consecutive audit that follows.

The IS Audit is performed internally as per audit charter or it may be outsourced to an external IS Auditor. In case it is outsourced, an audit engagement letter is issued as per details discussed earlier. It is critical to note that external IS audits would have specific scope, objectives, timelines and deliverables whereas in case of internal IS Audit, these may be flexible and could vary depending on the needs of the enterprise.

The audit assignment requires extensive involvement of the required personnel including management of the auditee environment, before, during and after completion of the assignment. Hence, continuing communication with the auditee is critical. The key principles of such communication is given here.

2.3.3 Communication with Auditee

Effective communication with Auditee involves:

- Describing the service, its scope, its availability and timeliness of delivery
- Providing cost estimates or budgets if they are available
- Describing problems and possible resolutions for them
- Providing adequate and readily accessible facilities for effective communication
- Determining the relationship between the service offered and the needs of the Auditee

The audit charter forms a sound basis for communication with Auditee and should include references to service level agreements for such things as:

- Availability for unplanned work
- Delivery of reports
- Costs
- Response to Auditee complaints
- Quality of service
- Review of performance
- Communication with Auditee
- Needs assessment
- Control risk self-assessment
- Agreement of terms of reference for audits

- Reporting process
- Agreement of findings

2.3.4 Quality Assurance Process

The IS Auditor should consider establishing a quality assurance process (e.g., interviews, customer satisfaction surveys, assignment performance surveys) to understand Auditee' needs and expectations relevant to the IS audit function. These needs should be evaluated against the charter with a view to improving the service or changing the service delivery or audit charter, as necessary. The IS Audit standards require IS Auditor to deploy and monitor completion of the assurance assignments with the staff having required competencies and skill-sets. If required, external experts may be used in the assignment as required. However, the responsibility of the assignment would still remain with the IS Auditor. IS auditor should develop standard approach, documentation and methodology with appropriate templates for various types of assignments. Best practices and frameworks along the required standards, guidelines and procedures should be used in developing quality assurance process and all the staff should be trained in the process to be followed in all stages of planning to execution and reporting of various types of assignments.

2.4 Audit Scope

A determination of the range of the activities and the period (of records that are to be subjected to an audit examination) is the scope of audit. The scope and objectives for every audit are determined through discussion with the auditee management and a specific risk assessment. The scope of audit would be specifically determined by the management in case of internal audit and is set by statute if it is as per regulatory requirement.

While each audit is unique, there are some general or common objectives applied to most audits. Once planning work begins, clearly defining the audit scope is important in determining the budget, human resources, and time required for audit and in determining what will have to be specifically reported and in which format. Scoping the audit involves narrowing the audit to relatively few matters of significance that pertain to the audit objective and that can be audited with resources available to the audit team. In a multi-entity audit, the scope includes identifying the specific departments or applications that will be included in the audit.

To identify matters of significance, the IS auditor has to conduct research on competitive environment, nature of business, technology used and the regulatory requirements to understand the auditee environment so as to plan and execute the assignment as per scope and objectives of the assignment:

- Are there areas that have an important impact on the organisation's results?

- Will the audit of the issue make a difference; that is, will it result in improved performance, accountability, or value for money?
- Are there issues with high visibility or of current concern?
- Are there areas that have undergone a significant degree of change? Examples of changes within an entity are new technology deployed, increased staff turnover, and reorganization; examples of changes to an entity's environment are new regulatory requirements, change in senior management, reporting of fraud amendments to enabling legislation, and budget cuts.
- Is the timing appropriate for auditing the issue?
- Are there any regulatory requirements which are critical? Are there any examples of past of non-compliance?
- What is the management style and the risk appetite and approach to risk management?
- Are there any cases of fraud or material errors of the past or reported which need review?

Carefully scoping the audit early in the process helps increase the efficiency and effectiveness of the audit. The statement of scope should be clear about any related areas that are not included.

2.5 Audit Planning

One of the primary and important phases in an IS Audit is planning which ensures that the audit is performed in an effective way and completed in a timely manner. Planning takes on more significance in case of IS Audit since audit risk in case of IS audits are significantly impacted by inherent risks. Hence, for the audit effort to be successful, a good audit plan is a critical success factor. In case of IS audit done by the internal IS Audit function, annual audit plan is developed based on the audit schedule, materiality, risk rating, business and regulatory requirements and previous audits done. Based on this and resource availability, specific teams and individuals are assigned for specific assurance reviews as per time plan. The audit planning process has to consider budgets of time and costs, and management priorities as per organizational goals and policies. The objective of audit planning is to optimize the use of audit resources. In case of independent assurance assignments, audit planning is done by external firm as per scope of audit engagement letter and considering available resource requirements and auditee availability schedule and schedule for reporting to regulatory authorities, if required.

As per SA 300 on "Planning" issued by ICAI:

- Adequate planning of the audit work helps to ensure that appropriate attention is devoted to important areas of the audit, those potential problems are identified and that the work

is completed expeditiously. Planning also assists in proper assignment of work to assistants and in coordination of work done by other Auditors and experts.

- The extent of planning will vary according to the size of the entity, the complexity of the audit and the IS Auditor's experience with the entity and knowledge of the business.
- Obtaining knowledge of the business is an important part of planning the work. The IS Auditor's knowledge of the business assists in the identification of events, transactions and practices which may have a material effect on the financial statements.
- The IS Auditor may wish to discuss elements of the overall audit plan and certain audit procedures with the entity's audit committee, management and staff to improve the effectiveness and efficiency of the audit and to coordinate audit procedures with work of the entity's personnel. The overall audit plan and the audit program; however, remain the IS Auditor's responsibility.

The IS Auditor should develop and document an overall audit plan describing the expected scope and conduct of the audit. While the record of the overall audit plan will need to be sufficiently detailed to guide the development of the audit program, its precise form and content will vary depending on the size of the entity, the complexity of the audit and the specific methodology and technology used by the IS Auditor.

The audit should be guided by an overall audit plan and underlying audit program and methodology. Audit planning is often mistaken as a one-time activity to be taken and completed in the beginning of the audit. While for all practical purposes, planning is a continuous activity which goes on throughout the entire audit cycle. Many times changes in conditions or circumstances or unexpected findings during the course of audit require changes in the audit procedures and methodology initially planned. Hence IS Auditor is expected to modify the audit plan as warranted by the circumstances. The documentation of the audit plan is also a critical requirement. All changes to the audit plan should follow a change management procedure with every change being recorded with reason for change. Information Technology Assurance Framework (ITAF), 2nd edition issued by ISACA provides the following standards to be followed by IS Auditor: **(ITAF is included as reference material in the DVD)**

1201.1 IS audit and assurance professionals shall plan each IS audit and assurance engagement to address:

- Objective(s), scope, timeline and deliverables
- Compliance with applicable laws and professional auditing standards
- Use of a risk-based approach, where appropriate
- Engagement-specific issues
- Documentation and reporting requirements

1201.2 IS audit and assurance professionals shall develop and document an IS audit or assurance engagement project plan, describing the:

- Engagement nature, objectives, timeline and resource requirements
- Timing and extent of audit procedures to complete the engagement

Risk Assessment in Planning

1202.1 The IS audit and assurance function shall use an appropriate risk assessment approach and supporting methodology to develop the overall IS audit plan and determine priorities for the effective allocation of IS audit resources.

1202.2 IS audit and assurance professionals shall identify and assess risk relevant to the area under review, when planning individual engagements.

1202.3 IS audit and assurance professionals shall consider subject matter risk, audit risk and related exposure to the enterprise.

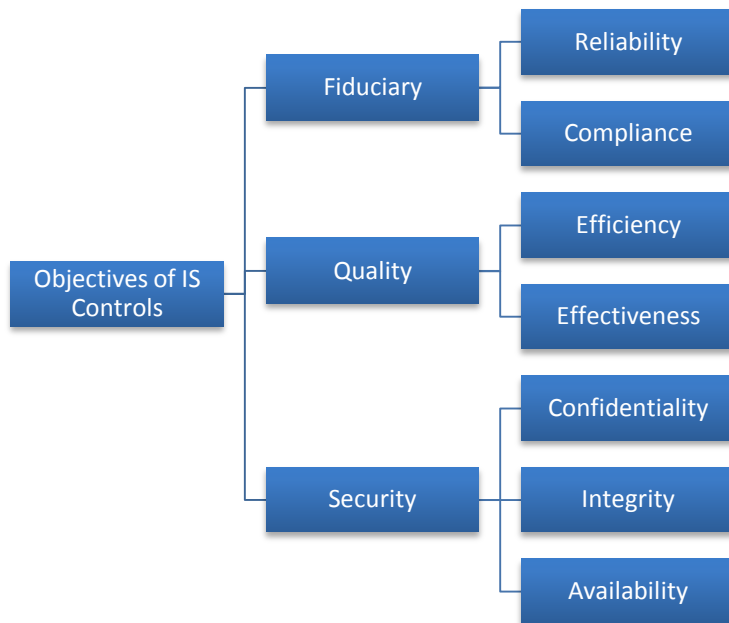
2.6 Objectives of IS Controls

IS audit requires primarily review of Controls in the IS environment and provide recommendations on areas of control weaknesses. The objective of IS controls is to ensure that risk management is implemented as per the risk management strategy which involves risk: avoid, eliminate, reduce or transfer and finally accept. Hence, controls should result in risk remediation as decided. Controls can be classified into 3 broad categories: Fiduciary which focuses on regulatory requirements, quality which focuses on efficiency and effectiveness and security which covers confidentiality, integrity and availability of information. These are the seven information criteria for implementing controls as per COBIT 4.1. It is important for IS Auditors to understand controls and control objectives as these form the most important criteria used for evaluation. Each of the controls are illustrated and explained above. Every IS Audit would have a combination of these controls which are used at time of scoping the assignment.

2.6.1 Principles of Fiduciary

Reliability: It relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities. The objective behind the rationale being that information should be reliable at any given point of time and the same is accessible as and when needed.

Compliance: It deals with complying laws, regulations and contractual regulations to which the business project is subject i.e. externally imposed business criteria as well as internal policies. For any business to succeed there is a need for compliance with regulations, hence one of the principles embedded in the framework deals with compliance parameters for all regulations at any given point of time.



2.6.2 Principles of Quality

Efficiency: A measure of whether the right amount of resources have been used to deliver a Process, Service or Activity. An Efficient Process achieves its Objectives with the minimum amount of time, money, people or other resources. Efficiency is one of the measures needed to determine value for money. It concerns the ratio of inputs (economy) to outputs (effectiveness) and is sometimes referred to as 'bangs per buck'. Typical measures will include money, time, people and quality.

Effectiveness: A measure of whether the Objectives of a Process, Service or Activity have been achieved. An Effective Process or Activity is one that achieves its agreed Objectives. Effectiveness, or Cost Effectiveness, is one of the measures needed to determine value for money. It concerns the cost of the outputs from an activity and the conformance of those outputs to a specification or need. Typical measures will include money, time, people and quality. Any investment that increases the cost of providing IT services should result in an enhancement to service quality or quantity. If this is not so, then the business case must be quite clear about why the Change is necessary.

2.6.3 Principles of Security (CIA)

Confidentiality: It refers to preventing the disclosure of information to unauthorized individuals or systems. Privacy or the ability to control or restrict access so that only authorized individuals can view sensitive information. One of the underlying principles of confidentiality is "need-to-know" or

"least privilege". In effect, access to vital information should be limited only to those individuals who have a specific need to see or use that information. Confidentiality is necessary for maintaining the privacy of the people whose personal information a system holds.

For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Integrity: Information is accurate and reliable and has not been subtly changed or tampered with by an unauthorized party. Integrity includes:

- **Authenticity:** The ability to verify content has not changed in an unauthorized manner.
- **Non-repudiation & Accountability:** The origin of any action on the system can be verified and associated with a user.

The term Integrity is used frequently when considering Information Security as it represents one of the primary indicators of security (or lack of it). The integrity of data is not only whether the data is 'correct', but whether it can be trusted and relied upon. Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people.

Availability: For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks. Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

It is important to note that confidentiality, integrity and availability are not the exclusive concern of information security. Business continuity planning places a significant emphasis on protecting the availability of information as part of the overall objective of business recovery. Common back office procedures, such as maker/checker, quality assurance, change control, etc. along with such regulatory areas as SOX 404 (Clause 49 is Indian version of Sarbanes Oxley Act i.e. SOX 2002) focus on ensuring the integrity of information.

The CIA Triad is entirely concerned with information. While this is the core factor of most IT security, it promotes a limited view of security that tends to ignore some additional, important factors. For instance, while Availability might serve to ensure that one does not lose access to resources, one

need to provide information when it is needed, thinking about information security in and of itself in no way guarantees that someone else isn't making unauthorized use of your hardware resources.

2.7 Understanding the Auditee Environment

IS Auditors will have to understand the business processes of the enterprise and organization structure to be able to perform an effective audit. This understanding of the business process has to be coupled with understanding of the enterprise's policies, procedures and practices as implemented. Any enterprise executes its business operations through its staff. These staff needs to have defined job responsibilities, which are provided in the organization structure. The organization structure needs to have internal control structure. IT implementation in the enterprise makes it imperative that the internal control structure is built into the IT as deployed. Further, IT impacts the way business operations could be performed and internal controls are implemented. Hence, it is critical for auditors to understand the organization structure of the enterprise being audited as relevant to the objectives and scope of the assignment. The four key areas which have to be specifically understood by the IS Auditors are explained here.

2.7.1 Business of the Entity

The IS Auditor should obtain a preliminary knowledge of the entity and of the nature of ownership, management, regulatory environment and operations of the entity. Industry factors and indicators affecting the entity, for e.g. market and competitive forces, technology or service delivery mechanism, key business risk, legislation and regulatory framework should be understood.

Entity specific information of management, ownership, board composition with key personnel, corporate ethics and policies, details on information systems of financial package and Enterprise Resource Planning (ERP) system and IT controls are few areas, not exclusive, which the IS Auditors should acclimatize himself with, which shall enable them to plan and perform the audit.

2.7.2 Organization Structure

Some of the organizational structure activities are task allocation, coordination and supervision, which are directed towards the achievement of organizational aims. It can also be considered as the viewing glass or perspective through which individuals see their organization and its environment. Organizations are a variant of clustered organisations. It can be structured in many different ways, depending on the objectives of the entity. Organizational structure allows the expressed allocation of responsibilities for different functions and processes to different organisations such as the branch, department, workgroup and individual. The IS Auditor has to factor the manner in which the organization is setup to understand definitions of roles and responsibilities, policy framework, etc. to ensure efficiency and effectiveness of audit.

2.7.3 IT Infrastructure

The IS Auditor has to obtain understanding on the present IT infrastructure of the entity. As a part of developing the audit plan the IS Auditor has to keep in mind the present IT infrastructure capacities, the age of hardware and software, licensing agreements, third party vendor agreements etc. which is essential during the development of the IS audit plan. This ensures that the plan is effective and efficient. IS Auditors can accordingly plan their assessment testing on various areas like architecture testing, vulnerability testing, and other control testing.

2.7.4 Regulations, Standards and Frameworks

The IS auditor should ensure that specific regulatory requirements as applicable for the assignment are included as one of the primary criteria for evaluation. The specific steps for understanding this would include:

- Identify various regulations that are applicable to the organisation, depending on the nature of the organisation
- Compliance under all the regulations as identified above for the organisation.
- SA 250 “Considerations of laws and regulations in conducting an Audit” mentions that the auditor has to obtain just a general understanding of the laws and regulations applicable to the organisation and he should alert the management of the material non compliances and the applicable penalties thereof, found during the engagement.

The auditor can exclusively perform engagements under any of the regulatory enactments to ensure its compliance depending on the nature of business organisation.

Information Technology Act 2000 (Amended in 2008)

Section 7A Audit of documents i.e. in Electronic Form: Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form. **(IT Act 2008 and rules are included in DVD)**

Under Section 43A of the (Indian) Information Technology Act, 2000, a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected. It is important to note that there is no upper limit specified for the compensation that can be claimed by the affected party in such circumstances.

The IT Act 2008 recognizes and punishes offences by companies and individual (employee) actions. For example: Section 66 to 66F and 67 deal with the following crimes:

- Sending offensive messages using electronic medium or using body corporate's IT for unacceptable purposes
- Dishonestly stolen computer resource
- Unauthorized Access to computer resources
- Identity theft/Cheating by personating using computer
- Violation of privacy
- Cyber terrorism/Offences using computer
- Publishing or transmitting obscene material

Under Section 72A of the (Indian) Information Technology Act, 2000, disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years and fine extending to INR 5,00,000

Sarbanes Oxley Act, 2002 (SOX)

As per section 404 of Sarbanes Oxley Act, 2002 (SOX), the independent Auditor of the organization is required to opine on the effectiveness of internal control over financial reporting in addition to the Auditor's opinion on the fair presentation of the organization's financial statements.

Section 404 draws attention to the significant processes that feed and comprise the financial reporting process for an organization. In order for management to make its annual assessment on the effectiveness of its internal control, management is required to document and evaluate all controls that are deemed significant to the financial reporting processes.

Public Company Accounting Oversight Board (PCAOB)

PCAOB released Auditing Standard 5 "An audit of Internal Control over Financial Reporting that is integrated with an Audit of Financial Statements". This standard establishes requirements and provides direction that applies when an Auditor is engaged to perform an audit of management's assessment of the effectiveness of internal control over financial reporting ("the audit of internal control over financial reporting") that is integrated with an audit of the financial statements. Effective internal control over financial reporting provides reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes. If one or more material weaknesses exist, the company's internal control over financial reporting cannot be considered effective.

Clause 49 of Listing Agreement on Corporate Governance

Clause 49 stipulates various requirements of corporate Governance and outlines need to implement enterprise risk management, internal control among others. It also outlines the role of the committee mandating specific responsibilities including recommending appointment of Auditors

and monitoring their independence and performance, approval of related party transactions, scrutiny of inter-corporate loans and investments, valuation of undertaking/assets etc. Audit committee is contemplated as a major vehicle for ensuring controls, sound financial reporting and overall good corporate governance.

Some of the critical areas to be reviewed by the Audit committee are:

- Internal audit reports relating to internal control weaknesses; and
- The appointment, removal and terms of remuneration of the Chief internal Auditor.

ISO 27000 Family

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, which form the subject of the ISMS family of standards, and defines related terms and definitions.

ISO/IEC 27001 formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information security risks. The ISMS is an overarching management framework through which the organization identifies, analyzes and addresses its information security risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts - an important aspect in such a dynamic field, and a key advantage of ISO27k's flexible risk-driven approach.

ISO/IEC 27001 is a formalized specification for an Information System Management System (ISMS) with two distinct purposes:

1. It lays out, at a high level, what an organization can do in order to implement an ISMS
2. It can (optionally) be used as the basis for formal compliance assessment by accredited certification IS Auditors in order to certify an organization.

ISO/IEC 27002 is a code of practice - a generic, advisory document, not a formal specification such as ISO/IEC 27001. It recommends information security controls addressing information security control objectives arising from risks to the confidentiality, integrity and availability of information.

The standard is structured logically around groups of related security controls. Many controls could have been put in several sections but, to avoid duplication and conflict, they were arbitrarily assigned to one and, in some cases, cross-referenced from elsewhere. For example, a card-access-control system for, say, a computer room or archive/vault is both an access control and a physical control that involves technology plus the associated management/administration and usage procedures and policies.

2.8 Using Standards, guidelines and best practices for IS Audit

2.8.1 ITAF

ISACA has issued Information Technology Assurance Framework (ITAF) which is a comprehensive and good-practice-setting reference model that:

- Establishes standards that address audit and assurance professional roles and responsibilities; knowledge and skills; and diligence, conduct and reporting requirements
- Defines terms and concepts specific to IS assurance
- Provides guidance and tools and techniques on the planning, design, conduct and reporting of IS audit and assurance assignments

ITAF audit and assurance standards are divided into three categories:

- **General standards (1000 series)**—Are the guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments, and deal with the IS audit and assurance professional's ethics, independence, objectivity and due care as well as knowledge, competency and skill.
- **Performance standards (1200 series)**—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilization, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgment and due care.
- **Reporting standards (1400 series)**—Address the types of reports, means of communication and the information communicated.

ITAF audit and assurance guidelines provide the auditor with information and direction about an IS audit or assurance area. In line with the three categories of standards outlined above, guidelines focus on the various audit approaches, methodologies and related material to assist in planning, executing, assessing, testing and reporting on IS processes, controls and related IS audit or assurance initiatives. Guidelines also help clarify the relationship between organisation activities and initiatives, and those undertaken by IT.

2.8.2 COBIT 5 Framework: Principles, Enablers, Processes, Assurance

As per COBIT 5, Information is the currency for organisations of the 21st century. Information, and the technology that supports it, can drive success, but it also raises challenging governance and management issues. This section explains the need for using the approach and latest thinking provided by globally recognized framework COBIT 5 as a benchmark for reviewing and implementing governance and management of enterprise IT. It explains the principles and enablers of COBIT 5 and how it can be as an effective tool to help organisations to simplify complex issues, deliver trust and value, manage risk, reduce potential public embarrassment, protect intellectual property and maximize opportunities. **You can download COBIT5 from www.isaca.org/cobit.**

COBIT 5 helps organisations to manage IT related risk and ensures compliance, continuity, security and privacy. COBIT 5 enables clear policy development and good practice for IT management including increased business user satisfaction. The key advantage in using a generic framework such as COBIT 5 is that it is useful for organisations of all sizes, whether commercial, not-for-profit or in the public sector.

Five Principles of COBIT 5

COBIT 5 simplifies governance challenges with just 5 principles. The five key principles for governance and management of enterprise IT in COBIT 5 taken together enable the organisation to build an effective governance and management framework that optimizes information and technology investment and use for the benefit of stakeholders.

Principles 1: Meeting stakeholders Needs: enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources. COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT. Because every enterprise has different objectives, and enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high level enterprise goals into manageable specific, IT related goals and mapping these to specific processes and practices.

The COBIT 5 goals cascade is the mechanism to translate stakeholder needs to specific, actionable and customized enterprise goals; IT related goals and enabler goals.

Principle 2: Covering the enterprise End to End: COBIT 5 integrates governance of enterprise IT into enterprise governance. It covers all functions and processes within the enterprise; COBIT 5 does not focus only on the IT function, but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise. It considers all IT related governance and management enablers to be enterprise wide and end to end i.e. inclusive of everything and everyone internal and external that is relevant to governance and management of enterprise information and related IT.

Principle 3: Applying a Single Integrated Framework: there are many IT related standards and best practices, each providing guidance on a subset of IT activities. COBIT 5 is a single and integrated framework as it aligns with other latest relevant standards and frameworks; this allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator. It is complete in enterprise coverage, providing a basis to integrate effectively other frameworks, standards and practices used.

Principle 4: Enabling a Holistic Approach: Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several integrating components. COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as anything that can help to achieve objectives of the enterprise.

Principle 5: Separating Governance from Management: The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities require different organizational structures and serve different purposes.

- **Governance:** It ensures that stakeholders needs, conditions and options are evaluated to determine balanced, agreed on enterprise objectives to be achieved; setting direction through prioritization and decision making, and monitoring performance and compliance against agreed on direction and objectives. In most organizations the governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, especially in larger, complex organizations.
- **Management:** It plans, builds, runs and monitors activities in alignment with the direction set by the governing body to achieve the objectives. In most go the enterprises; management is the responsibility of the executive management under the leadership of the Chief Executive Officer (CEO).

From the definition of governance and management it is clear that they comprise different types of activities, with different responsibilities; however, given the role of governance to evaluate, direct and monitor a set of interactions is required between governance and management to result in an efficient and effective governance system.

Seven enablers of COBIT 5

Enablers are factors that, individually and collectively, influence whether something will work, in this case, governance and management over enterprise IT. Enablers are driven by the goals cascade, i.e. higher level IT related goals defining what the different enablers should achieve.

The seven categories of enablers are:

- Principles, Policies and Frameworks
 - Processes
 - Organizational structures
 - Culture, Ethics and Behavior
 - Information
 - Services, Infrastructure and Applications
 - People, Skills and Competence
- (These are discussed in more detail in module 3)

Using COBIT 5 for IS Assurance

COBIT 5 has been engineered to meet expectation of multiple stakeholders, It is designed to deliver benefits to both an enterprise's internal stakeholders, such as the board, management, employees, etc. as well as external stakeholders – customers, business partners, external IS Auditors, shareholders, consultants, regulators, etc. It is written in a non-technical language and is therefore, usable not only by IT professionals and consultants but also by senior management personnel, assurance providers; regulators for understanding and addressing IT related issues as relevant to them. Globally from the GRC perspective, COBIT has been widely used with COSO by management, IT professionals, and regulators and Auditors (internal/external) for implementing or evaluating governance and management practices from an end to end perspective.

In the rapidly changing digital world, enterprises are inundated with new demands, stringent regulations and risk scenarios emerging daily, making it critical to effectively govern and manage information and related technologies. This has resulted in enterprise leaders being under constant pressure to deliver value to enterprise stakeholders by achieving business objectives. This has made it imperative for management to ensure effective use of information and technology investments and related IT for not only supporting enterprise goals but also to maintain compliance with internally directed and externally imposed regulations. This dynamic changing environment provides a challenge for Chartered Accountants (as assurance providers) to provide assurance with the required level of confidence. However, with the right type of skills and toolsets, this provides an excellent opportunity for Chartered Accountants to act as consultants, who provide relevant IT enabled services. A key component of this knowledge base is usage of globally accepted good practices and frameworks and developing a holistic approach, which meets the needs of stakeholders.

Evaluating system of internal controls

COBIT 5 has specific process: “MEA 02 monitor, Evaluate and Assess the system of Internal Control”, who provides guidance on evaluating and assessing internal controls implemented in an enterprise. Providing such review would provide assurance on the transparency for key stakeholders on the adequacy of the system of internal controls and this provide trust in operations, confidence in the achievement of enterprise objectives and understanding of residual risks. The key management practices for assessing and evaluating the system of internal controls in an enterprise are as follows:

- Monitor internal controls
- Review business process controls effectiveness
- Perform control self-assessment
- Identify and report control deficiencies
- Ensure that assurance providers are independent and qualified
- Plan, Scope and execute the assurance initiatives

2.9 Risk Assessment

As soon as the audit engagement begins, the IS Auditor should identify all the risks that are present in the IT Environment. IS Auditors have to perform a risk assessment to provide reasonable assurance that all material items will be adequately covered during the assignment. Based on this the required audit strategies, materiality levels and resource requirements can then be developed. The IS Auditor should perform this step bearing in mind that the said risks identified in this stage would be evaluated for the controls that have been incorporated to treat the risk. Thus the IS Auditor can focus on the High Risk areas and decide the sampling that would be performed on the identified areas. The risks can be identified by reviewing the factors implemented by the enterprise:

1. Reviewing IT principles, policies and frameworks.
2. Reviewing Processes, including risk-function-specific details and activities.
3. Reviewing organizational structures.
4. Observing culture, ethics and behavior, factors of the employees.
5. Risk-specific information types for enabling risk governance and management within the enterprise.
6. With regard to services, infrastructure and applications, review service capabilities required to provide risk and related functions to an enterprise.
7. For the people, skills and competencies enabler, review the skills and competencies specific for risk.

The key business applications in use at a client are identified and addressed at a high level, in order to incorporate them into the future planning process. The controls within the client business application systems residing on the various platforms are evaluated during the course of the review. The management of the enterprise is expected to “Continually examine and make judgment on the effect of risk on the current and future use of IT in the enterprise. Consider whether the enterprise risk appetite is appropriate and that risk to enterprise value related to the use of IT is identified and managed.

2.9.1 Guidance on risk assessment by ISACA

The guidance provided by ISACA on risk assessment to be performed by IS Auditor is outlined here. When planning ongoing activities, the IS audit and assurance function should:

- Conduct and document, at least annually, a risk assessment to facilitate the development of the IS audit plan.
- Include, as part of the risk assessment, the organisational strategic plans and objectives and the enterprise risk management framework and initiatives.
- For each IS audit and assurance engagement, quantify and justify the amount of IS audit resources needed to meet the engagement requirements.

- Use risk assessments in the selection of areas and items of audit interest and the decisions to design and conduct particular IS audit and assurance engagements.
- Seek approval of the risk assessment from the audit stakeholders and other appropriate parties.
- Prioritise and schedule IS audit and assurance work based on assessments of risk.
- Based on the risk assessment, develop a plan that:
 - Acts as a framework for IS audit and assurance activities
 - Considers non-IS audit and assurance requirements and activities
 - Is updated at least annually and approved by those charged with governance
 - Addresses responsibilities set by the audit charter

When planning an individual engagement, IS audit and assurance professionals should:

- Identify and assess risk relevant to the area under review.
- Conduct a preliminary assessment of the risk relevant to the area under review for each engagement.

Objectives for each specific engagement should reflect the results of the preliminary risk assessment.

- In considering risk areas and planning a specific engagement, consider prior audits, reviews and findings, including any remedial activities. Also consider the board's overarching risk assessment process.
- Attempt to reduce audit risk to an acceptable level, and meet the audit objectives by an appropriate assessment of the IS subject matter and related controls, while planning and performing the IS audit.
- When planning a specific IS audit procedure, recognise that the lower the materiality threshold, the more precise the audit expectations and the greater the audit risk.
- To reduce risk for higher materiality, compensate by either extending the test of controls (reduce control risk) and/or extending the substantive testing procedures (reduce detection risk) to gain additional assurance.

2.9.2 Risk Management steps

Risk management process practices, input/output and activities describe the following steps to be undertaken to assess risk:

Collect Data

1. Identify and collect relevant data to enable effective IT related risk identification, analysis and reporting.

2. Establish and maintain a method for the collection, classification and analysis of IT risk-related data, accommodating multiple types of events, multiple categories of IT risk and multiple risk factors.
3. Record relevant data on the enterprise's internal and external operating environment that could play a significant role in the management of IT risk.
4. Survey and analyses the historical IT risk data and loss experience from externally available data and trends, industry peers through industry-based event logs, databases, and industry agreements for common event disclosure.
5. Record data on risk events that have caused or may cause impacts to IT benefit/value enablement, IT programmer and project delivery, and/or IT operations and service delivery. Capture relevant data from related issues, incidents, problems and investigations.
6. For similar classes of events, organize the collected data and highlight contributing factors. Determine common contributing factors across multiple events.
7. Determine the specific conditions that existed or were absent when risk events occurred and the way the conditions affected event frequency and loss magnitude.
8. Perform periodic event and risk factor analysis to identify new or emerging risk issues and to gain an understanding of the associated internal and external risk factors.

Analyze Risk

1. Develop useful information to support risk decisions that take into account the business relevance of risk factors.
2. Define the appropriate breadth and depth of risk analysis efforts, considering all risk factors and the business criticality of assets. Set the risk analysis scope after performing a cost-benefit analysis.
3. Build and regularly update IT risk scenarios, including compound scenarios of cascading and/or coincidental threat types, and develop expectations for specific control activities, capabilities to detect and other response measures.
4. Estimate the frequency and magnitude of loss or gain associated with IT risk scenarios. Take into account all applicable risk factors, evaluate known operational controls and estimate residual risk levels.
5. Compare residual risk to acceptable risk tolerance and identify exposures that may require a risk response.
6. Analyze cost-benefit of potential risk response options such as avoid, reduce/mitigate, transfer/share, and accept and exploit/seize. Propose the optimal risk response.

7. Specify high-level requirements for projects or programmers that will implement the selected risk responses. Identify requirements and expectations for appropriate key controls for risk mitigation responses.
8. Validate the risk analysis results before using them in decision making, confirming that the analysis aligns with enterprise requirements and verifying that estimations were properly calibrated and scrutinized for bias.

SA 315 – Standard on Risk Assessment procedures issued by ICAI is also applicable for risk assessment pertaining to IS Audit assignment. This requires that the IS Auditor perform Risk Assessment Activities.

2.9.3 Risk Assessment procedures and related activities

The IS Auditor shall perform risk assessment procedures to provide a basis for the identification and assessment of risks and assertion levels. Risk assessment procedures by themselves, however, do not provide sufficient appropriate audit evidence on which to base the audit opinion. The risk assessment procedures shall include:

- (a) Inquiries of management and of others within the entity who in the IS Auditor's judgment may have information that is likely to assist in identifying risks.
- (b) Analytical procedures.
- (c) Observation and inspection.

When the IS Auditor intends to use information obtained from the IS Auditor's previous experience with the entity and from audit procedures performed in previous audits, the IS Auditor shall determine whether changes have occurred since the previous audit that may affect its relevance to the current audit. The IS Auditor shall then assess the risk which is present in the business environment and in the internal control system that have the influence of the information systems and determine the nature and extent of the audit engagements on the relevant subjects.

2.9.4 Use of Risk Assessment in Audit Planning

When determining the functional areas to be audited, the IS Auditor could face a large variety of audit subjects. Each of these subjects may represent different types of risk. The IS Auditor should evaluate these various risk candidates to determine the high-risk areas that should be audited.

There are many risk assessment methodologies, computerized and non-computerized from which the IS Auditor may choose. These range from simple classifications of high, medium and low, based on the IS Auditor's judgment, to complex scientific calculations that provide a numeric risk rating.

One such risk assessment approach is a scoring system that is useful in prioritizing audits based on an evaluation of risk factors. The system considers variables such as technical complexity, level of control procedures in place and level of financial loss. These variables may or may not be

weighted. The risk values are then compared to each other and audits are scheduled accordingly. Another form of risk assessment is judgmental, where an independent decision is made based on business knowledge, executive management directives, historical perspectives, business goals and environmental factors. A combination of techniques may be used as well. Risk assessment methods may change and develop over time to best serve the needs of the organization. The IS Auditor should consider the level of complexity and detail appropriate for the organization being audited.

2.10 Governance and Management Controls

2.10.1 IT General Controls areas

A general controls review attempts to gain an overall impression of the controls that are present in the environment surrounding the information systems. These include the organizational and administrative structure of the IS function, the existence of policies and procedures for the day-to-day operations, availability of staff and their skills and the overall control environment. It is important for the IS auditor to obtain an understanding of these as they are the foundation on which other controls reside.

A general controls review would also include the infrastructure and environmental controls. A review of the data center or information processing facility should cover the adequacy of air conditioning (temperature, humidity), power supply (uninterruptible power supplies, generators) and smoke detectors/fire suppression systems, a conducive clean and dust free environment, protection from floods and water seepage as well as neat and identifiable electrical and network cabling.

Physical access control is another important area for review. Today in a highly networked world, logical access to computer systems is literally universal, yet there is a necessity to control physical access too. There are certain commands and settings that can be executed only from the console of the server and hence it is important to enclose all servers in a secure location protected by suitable mechanisms like locked doors, access swipe cards, biometric access devices or a combination of these. Further the IS auditors also should review the overall access control measures to the entire facility for controls like security guards at the entry gates, displaying of identification badges and logging visitor access.

IT General controls are controls that are not specific to any application, but exist in an IT environment. The general controls are designed for the environment as a whole. Some of the IT General Controls are as follows:

Operating System controls

Operating system is the computer control program. It allows users and their applications to share and access common resources, such as processor, main memory, database and printers. It performs the main tasks of scheduling jobs, managing hardware and software resources, maintaining system security, enabling multi user resource sharing, handling interrupts and maintaining usage records.

Organisational controls

These controls are concerned with the decision-making processes that lead to management authorization of transactions. Companies with large data processing facilities separate data processing from business units to provide control over its costly hardware, software, and human resources. Combining data processing into the business units would be too much responsibility for one manager. Organizational control techniques include documentation of:

- Reporting responsibility and authority of each function,
- Definition of responsibilities and objectives of each function,
- Policies and procedures,
- Job descriptions, and
- Segregation of duties.

These are discussed as follows:

(i) Responsibilities and objectives: Each IS function must be clearly defined and documented, including systems software, application programming and systems development, database administration, and operations. The senior manager, of all these groups, and managers of the individual groups make up the IS management team responsible for the effective and efficient utilization of IS resources. Their responsibilities include:

- Providing information to senior management on the IS resources, to enable senior management to meet strategic objectives;
- Planning for expansion of IS resources;
- Controlling the use of IS resources; and
- Implementing activities and functions that support accomplishment of company's strategic plan.

(ii) Policies, standards, procedures and practices: Policies establish the rules or boundaries of authority delegated to individuals in the enterprise. These are the standards and instructions that all IS personnel must follow when completing their assigned duties. Procedures establish the instructions that individuals must follow to complete their daily assigned tasks. Mandating all requests for changes to existing programs must be approved by user and IS management before programmers and analyst can work on them

is an example of a policy. Documented instructions for filling out a standard change request form, how to justify the costs of the change, how to specify the changes needed, how to obtain approvals, and from whom obtain the approvals are examples of procedures. Documented policies should exist in IS for:

- Use of IS resources,
- Physical security,
- Data security
- On-line security,
- Use of Information systems,
- Reviewing, evaluating, and purchasing hardware and software,
- System development methodology, and
- Application program changes.
- Documented procedures should exist for all data processing activities.

(iii) Job descriptions

These communicate management's specific expectations for job performance. Job procedures establish instructions on how to do the job and policies define the authority of the employee. All jobs must have a current documented job description readily available to the employee. Job descriptions establish responsibility and the accountability of the employee's actions.

(iv) Segregation of duties

Segregation of duties refers to the concept of distribution of work responsibilities such that individual employees are performing only the duties stipulated for their respective jobs and positions. The main purpose is to prevent or detect errors or irregularities by applying suitable controls. It reduces the likelihood of errors and wrongful acts organization structure and allied controls should be structured in a manner that ensures the highest level of separation of duties. The critical factors to be considered in segregation of duties in a computerized information system are:

- Nature of business operations;
- Managerial policy;
- Organization structure with job description; and
- IT resources deployed such as: Operating system, Networking, Database, Application software, technical staff available, IT services provided in-house or outsourced, centralized or decentralized IT operations.

Segregation of duties is the most common control technique aimed at separating conflicting job duties, primarily to discourage fraud, because separating duties makes collusion necessary to commit a fraud.

Such separation can also force an accuracy check of one-person work by another, so that employees to some extent police each other. Examples of segregation of duties are:

- Systems software programming group from the application programming group;
- Database administration group from other data processing activities;
- Computer hardware operations from the other groups;
- Systems analyst functions from the programming function;
- Physical, data, and online security group(s) from the other IS functions; and
- IS Audit from business operations groups.

It is the responsibility of the senior management to implement a division of roles and responsibilities, which should exclude the possibility for a single individual to subvert a critical process. Management should also make sure that personnel are performing only those duties stipulated for their respective jobs and positions. From a functional perspective, segregation of duties should be maintained between the following functions:

- Information systems use,
- Data entry,
- Computer operation,
- Network management,
- System administration,
- Systems development and maintenance,
- Change management,
- Security administration, and
- Security audit.

Guidelines on segregation of duties

There are various general guidelines, with reference to 'Segregation of Duties', which may be followed in addition with concepts like, the maker should not be the checker:

- Separate those, who can run live programs e.g. operations department, from those who can change programs e.g. programmers. This is required in order to ensure that unauthorized programs are prevented from running.
- Separate those, who can access the data e.g. data entry and the DBA, from those who can run programs e.g. computer operators. This is required in order to ensure that unauthorized data entry cannot take place.
- Separate those, who can input data e.g. data entry, from those, who can reconcile or approve data e.g. data authorization persons. This is required in order to ensure that unauthorized data entry cannot take place.
- Separate those, who can test programs e.g. users, quality assurance and security, from those, who can develop programs e.g. application programmers. This is required in order to ensure that unauthorized programs cannot be allowed to run.
- Separate those, who can enter errors in a log e.g. data entry operator, who transfer the data to an error log, from those who can correct the errors like the end user

departments. This is required in order to ensure that unauthorized data entry cannot take place.

- Separate those, who can enter data e.g. data entry personnel, from those who can access the database e.g. the DBA. This is required in order to ensure that unauthorized data entry or data modification cannot take place.

Management Controls

The controls adapted by the management of an enterprise are to ensure that the information systems function correctly and they meet the strategic business objectives. The management has the responsibility to determine whether the controls that the enterprise system has put in place are sufficient to ensure that the IT activities are adequately controlled. The scope of control here includes framing high level IT policies, procedures and standards on a holistic view and in establishing a sound internal controls framework within the organization. The high level policies establish a framework on which the controls for lower hierarchy of the enterprise. The controls flow from the top of an organization to down; the responsibility still lies with the senior management. The controls considerations while reviewing management controls in an IS system shall include:

- **Responsibility:** The strategy to have a senior management personnel responsible for the IS within the overall organizational structure.
- **An IT Organization Structure:** There should be a prescribed IT organizational structure with documented roles and responsibilities and agreed job descriptions.
- **An IT Steering Committee:** The steering committee shall comprise of representatives from all areas of the business, and IT personnel. The committee would be responsible for the overall direction of IT. Here the responsibility lies beyond just the accounting and financial systems; for example, the telecommunications system (phone lines, videoconferencing) office automation, and manufacturing processing systems.

Financial Controls

These controls are generally defined as the procedures exercised by the system user personnel over source, or transactions origination, documents before system input. These areas exercise control over transactions processing using reports generated by the computer applications to reflect un-posted items, non-monetary changes, item counts and amounts of transactions for settlement of transactions processed and reconciliation of the applications (subsystem) to general ledger. The financial control techniques are numerous. A few examples are highlighted here:

- **Authorization:** This entails obtaining the authority to perform some act typically accessing to such assets as accounting or application entries.

- **Budgets:** These estimates of the amount of time or money expected to be spent during a particular period, project, or event. The budget alone is not an effective control. Budgets must be compared with the actual performance, including isolating differences and researching them for a cause and possible resolution.
- **Cancellation of documents:** This marks a document in such a way to prevent its reuse. This is a typical control over invoices marking them with a “paid” or “processed” stamp or punching a hole in the document.
- **Documentation:** This includes written or typed explanations of actions taken on specific transactions; it also refers to written or typed instructions, which explain the performance of tasks.
- **Dual control:** This entails having two people simultaneously access an asset. For example, the depositories of banks’ 24-hour teller machines should be accessed and emptied with two people present, many people confuse dual control with dual access, but these are distinct and different. Dual access divides the access function between two people: once access is achieved, only one person handles the asset. With teller machines, for example, two tellers would open the depository vault door together, but only one would retrieve the deposit envelopes.
- **Input/ output verification:** This entails comparing the information provided by a computer system to the input documents. This is an expensive control that tends to be over-recommended by auditors. It is usually aimed at such non-monetary by dollar totals and item counts.
- **Safekeeping:** This entails physically securing assets, such as computer disks, under lock and key, in a desk drawer, file cabinet storeroom, or vault.
- **Sequentially numbered documents:** These are working documents with preprinted sequential numbers, which enables the detection of missing documents.
- **Supervisory review:** This refers to review of specific work by a supervisor but this control requires a sign-off on the documents by the supervisor, in order to provide evidence that the supervisor at least handled them. This is an extremely difficult control to test after the fact because the auditor cannot judge the quality of the review unless he or she witnesses it, and, even then, the auditor cannot attest to what the supervisor did when the auditor was not watching.

Note: The topics of 2.11 are covered in more detail in module 4: Protection of Information assets.

Data management controls

Data management controls fall in 2 categories being:

- **Access controls:** Access controls are designed to prevent unauthorized individual from viewing, retrieving, computing or destroying the entity’s data.

- **Back up control:** It ensures the availability of system in the event of data loss due to unauthorized access, equipment failure or physical disaster, the organization can restore its files and database.

Organizational structure controls

In a computerized environment, transaction initiation is a critical activity. It requires segregation of duties at authorization, processing and recording all aspects of a transaction. Segregation is done at many levels like segregation of maker and checker, asset record keeper and physical asset keeper, regular checking of effectiveness of internal controls.

Data Processing Controls

These controls are related to hardware and software and include procedures exercised in the IS environment. This includes on-line transaction systems, database administration, media library, application program change control, the data center.

Physical Access Controls

These controls are personnel; hardware and software related and include procedures exercised on access to IT resources by employees/outside. The controls relate to establishing appropriate physical security and access control measures for IT facilities, including off-site use of information devices in conformance with the general security policy. These Physical security and access controls should address supporting services (such as electric power), backup media and any other elements required for the system's operation. Access should be restricted to authorized individuals. Where IT resources are located in public areas; they should be appropriately protected to prevent or deter loss or damage from theft or vandalism. Further, IT management should ensure zero visibility.

Logical Access Controls

Logical access controls are implemented to ensure that access to systems, data and programs is restricted to authorized users so as to safeguard information against unauthorized use, disclosure or modification, damage or loss. The key factors considered in designing logical access controls include confidentiality and privacy requirements, authorization, authentication and incident handling, reporting and follow-up, virus prevention and detection, firewalls, centralized security administration, user training and tools for monitoring compliance, intrusion testing and reporting.

System development controls

Such controls are targeted to ensure that proper documentation and authorizations are available for each phase of the system development process. It includes controls at controlling new system development activities and includes six activities of System authorization activities, user specification activities, technical design activities, internal IS Auditor's participation, program testing and user test and acceptance procedures as a part of the system development controls. **These are covered in detail in module-5.**

Business Continuity Planning Controls

These controls are related to having an operational and tested IT continuity plan, which is in line with the overall business continuity plan, and its related business requirements so as to make sure IT services are available as required and to ensure a minimum impact on business in the event of a major disruption. The controls include criticality classification, alternative procedures, back-up and recovery, systematic and regular testing and training, monitoring and escalation processes, internal and external organizational responsibilities, business continuity activation, fallback and resumption plans, risk management activities, assessment of single points of failure and problem management. **These are covered in detail in module-6.**

System maintenance controls

Management activities do include changes to program logic, additional controls insertion and regular system maintenance activity. It is needed for efficient functioning of present systems.

Computer Centre security controls

Computer security can be of the following types: Physical security, software & data security and data communication security. Physical security attempts to restrict breach of computers and unauthorized access to records. Software and data security ensures that there is use of passwords, authorizations, screening and logs of all activity of the entity. Data communication security is implemented by terminal locks, encryption of data, network administration, sign on user identifiers, etc.

Internet and Intranet controls

There are two major exposures in the communication sub-system of component failure and subversive threats. Component failure can cause failure of transmission between sender and receiver. Subversive threats are invasion attempts to violate the integrity of some components in the system. It can provide intruders with important information about messages being transmitted and the intruder can manipulate these messages.

Personal computers controls

Some of the risks related to personal computer controls are that being small in size and portable the same can be carried within and outside the organization resulting in loss of information, weak access controls and access to pen drives and external drives makes personal computers vulnerable for information loss.

Audit Trails

Audit trails are logs that can be designed to record activity at the system, application, and user level.

2.10.2 Types of IT Application Controls

Application software is the software that processes business transactions. The application software could be a payroll system, a retail banking system, an inventory system, and a billing system or, possibly, an integrated ERP (enterprise resource planning) system. It is the application software that understands data with reference to their business context. The rules pertaining to the business processes are implemented in the application software.

Most users interact with the computer systems only through the application software. The application software enables and also limits the actions that a user can do. It is very important to subject application software to a thorough audit because the business processes and transactions involving money, material and services flow through the application software package.

The first question to ask in an application software review is, "What does the application software do; what business function or activity does it perform?" In this context it is very necessary for the IS auditor to know the business. For application reviews, the IS auditor's knowledge of the intricacies of the business is as important, if not more so, as the technical knowledge. Hence the first step in an application review is to understand the business function/activity that the software serves. This can be done through the study of the operating/work procedures of the organization or other reference material. The other alternative is by interviewing the personnel.

Once this is done, it is necessary to identify the potential risks associated with the business activity/function served by the application (what can go wrong?) and to see how these risks are handled by the software (what controls it?).

Note: Application controls are covered in more detail in module-6: Business application software audit.

IT Applications controls are the controls that are in-built in the application itself. As the controls are built within the applications the same can be monitored, edited, re-structured and configured without the need for making changes to the whole environment. The objectives of application controls are:

- Input data is accurate, complete, authorized and correct.
- Data is processed in an acceptable time period.
- Data stored is accurate and complete
- Output is accurate and complete

A record is maintained to track the data from input to storage and to the eventual output.

Some of the categories of application control are:

1. Boundary Controls

Controls to ensure that access to the application is restricted only to authorized users and that it protects systems from unauthorized access.

The objective of boundary controls is to prevent unauthorized access to applications and their data. Such data may be in any stage, in input, processing, transit or output. The controls restrict user access in accordance with the business policy of an organization and its structure; and protect other associated applications, systems software, database and utilities from unauthorized access.

Access controls may be implemented by using any of the logical security techniques embedded in the application software. Besides access security implemented at the operating system and/or database management systems level, a separate access control mechanism is required for controlling access to application. The application is to have boundary controls to ensure adequate access security to prevent any unauthorized access to:

- Applications themselves
- Application data during communication or transit
- Stored application data
- Resources shared with other processes

2. Input Controls

Controls to ensure that only complete, accurate and valid data and instructions form an input to the application.

Input controls address the following:

- a. Source Document Design
- b. Data entry screen design
- c. Data code controls
- d. Batch Controls

- e. Data Input Validation Controls
- f. Data Input Error Handling and Reporting
- g. Instruction Input Controls

3. Processing Controls

Controls to ensure that there is only authorized processing and integrity of processes and data is ensured. Data processing controls perform validation checks to identify errors during the processing of data. They are required to ensure both the completeness and accuracy of the data being processed. Normally the processing controls are enforced through the database management system. However, adequate controls should be enforced through the front end application system also to ensure consistency in the control. Some of the data processing controls are:

- Run to run totals
- Reasonableness verification
- Edit checks
- Exception reports

4. Data file controls

Controls to ensure that data resident in the files are maintained consistently with the assurance of integrity and confidentiality of the stored data. Some of the data file controls are:

- Version usage
- Internal and external labelling
- Data file security
- Before and after image and logging
- File updating and maintenance authorization
- Parity checking

5. Output Controls

Controls to ensure that outputs delivered to the users in a consistent and timely manner in the format prescribed/required by the user. Output controls ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secured manner. Output can be in any form: either printed data report or a database file in a removable media such as a floppy disk, CDROM or removable hard disk. Whatever the type of output, confidentiality, integrity, and consistency of the output is to be maintained. The following form a part of output controls:

- Storage and logging of sensitive, critical forms
- Logging of output program executions

- Spooling / queuing
- Controls over printing
- Report distribution and collection controls
- Retention controls

Existence controls ensure the continued availability of the application system and data in a consistent manner to the users. These form an integral part of the input, processing and output controls. Recovery of the application system from failures and restoration of both standing data as well as transaction data is very critical. Therefore, existence controls should include backup and recovery procedures of data. This requires secure storage of data files. Existence controls over processing of data should include adequate checkpoint/restart controls that recover the process from a failure without having to repeat the entire process from the beginning. Existence controls should also be exercised over output to prevent loss of output in any form.

Scope of IS Audit of Application software

The information systems audit of application software should mainly cover the following areas:

- Adherence to business rules in the flow and accuracy in processing
- Validations of various data inputs
- Logical access control and authorization
- Exception handling and logging

Steps for IS Audit of Application software

The steps to be performed in carrying out an application software review are as follows:

- Study and review of documentation relating to the application. However, the IS auditor may find situations in real life where documentation is not available or is not updated. In such cases, the auditor should obtain technical information about the design and architecture of the system through interviews.
- Study key functions of the software at work by observing and interacting with operating personnel during work. This gives an opportunity to see how processes actually flow and also observe associated manual activities that could act as complementary controls.
- Run through the various menus, features and options to identify processes and options for conformance to business rules and practices. (Studying the documentation before this can significantly hasten the activity.) To illustrate with an example, it is a well-accepted rule in financial accounting that once an accounting transaction has been keyed in and confirmed on the system to update the ledgers it should not be edited or modified. The

correct method would be to pass a fresh reversal transaction to correct errors, if any. However, if the IS auditor observes that there is an option in the software to "edit/modify transactions," this would be noted as a control deficiency for correction. This kind of run-through can be done more effectively if a development/test system is made available to the IS auditor. In the absence of such a facility, the auditor only can watch the system run by the system administrator and make notes. The auditor is advised not to do any testing on a production system as this could affect adversely a "live" system.

- Validate every input to the system against the applicable criteria. Such validations go a long way in eliminating errors and ensuring data integrity. Apart from simple validations for numeric, character and date fields, all inputs should be validated with range checks, permissible values, etc. Validation checks that are built on application-specific logic can act as powerful controls not only for ensuring data accuracy but also to prevent undesirable data manipulations. The IS auditor can check validations by actually testing them out in the development/test system. Alternatively, looking at the database definitions, the associated triggers and stored procedures would be the way for a technically savvy IS auditor to review the validations.
- Verify access control in application software. This consists of two aspects--the inherent design of the access control module and the nature of access granted to various users and its maintenance. Every application software has a number of modules/options/menus that cater to the different functionality provided by the software. Different users will need access to various features based on their responsibilities and job descriptions. All access should be strictly based on the need to know and do. The design of the access control module may be of varied types. Most software would check a combination of user id and passwords before allowing access. Access may be controlled for each module, menu option, each screen or controlled through objects. Often the matrix of users versus the options/actions becomes too large and complex to maintain hence it is normal to define certain roles for different classes of employees and group them together and assign them similar access. The IS auditor should review the design of the access control module keeping in mind the criticality of the functions/actions possible in the software and evaluate whether the design provides the level of control and granularity to selectively and strictly allows access as per the job requirements of all the users. Having done this, the auditor should proceed to verify whether all existing users have appropriate access as evidenced by their job descriptions and whether access to certain critical activities are allowed only to select personnel duly authorized. It also is necessary to verify who has administrator/SuperUser rights and how such rights are used/controlled. Ideally no one in the IT/development group should have any access to the production data. All actions on the data by the SuperUser should be logged and verified by the data owners regularly.

- Verify how errors and exceptions are handled. In many activities software provides options and ways to reverse transactions, correct errors, allow transactions under special circumstances, etc. Each one of these is special to the business and based on the rules and procedures defined by the organization for these. The IS auditor needs to see how the software handles these. Are these circumstances properly authorized in the software? Does it capture the user id and time stamp for all transactions to provide suitable trails? Are the exceptions and critical activities like updates to global parameters logged for independent review later?
- Correct any weaknesses found at the end of an applications review in the software that could lead to errors or compromises in security. These would need to be corrected by either changes in design and/or some recoding. While this would be addressed by the IT department, the user or owner of the application from the functional area would want to know if any of these weaknesses have been exploited by anyone and whether there have been any losses. To provide an answer to this question the IS auditor should download all the data for the period in question and run a series of comprehensive tests using an audit software and determine if any error or fraud really occurred or not.
- Evaluate the environment under which the application runs. The audit of the application software alone is not enough. Generally, it is prudent to conduct a security review of the operating system and the database in which the application runs while doing an application review.

All critical applications used in an organization need to be subjected to detailed review by an IS auditor. This is one of the most important aspect of IS audit for a business. The job of application review becomes more complex as the application becomes larger and integrated. While auditing complex applications, it is always good to start with a generic industry-based template of an audit work program and slowly customize the work program to the specific situation as the audit progresses.

2.11 Creation of Risk Control Matrix

An IS Audit is performed using the Risk Based approach. An IS Auditor charts a Risk and Control Matrix and uses the same for the audit engagement. The risk and control matrix is a matrix of the risks that have been identified in the Risk assessment phase. A typical RCM would consist the following –

- A series of spreadsheets marking a single process (Purchase Process), application (Custom Business Application), area (Information security, Logical Security, Physical security) etc.
- Each Spread sheet would contain generally the following columns:
 - Risk No., Risk in depth

- Control Objective: This column would contain the control(s) that is ideal to counter the identified risk.
- Control No.
- Controls present: The present control that is implemented by the enterprise to counter the risk.

In addition to the above columns, the RCM may also be used as an Audit Notebook which contains the details of the control owner, process owner, testing plans and results, audit observations, evidences, Risk Ranking, Recommendations etc.

By using the RCM Methodology, an IS Auditor would be able to effectively identify evaluate the controls that are in place. The adequacy of the controls would be evaluated better and thus would be able to provide better assurance with regards to the controls that are in place and is sufficient.

2.12 Audit Sampling, Data Analysis and Business Intelligence

2.12.1 Audit Sampling

Audit sampling is defined as the application of audit procedures to less than 100 percent of the population to enable the IS auditor to evaluate audit evidence about some characteristic of the items selected to form or assist in forming a conclusion concerning the population.

ISACA has issued guideline on audit sampling which may be referred and used for sampling in case of IS Audits. It states that the IS auditor should consider selection techniques that result in a statistically based representative sample for performing compliance or substantive testing. Examples of compliance testing of controls, where sampling could be considered, include user access rights, program change control procedures, procedures documentation, program documentation, follow-up on exceptions, review of logs and software licenses audits. Examples of substantive tests, where sampling could be considered, include re-performance of a complex calculation (e.g., interest) on a sample of accounts, sample of transactions to vouch to supporting documentation, etc.

SA 530 – Audit Sampling: This Standard on Auditing (SA) applies when the auditor has decided to use audit sampling in performing audit procedures. It deals with the auditor's use of statistical and non-statistical sampling when designing and selecting the audit sample, performing tests of controls and tests of details, and evaluating the results from the sample.

The IS auditor can use the following methods for sampling:

1. Statistical Sampling which includes methods of Random sampling & Systematic Sampling
2. Non Statistical Sampling which includes haphazard sampling, judgmental sampling.

While designing the sample the auditor should consider the objectives of the test and attributes of the population from which the sample would be drawn. Also the IS auditor has to keep in mind the conditions that constitute errors in reference to the objectives of the test. When using either statistical or non-statistical sampling methods, the IS auditor should design and select an audit sample, perform audit procedures, and evaluate sample results to obtain sufficient, reliable, relevant and useful audit evidence. The IS auditor can use the sampling technique while assessing the controls designed in the environment. On the basis of the initial assessment the sample size can be increased or decreased to achieve the objective of assessing the tests of existence of control for the IT environment.

2.12.2 Data Analysis

In the digital decade, the need for IT governance and IS assurance services is gaining increasing prominence. Rapid deployment of Information technology is making it imperative that Auditors have practical knowledge of using IT as a tool for drawing inferences and gathering relevant and reliable evidence as per requirements of the assignment. Data analysis through use of Computer Assisted Audit Techniques (CAATs) provide the tools for Auditors to directly access digital information and facilitate in conducting an effective and efficient audit. The need for understanding and auditing IT is not only relevant for specialist IS auditors but is imperative even for any audit. Understanding of data analysis tool and techniques will help auditors not only to perform their existing audits more efficiently and effectively but also facilitate the auditor in knowing how to create and execute new type of IT related audit assignments.

CAATs are a significant tool for auditors to gather information independently. CAATs can be used in various types of Audits including IS Audits. CAATs provide a means to gain access and to analyze data for a predetermined audit objective and to report the audit findings with emphasis on the reliability of the records produced and maintained in the system. The reliability of the source of the information used provides reassurance on findings generated. Auditors and more particularly IS Auditors should have a thorough understanding of CAATs and know where and when to apply them. Auditors to be effective in auditing IT environments need to gain practical experience in using CAATs for various audit and assurance assignments.

The use of Data analytics tools and techniques helps the IS auditor to improve audit approaches, unlike in the traditional approach which is based on a cyclical process involving manually identifying controls, performing tests and sampling a small population to measure the effectiveness. Data analytics also accommodates the growing risk focus on fraud detection.

The IS auditor can use data analytics by which insights are extracted from financial, operational and other forms of electronic data internal or external to the organization. These insights can be historical, real time or predictive and can also be risk focused enabling the IS auditor to cover the audit from all dimensions and ensure effectiveness of audit.

2.12.3 Business Intelligence

Business intelligence (BI) is a set of theories, methodologies, architectures, and technologies that transform raw data into meaningful and useful information for business purposes. BI encompasses the collection and analysis of information to assist decision making and assess organizational performance. BI can handle enormous amount of unstructured data to help identify, develop and otherwise create new opportunities. IS Auditors have to be familiar with the concepts of BI and use them as required for data analysis. **The concepts of BI are covered in Module-1 in detail.**

2.12.4 Analytical Review Procedures: CAAT Tools

Analytical Review Procedures

Analytical review procedures may be defined as substantive tests for a study of comparisons and relationship among data. An accounting system, whether it is manual or computer-based, is subject to mismanagement, error, fraud, and general abuse. The most direct way to combat these potential problems is to implement and maintain a strong system of internal controls for preventing and for detecting errors and irregularities. Analytical review procedures involve comparison of various related information at macro level. This includes comparison of current year with previous year data and also comparison of ratios as required.

CAATs

CAAT refer to the computer-based tools and techniques that give auditors ability to maximize their efficiency and effectiveness in performing audit function. CAATs are considered to be essential part of Toolkit for Auditors. CAATS can greatly enhance effectiveness and efficiency in the audit process during the planning, fieldwork, and reporting phases. IS auditors can use CAATs to perform tests that would normally be impossible or time-consuming to perform manually. For example: sorting, calculations, matching, and extracting of information as required. CAATs can allow an auditor to interrogate and analyze data more interactively, by removing the boundaries that can be imposed by a fixed audit program. For example, an auditor can analyze data and react immediately to the results of the analysis by simply modifying the parameters

The underlying reasons strongly call for controls and auditing in a computerized setup.

- **Absence of input documents:** Data may be entered directly into the computer system without supporting documents. In some on-line transaction systems written evidence of data entry authorization (for example, approval for order entry) may be replaced by other procedures, such as authorization controls contained in computer programs (for example, credit limit approval).
- **Lack of visible transaction trail:** Certain data may be maintained on computer files only. In a manual environment, it is normally possible to follow a transaction through the system by examining source documents, books of account and reports. In a computerized

environment, however, the transaction trail may be partly in machine -readable form, or it may exist only for a limited period of time.

Functional Capabilities of CAATs

1. **File access:** Enables the reading of different record formats and file structures. All common formats of data such as database, text formats, excel files are accessible through the import function.
2. **File reorganization:** Enables the indexing, sorting, merging and linking with another file. These functions facilitate the auditor to get an instant view of the data from different perspectives.
3. **Data selection:** Enables global filtration conditions and selection criteria. These functions enable selection of data based on defined criteria.
4. **Statistical functions:** Enables sampling, stratification and frequency analysis. These functions facilitate analysis of data.
5. **Arithmetical functions:** Enables arithmetic operators and functions. These functions facilitate re-computations and re-performance of results.

How to use CAATs?

IS Auditors need to have adequate computer knowledge, expertise and experience in using CAATs. They need to formulate appropriate methodology for using CAATs. This includes having a walk- through of the system to identify areas of weakness. Based on the results, Auditors will perform compliance tests, evaluate the results and if required, design substantive tests. CAATs can also be used to carry out detailed testing and collect evidences. Based on the results of these tests, Auditors would recommend suitable control measures as relevant. The step-by-step approach for using CAATs is given below:

1. Set the objective of the CAAT application
2. Determine the content and accessibility of the entity's files
3. Define the transaction types to be tested
4. Define the procedures to be performed on the data
5. Define the output requirements
6. Identify audit and IT personnel to be involved in design and use of tests for CAATs.

General Uses and Applications of CAATs:

CAATs can be used for various types of tests. Some examples of tests are given below:

1. Exception identification: Identifying exceptional transactions based on set criteria
2. Control analysis: Identify whether controls as set have been working as prescribed.
3. Error identification: Identify data, which is inconsistent or erroneous.
4. Statistical sampling: Perform various types of statistical analysis.
5. Fraud detection: Identify potential areas of fraud
6. Verification of calculations: Perform various computations to confirm the data stored.
7. Existence of records: Identify fields, which have null values.

8. Completeness of data: Identify whether all fields have valid data.
9. Consistency of data: Identify data, which are inconsistent. For example: identify data, which is not in a particular sequence.
10. Duplicate payments: Establish relationship between two or more tables as required and identify duplicate transactions.
11. Undeserved discounts for rapid payment: Identify this based on analysis of set criteria.
12. Obsolescence of inventory: Identify obsolescence of inventory based on stratification, classification or aging.
13. Accounts exceeding authorized limit: Identify data beyond specified limit.
14. Overdue invoices: Identify data based on aging of invoices.

Strategies for using CAATs

CAATs are important tools for Auditors. They need to work out effective strategies to ensure their effective use. The key strategies for using CAATs are:

1. Identify the goals and objectives of the investigation or audit. This may not always mean that CAATs will be used for a particular audit. The point is to keep in mind all relevant techniques and technologies and to avoid traditional attitudes and thinking
2. Identify what information will be required, to address the goals and objectives of the investigation or audit.
3. Determine what the sources of the information are (Accounts payable system, payroll master file system, contracts system)
4. Identify who is responsible for the information (supervisors, department leaders, IT personnel)
5. Review documentation that describes the type of data in the system
6. Review documentation that describes how the information flows. Take time to understand the data. Know what each field in the data set represents and how it might be relevant to performing the audit. Review the record layout for the file. Verify that the data is complete (Compare it to a hard copy).
7. Understand the system generating the data. The best defense against misunderstanding how the system processes data:
8. Review documentation on the system. For example, user manuals, flowcharts, output reports
9. Develop a plan for analyzing the data (What, When, Where, Why, and How)
 - **What:** Specific objectives that should be addressed by the analysis
 - **When:** Define the period of time that will be audited, and arrange with IT personnel to secure the data for that period
 - **Where:** Define the sources of the data to be analyzed (Accounts payable, payroll)
 - **Why:** Reason for performing the tests and analysis (general review, fraud audit, VFM: Value for Money)
 - **How:** The types of analysis planned to be carried out by the audit (Note- Because of the nature of CAATs, the analysis plan should be viewed as a framework and not set

Module 2

in stone For example, additional ad-hoc test might be performed, based on preliminary findings)

Please refer to Module 6: Business application software audit which detailed coverage of CAATs with some case studies.

A sample listing of tools with brief outline of their category and key functions they are perform are given here. These tools provide specific functionalities and need to be used as per the requirements of audit. Most of these tools are specialized in nature and perform specialized functions.

Tool Category	Example Tools	Tool Function
Data Reverse Engineering - Metadata based and relationships.	Bachman Logic Works ERWIN/ERX Embarcadero ER/1 Kismet	Process metadata to document systems and abstract business rules and relationships (High-end tools also derive some logical and conceptual schema information)
Data reverse Engineering – Data Content Based	Vanity Integrity QDB Analyze Data Star Wiz Rule	Process data content in conjunction with metadata to abstract business rules and relationships, automatically.
Batch Export/Transport – Parameter based extraction code generators	Carleton Passport ETI Extract Prism Warehouse Manager	Extraction is centrally controlled by parameters, code programs are automatically generated. The tool accommodates data conversion and abstraction, as well as transport.
Data Content Quality – Filter based	Apercus Trillium	Positioned between export and import, it supports parameter based data filtering, they are used with

		different keys to keep data in alignment.
Special purpose data quality	Vality DB star IDI WizRule	Data quality is evaluated based on data content. Data patterns, rules and relationships discovered assist analysts determine data quality problem areas.

2.13 Compliance Testing

Compliance testing is evidence gathering for the purpose of testing an organizations' compliance with control procedures. A compliance test determines if controls are being applied in a manner that complies with management policies and procedures. For example, if the IS Auditor is concerned about whether production program library controls are working properly, the IS Auditor might select a sample of programs to determine if the source and object versions are the same. The broad objective of any compliance test is to provide IS Auditors with reasonable assurance that the particular control on which the IS Auditor plans to rely is operating as the IS Auditor perceived in the preliminary evaluation. Compliance Procedures are tests designed to obtain reasonable assurance that those internal controls on which audit reliance is to be placed are in effect.

It is important that the IS Auditor understands the specific objective of a compliance test and of the control being tested. Compliance tests can be used to test the existence and effectiveness of a defined process, which may include a trail of documentary and/or automated evidence for example, to provide assurance that only authorized modifications are made to production programs.

The IS Auditor needs to ensure that internal control exist and that the internal control is operating effectively and being operating continuously throughout the period under audit to ensure that they can be relied upon. By performing Compliance Tests, the IS Auditor is able to ascertain the existence, effectiveness and continuity of the internal control system. Examples of compliance testing of controls where sampling could be considered include user access rights, program change control procedures, documentation procedures, program documentation; follow up of exceptions, review of logs, software license audits, etc.

2.14 Substantive Testing

Substantive testing is testing where evidence is gathered to evaluate the integrity of individual transactions, data or other information. Substantive Procedures are tests designed to obtain evidence to ensure the completeness, accuracy and validity of the data. A substantive test substantiates the integrity of actual processing. It provides evidence of the validity and integrity of financial statements, and the transactions that support these balances. IS Auditors could use substantive tests to test for monetary errors directly affecting financial statement balances, or other relevant data.

Substantive testing is that which validates the details of financial transactions and balances, whereas compliance testing concentrates on validating the internal control procedures exercised over those financial transactions. Substantive testing validates the amounts of the transactions themselves. Substantive Testing are those which are performed in every audit and are sometimes known as default procedures. These procedures relate to the checking the completeness, accuracy and validity of the data produced by the enterprise. Examples of substantive tests where sampling could be considered include performance of a complex calculation on a sample of accounts or a sample of transactions to vouch for supporting documentation, etc.

2.15 Design and Operational effectiveness

2.15.1 Design Effectiveness

Testing of Design Effectiveness and testing of operating effectiveness would be performed by the IS Auditor on every identified control. Testing and operational effectiveness would be performed using CAAT, substantive testing and compliance testing as applicable. Testing of Design Effectiveness refers to the working design of the control as documented. It is a blue print of the control. The IS Auditor evaluates in general that the documented control is effective to remove the risk. It can be evaluated by reviewing the policies, procedure documents, brainstorming sessions etc.

A walkthrough of a business process and the risk controls within it can help evaluate its design effectiveness for compliance. Performing a walkthrough of the relevant functions or transactions and tracing them all the way through the complete process, from instigation, through authorization, recording, processing and reporting will assist with the identification or existence of control activities to establish whether control activities are being performed (i.e. are in place), appraisal of the design of the risk controls, as well as substantiating the accuracy of process documentation.

A walkthrough is an end to end evaluation, step-by-step of a process and its controls to verify and validate understanding on the operation of the process and its associated controls and to evaluate whether the actual controls, if operated as designed can effectively mitigate risk to an acceptable level. In conducting the walkthrough it would be ensured sufficient evidence exists that

reconciliations are being prepared by the nominated personnel (i.e. a reconciliation statement together with documentary evidence of the balance, and documentation intended to explain/justify/evidence clearance of 'reconciling items') and that these are being reviewed (i.e. supervisor's signature). Where there is such evidence it can be concluded that the control has been placed in operation and (assuming that it is properly mitigating the related risk) considered 'design effective'.

Evaluation of design effectiveness is critical because only properly designed controls are capable of operating effectively. A control deficiency exists when the design or operation of a control, or group of controls, does not allow management or employees, in the normal course of performing their assigned roles and responsibilities, to prevent or detect failures on a timely basis.

2.15.2 Operational Effectiveness

Testing of Operating Effectiveness refers to actual performance of the Control in the IT Environment. The IS Auditor should evaluate the controls that have been documented. The purpose of operational self-testing is to gather sufficient documented evidence to enable a conclusion and testimony whether or not the controls as documented are operating in practice.

The IS Auditor will evaluate the effectiveness and efficiency of the control and would gain reasonable assurance whether the said control is sufficient to counter the identified risk. The IS Auditor would primarily check that the control is working to its expectations in accordance with its documented design.

Sample based self-testing. This involves the selection of samples (for each control tested) from the entire population of the particular control being tested, and the performance of specific test procedures on the selected sample. Testing requires accurately documented controls that are tested to ensure conformance to a requirement and, therefore, compliance.

The test will either start from the initiating documents within a process such as purchase order / requisitions, for the purchasing process or the test starts from the end of the process, i.e. the records in the accounting system. This flow of the test is determined by the assertions that need to be addressed. Once the sample has been selected from the complete population, evidence must be obtained that the control has been performed. For example, for a manual authorization control this evidence will be the signature of the person who performs that control.

Documented evidence must be obtained to ascertain that the control has been performed as it has been designed. For manual controls; the evidence that the control has been performed should be available through physical records created when these controls have operated.

For system controls, the evidence of the control will be obtained through obtaining appropriate reports and screen shots to prove that the system configuration, system access, and system reports are as documented within the design. System controls, once established either work, or

they do not. Evidence gathered to prove that a system control operated also proves that the control operated consistently and effectively.

Manual controls however, are subject to human error, and therefore we should test the quality of the control to gain assurance that the control has operated consistently and effectively. For example a signature on a User Access request does not necessarily mean that the person has carefully reviewed it. The signature itself does not provide sufficient evidence that the control has operated as intended; therefore we also need to test that the control has been performed correctly.

This would involve selecting a sample of the user access request process that is being tested (sampling guidance is provided below for 'sample within a sample') and inspecting that the details on user access requests followed the process, so as to provide after the fact evidence that the individual carefully reviewed the user access request before approving it and was authorized to do so.

2.16 Audit Evidence: Methods

Evidence is any information used by the IS Auditor to determine whether the entity or data being audited follows the established criteria or objectives, and supports audit conclusions. It is a requirement that the IS Auditor's conclusions be based on sufficient, relevant, competent and appropriate audit evidence. When planning the IS audit, the IS Auditor should take into account the type of audit evidence to be gathered, its use as audit evidence to meet audit objective and its varying levels of reliability.

Audit evidence may include the IS Auditor's observations, notes taken from interviews, results of independent confirmations obtained by the IS Auditor from different stakeholders, material extracted from correspondence and internal documentation or contracts with external partners, or the results of audit test procedures. While all evidence will assist the IS Auditor in developing audit conclusions, some evidence is more reliable than others. The rules of evidence and sufficiency as well as the competency of evidence must be taken into account as required by audit standards.

2.16.1 Evaluating audit evidence

Determinants for evaluating the reliability of audit evidence include:

- **Independence of the provider of the audit evidence** – Evidence obtained from outside sources is more reliable than from within the organization. This is why confirmation letters are used for verification of accounts receivable balances.
- **Qualifications of the individual providing the information/evidence** – Whether there providers of the information/evidence are inside or outside of the organization, the IS Auditor should always consider the qualifications and functional responsibilities of the persons providing the information. This can also be true of the IS Auditor. If an IS Auditor doesn't have a good understanding of the technical area under review, the information

gathered from testing that area may not be reliable, especially if the IS Auditor doesn't fully understand the test.

- **Objectivity of evidence** – Objectivity evidence is more reliable than evidence that requires considerable judgment or interpretation. An IS Auditor's review of media inventory is direct, objective evidence. An IS Auditor's analysis of the efficiency of an application, based on discussions with certain personnel, may not be objective audit evidence.
- **Timing of the evidence** – The IS Auditor should consider the time during which information exists or is available in determining the nature, timing and extent of compliance testing and, if applicable, substantive testing.

The IS Auditor gathers a variety of evidence during the audit. Some evidence may be relevant to the objectives of the audit, while other evidence may be considered as peripheral. The IS Auditor should focus on the overall objectives of the review and not the nature of the evidence gathered.

The quality and quantity of evidence must be assessed by the IS Auditor. These two characteristics are referred to be competent and sufficient. Evidence is competent when it is both valid and relevant. Audit judgment is used to determine when sufficiency is achieved in the same manner that is used to determine the competency of evidence.

2.16.2 Types of evidence

IS Audit is said to be primarily a process for collecting and evaluating evidence as per the scope and objectives of assignment. Hence, the most critical skill for an IS Audit is in identifying, collecting, analysing and evaluating different types of audit evidence which is mostly available in electronic form. The evaluation of evidence will result in appropriate audit findings which form part of IS Audit report. The various types of evidence are discussed here.

- **Physical examination:** Is the inspection or count by the IS Auditor of a tangible asset. Most often associated with inventory and cash, but it is also applicable to the verification of securities, notes receivable and tangible fixed assets.
- **Confirmation:** Is the receipt of a direct written response from a third party verifying the accuracy of information that was requested by the IS Auditor. The request is made to the client, and the client asks the third party to respond directly to the IS Auditor.
- **Documentation:** Is the IS Auditor's inspection of the client's documents and records to substantiate the information that is, or should be, included in the Financial Statements. Documents can be Internal (has been prepared or used within the client's organization and is retained without going to an outside party) or external (has been handled by someone outside the client's organization who is a party to the transaction being documented, which are either currently held by the client or readily accessible).

- **Analytical procedures:** Uses comparisons and relationships to assess whether account balances or other data appear reasonable compared to the IS Auditor's expectations. An IS Auditor may compare the gross margin in the current year with the preceding years.
- **Inquiries of the Client:** Is the obtaining of written or oral information from the client in response to questions from the IS Auditor. This type of evidence is usually not conclusive because it is not from an independent source. The IS Auditor must obtain additional evidence through other procedures.
- **Recalculation:** Involves rechecking a sample of calculations made by the client. Rechecking client calculations consists of testing the client's arithmetical accuracy and includes such procedures as extending sales invoices and inventory, adding journals and subsidiary records, and checking the calculation of the depreciation expense and prepaid expenses.
- **Performance:** Is the IS Auditor's independent tests of client accounting procedures or controls that were originally done as part of the entity's accounting and internal control system. Recalculation is rechecking a calculation, where performance involves checking other procedures.
- **Observation:** Is the use of the senses to assess client activities. Observation is rarely sufficient by itself because of the risk of an IS Auditor changing their behavior because of the IS Auditor's presence.

2.16.3 Types of Audit Evidences

The following are the different types of audit evidences that is usually generated.

- Documentation: Policy Documents, Procedure Documents
- Screenshots
- Photographs
- Email correspondence with time stamps
- Memory Dump, Log Dump generated from the applications under consideration
- Surveys
- Audit work papers
- External Confirmations
- Written Representations: Refer SA 580

2.16.4 Evidence preservation

The evidence of a computer crime exists in the form of log files, file time stamps, contents of memory, etc. rebooting the system or accessing files could result in such evidence being lost, corrupted or overwritten. Therefore, one of the first steps taken should be copying one or more images of the attacked system. Memory content should also be dumped to a file before rebooting

the system. Any further analysis must be performed on an image of the system and on copies of the memory dumped – not on the original.

In addition to protect the evidence, it is also important to preserve the chain of custody. Chain of custody is a term that refers to documenting, in detail, how evidence is handled and maintained, including its ownership, transfer and modification. This is necessary to satisfy legal requirements that mandate a high level of confidence regarding the integrity of evidence.

2.16.5 Standards on evidence

Standards by ICAI

Standard on Auditing (SA) 230, “Audit documentation” deals with the Auditor’s responsibility to prepare audit documentation for financial statements. As a good practice the Auditor must document work in all stages which helps in maintaining the same not only as a progress report but later it can be used as evidence in courts of law.

Standard on Auditing (SA) 500, “Audit Evidence” explains what constitutes audit evidence in an audit of financial statements, and deals with the Auditor’s responsibility to design and perform audit procedures to obtain sufficient appropriate audit evidence to be able to draw reasonable conclusions on which to base the Auditor’s conclusions. Hence, the Auditor should clearly understand the importance of what constitutes as audit evidence and then the same should be preserved as a part of audit procedure.

Standard on Auditing (SA) 580 “Written Representations” deals with the Auditor’s responsibility to obtain written representations from the management and, where appropriate, those charged with governance. The Auditor should document all the written representations as obtained from the management as a part of working papers and the same can be produced in the court of law, if the need arises.

Standards by ISACA

The standards by ISACA on evidence require the following compliance by IS Auditors>

1205 Evidence

1205.1 IS audit and assurance professionals shall obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the engagement results.

1205.2 IS audit and assurance professionals shall evaluate the sufficiency of evidence obtained to support conclusions and achieve engagement objectives.

Guidance by ISACA on evidence covers following key aspects

In performing an engagement, IS audit and assurance professionals should:

- Obtain sufficient and appropriate evidence, including:
 - The procedures as performed
 - The results of procedures performed
 - Source documents (in either electronic or paper format), records and corroborating information used to support the engagement
 - Findings and results of the engagement
 - Documentation that the work was performed and complies with applicable laws, regulations and policies
- Prepare documentation, which should be:
 - Retained and available for a time period and in a format that complies with the audit or assurance organisation's policies and relevant professional standards, laws and regulations.
 - Protected from unauthorised disclosure or modification throughout its preparation and retention.
 - Properly disposed of at the end of the retention period.
- Consider the sufficiency of the evidence to support the assessed level of control risk when obtaining evidence from a test of controls.
- Appropriately identify, cross-reference and catalogue evidence.
- Consider properties such as the source, nature (e.g., written, oral, visual, electronic) and authenticity (e.g., digital and manual signatures, stamps) of the evidence when evaluating its reliability.
- Consider the most cost-effective and timely means of gathering the necessary evidence to satisfy the objectives and risk of the engagement. However, difficulty or cost is not a valid basis for omitting a necessary procedure.
- Select the most appropriate procedure to gather evidence depending on the subject matter being audited (i.e., its nature, timing of the audit, professional judgement). Procedures used to obtain the evidence include:
 - Inquiry and confirmation
 - Re-performance
 - Recalculation
 - Computation
 - Analytical procedures
 - Inspection
 - Observation
 - Other generally accepted methods
- Consider the source and nature of any information obtained to evaluate its reliability and further verification requirements. In general terms, evidence reliability is greater when it is:
 - In written form, rather than oral expressions
 - Obtained from independent sources
 - Obtained by the professional rather than by the entity being audited
 - Certified by an independent party

- Kept by an independent party
- The result of inspection
- The result of observation
- Obtain objective evidence that is sufficient to enable a qualified independent party to re-perform the tests and obtain the same results and conclusions.
- Obtain evidence commensurate with the materiality of the item and the risk involved.
- Place due emphasis on the accuracy and completeness of the information when information obtained from the enterprise is used by the IS audit or assurance professional to perform audit procedures.
- Disclose any situation where sufficient evidence cannot be obtained in a manner consistent with the communication of the IS audit or assurance engagement results.
- Secure evidence against unauthorised access and modification.
- Retain evidence after completion of the IS audit or assurance work as long as necessary to comply with all applicable laws, regulations and policies.

2.17 Audit Documentation

As in any other audits, documentation of audit work forms a critical task which the IS Auditor should retain in support of his audit work. Significant amount of information may be generated during the course of the IS Auditor's work. The IS Auditor is required to ensure the evidence obtained by him on whom he bases his audit opinion is sufficient, reliable, relevant and useful and enables effective achievement of audit objectives. The audit documentation generally includes:

- Basic documents relating to the business, technology and control environment
- Documents relating to laws, regulations and standards applicable
- Preliminary review and how the audit objectives and scope were evaluated and agreed upon.
- Documents relating to Risk analysis
- Audit plan and progress against plan, Audit programs
- Audit procedures as applied to the audit
- Audit findings, observations, inspection reports, management representations, logs, audit trails and other related evidence
- Interpretation of audit evidence
- Audit Report issued
- Auditor's observations and response to findings and recommendations.
- Reports by third party experts
- Peer Reviews

The audit working papers:

- Aid in the planning and performance of the audit
- Aid in the supervision and review of the audit work

- Provide evidence of the audit work performed to support the IS Auditor's opinion

The IS Auditor's work must be documented and organized in a standardized fashion for easy reference in future audits and reference by other IS Auditors. For purposes of easy reference, the documents may be organized as follows:

- Test work papers
- Permanent work papers
- Pending files
- Report files

Test working papers

The testing work papers, either electronic or otherwise are those prepared or obtained as a result of the compliance and substantive testing procedures performed by the IS Auditor, relevant to the audit engagement. Each working paper should follow a naming convention and numbering convention for naming and numbering of the work papers. The files should also contain a brief description of the content. The compliance test files should contain documentation of:

- Review of the existing internal controls
- A summary of the tests conducted
- Documentation of procedures performed and tools, if any used
- Supporting documentation of detailed tests

Substantive test files require the same elements as compliance test files except for the review of existing internal controls.

Organization of audit working papers:

Each document must describe the following:

- Objective – why the work was done?
- Work done – what was actually done?
- Finding – What issues arose?
- Risk – what are the risks associated with the finding, expressed in terms of impact on business?
- Recommended action – what is being recommended?
- Action – what action was agreed with management?
- Each working paper should be supported by evidence of the weaknesses observed

Documentation Controls

Information systems audit documentation is the record of the audit work performed and the audit evidence supporting the IS Auditor's findings and conclusions.

- Each working paper (or work paper) should be:
- Dated and manually or digitally signed by the person completing the work
- Referenced with a unique number

In case of work papers and evidence in electronic format, special care must be taken to ensure their recoverability at any subsequent date with sufficient controls to prove the date of creation and ensure protection against any modifications to the content or the state of such documents. This would require the IS Auditor to use necessary technology such as use of appropriate media for storage of electronic evidence and their assured recoverability, use of digital signatures for protecting authenticity of documents, use of encryption techniques to safeguard the confidentiality of such documents. The IS Auditor should also take care to ensure retention of such audit documentation to be retained for sufficient length of period such that it complies with legal, regulatory, professional and organizational requirements.

Audit documentation should include, at a minimum a record of the

- Planning and preparation of the audit scope and objectives
- Description and/or walkthroughs on the scoped audit areas
- Audit program
- Audit steps performed and audit evidence gathered
- Use of services of other IS Auditors and experts
- Audit findings, conclusions and recommendations
- Audit documentation relation with document identification and dates
- A copy of the report issued as a result of the audit work.
- Evidence of audit supervisory review

Documents should include audit information that is required by laws and regulations, contractual stipulations and professional standards. Audit documentation is the necessary evidence supporting the conclusions reached, and hence should be clear, complete, easily retrievable and sufficiently comprehensible. Audit documentation is generally the property of the auditing entity and should be accessible only to authorized personnel under specific or general permission. Where access to audit documentation is requested by external parties, the IS Auditor should obtain appropriate prior approval of senior management and legal counsel.

The IS Auditor/IS audit department should also develop policies regarding custody, retention requirements and release of audit documentation. The documentation format and media are optional, but due diligence and best practices require that work papers are dated, initiated, page-numbered, relevant, complete, clear, self-contained and properly labeled, filed and kept in custody. Work papers may be automated. IS Auditors should particularly consider how to maintain integrity and protection of audit test evidence to preserve their proof value in support of audit results.

Audit documentation or work papers can be considered the bridge or interface between the audit objectives and the final report. They should provide a seamless transition with traceability and accountability from objectives to report and from report to objectives. The audit report, in this contact, can be viewed as a sort of particular work papers. Audit documentation should support the finding and conclusions/opinion. Time of evidence sometimes will be crucial to supporting audit findings and conclusions. The IS Auditor should take enough care to ensure that the evidence gathered and documented will be able to support audit findings and conclusions. An IS Auditor should be able to prepare adequate working papers, narratives, questionnaires and understandable system flowcharts.

IS Auditors are a scarce and expensive resource. Any technology capable of increasing the audit productivity is welcome. Automating work papers affects productivity directly and indirectly. The quest for integrating work papers in the IS Auditor's environment has resulted in all major audit and project management packages, CAATs and expert systems offering a complete array of automated documentation and import-export features.

2.18 Using work of another auditor and expert

Due to the scarcity of IS Auditors and the need for IT security specialists and other subject matter experts to conduct audits of highly specialized areas, the audit department or IS Auditors entrusted with providing assurance may require the services of other IS Auditors or experts. Outsourcing of IS assurance and security services is increasingly becoming a common practice. External experts could include experts in specific technologies such as networking, automated teller machine, wireless, systems integration and digital forensics, or subject matter experts such as specialists in a particular industry or area of specialization such as banking, securities trading, insurance, legal experts etc. When a part of IS audit services are proposed to be outsourced to another audit or external service provider, the following should be considered with regard to using the services of other IS Auditors and experts:

- Restrictions on outsourcing of audit/security services provided by laws and regulations
- Audit charter or contractual stipulations
- Impact on overall and specific IS audit objectives
- Impact on IS audit risk and professional liability
- Independence and objectivity of other auditors and experts
- Professional competence, qualifications and experience
- Scope of work proposed to be outsourced and approach
- Supervisory and audit management controls
- Method and modalities of communication of results of audit work
- Compliance with legal and regulatory stipulations
- Compliance with applicable professional standards

Based on the nature of assignment, the following may also require special consideration:

- Testimonials/references and background checks
- Access to systems, premises and records
- Confidentiality restrictions to protect customer related information
- Use of CAATs and other tools to be used by the external audit service provider
- Standards and methodologies for performance of work and documentation
- Non-disclosure agreements

The IS Auditor or entity outsourcing the services should monitor the relationship to ensure the objectivity and independence throughout the duration of the engagement. It is important to understand that often, even though a part of or whole of the audit work may be delegated to an external service provider, the related professional liability is not necessarily delegated. Therefore, it is the responsibility of the IS Auditor or entity employing the services providers to:

- Clearly communicate the audit objectives, scope and methodology through a formal engagement letter.
- Put in place a monitoring process for regular review of the work of the external service provider with regard to planning, supervision, review and documentation.
- Assess the usefulness and appropriateness of reports of such external providers, and assess the impact of significant findings on the overall audit objectives.

ISACA standards require the following to be complied by IS Auditor in using services of external experts.

1206 Using the Work of Other Experts

- 1206.1 IS audit and assurance professionals shall consider using the work of other experts for the engagement, where appropriate.
- 1206.2 IS audit and assurance professionals shall assess and approve the adequacy of the other experts' professional qualifications, competencies, relevant experience, resources, independence and quality-control processes prior to the engagement.
- 1206.3 IS audit and assurance professionals shall assess, review and evaluate the work of other experts as part of the engagement, and document the conclusion on the extent of use and reliance on their work.
- 1206.4 IS audit and assurance professionals shall determine whether the work of other experts, who are not part of the engagement team, is adequate and complete to conclude on the current engagement objectives, and clearly document the conclusion.
- 1206.5 IS audit and assurance professionals shall determine whether the work of other experts will be relied upon and incorporated directly or referred to separately in the report.

- 1206.6 IS audit and assurance professionals shall apply additional test procedures to gain sufficient and appropriate evidence in circumstances where the work of other experts does not provide sufficient and appropriate evidence.
- 1206.7 IS audit and assurance professionals shall provide an appropriate audit opinion or conclusion, and include any scope limitation where required evidence is not obtained through additional test procedures.

2.19 Evaluation of strengths and Weaknesses: Judging by materiality

The IS Auditor will review evidence gathered during the audit to determine if the operations reviewed are all well controlled and effective. This is also an area that requires the IS Auditor's judgment and experience. The IS Auditor should assess the strengths and weaknesses of the controls evaluated and determine if they are effective in meeting the control objectives established as part of the audit planning process.

A control matrix is often utilized in assessing the proper level of controls. Known types of errors that can occur in the area under review are placed on the top axis and known controls to detect or correct errors are placed on the side axis. Then, using a ranking method the matrix is filled with the appropriate measurements. When completed the matrix will substrate areas where controls are weak or lacking.

In some instances, one strong control may compensate for a weak control in another area. For example, if the IS Auditor finds weaknesses in a system's transaction error report, the IS Auditor may find that a detailed manual balancing process over all transactions compensates for the weaknesses in the error report. The IS Auditor should be aware of compensating controls in areas where controls have been identified as weak.

While a compensating control situation occurs when one stronger controls supports a weaker one, overlapping controls are two strong controls. Normally a control objective will not be achieved by considering one control adequate. Rather the IS Auditor will perform a variety of testing procedures and evaluate how these relate to one another. Generally a group of controls when aggregated together may act as compensating control and thereby minimize the risk. An IS Auditor should always review for compensating controls prior to reporting a control weakness. The IS Auditor may not find each control procedure to be in place but should evaluate the comprehensiveness of controls by considering the strengths and weaknesses of control procedures.

Judging the materiality of findings

The concept of materiality is a key issue when deciding which findings to bring forward in an audit report. Key to determining the materiality of audit findings is the assessment of what would be

significant to different levels of management. Assessment requires judging the potential effect of the finding if corrective action is not taken. A weakness in computer security physical access controls at a remote distributed computer site may be significant to management at the site, but will not necessarily material to senior management at headquarters. However, there may be other matter at the remote site that would be material to upper management.

The IS Auditor must use judgment when deciding which findings to present to various levels of management. For example the IS Auditor may find that the transmittal form for delivering tapes to the offsite storage location is not properly initialled or authorization evidenced by management as required by procedures. If the IS Auditor finds that management otherwise pays attention to this process and that there have been no problems in this area, the IS Auditor may decide that the failure to initial transmittal documents is not material enough to bring to the attention of upper management. The IS Auditor might decide to discuss this only with local operations management. However, there may be other control problems that will cause the IS Auditor to conclude that this is a material error because it may lead to a larger control problem in other areas. The IS Auditor should always judge which findings are material to various levels of management and report them accordingly.

2.20 Risk Ranking

Risks are typically measured in terms of impact and likelihood of occurrence. Impact scales of risk should mirror the units of measure used for organizational objectives, which may reflect different types of impact such as financial, people, and/or reputation. Similarly, the time horizon used to assess the likelihood of risks should be consistent with the time horizons related to objectives.

Risk rating scales may be defined in quantitative and/or qualitative terms. Quantitative rating scales bring a greater degree of precision and measurability to the risk assessment process. However, qualitative terms need to be used when risks do not lend themselves to quantification, when credible data is not available, or when obtaining and analyzing data is not cost-effective.

Organizations typically use ordinal, interval, and/or ratio scales. Ordinal scales define a rank order of importance (e.g., low, medium, or high), interval scales have numerically equal distance (e.g., 1 equals lowest and 3 equals highest, but the highest is not 3 times greater than the lowest), and ratio scales have a “true zero” allowing for greater measurability (e.g., a ranking of 10 is 5 times greater than a ranking of 2). Risk rating scales are not one-size-fits-all and should be defined as appropriate to enable a meaningful evaluation and prioritization of the risks identified and facilitate dialog to determine how to allocate resources within the organization.

An example of a Risk Rating Model is given below -

Green Areas: These are areas that have been identified as being low risk, from a business as well as an audit perspective. It is not critical that the controls over these areas are reviewed in detail on an annual or a rotational basis. However, the decision not to rotate is a management decision.

Orange Areas: These are areas that have been identified as medium risk (i.e., an important risk exists, but it is not so material that it is likely to result in significant loss or embarrassment should the required controls not operate effectively). The controls over these areas should be reviewed at least once every two to three years on a rotational basis.

Red Areas: These are areas considered to be inherently high risk from either a business or audit perspective and therefore capable of resulting in significant financial loss or embarrassment. The controls over these systems should be reviewed on an annual basis to confirm that the controls are in place and continue to be adequate to mitigate the inherent risks.

2.21 Audit Report Structure and contents

ISACA standards require IS audit and assurance professionals shall provide a report to communicate the results upon completion of the engagement including:

- Identification of the enterprise, the intended recipients and any restrictions on content and circulation
- The scope, engagement objectives, period of coverage and the nature, timing and extent of the work performed
- The findings, conclusions, and recommendations
- Any qualifications or limitations in scope that the IS audit and assurance professional has with respect to the engagement
- Signature, date and distribution according to the terms of the audit charter or engagement letter

Further, it requires IS audit and assurance professionals shall ensure findings in the audit report are supported by sufficient and appropriate audit evidence.

The exit interview, conducted at the end of the audit, provides that the IS Auditor with the opportunity to discuss findings and recommendations with management. During the exit interview the IS Auditor should:

- Ensure that the facts represented in the report are correct
- Ensure that the recommendations are realistic and cost effective, and if not, seek alternatives through negotiation with Auditee management.
- Recommend implementation dates for agreed on recommendations.

The IS Auditor will frequently be asked to present the results of audit work to various levels of management. The IS Auditor should have a thorough understanding of the presentation techniques necessary to communicate the results. Presentation techniques could include the following:

- **Executive summary:** an easy to read concise report that presents findings to management in an understandable manner. Findings and recommendations should be communicated from a business perspective. Detailed attachments can be more technical

in nature since operations management will require the details to correct the reported situations.

- **Visual presentation:** may include slides or computer graphics

IS Auditors should be aware that ultimately they are responsible to senior management and the audit committee of the board of directors. IS Auditors should feel free to communicate issues or concerns to such management. An attempt to deny access by levels lower than senior management would limit the independence of the audit function.

Before communicating the results of an audit to senior management, the IS Auditor should discuss the findings with the management staff of the audited entity. The goal off such a discussion would be to gain agreement on the findings and develop a course of corrective action. In cases where there is disagreement, the IS Auditor should elaborate on the significance of the findings, risks and effects of not correcting the control weakness. Sometimes the auditor's management may request assistance form the IS Auditor in implementing the recommended control enhancements. The IS auditor's role and that of a consultant, and give careful consideration to how assisting the Auditee may adversely affect the IS Auditor's independence.

Once agreement has be reached with the audited, IS audit management should brief senior management of the audited organization. A summary of audit activities will be presented periodically to the audit committee. Audit committees typically are composed of individuals who do not work directly for the organization and thus provide the IS Auditors with an independent route to report sensitive findings.

Audit report structure and contents

Audit reports are the end product of the IS audit work. They are used by the IS Auditor to report findings and recommendations to management. The exact of tan audit report will vary by organization, however the skilled IS Auditor should understand the basic components of an audit report and how it communicates audit findings to the management.

There is no specific format for an IS audit report; the organization's audit policies and procedures will dictate the general format. Audit reports will usually have the following structure and content:

- An introduction to the report, including a statement of audit objectives, limitations to the audit and scope, the period of audit coverage, and a general statement on the nature and extent of audit procedures conduct and processes examined during the audit, followed by a statement on the IS audit methodology and guidelines.
- A good practice is to include audit findings in separate sections. These findings can be grouped in sections by materiality and/or intended recipient.
- The IS Auditor's overall conclusion and opinion on the adequacy of controls and procedures examined during the audit, and the actual potential risks identified as a consequence of detected deficiencies.

- The IS Auditor's reservations or qualifications with respect to the audit. This may state that the controls or procedures examined were found to be adequate or inadequate. The balance of the audit report should support that conclusion and the overall evidence gathered during the audit should provide an even greater level of support for the audit conclusions.
- Detailed audit findings and recommendations – the IS Auditor would decide whether to include specific findings in an audit report. This should be based on the materiality of the findings and the intended recipient of the audit report
- A variety of findings some of which may be quite material while others are minor in nature. The IS Auditor may choose to present minor findings to management in an alternative format such as by memorandum.

The IS Auditor however should make the final decision about what to include or exclude from the audit report. Generally, the IS Auditor should be concerned with providing a balanced report, describing not only negative issues in terms of findings but positive constructive comments regarding improving process and controls or effective controls already in place. Overall, the IS Auditor should exercise independence in the reporting process.

Auditee management evaluates the findings, stating corrective actions to be taken and timing for implementing these anticipated corrective actions. Management may not be able to implement all audit recommendations immediately. For example, the IS Auditor may recommend changes to an information system that is also undergoing other changes or enhancements. Rather, all may be implemented at once.

The IS Auditor should discuss the recommendations and any planned implementation dates while in the process of releasing the audit report. The IS Auditor must realize that various constraints, such as staff limitations, budgets or other projects may limit immediate implementation. Management should develop a firm program for corrective actions. It is important to obtain a commitment from the Auditee/management on the date by which the action plan will be implemented and the manner in which it will be performed since the corrective action may bring certain risks that may be avoided if identified while discussing and finalizing the audit report. If appropriate, the IS Auditor may want to report to upper management on the progress of implementing recommendations. **Sample format of IS Audit finding, audit report and executive summary of audit report are given in Section-3.**

2.22 Management Implementation of recommendations

IS Auditors should realize that auditing is an ongoing process. The IS Auditor is not effective if audits are performed and reports issued. But no follow up is conducted to determine whether management has taken appropriate corrective actions. IS Auditors should have a follow up program to determine if agreed on corrective actions have been implemented. Although IS Auditors

who work for external audit firms may not necessarily follow this process, they may achieve these tasks if agreed to by the audited entity.

The timing of the follow-up will depend on the criticality of the findings and would be subject to the IS Auditor's judgment. The results of the follow up should be communicated to appropriate levels of management. The level of the IS Auditor's follow up review will depend on several factors. In some instances, the IS Auditor may merely need to inquiries to the current status. In other instances, the IS Auditor who works in an internal audit function may have to perform certain audit steps to determine whether the corrective actions agreed on by management have been implemented.

2.23 Follow up review

ISACA standards require IS audit and assurance professionals shall monitor relevant information to conclude whether management has planned/taken appropriate, timely action to address reported audit findings and recommendations. The effectiveness of an IS Audit is realized only if the action points and recommendations committed and agreed to by the Auditee management are implemented. Hence an important task of the IS Auditor is to review the previous audit reports and follow up on the corrective actions and recommendations implemented within the time schedules committed by the Auditee management. It is a limited scope review and do not entail going beyond the examination of actions agreed upon by the client to correct deficiencies. Normally, the status of follow up activities is included in a separate Compliance Audit Report which is issued after the completion of follow-up review. IT audit is not effective if audits are performed and reports issued, but no follow-up is conducted to determine if Auditee organization has taken appropriate corrective action. The IS Auditor should have a follow-up program to determine if agreed corrective actions have been implemented. The level of the IS Auditor's follow-up review will depend upon several factors. In some instances, the IS Auditor may merely need to inquire as to the current status. In other instances, the IS Auditor may have to perform certain audit steps to determine if the corrective action agreed to by the Auditee organization have been implemented.

The Institute of Internal IS Auditors definition of a follow-up: "A follow-up is defined as a process by which the internal IS Auditors determine the adequacy, effectiveness and timeliness of actions taken by management on reported audit findings." Where agreed action plans are not completely implemented the IS Auditor asks the following questions:

- What remains to be done?
- By whom and when?
- Have alternatives been implemented that may be more appropriate?
- Has the agreed action plan ceased to be of value?
- If no action was taken, why not?
- What is the issue or concern causing inaction?

The end result should be a brief summary of the status of every action plan agreed upon. The final summary is reviewed with the person responsible for clearing the audit report before the follow-up report is issued.

2.24 Summary

This chapter has provided detailed explanation of how an IS Audit is executed in all its phases from planning to execution to reports. IS auditors to be able to perform IS Audit assignments need to have good understanding of concepts of auditing, IT and management. This chapter has covered in the following concepts along with extracts from relevant standards and guidelines as applicable.

- How to conduct various types of IS audit as per scope and objective of assignment after understanding the auditee environment including the nature of business, organisation structure, technology environment, applicable regulations using relevant standards and best practices framework?
- How to review and evaluate various types of risk and its assessment which form the basis on which the audit conclusions can be made?
- How to use analytical procedures, compliance and substantive testing method for performing the audit.
- How to review the design effectiveness and control effectiveness?
- How to collect and evaluate evidence and maintain relevant documentation during the course of IS audit?
- How to perform risk ranking and prepare the final audit report with recommendations and follow up procedures?

The primary objective of this chapter was to provide understanding of both the concepts and practice of IS audit and the various phases involved covering the planning of audit process, understanding of the risks involved, conducting the audit by obtaining and evaluating evidence using CAATs and issuing the final audit report containing recommendations. This chapter has highlighted the difference in approach between auditing in a computerised environment and IS Audit and the specific process of IS Audit right from scoping to reporting.

2.25 Questions

1. The IS Auditor should use which of the following when developing the overall IS Audit Plan and determining priorities for the effective allocation of IS Audit Resources?
 - A. Audit Materiality
 - B. The work of outside experts
 - C. Risk Assessment
 - D. IT Governance
2. Which of the following sampling types is used to estimate the rate of occurrence of a specific quality in population?

- A. Discovery Sampling
 - B. Statistical Sampling
 - C. Attribute Sampling
 - D. Stop-or-go Sampling
3. Which of the following criteria for selecting the applications to be audited is LEAST likely to be used?
- A. Materiality of audit risk
 - B. Sensitivity of transactions
 - C. Technological complexity
 - D. Regulatory agency involvement
4. The first step the IS Audit Manager should take when preparing the annual IS audit plan is to:
- A. Meet with the audit committee members to discuss the IS audit plan for the upcoming year.
 - B. Ensure that the IS audit staff is competent in areas that are likely to appear on the plan and provide training as necessary.
 - C. Perform a risk ranking of the current and proposed application systems to prioritize the IS audits to be conducted.
 - D. Begin with the prior year's IS audit plan and carry over any IS audits that had not been accomplished.
5. The purpose of compliance tests is to provide reasonable assurance that:
- A. Controls are working as prescribed.
 - B. Documentation is accurate and current.
 - C. The duties of users and data processing personnel are segregated.
 - D. Exposures are defined and quantified.
6. While reviewing internal controls in a microcomputer environment, an IS auditor recommends that duties should be regularly rotated. The effect of implementing this recommendation would ensure which of the following controls?
- A. Detective
 - B. Compensating
 - C. Corrective
 - D. Preventive

7. Which of the following is the least important factor in determining the need for an IS Auditor to be involved in a new system development project?
- A. The cost of the system
 - B. The value of the system to the organization.
 - C. The potential benefits of the system.
 - D. The number of lines of code to be written.
8. Each of the following is a general control concern EXCEPT:
- A. Organization of the IS Department.
 - B. Documentation procedures within the IS Department.
 - C. Balancing of daily control totals.
 - D. Physical access controls and security measures.
9. Which of the following types of audits requires the highest degree of data processing expertise?
- A. Systems software audits
 - B. General controls reviews
 - C. Microcomputer application audits
 - D. Mainframe application audits

2.26 Answers and Explanations

1. C. The IS Auditor should use Risk Assessment while developing an overall IS Audit Plan. The other examples are examples of audit standards.
2. C. Attribute sampling is used to estimate the rate of occurrence of a specific quality in population. The other sampling methods described are legitimate sampling methods often employed by auditors during audit.
3. C. Because technical complexity of an application is not as important as the materiality of the audit risk associated with an application or sensitivity of the transactions. Regulatory agency requirements also play an important role in determining what to audit. Answer "b" is NOT the best choice because sensitivity of transactions would be an exposure to a company and should be considered in determining which applications should be audited. Answer "a" is NOT the best choice because the measurement of audit risk is an important component when determining the scope of an audit plan. The materiality of the audit risk associated with specific application would have an impact on whether the application is included in the audit scope. Answer "d" is NOT the best choice because applications may relate to operational areas of the Company where regulatory agencies have required audits.

4. C. Because IS audit services should be expended only if the risk warrants it. Answers a, b, and d occur after c has been completed. Answer "b" is NOT correct because the IS Audit Manager does not know what areas are to appear on the IS audit plan until a risk analysis is completed and discussions are held with the audit committee members. Answer "a" is NOT correct because the IS Audit Manager would not meet with the audit committee until a risk analysis of areas of exposure has been completed. Answer "d" is NOT correct because a risk analysis would be the first step before any IS audit services are expended.
5. A. The compliance tests determine whether prescribed controls are working. Answer "b" is NOT the best choice. Current and accurate documentation may be a good procedure but it is only one type of control procedure, therefore, answer 'A' is a better choice as more control procedures are evaluated. Answer "c" is NOT the best choice because segregation of duties is only one type of control procedure; therefore, answer 'A' is a better choice as more control procedures are evaluated. Answer "d" is NOT the correct choice. Exposures are defined and quantified to determine audit scope. Compliance tests provide reasonable assurance that controls are working as prescribed.
6. B. A small institution may find that separation of duties (which is a preventative control) may not be practical since there are too few employees. In such a circumstance, it may be possible to establish an acceptable control environment by instituting compensating measures such as rotation of job duties.
7. D. The size of the system is the least important of the factors listed. All other factors have specific financial implications and an IS Auditor can be used to help mitigate the risk to the corporation with the development of a new system.
8. C. Balancing of daily control totals relates to specific applications and is not considered an overall general control concern. Answer "b" is NOT the best answer since documentation procedures within the IS Department is an important general control concern. Answer "a" is NOT the best answer since organization of the IS Department is an important general control concern. Answer "d" is NOT the best answer since physical access controls and security measures are important general control concerns.
9. A. The IS Auditor needs specialized education in hardware and operating systems software. Answers b, c, and d can be performed when an IS Auditor has a basic level of data processing technical knowledge and usually requires no special training. Answer "b" is NOT correct because general controls reviews typically do not require as technical a level of knowledge. Answer "c" is NOT correct because microcomputer application reviews generally do not require as technical a background as an audit of systems software. Answer "d" is NOT correct because mainframe application audits typically do not require special training or as technical level of knowledge as system software reviews.

CHAPTER 3: IT ENABLED SERVICES

Learning Objectives

This chapter provides an overview of different types of audit engagements that can be undertaken by the IS auditor. Further, there is an insight into the world of frauds and cyber-crimes which have grown as a part of the technological advances. The IS auditor may also undertake role of an investigator on behalf of the enterprise to investigate various modes of data leakage and theft and use digital forensics to retrieve data from damaged hard disks, and other mediums of data storage. This requires advance technical skills but a brief overview is provided so that DISAs who are interested can venture into new area.

3.1 Introduction

As information systems' presence has become an indispensable part of our day to day living and as enterprise processes have become inseparable from IT, it has becoming increasingly critical to ensure safe and secure access to information from a computing environment and make it available to anyone at any point of time. This heavy reliance on information from information systems maintained on computers has become the very edifice of enterprises today. Information has to be available but with security as the information when accessed and mis-used by unauthorized people can lead to loss of revenue, reputation and non-compliance with regulations thereby impacting the very survival of enterprises. There are new types of computer fraudster who are tech-savvy who using their technical expertise can exploit information for wrong purposes. Hence, ensuring security of any IS environment is of utmost importance within the organization as the loss of which can not only lead to huge financial losses but the enterprise can incur damages for loss of private data of customers, loss of goodwill and market share. Due to the increase in sophistication of technology there has been an unprecedented growth in frauds and cyber-crimes. On the positive side, using technology effectively can help enterprises to reach out to customers anytime, anywhere leading to growth in geometric progression. Enterprise management look for assurance on security and consulting on value addition using IT. This provides a great opportunity for IS auditors who are equipped with the right competencies and skill-sets to provide assurance and value added services.

3.2 Classification of Audits

An information technology audit, or information systems audit, is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other

form of attestation engagement. IT audits are also called IS Audits and computer audits or IT or IS assurance services.

The wide range or spectrum of IT audits cover the whole gamut of IT right from conception to post-implementation review as also consulting on effective deployment. Some examples of these services areas:

- **Systems and Applications:** An audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.
- **Information Processing Facilities:** An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.
- **Systems Development:** An audit to verify that the systems under development meet the objectives of the organization and to ensure that the systems are developed in accordance with generally accepted standards for systems development.
- **Management of IT and Enterprise Architecture:** An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.
- **Client/Server, Telecommunications, Intranets, and Extranets:** An audit to verify that telecommunications controls are in place on the client (computer receiving services), server, and on the network connecting the clients and servers.
- **Compliance Audits:** Compliance audits include specific tests of controls to demonstrate adherence to specific regulatory or industry standards. These audits focus on particular systems or data. Examples include Payment card industry Data security standard audits, Health insurance portability and accountability act audit (HIPAA) etc.
- **Operational Audit:** An operational audit is designed to evaluate the internal control structure in a given process or area. Audits of application controls or logical security systems are some examples of operational audits.
- **Financial Audit:** The purpose of a financial audit is to assess the accuracy of financial reporting. A financial audit will often involve detailed, substantive testing, although increasingly, IS Auditors are placing more emphasis on a risk and control based audit approach. This kind of audit relates to financial information integrity and reliability.
- **Integrated audits:** An integrated audit combines financial and operational audit steps. An integrated audit is also performed to assess the overall objectives within an organization, related to financial information and assets' safeguarding, efficiency and compliance.
- **Administrative Audits:** These are oriented to assess issues related to the efficiency of operational productivity within an organization.
- **IS audits:** This process collects and evaluates evidence to determine whether the information systems and related resources adequately safeguard assets, maintain data

and system integrity and availability, provide relevant and reliable information, achieve organizational goals effectively, consume resources efficiently, and have, in effect, internal controls that provide reasonable assurance that business, operational and control objectives will be met and that undesired events will be prevented or detected or corrected, in a timely manner.

- **Specialized Audit:** Within the category of IS audits, there are a number of specialized reviews that examine areas such as serviced performed by third parties. Because businesses are becoming increasingly reliant on third party service providers, it is important that internal controls be evaluated in these environments.
- **Forensic Audit:** Forensic Auditing has been defined as the auditing specialized in discovering, disclosing and following up on frauds and crimes. The primary purpose of such a review is the development of evidence for review by law enforcement and judicial authorities.
- **Control Self-assessments:** This is conducted by the business process owners but facilitated by the auditors. The main difference between this and the other engagement types is that the auditors as control experts identify with those responsible for implementing controls the required controls and assist them in self-assessment. Therefore, setting the evaluation criteria and executing the evaluation are carried out by the business owners themselves. It is clear that proper guidance and follow-up are required to optimize the added value of this type of engagement within the enterprise. Especially with regard to approach, tools and reporting, the auditors should clearly lead the way and verify whether assessors are using the existing guidelines.
- **Internal audit/compliance review:** Performed by a third party who is not involved in the functioning of the enabler, but who is employed by the same enterprise as the business owners of the enablers. Commonly, in a (medium- to large-sized) enterprise, the evaluation criteria are set and the review is performed by the internal audit or compliance department. This type of review is more independent than a self-assessment because the auditor is not involved in the functioning of the enabler and therefore contributes to the reliability/credibility of the evaluation outcome. Good practices and consistent guidance are required to optimize the added value of this type of engagement.

A number of IT Audit professionals from the Information Assurance realm consider there to be three fundamental types of controls regardless of the type of audit to be performed, especially in the IT realm. Many frameworks and standards try to break controls into different disciplines or arenas, terming them “Security Controls”, “Access Controls”, “IA Controls” in an effort to define the types of controls involved. At a more fundamental level, these controls can be shown to consist of three types of fundamental controls: Protective/Preventative Controls, Detective Controls and Reactive/Corrective Controls. IS auditing considers all the potential risks and controls in information systems. It focuses on issues such as: operations, data, integrity,

software applications, security, privacy, budgets and expenditures, cost control, and productivity.

In an IS system, there are two types of IS Auditors and audits: internal and external. IS auditing is usually a part of internal auditing, and is frequently performed by corporate internal IS Auditors. An external IS Auditor reviews the findings of the internal audit as well as the inputs, processing and outputs of information systems. The external audit of information systems is frequently a part of the overall external auditing performed by an assurance professional.

3.3 IT Enabled Services

There is a wide variety of services that can be offered by the IS Auditor. There are innumerable opportunities in every area of IT implementation depending on area of technical expertise. Hence, IS Auditors can provide assurance or consulting services at various stages of technology deployment right from conception to post-implementation. Given below is a sample problem statement with proposed solution and listing of service opportunities for the IS Auditor. This is only an illustrative list for one problem statement. **Please refer to Module 1: Facilitated eLearning for more details and examples of IT Enabled services.**

Problem: There are no proper IT management practices in the enterprise.

Solution	Opportunity for an IS Auditor
Policies should be drafted and enforced around the environment	- Create the appropriate policies that the enterprise needs in terms of scope and enforcement of the policy. - Provide services of performing the review of the policies.
Procedures should arise from the policies	Assist in development of the procedures that the employees of the enterprise should follow. Review designed procedures and provide recommendations for a better solution in order to reduce costs.
Correct software should be installed and enforced	- Assist in application implementation. - Participate as an PMO in terms of development and procurement of the applications - Assist as scope Manager in the SDLC process in terms of requirement gathering

Business workflows should be designed and enforced in the applications	• Apart from procedures design, develop necessary workflows that are to be enforced through the information system. • Perform a BPR on information system requirements of the enterprise and provide recommendations or assist in implementation.
Perform risk assessment and rank the risk	• Perform the risk assessment exercise on the existing workflows and processes and identify those areas of high risk that need a higher level of attention.
Ensure appropriate segregation of duties by ensuring right Access is given to the right employees	• Provide in designing the roles and responsibilities of the employees. • Review the existing roles and responsibilities of the employees and can identify conflicts in segregation of duties.
Training is to be provided	• Provide necessary training to the employees regarding the new workflows, procedures, applications etc.

3.4 Fraud

“Fraud is the wrongful or criminal description intended to result in financial or personal gain”

Fraud is a deception deliberately practiced in order to secure unfair or unlawful gain. Defrauding people or organizations of money or valuables is the usual purpose of fraud, but it sometimes instead involves obtaining benefits without actually depriving anyone of money or valuables, such as obtaining a driver's license by way of false statements made in an application for the same. The establishment of a strong internal control environment where written policies and procedures are enforced, internal controls are appropriately implemented and employees are educated about fraud and its consequences is one of the best deterrents and methods of curtailing fraud. For internal controls to be effective, they must be constantly evaluated for effectiveness and changed as business processes are changed or altered.

3.4.1 Fraud Detection

The use of information technology for business has immensely benefited enterprises in terms of significantly increased quality of delivery of information. However, the widespread use of information technology and the Internet leads to risks that enable the perpetration of errors and

frauds. Fraud is any act involving the use of deception to obtain illegal advantage. Detecting fraud in IT environment poses its own challenges as the data is in digital format and can be easily erased by the fraudster.

Management is primarily responsible for establishing, implementing and maintaining a framework and design of IT controls to meet the internal control objectives. A well-designed internal control system provides good opportunities for deterrence and/or timely detection of fraud, internal controls may fail where such controls are circumvented by exploring vulnerabilities or through management perpetrated weakness in controls or collusion among people. Legislation and regulations relating to corporate governance cast significant responsibilities on management, IS Auditors and the audit committee regarding detection and disclosure of any frauds, whether material or not. Understanding the auditee's business and the risks it faces is a critical step to developing an effective audit plan focused on the areas most sensitive to fraudulent or inaccurate practices. IS Auditors should observe and exercise due professional care in all aspects of their work. IS Auditors entrusted with assurance functions should ensure reasonable care while performing their work and be alert to the possible opportunities that allow fraud to materialize.

The presence of internal controls does not altogether eliminate fraud. IS Auditors should be aware of the possibility and means of perpetrating fraud, especially by exploiting the vulnerabilities and overriding controls in the IT enabled environment. IS Auditors should have knowledge of fraud and fraud indicators, and be alert to the possibility of fraud and errors while performing an audit. During the course of regular assurance work, the IS Auditor may come across instances or indicators of fraud. The IS Auditor may, after careful evaluations, communicate the need for a detailed investigation to appropriate authorities. In the case of the IS Auditor identifying major fraud, or if the risk associated with the detection is high, audit management should also consider communicating in a timely manner to the audit committee.

Regarding fraud prevention, the IS Auditor should be aware of potential legal requirements concerning the implementation of specific fraud detection procedure and reporting fraud to appropriate authorities. Where the IS auditor is aware that management is required to report fraudulent activities to an outside organisation, the IS auditor should formally advise management of this responsibility.

Let us look at the regulatory requirements of fraud as per Indian legislations.

1. **Information Technology (Amendment) Act 2008:** Casts responsibility on body corporates to protect sensitive personal information by implementing reasonable security practices and procedures. It also recognises and punishes offences committed by companies and individuals through the misuse of IT.
2. **Clause 49 of the Listing Agreement:** Makes the top management accountable for weaknesses in the internal control systems. It requires CEOs and CFOs to certify on the effectiveness of the Internal Controls.

3. **CARO 2003:** Requires verifying the adequacy of internal control procedures and determining whether there were any continuing failures to correct major weaknesses in internal controls. It also requires to report whether any frauds on or by the company had been noticed or reported during the year.

The Government of India last year released the National Cyber Security Policy. This policy aims at protecting information and information infrastructure in cyberspace and building capabilities to prevent and respond to cyber threats. It aims to reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation

The **Standard on Internal Audit (SIA) 11 defines Fraud** as: *“an intentional act... involving the use of deception to obtain unjust or illegal advantage”*. A fraud that involves use of Computers and Computer Networks is called a Cyber fraud. Frauds don't occur randomly, but result from opportunities available to commit them. Thus the goal should be to eliminate the factors that cause fraud rather than looking for temporary solutions. Strengthening the system of internal controls is by and large the best deterrence to frauds and IS auditors have an important role to play here. By evaluating the adequacy of internal controls and identifying high risk areas in the system they can provide valuable guidance on dealing with the risk of frauds. They need to have appropriate knowledge of relevant standards and regulations as well as the various data analysis tools and techniques available.

Standard on Auditing (SA) 505 “External Confirmations” deals with the Auditors' use of external confirmation procedures to obtain audit evidence in accordance with the requirements of SA 330 and SA 500. The reliability of audit evidence is influenced by its source and nature and dependent on the circumstances on which it was obtained. Audit evidence is more reliable when it is obtained from independent sources outside the entity. Further, evidence obtained directly by the IS Auditor is more reliable than obtaining indirectly. Hence the IS Auditor can use these guidelines while conducting the investigation and design the audit program to obtain evidence from external sources.

Standard on Auditing (SA) 580 “Written Representations” deals with the Auditor's responsibility to obtain written representations from the management and, where appropriate, those charged with governance. The IS Auditor during the course of audit should try and obtain written representations from the management as and when needed. However, it should also be noted that it does not absolve the IS Auditor from performing his duties while conducting the audit.

Standards on Internal Audit: SIA 2 requires internal auditors to use their knowledge and skills to reasonably enable them to identify fraud indicators. SIA 11 defines fraud and lays the responsibility for prevention and detection of frauds on the management and those charged with governance.

Standards on Auditing: SA 240 requires an auditor to evaluate whether the information obtained from risk assessment procedures and related activities indicate presence of fraud risk factors. SA 315 requires an auditor to identify risks of material misstatement arising due to fraud.

3.4.2 Cyber fraud Investigation

In case of cyber fraud, the fraud is carried out using a mouse of computer rather than traditional methods of paper and pen. The computer is simply the mechanism for perpetrating the fraud. Cyber fraud investigations procedures are similar to a fraud investigation where the procedure is divided into many phases such as:

1. Collecting and analyzing documentation
2. Conducting interviews
3. Data mining & digital forensics

Fraud risk assessment is a tool that helps in identifying areas of fraud vulnerabilities and assessing the effectiveness of internal controls. IS Auditors need to validate that the risk assessment is regular and complete and that the controls designed are appropriate and effective. The assessment essentially involves:

- Identifying significant risk areas where an organisation is vulnerable to cyber frauds,
- Assessing their likelihood and impact,
- Determining where, how & by whom they may be committed, and
- Assessing whether the existing controls would be able to prevent their occurrences.

A Sample Cyber fraud risk assessment list is given below:

Cyber Fraud	Likelihood	Impact	Internal Controls
<u>Physical theft</u> – Unauthorised access to computer Hardware. (eg. Data centers, Server rooms, etc.)	Low	High	1. Key Cards 2. Security Guards 3. Visitor Logs 4. Circuit Cameras 5. Back up & Recovery Plans
<u>Identity theft</u> – Unauthorised access to personal information of Customers and Employees. (eg. Credit card information of customers, Login IDs & Passwords of employees, etc.)	Medium	High	1. Unique user IDs 2. Strict password policy 3. IDS & Firewalls 4. Incident response policy 5. Delete terminated employee access

Information theft - Unauthorised access to confidential information of Company. (eg. Strategic Plans, Unpublished financial reports, etc.)	Medium	High	1. Segregation of Duties 2. Access Logs 3. Transaction Logs 4. Security violation logs 5. Encryption
<u>Copyright Infringement</u> – Unauthorised access to Software and Database. (eg. Software piracy, Peer-to-peer file sharing, etc.)	Medium	High	1. Block peer-to-peer sharing 2. Internet Surveillance 3. Software Licensing 4. Information sharing policy 5. Protection of Software code

A holistic approach to *fraud deterrence and fraud prevention* would be strengthening the Governance and Management framework. IS auditor could assist in evaluating control framework for fraud prevention and detection by assessing the adequacy of the internal control framework and related policies by reviewing following enablers. Sample questions for review for each of seven enablers adapted from COBIT 5 are given below:

1. **Principles, Policies and Frameworks:** Whether the organisation has a documented Cyber Fraud Governance and management Program which is approved by board.
2. **Processes & Internal Controls:** Does the board approve the security policy and direct that senior management conduct cyber fraud risk assessment regularly and evaluate whether remedial measures are implemented controls to address cyber fraud risks and these are formalised and performed?
3. **Organisation Structures:** Whether the organisation has clearly defined roles and responsibilities in relation to cyber fraud management which meets both regulatory and stakeholder requirement?
4. **Culture, Ethics and Behaviour:** Does management conduct periodic employee awareness programs and training in relation to corporate governance, compliance and cyber fraud?
5. **Information:** Whether the organisation has a proper reporting mechanism for notifying fraud concerns to the top management and these are escalated to the board and reviewed by audit committee.
6. **Services, Infrastructure and Applications:** Has the organisation made appropriate use of technology in preventing and detecting Cyber Fraud?
7. **People, Skills and Competencies:** Has the organisation formed expert teams or arranged for services of experts to conduct periodic fraud investigations?

3.4.3 Cyber Forensics: Digital Forensics

By definition, computer forensics is the “process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings (i.e. court of law). An IS Auditor may be required or asked to be involved in a forensic analysis in progress to provide expert opinion or to ensure the correct interpretation of information gathered. Computer forensics includes activities that involve the exploration and application of methods to gather, process, interpret and use digital evidence that help to substantiate whether an incident happened such as:

- Providing validation that an attack actually occurred
- Gathering digital evidence that can later be used in judicial proceedings

Any electronic document or data can be used as digital evidence, provided there is sufficient annual or electronic proof that the contents of digital evidence are in their original state and have not been tampered with or modified during the process of collection and analysis. It is very important to preserve evidence in any situation. Most organizations are not well equipped to deal with intrusions and electronic crimes from an operational and procedural perspective, and they respond to it only when the intrusion has occurred and the risk is realized. The evidence loses its integrity and value in legal proceedings if it has not been preserved and subject to a documented chain of custody. This happens when the incident is inappropriately managed and responded to in an ad hoc manner. For evidence to be admissible in a court of law, the chain of custody needs to be maintained professionally. The chain of evidence essentially contains information regarding:

- Who had access to the evidence (chronological manner)
- The procedures followed in working with the evidence (such as disk duplication, virtual memory dump)
- Providing that the analysis is based on copies that are identical to the original evidence (could be documentation, checksums, timestamps)

It is important to demonstrate integrity and reliability of evidence for it to be acceptable to law enforcement authorities.

Identify: Refers to identification of information that is available and might form the evidence of an incident

Preserve: Refers to practice of retrieving identified information and preserving it as evidence. The practice generally includes the imaging of original media in presence of an independent third party. The process also requires being able to document chain of custody so that it can be established in a court of law.

Analyze: Involves extracting, processing and interpreting the evidence. Extracted data could be unintelligible binary data after it has been processed and converted into human readable format. Interpreting the data requires an in depth knowledge of how different pieces of evidence may fit together. The analysis should be performed using an image of media and not the original.

Present: Involves a presentation to the various audiences such as management, attorneys, court, etc. acceptance of the evidence depends upon the manner of presentation, qualifications of the presenter, and credibility of the process used to preserve and analyze the evidence.

3.4.4 Fraud investigation tools and techniques

Data analysis technologies using Computer Assisted Audit Techniques (CAAT) are the most effective tools and techniques to combat fraud. CAATs provide powerful software capable of running through large volumes of data and drawing inferences from them quickly. This makes it possible to analyse the entire population instead of adopting the sampling approach. CAATs are extensively used in the process of *fraud detection*. Some useful CAAT are:

1. **Stratification:** To identify abnormal strata.
2. **Classification:** To identify abnormal patterns.
3. **Summarisation:** To compute control totals and identify analyse variances.
4. **Outliers:** To identify outlying transactions which are outside normal range.
5. **Benford Law:** To identify possible fraud areas.
6. **Trend Analysis:** To analyse trends by reviewing patterns which vary from normal.
7. **Gap Test:** To identify gaps in a sequence.
8. **Duplicate Test:** To identify duplicate records.
9. **Relation:** To relate records from different tables.
10. **Compare:** To compare records and identify differences.

3.4.5 Some Case Studies of frauds and lessons

Case Study 1: The WorldCom fraud

This is a popular example of using technology for fraud detection. The Internal Auditors had found a round \$500 million debit in the Property, Plant and Equipment (PP&E) account for which they could not find any invoices or documentation to back up. As the Company would not provide full access to the financial system, the Auditors had to apply data mining techniques to search the data by using a small script and MS Access. Thereby they were able to search the entire populations of data for anomalies in the trends & patterns. As they followed through the accounts they discovered misallocated expenses of several billion dollars and bogus accounting entries that inflated the revenues.

Lessons and Tips:

While sampling techniques may be good for identifying weaknesses in internal controls, they are not recommended in fraud detection. Frauds involve human intelligence and may affect only a few transactions which may not be represented in a sample. Hence fraud detection methodologies require analysis of the entire population, which needs the aid of computer technology and data analytics techniques.

Case Study 2: The \$54 million fraud

This is a typical example of how lack of segregation of duties could lead to a phenomenal fraud. The treasurer of an Illinois town, with an annual budget of \$6 million to \$8 million, was able to embezzle nearly \$54 million over two decades. The fraud remained undetected in annual audits by two independent accounting firms and in annual audit reviews by state regulators. She launched the fraud scheme on Dec. 18, 1990, when she opened a secret bank account in the name of the City of Dixon. Crundwell was the only signatory on the account, which was called the RSCDA - Reserve Fund. She began transferring funds from city accounts into the RSCDA account in 1991. The city, which does not have a city manager, gave Crundwell wide rein over its finances and set the stage for her massive fraud. The failure to segregate duties allowed Crundwell to set up and operate a fairly simple fraud scheme.

Lessons and Tips

Roles and responsibilities must be clearly defined and proper segregation of duties must be done to ensure that no single person can be maker as well as the checker of a particular transaction flow. Ensure the existence of internal control with systems designed to prevent or deter these types of fraud. Conduct regular fraud risk assessment to identify areas of risk where theft or manipulation are likely to occur.

Case Study 3: The Satyam Fraud

This is a case of manipulation of the books of account by inflating revenues through fake invoices. The Company's standard billing systems were subverted to generate false invoices to show inflated sales. 7,561 invoices worth Rs.51 billion (US\$1.01 billion) were found hidden in the invoice management system using a Super User ID. The value of these fake invoices were shown as receivables in the books of account thereby inflating the revenues of the company. The charge framed against the Auditors was that they did not bring the internal control deficiencies to the notice of audit committee and thereby, facilitated the continuance of the fraudulent practices unabated.

Lessons and Tips

Auditors must remember that anyone of any stature could act with monumental recklessness, selfishness and self-destructiveness as Ramalinga Raju did. They must also be conscious of the fact that anything can be faked in the IT world and that they need to continuously update their skills and knowledge in order to keep up with the new challenges.

3.4.6 Overview of lessons learned

More often than not, it is poor governance and mismanagement that makes an organisation vulnerable to the risk of Cyber Fraud. Management must ensure that their responsibility of protecting the organisation from these risks is ensured by implementing that adequate and appropriate internal control systems and framework. IS Auditors can assist organisations not only in investigating and detecting fraud but also play a proactive role in helping organisations to maintain effective fraud management program that would include fraud deterrence, fraud prevention, fraud detection, fraud investigation and effective and prompt response to frauds.

3.5 Summary

We have learnt the various types of assurance and advisory services which can be provided IS Auditors. Further, an insight into fraud related activity which results in loss of critical information of the enterprise and how to conduct investigation into fraud related activity by using data analysis and forensic tools with case studies has been provided.

3.6 References

www.icai.org
www.isaca.org
www.csoonline.com
www.businessdictionary.com
www.sans.org

3.7 Questions

1. Which of the following factors should not be considered in establishing the priority of audits included in an annual audit plan?
 - A. Prior audit findings
 - B. The time period since the last audit
 - C. Auditee procedural changes
 - D. Use of audit software

Module 2

2. Which of the following is LEAST likely to be included in a review to assess the risk of fraud in application systems?
 - A. Volume of transactions
 - B. Likelihood of error
 - C. Value of transactions
 - D. Extent of existing controls
3. An IS auditor discovers evidence of fraud perpetrated with a manager's user id. The manager had written the password, inside his/her desk drawer. The IS auditor should conclude that the:
 - A. Manager's assistant perpetrated the fraud.
 - B. Perpetrator cannot be established beyond doubt.
 - C. Fraud must have been perpetrated by the manager.
 - D. System administrator perpetrated the fraud.
4. Which of the following situations would increase the likelihood of fraud?
 - A. Application programmers are implementing changes to production programs.
 - B. Application programmers are implementing changes to test programs.
 - C. Operations support staff are implementing changes to batch schedules.
 - D. Database administrators are implementing changes to data structures.
5. Neural networks are effective in detecting fraud, because they can:
 - A. Discover new trends since they are inherently linear.
 - B. Solve problems where large and general sets of training data are not obtainable.
 - C. Attack problems that require consideration of a large number of input variables.
 - D. Make assumptions about the shape of any curve relating variables to the output.
6. The FIRST step in managing the risk of a cyber-attack is to:
 - A. Assess the vulnerability impact.
 - B. Evaluate the likelihood of threats.
 - C. Identify critical information assets.
 - D. Estimate potential damage.
7. What generally includes the imaging of original media in presence of an independent third party?

- A. Identify
 - B. Preserve
 - C. Analyze
 - D. Present
8. What involves extracting, processing and interpreting the evidence?
- A. Identify
 - B. Preserve
 - C. Analyze
 - D. Present
9. What is also performed to assess the overall objectives within an organization, related to financial information and assets' safeguarding, efficiency and compliance?
- A. Operational Audit
 - B. Financial Audit
 - C. Integrated Audit
 - D. IS Audits
10. What is designed to evaluate the internal control structure in a given process or area?
- A. Operational Audit
 - B. Financial Audit
 - C. Integrated Audit
 - D. IS Audits
11. After initial investigation, IS auditor has reasons to believe that there is possibility of fraud, the IS auditor has to:
- A. Expand activities to determine whether an investigation is warranted.
 - B. Report the matter to the audit committee.
 - C. Report the possibility of fraud to top management and ask how they would like to proceed.
 - D. Consult with external legal counsel to determine the course of action to be taken.

3.8 Answers and Explanations

- 1. D. Use of audit software merely refers to a technique that can be used in performing an audit. It has no relevance to the development of the annual audit plan.
- 2. B. An error is the least likely element to contribute to the potential for fraud. Answer A and C are incorrect since volume times value of transactions gives an indication of the maximum potential loss through fraud. Answer D is incorrect since gross risk less existing control gives net risk.

3. B. The password control weaknesses means that any of the other three options could be true. Password security would normally identify the perpetrator. In this case, it does not establish guilt beyond doubt.
4. A. Production programs are used for processing an enterprise's data. It is imperative that controls on changes to production programs are stringent. Lack of control in this area could result in application programs being modified to manipulate the data. Application programmers are required to implement changes to test programs. These are used only in development and do not directly impact the live processing of data. The implementation of changes to batch schedules by operations support staff will affect the scheduling of the batches only; it does not impact the live data. Database administrators are required to implement changes to data structures. This is required for reorganization of the database to allow for additions, modifications or deletions of fields or tables in the database.
5. C. Neural networks can be used to attack problems that require consideration of numerous input variables. They are capable of capturing relationships and patterns often missed by other statistical methods, and they will not discover new trends. Neural networks are inherently nonlinear and make no assumption about the shape of any curve relating variables to the output. Neural networks will not work well at solving problems for which sufficiently large and general sets of training data are not obtainable.
6. C. The first step in managing risk is the identification and classification of critical information resources (assets). Once the assets have been identified, the process moves onto the identification of threats, vulnerabilities and calculation of potential damages.
7. B. Preserve refers to practice of retrieving identified information and preserving it as evidence. The practice generally includes the imaging of original media in presence of an independent third party.
8. C. Analyse involves extracting, processing and interpreting the evidence. Extracted data could be unintelligible binary data after it has been processed and converted into human

readable format. The analysis should be performed using an image of media and not the original.

9. C. An integrated audit combines financial and operational audit steps. An integrated audit is also performed to assess the overall objectives within an organization, related to financial information and assets' safeguarding, efficiency and compliance.
10. A. An operational audit is designed to evaluate the internal control structure in a given process or area. Audits of application controls or logical security systems are some examples of operational audits.
11. A. An IS auditor's responsibilities for detecting fraud include evaluating fraud indicators and deciding whether any additional action is necessary or whether an investigation should be recommended. The IS auditor should notify the appropriate authorities within the organization only if it has determined that the indicators of fraud are sufficient to recommend an investigation. Normally, the IS auditor does not have authority to consult with external legal counsel.

SECTION: 3 APPENDIX CHECKLISTS AND OTHER RELATED MATERIALS

Reference material (available in DVD only)

Following publications are available in DVD as reference material:

1. Compendium of Standards on Internal Audit
2. Data Analysis For Auditors
3. Data Analytics and Continuous Control Monitoring
4. Guide on Risk Based Internal Audit
5. Guide to Internal Controls Over Financial Reporting
6. Information Technology Amendment Act 2008
7. ITAF 2nd Edition
8. National Cyber Security Policy 2013
9. Notifications of Rules under Section 6A to 43A
10. Technical guide to IT Migration Audit
11. Technical guide to IS Audit

Useful checklists (available in DVD only)

1. IS General Control Review - Audit Report Sample
2. IS Application Control Review - Audit Report Sample
3. Risk Control Matrix Sample for Physical access controls
4. Risk Control Matrix Sample for Logical access controls
5. Risk Control Matrix Sample for Data Center and Server

Useful checklists available as soft copy in DVD and in section 3: appendix 1 to 6

1. Request for proposal from bank for IS Audit of application software

2. Sample proposal in response to request for Logical access controls review of SAP
3. Sample IS Audit Finding of OS review
4. Sample report using CAAT for auditing Database
5. Sample IS Audit report (Executive Summary)
6. Self-assessment questionnaire for providing assurance services on eCommerce

APPENDIX 1: RFP FROM BANK FOR IS AUDIT OF APPLICATION SOFTWARE

Below is the request received from a Public Sector Bank for submitting a proposal for IS Audit.

Extract from this simple RFP are:

Software Packages to be audited are:

Category A: Developed In-house (Standalone)

1. Bills
2. Remittance
3. Vostro Accounts
4. Preventive Monitoring System

Category B: (Outsourced)

1. Cash Management Services
2. Centralised Banking Solution

The Scope of Audit is as under:

- Evaluation of Effectiveness & Effectiveness of the package vis-à-vis business process and requirements
- Application Security & Controls review
- Database Security and Integrity review
- Review of Interface Controls with other applications
- Review of Network & Communications controls with relation to the application package

Inter-alia, the above scope shall include the following:

1. Whether the design of the software conforms to the Requirements Specification.
2. Objectives of the application - whether these have been fulfilled/ likely to be fulfilled by implementation.
3. Whether bank's systems & procedures are being followed in the application.
4. What are the controls built in the application? Whether these take care of bank's systems and procedures.

5. What are the security features available / built into the application package and whether these are sufficient to take care of the risks in a financial transaction.
6. What is the relative efficiency of the application in conduct of transactions vis-à-vis the performance in similar packages?
7. Testing robustness of the application package by running a specified number of transactions on int.
8. Assessment of the Risk component in the package.
9. To test and verify for any bugs in the application package.
10. To specify clearly methodology to be adopted in carrying out each of the above steps.

APPENDIX 2: RESPONSE TO RFP FOR LOGICAL ACCESS CONTROLS REVIEW OF SAP

Introduction

The Client Company (Max Infotech)

Max Infotech began its business operations in 1959 with the roll out of India's first tractor. Today the Max Infotech Group is a significant player in the Indian software industry with a gross sales turnover of Rs 10.20 Billion in 2013-14. The Max Infotech Group offers a range of IT enabled services. The services of the Group are divided into the specific business units covering specific business interests. Max Infotech has over 5000 employees located in 10 ITPs and 20 marketing offices in India and abroad. Max Infotech has implemented SAP Ver. X and has been using it successfully since more than 3 years. It has more than 500 SAP users in the group. Max Infotech is also considered as one of the SAP Competency Centres in India. The primary SAP modules used are SD, FD, PD, HR, QM and PM. It intends to provide information access to its dealers. Max Infotech intends to have an IS Audit of SAP implementation covering Logical Access Security encompassing security at Network, OS, Database and functionality layers.

IS Assurance and Consulting Firm

IS Assurance and Consulting Company (ISACC) is a 20-year-old firm of Chartered Accountants specializing in Information Systems Assurance, Training and Consulting including Management consultancy services. ISACC provides services in the areas of Information Systems Audit, Training, Implementation and Consultancy. ISACC is led by Mr. Abraham who is a Chartered Accountant and has a diploma in Information Systems Audit of ICAI. The firm has qualified and trained IS audit personnel. We are enclosing brief profile of the firm. The firm also has on its panel Technology\Domain experts available, as required. ISACC have been involved in providing Information Systems Assurances for both the public and private sector in India and abroad. ISACC's clients include IT Companies, Banks and public sector companies.

Background

Objective of SAP Review

Max Infotech Group has been using Information Technology as a key enabler for facilitating business process Owners and enhancing services to its customers. The senior management of Max Infotech has been very proactive in directing the management and deployment of Information Technology. Most of the mission critical applications in the company have been computerised and networked. The IT department of Max Infotech has issued Information Systems Controls (Policies, Procedures, practices and organisation structure) as envisaged by the management for ensuring uniformity and standardization in implementation of IT Solutions across the company. The internal audit team of the company has been well trained in IT and has gained extensive experience in auditing all IT applications and they have also specific competency in all the key functionality of SAP.

Need for SAP review

Max Infotech has successfully implemented SAP covering all its critical operations and has been using it since more than 2.5 years. The implementation has stabilised and standardised across all the operational locations \ functions. A functionality assessment was performed by SAP to confirm the effective usage of SAP about one year ago. The internal audit team now intends to have a security assessment of SAP implementation, primarily to assess the logical access security framework. The objective is to identify areas of control weaknesses by benchmarking against global best practices. The risks identified are to be expected to be mitigated by implementing controls as deemed relevant to ensure that SAP implementation is secure and safe and provide assurance to the senior management of Max Infotech.

Need for Logical Access Controls Review of SAP

Max Infotech has formulated and implemented documented policies and procedures covering all key areas of SAP implementation. The internal audit team have been involved in conducting audits using SAP Functionalities and features for all business related aspects. However, being proactive, Max Infotech has envisaged the need to have an Information Systems Audit covering review of Logical Access Security for SAP users across the company. They intend to benchmark the prevailing Policies, Procedures and practices with the global best practices as relevant to SAP implementation in the company. The objective of this IS Audit is to have an independent assessment of the prevailing procedures, practices and procedures relating to Logical Access Security and identify areas of improvement. Further, they expect that all mission critical operational practices be identified and benchmarked with global best practices. To achieve this, Max Infotech proposes to engage external consultants who have expertise in IS Assurance and Information Technology. ARA having expertise in these areas have been asked to provide their techno-commercial offer for the assignment.

Understanding the need

Based on the discussion held with the internal audit team headed by Mr. B.S.Sinha at the Max Infotech premises at Ghaziabad on 6th march 2014, the scope has been proposed and defined. This proposal outlines the overall strategy and methodology for this assignment.

Methodology for executing the Assignment

Primary Objective

The primary objective of the assignment is to conduct Logical Access Controls Review of SAP by using the Latest and globally recognised standard COBIT 5 issued by the Information Systems Audit and Control Association, USA. The review of SAP would be with the objective of providing comfort on the adequacy and appropriateness of controls so as to mitigate the following system operational risks and ensure that the information systems are implemented so as to provide a safe and secure computing environment.

Scope and Terms of Reference

Based on our understanding of Max Infotech's needs for conducting systems audit of SAP, it was decided to primarily focus on Review of Logical Access Controls in SAP. We propose the scope of review and the terms of reference as laid down in the following paragraphs. The envisaged terms of reference are based on the personal discussions key members of assignment team had with the internal audit team of Max Infotech on 7th March 2014 at Bangalore. The detailed scope of review and methodology followed are given in the annexure. The methodology would be further enhanced and refined as the audit progresses based on specific needs of the audit environment. Broadly the scope of review primarily from security\controls and would involve:

- A. Review of IT Resources as relevant
 - a. Operating Software - Access controls
 - b. Telecommunications Software - Access Controls
 - c. RDBMS - Access Controls
 - d. SAP - Major focus area – Configuration of Parameters and Access Controls
 - e. Application controls at various stages such as Input, Processing, Output, Storage, Retrieval and transmission so as to ensure Confidentiality, Integrity and Availability of data.
- B. Organisation structure policies, procedures and practices as mapped in the information systems - efficiency\controls.

Our Approach/Methodology

Audit Approach

A. Our approach to the assignment would be as follows:

(i) We propose to deploy a core team of 4 to 6 IS audit personnel for this assignment in batches of 2 to 3 as per the skill sets required, under the personal direction and liaison of the Principal, Mr. Abraham.

(ii) Max Infotech should designate a person at a senior level to coordinate between us. Max Infotech should also depute one personnel each from systems and audit group to form part of the audit team.

(iii) Detailed systematic audit procedures would be finalized after completing review of the documentation and discussion with the systems staff and the users.

In tune with terms and scope of reference of the assignment, we will adapt the methodology from COBIT®. Specific Control Objectives/Management Guidelines of the relevant IT process of Logical Access controls shall be selected for this assignment after obtaining understanding of the organisation structure, Information Technology deployment and available documented policies and procedures.

Structured Methodology

The above-mentioned objectives shall be achieved through the following structured methodology

- Obtain understanding of IT Resources deployment at Max Infotech
- Obtain understanding of the IT Strategy and internal control system at Max Infotech
- Identification and documentation of IT related Circulars issued by Max Infotech.
- Identification and documentation of Organisation Structure and Information Architecture
- Identification and documentation of existing policies, procedures and practices
- Application of COBIT® for formulating IT best practices for the Policy and procedures of Max Infotech
- Formulation of draft report on our findings covering our review and benchmarking.
- Presentation of final report with agreed action plan based on feedback of IT management of Internal Audit team of Max Infotech

Max Infotech shall make available all the required resources on time and provide one coordinator for interaction and clarifications as required.

Audit plan

The audit plan would cover the following activities:

Discussions with the

- Internal Audit Team
- Systems\Implementation Team
- Users and user management
- Review of Operating Systems (OS) documentation
- Examination of OS access rights
- Review of Oracle\SAP Manuals
- Examination of selected Modules access profiles
- Observation of the Users and the systems in operation
- Review of access controls over Computers as relevant
- Examination of computerised processing controls incorporated within the selected modules.

Audit Program\procedures

Our audit team would perform the following tasks based on the audit methodologies given in annexure 'A' to 'B' and include the following programs\procedures:

1. Undertake an in-depth study and analysis of all aspects of SAP as implemented at Max Infotech. We will take steps to identify the way in which the system currently operates. In doing so, the following objectives would be kept in mind while setting the overall goals:
 - Accurate and complete processing of data
 - Error messages in case of incomplete/aborting of processing of data
 - Optimise data handling and storage
 - Better management of information
2. Review the software in operation; understand how the various modules interact within the overall system.
3. Review how each module in the system has been tested including the documentation prepared in respect of each.
4. Review the methods employed for implementation of the system, including post-implementation review procedures undertaken to ensure that the objectives set out were actually achieved.
5. Understand the business processes and review how these have been mapped in the information systems by tracing the modules with a top down approach.
6. Review the modules by performing detailed documented tests of all the menu options and their related effects.
7. Review the controls established over the continuity of stored data, necessary to ensure that once data is updated to a file, the data remains correct and current on the file.

8. Review the in-built controls for stored data so as to ensure that only authorised persons have access to data on computer files.
9. Review the controls established which ensure that all transactions are input and accepted for further processing and that transactions are not processed twice.
10. Review the controls established so as to ensure that only valid transactions are processed.
11. Review the procedures established for back-up and recovery of files in the package.
12. Review controls established for the development, documentation and amendment of programs so as to ensure that they go live as intended.

Assignment Team

Our approach to selecting the right people for a project is to bring together the necessary skills and experience for a particular assignment from the rich mix of skills and experience available. The assignment would be executed under the personal supervision and lead by Mr. Abraham. The team would be a blend of professionals with extensive experience in management, Information Technology and Auditing. The team includes Chartered Accountants, IT Professionals, Management Consultants and Certified Information System Auditors. The senior members of the team are:

- Abraham
- Ramprakash
- Ravindra Jain
- Hariram

Logistic arrangements

Infrastructure Required

It will be necessary for Max Infotech to appoint one coordinator who will be part of the discussion on the work plan initially and continue to work with the ARA team till the assignment is complete. Max Infotech will make available the necessary computer time, software resources and support facilities necessary for completing the assignment within the agreed timeframe. The conduct of the assignment should be adequately communicated to the required personnel so as to facilitate extensive co-operation from the respective personnel. During the course of the assignment, we will require the following infrastructure.

- Three Nodes with Read only access to SAP
- One Laptop with windows 8/Microsoft office 2013.
- Access to a laser printer for printing reports as required.
- Adequate seating and storage space for audit team
- Facilities for discussions amongst our team and your designated staff.

Documentation Required

- User Manuals and Technical Manuals relating to System Software and SAP.
- Organisation chart outlining the organisation hierarchy and job responsibilities
- Access to circulars\guidelines issued to employees.
- Access to user manuals and documentation relating to SAP Implementation by Max Infotech.
- Any other documentation as identified by us as required for the assignment

Estimated Timeframe, Deliverables and Fees

Deliverables

1. Draft Report including executive summary of the result of the review along with the recommendations of findings and recommendations with risk analysis of findings.
2. Final Report incorporating Management Comment and agreed priority plan of action based on exposure analysis.
3. Soft or hard Copy of Checklist used for the audit.
4. Soft or hard Copy of Audit Methodology and documentation

Time Frame

The elapsed time for the assignment is approximately 4 weeks (three man months). We would require lead-time of two weeks for commencing the assignment. The availability of coordinating team, user involvement, availability of resources and information by the auditee would also impact the audit duration and time schedule, which we would be communicating to you in advance.

Fees

The Fees for this assignment is Rs. x.xx Lakhs (Rupees xxx Only) to be paid as follows:

- 50% Advance with Order
- 50% on presentation of Final Report

Out of pocket Expenses

Travelling, Boarding, Lodging and conveyance expenses to be reimbursed on actuals in case of outstation travel. As our HO is in Bangalore, the assignment may involve one/two trips of Mr. Abraham from Bangalore to Delhi for the assignment.

Authorised Signatory

Encl: Profile of ISACC

APPENDIX 3: SAMPLE IS AUDIT FINDING

Logical Access Controls Review of Operating System

We have reviewed procedure of granting access to the Operating system and Toll Operations Package. Our specific findings and recommendations with agreed action plan are given below:

The overall control objective in implementing OS Access controls:

“The creation of users and their access need to be controlled through appropriate Authorization levels. Controls have to be laid down and adhered to while granting authorization. Access logs are to be generated whenever the O/S is accessed and Access logs should show details as to the users accessing the O/S, the period of access and the resources accessed. System must enforce a systematic procedure for logins and logouts. All access points to the system are to be monitored by way of access logs and these access points are available only on the administrators console and terminals”.

1. System Users have blank user-id:

Issue: Presently, system manager has the system administration rights and toll manager is also created as a user who can modify the ini settings in PQR. These users have a blank user-id and passwords have not been changed since installation.

Implication: High

User accountability may not be established on account of lack of documentation. The operations of PQR may be affected in case of breakdown and non-availability of the relevant personnel.

Recommendations:

- The users of Operating System and Toll Operations Package in PQR Computer need to be authorized in writing by senior management. Creation of their user id and password should be documented and accepted by the user and kept by senior management in sealed cover in safe custody to be available in case of need.
- Password policy has to be formulated and passwords should be changed at least once in 90 days without being reused.

Management comment: Agree. System manager will create user ids for all authorized users.

2. PQR Computer is networked to other office computers

Issue: The PQR Computer is linked to other Computers in the Network. These computers are only being used by the Toll Manager and his Staff for performing administration jobs such as preparing

Toll Reports. Networking of these office computers with PQR computer makes it vulnerable to unauthorized access.

Implication: High

PQR System could be accessed by any of the users of the office computers.

Recommendations:

A review of security and operations settings needs to be done and all access to PQR Computer from any of the office computers has to be removed or restricted.

Management comment: Agree. Will be reviewed and modified as required.

APPENDIX 4: CAAT REPORT USING SQL

Sample Results of using CAAT

As a part of our audit procedure, we have used SQL to directly access and analyze the data stored in the tables. Our observations and the related analysis are given below. As these observations relate to the data stored which could impact financial accounts, we have submitted this information to Statutory Auditors and user department of ABC with a request to verify these SQL results and confirm the impact on the financial statements. The detail tables of SQL Statements can be obtained from ABC, IT Department. We have given a copy of this draft report to ABC with a request to confirm the facts to us. Our observations with implications, comments and our Risk assessment are given below.

Users available with Invalid employee codes:

Rating: High

There are two user ids within user id 15, which is still being used. These transactions used by live users will result in user accountability not being established.

Implications

As the employer code is invalid, it will be difficult to establish accountability for transactions entered using this ID in case of errors or frauds.

IT Department's feedback and Agreed Action

This user-id has been created during the time of data conversion. This user-id has been disabled so that transactions can be entered using this.

Past employees having ID in user table

Rating: High

There are 19 Users who have user ID. Their employee ID and name is given so that a final list may be prepared with actual users who are expected to have access in the system.

Implications

The number of users in the system is much more than the actual users. This is on account of the fact that past and temporary users have not been disabled.

IT Department's feedback and Agreed Action

The number of users will correspond with actual users. All other users will be disabled.

Transactions with amount as Null in FA Trans_table

Rating: Medium

Transactions with Amount as Null are listed day-wise. There are 181 transactions, which need to be analyzed.

Implications

These results in dummy transactions, which may not have any value, or genuine transactions might have been stored without values.

IT Department's feedback and Agreed Action

This has occurred on account of transactions where DD charges are deducted from loan amount for obtaining DD whereas the loan account is debited with the total amount including DD Charges. This does not have any financial impact.

APPENDIX 5: SAMPLE IS AUDIT REPORT

Objectives of the Assignment

The primary objective of this Information Systems Audit assignment was to provide assurance to the management of ABC Limited (ABC) on the availability, appropriateness and adequacy of controls in the Financial Accounting and Loan Processing System (FALPS) through review of the control framework of their in-house package - Financial Accounting and Loan Processing System (FALPS), review of Logical access controls of FALPS and conduct Implementation audit of General Controls at 2 select branches with specific emphasis on implementation of FALPS.

Proposed Scope of Review/Terms of Reference

Based on understanding of ABC's needs for conducting systems audit of FALPS Package, it was decided to primarily focus on Review of data integrity in FALPS Package. The review of FALPS Package was with the objective of providing comfort on the adequacy and appropriateness of controls and data so as to mitigate the following system operational risks and ensure that the information systems are implemented so as to provide a safe and secure computing environment. The detailed scope of review \ methodology were also agreed to. Broadly the overall scope of review primarily from security \ controls involved the following: Application controls at various stages such as Input, Processing, Output, Storage, Retrieval and Transmission so as to ensure Confidentiality, Integrity and Availability of data. Further, organization structure policies, procedures and practices as mapped in the information systems focusing on efficiency\ controls were also reviewed. Broadly, the areas reviewed covering the following:

1. Logical Access Controls Review as implemented through:
 - a. Operating System Software (Unix) - Access controls

- b. Telecommunications Software - Access Controls
 - c. RDBMS (Oracle)- Access Controls
 - d. FALPS Package - Major focus area - Access, security and effectiveness
2. Review of General controls at 2 select branches covering Environmental and Physical Access Controls Review, Logical access Controls review as implemented, Application Controls as implemented and review of policies, procedures and practices relating to IT Implementation.

Our Approach/Methodology

The Audit was carried out as pre-planned Audit Plan and program, which was discussed with the statutory auditors and ABC's senior management. We have used the international accepted standard for IS Audit – COBIT (Control Objectives for Information and Related Technology, issued by the Information Systems Audit and Control Association, USA for this review. The Key tasks of our Audit plan are highlighted below:

- Discussions with the IT department and user management.
- Review of Circulars issued by ABC Ltd relating to IT operations
- Review of Environmental Access and Physical Access controls
- Review of Operating Systems (Unix) and RDBMS (Oracle) Manuals
- Examination of OS and RDBMS access rights
- Review of FALPS Package Technical and User Manuals
- Examination of access profiles and parameter settings in FALPS package
- Review of Application Controls in FALPS package
- Observation of the Users and the system in operation
- Examination of processing controls in FALPS using test data.
- Review of Reports and Audit Logs in System Software and FALPS package

Audit Environment

We have conducted IS Audit at the IT department of ABC in a simulated environment using a Windows 7 Computer connected to Server with SCO UNIX as Operating System and RDBMS as Oracle using latest version of FALPS with copy of data of Bangalore Branch (upto 31st march 2012). We have also visited reviewed two branch operations at Mangalore and Hassan.

Audit Reports

We issued a draft report outlining our issues and recommendations and obtained feedback from the IT Department. Further, a meeting was held with IT department represented by Mr. Sam, AGM (IT) and Mr. Ram, AGM (Finance and Accounts) where the issues and recommendations were discussed in detail. The IT Department has been very proactive in incorporating our suggestions. The issues rectified so far are given in separately in Annexure-3 for the purpose of record. The report incorporates all the issues, which have been agreed and confirmed. This IS Audit report includes the following annexure and has to be read in its totality:

1. Summary of Findings: Outlines all key issues with exposures
2. Specific Issues and recommendations: Issues which need to be implemented
3. Issues identified which have been rectified by it dept. Issues rectified as on date
4. Logical access control Review of Unix: Access Controls issues of Unix
5. Logical access control Review of Oracle: Access Controls issue of Oracle
6. Review of Financial data using SQL: Highlights data integrity issues in existing data

Overall Conclusions

Based on our review our overall conclusions on specific areas are:

Security and Access Controls

Our review of security and access controls at the IT Environment as reviewed by us and as implemented in ABC using Unix, Oracle and FALPS confirms that appropriate security and access controls have been implemented by using related functions and features of the packages. Our test checks have revealed that systems of security and controls are reliable. However, there are some areas where controls need to be strengthened and these are given in annexure.

Business Process Controls

Our review of business process validations and data integrity controls covering all the core functions of ABC as facilitated by FALPS such as interest computation, allocation and aging, confirms that all related data have been duly captured, processed and stored correctly and completely subject to some transaction data not available pertaining to previous years. However, there are also missing data in master tables which impact the MIS and statements of accounts. The issues, which have come to our notice during the process of our review, are given in annexure.

Further Action

We consider that the recommendations given in annexure to this report would be very useful for facilitating business process controls of ABC and will aid in improving the effectiveness of FALPS package and computer operations. We would like to affirm that the matters included in this report are those which came to our notice during our review by following normal Information System audit procedures by complying with globally applicable Information Systems Auditing Standards, Guidelines and procedures that apply specifically to Information Systems Auditing issued by Information Systems Audit and Control Association, USA and Security and Control Practices as outlined in COBIT 5 issued by ISACA as adapted to ABC operations for review of Application software and implementation audit. Further, on account of limitations of scope and time, we have used sample test and test check approach. Hence, certain areas, which are outside the scope of this review such as source code, review, implementation controls and general controls specific to branches are not covered.

APPENDIX 6: QUESTIONNAIRE FOR PROVIDING ASSURANCE SERVICES IN E-COMMERCE

1. How many (approximately) of the businesses you audit will be electronic in that there is no paper, or other non-electronic forms of audit trail available?
2. In general, as an auditor, what special steps or approach would you take when auditing a business that is engaged in eCommerce compared with a comparable business not engaged in electronic commerce?
3. Which national or international standards or pronouncements would you use or are using in undertaking an audit of a business engaged in electronic commerce?
4. To what extent would you want that records and audit trails of eCommerce transactions be maintained and in what form?
5. How would you assure the management that records and audit trails are being properly created?
6. To what extent would you recommend that records and audit trails of eCommerce transactions be maintained over time?
7. To what extent do you foresee that records and audit trails of eCommerce transactions will be combined with other transactions or otherwise consolidated, so that the transactional trail is lost?
8. How do you satisfy yourself that records and audit trails of eCommerce transactions have not been altered?
9. How would you test the above – through review of system controls or substantive testing?
10. To what extent do you perceive the risks that records and audit trails of eCommerce transactions could be incorrectly transferred through into accounting systems? How would perceive such a risk?

11. If you find that that records and audit trails of eCommerce transactions are inaccessible either through being stored remotely, or through the effects of data security mechanisms, or otherwise, how would you, as auditors, audit the same?
12. What are the minimum types of records that must be archived, by the business entity, which will allow both external financial or statutory auditors to perform their functions? On what basis do you expect these records to be maintained? In what form do you want these records - Digital or manual?
13. How would you face the following issues and problems you could be facing in practice when carrying out audits of businesses engaged in eCommerce?
 - ✓ Accessing initial transaction data
 - ✓ Processing of the transaction by accounting systems
 - ✓ Identifying suitable sources of confirmation
 - ✓ Determining the system processing “rules”
 - ✓ Storage and retrieval of the eCommerce records, and
 - ✓ Forming an opinion as to the timeliness, completeness and accuracy of the Transaction data.
14. What issues and problems do you anticipate arising in the future when carrying out audits of businesses engaged in electronic commerce? These could be from perspectives of:
 - Accessing initial transaction data
 - Processing of the transaction by accounting systems
 - Identifying suitable sources of confirmation
 - Determining the system processing “rules”
 - Storage and retrieval of the eCommerce records, and
 - Forming an opinion as to the timeliness, completeness and accuracy of the Transaction data.
15. How many of your present clients do you perceive could be engaged in electronic commerce?
16. What specific approaches, solutions, methods, procedures or techniques do you need to develop to assist in the auditing of businesses engaged in electronic commerce?
17. What approaches, solutions, etc. do you anticipate might help you in the future when auditing businesses engaged in electronic commerce?

Module 2

- 18.** In what way would the solutions, methods, etc. you devised for auditing non-eCommerce clients differ from auditing the eCommerce Clients?
- 19.** Do you think there are differences in business-to-business eCommerce compared with business-to-consumer eCommerce that would warrant different audit considerations and if so, what are the considerations?

Module-3

Governance and Management of Enterprise Information Technology, Risk Management and Compliance Reviews

TABLE OF CONTENTS

MODULE 3: GOVERNANCE AND MANAGEMENT OF ENTERPRISE INFORMATION TECHNOLOGY, RISK MANAGEMENT AND COMPLIANCE (12%)	487
SECTION 1: OVERVIEW	487
Objective.....	487
Task Statements.....	487
Knowledge Statements	488
Mapping of Knowledge Statements to Task Statements.....	489
Knowledge Statement Reference Guide	492
SECTION 2: CONTENTS	495
Chapter 1: Concepts of Governance and Management of Information Systems	495
Learning Objectives.....	495
1.1 Introduction	495
1.2 Organisation of chapters	496
1.3 Key Concepts of Governance	497
1.3.1 Enterprise Governance	498
1.3.2 Corporate Governance	498
1.3.3 Need for Corporate Governance.....	498
1.4 Corporate Governance and Regulatory requirements	499
1.4.1 Conformance or Corporate Governance Dimension.....	502
1.4.2 Performance or Business Governance Dimension	502
1.5 Enterprise governance framework	503
1.6 Enterprise Risk Management	504
1.7 Governance of Enterprise IT (GEIT)	504
1.7.1 Governance Objectives	505
1.7.2 Internal Controls	505
1.7.3 Implementing GEIT	506
1.7.4 Guidelines for implementing GEIT	508
1.7.5 Systemic approach to implementing GEIT	508

1. Aligning IT Goals with Business Goals	509
2. Formalise and implement right IT Governance Processes	509
3. Establish required IT Organisation and decision structure.....	509
4. Involve Board of Directors/Executive Management in IT related matters	510
5. Govern and manage roles and responsibilities.....	510
6. Establish IT Strategy and IT Steering Committee.....	510
7. Plan, align and manage IT enabled Investment as a Portfolio	510
8. Implement Performance Measurement system integrated with regular process.....	511
9. Establish Sustainability through support, monitoring and regular communication	511
1.8 Summary	511
1.9 Questions	512
1.10 Answers and Explanations	513
Chapter 2: GRC Frameworks and Risk management practices	517
Learning Objectives.....	517
2.1 Introduction	517
2.2 GRC frameworks.....	518
2.2.1 COSO	518
Requirements for effective internal control.....	521
2.2.2 COBIT 5	522
Need for Enterprises to Use COBIT 5	522
Integrating COBIT 5 with other frameworks	523
Customizing COBIT 5 as per requirement	523
Five Principles of COBIT 5	523
Principle 1: Meeting Stakeholder Needs.....	524
Principle 2: Covering the Enterprise End-to-End.....	524
Principle 3: Applying a Single Integrated Framework	525
Principle 4: Enabling a Holistic Approach	525
Principle 5: Separating Governance from Management.....	525
Seven Enablers of COBIT 5	527
2.2.3 ISO 38500.....	528

2.2.4 ISO 31000.....	528
2.2.5 RIMS ERM.....	528
2.2.6 RiskIT: Risk Management framework by ITGI and ISACA.....	529
2.3 Enterprise risk management and IT risk management.....	530
2.3.1 Risk Management	530
2.3.2 Risk Management in COBIT 5.....	531
Key Governance Practices of Risk Management	531
Key Management Practices of Risk Management.....	532
Metrics of Risk Management.....	532
2.3.3 Risk Factors.....	533
2.3.4 Categories of Risks	533
2.3.5 Elements of Risk Management	534
2.4 Risk Management strategies.....	534
2.4.1 Developing Strategies for Information Risk Management	535
2.4.2 Risk Register and control catalogue	535
2.5 Risk management process.....	536
2.5.1. Risk Identification	536
Threat profile/ Inventory.....	537
Vulnerability Assessment	537
Asset Inventory	538
Risk components.....	538
2.5.2. Risk Evaluation.....	539
Determine likelihood of risk	539
2.5.3. Risk prioritization	540
2.5.4. Risk Response	540
2.5.5. Risk Mitigation	541
2.5.6. Risk Monitoring.....	541
2.6 IS Risks and Risk Management.....	542
2.7 Summary	543
2.8 Questions	543

2.9 Answers and Explanations	545
Chapter 3: GEIT and GRC	547
Learning Objectives.....	547
3.1 Introduction	547
3.2 What is GRC?	548
3.2.1 GRC from Corporate Governance perspective (Clause 49).....	549
Risk Management	549
CEO/CFO Certification	549
Internal Control.....	550
Auditor Certification.....	550
3.2.2 GRC program implementation.....	550
3.2.3 Using COBIT 5 for effective GRC program	551
3.2.4 Responsibility of Senior Management in GRC	552
3.3 IT Compliance Review.....	552
3.3.1 SOX requirements.....	552
3.3.2 Clause 49 Requirements	553
3.3.3 Risk management	553
3.3.4 Internal control requirements and Clause 49	553
3.3.5 Compliance in COBIT 5	554
3.4 Key Management Practices of IT Compliance	555
3.4.1 Key Metrics for Assessing Compliance Process.....	555
Compliance with External Laws and Regulations:	555
IT Compliance with Internal Policies:	555
3.5 Using COBIT 5 Best Practices for GRC.....	556
3.6 Summary	557
3.7 Questions	557
3.8 Answers and Explanations	559
Chapter 4: Key Enablers of GEIT	561
Learning Objectives.....	561

4.1 Introduction	561
4.2 Overview of Seven Enablers of COBIT 5	562
4.2.1 Principles, policies and framework	562
4.2.2 Processes	563
4.2.3 Organisation Structures	564
IT Strategy Committee	565
IT Steering Committee	565
4.2.4 Roles, Responsibilities and Risks of IT department.....	567
Chief Information Officer (CIO)	567
Risks.....	567
Controls.....	567
Application Systems Development Manager (ASDM)	567
Risks.....	568
Controls.....	568
Application Systems Analysts	568
Risks.....	568
Controls.....	568
Application Systems Programmers (ASP).....	568
Risks.....	568
Controls.....	569
Data Administrator (DA)	569
Database Administrator (DBA).....	569
Quality management.....	570
Quality Assurance Manager	570
Quality Control Manager.....	570
Risks.....	570
Controls.....	570
Security management.....	571
Security Manager	571
Risks.....	571

Controls.....	571
Technical support manager	572
Risks.....	572
Controls.....	572
Systems Analyst.....	572
Risks.....	572
Controls.....	572
Systems Administrator	572
Risks.....	573
Controls.....	573
Network Administrator	573
Risks.....	573
Controls.....	573
End User Support Manager.....	574
Operations Manager	574
Risks.....	574
Controls.....	574
4.2.5 Culture, Ethics and Behaviour	575
4.2.6 Information	575
4.2.7 Services, Infrastructure and Applications	576
4.2.8 People, Skills and Competencies.....	577
4.3 Summary	578
4.4 Questions	578
4.5 Answers and Explanations	580
Chapter 5: Performance Management Systems	583
Learning Objectives.....	583
5.1 Introduction	583
5.2 Performance Measurement	583
5.3 Performance measurement system	584

5.4 Goal Setting	585
5.5 Performance measurement in COBIT 5.....	585
5.5.1 Goal setting and stakeholder needs	586
5.5.2 Category of Enterprise Goals	587
5.5.3 COBIT 5 enterprise and IT relates goals	588
5.5.4 Requirements for Measures	588
5.5.5 Performance Measurement processes / indicators.....	588
Phases of performance measurement	589
Examples of performance measures	589
5.5.6 Measures defined in COBIT	589
5.5.7 Enterprise Goals.....	590
Sample metrics for enterprise goal	590
5.5.8 IT related Goals.....	590
Sample metrics for IT related is given below:	591
5.5.9 Sample goals and metrics for Resource optimisation	591
5.6 Balanced scorecard (BSC)	593
5.6.1 BSC perspectives.....	594
5.6.2 BSC as a Management tool.....	595
5.6.3 IT Balanced Scorecard	596
5.7 Strategic scorecard	598
5.8 Methods to report on IT resource performance.....	601
5.8.1 Strategic Metrics for IT Projects	601
5.8.2 Strategic Metrics for IT Operations	601
5.9 Maturity Model.....	602
5.10 Total Quality Management	602
5.11 Quality Management	602
5.12 Summary.....	603
5.13 Questions	604
5.13 Answers and Explanations	605

Chapter 6: Implementing Governance and Management Practices	607
Learning Objectives.....	607
6.1 Introduction	607
6.2 Stakeholders in implementing GEIT	608
6.3 Critical Success factors of GEIT implementation	608
6.4 Using systematic approach for implementing GEIT	609
6.4.1 Phase 1: Establish the desire to change	609
6.4.2 Phase 2: Form an effective implementation team.....	609
6.4.3 Phase 3: Communicate desired vision	610
6.4.4 Phase 4: Empower role players and identify quick wins.....	610
6.4.5 Phase 5: Enable operation and use.....	611
6.4.6 Phase 6: Embed new approaches	611
6.4.7 Phase 7: Sustain	611
6.5 Implementing Governance and Management practices	611
6.5.1 Governance Processes and Practices.....	612
Governance processes.....	612
Governance practices.....	612
6.5.2 Key Management Processes and Practices.....	612
Management processes	612
Management practices	613
6.6 Implementing GEIT in specific areas	613
6.6.1 Strategic alignment of IT with Business.....	613
Objective of IT Strategy	614
IT Strategy Planning	614
IT Strategic Planning Process.....	615
Aligning IT Strategy with Enterprise Strategy.....	615
Role of IS Auditors	616
6.6.2 Value optimization	616
Key Governance practices	616
Metrics for value optimisation.....	617

6.6.3 Resource Optimization.....	617
Key Governance practices	618
6.6.4 Sourcing processes.....	618
6.6.5 Outsourcing	619
6.6.6 Capacity Management & Growth Planning processes	619
6.6.7 Capex and Opex	620
6.7 Auditing Governance and Management practices	621
6.8 Summary	622
6.9 Questions	623
6.10 Answers and Explanations	624
6.11 References	626

MODULE 3: GOVERNANCE AND MANAGEMENT OF ENTERPRISE INFORMATION TECHNOLOGY, RISK MANAGEMENT AND COMPLIANCE (12%)

SECTION 1: OVERVIEW

Objective

Evaluate structures, policies, procedures, practices, accountability mechanisms and performance measures for ensuring Governance and management of Information Technology, risk management and compliance as per internal and external stakeholder requirements.

Task Statements

- 3.1 Review governance mechanisms and structures in place to assess whether these are adequate to meet internal/ external stakeholder needs and facilitate value delivery and benefit optimisation.
- 3.2 Distinguish between appropriate and inappropriate governance structures in an enterprise (e.g. tone at the top, policies, steering committees, strategies, oversight, etc.)
- 3.3 Assess framework for IT governance and evaluate whether the governance and management processes are meeting stakeholder needs and governance objectives.
- 3.4 Distinguish Governance and management processes and their objectives.
- 3.5 Evaluate key enablers as relevant: principles, policies and framework, processes, organisation structure, culture, ethics and behaviours and resources (information, services, infrastructure and applications, people, skills and competencies) in the areas of Governance and Management of Enterprise IT.
- 3.6 Review information architecture and processes to determine compliance with specified standards or criteria.
- 3.7 Review alignment of IT strategy with the enterprise strategy so as to achieve enterprise objectives.
- 3.8 Review risk optimisation processes and practices in place to assess whether these are appropriate to mitigate risks as per risk management strategy.
- 3.9 Evaluate resource management practices to assess whether they ensure optimum utilisation
- 3.10 Review usage of IT resources considering value proposition of IT investments using CAPEX and OPEX Models.
- 3.11 Determine the current status of the entity's use of Information Technology to support its business processes

- 3.12 Evaluate monitoring and assurance practices and the ways to measure and manage IT performance and costs through use of Key Goal Indicators, Key Goal Indicators including balance score cards, strategic score cards etc. to ensure timely reporting and monitoring
- 3.13 Review the process of IT Infrastructure management, IT operational procedures and practices, service management practices, outsourcing, end-user procedures, IT service help desk, problem including incidence Management, Problem Management, Change Management, Configuration Management, Capacity Management and Performance Management.
- 3.14 Evaluate IT management and monitoring of controls (e.g., continuous monitoring, QA) for compliance with the organization's policies, standards and procedures
- 3.15 Review enterprise controls to ensure compliance with internal and external regulatory requirements and external service providers such as SOX, Clause 49 Listing requirements, Information Technology Act, etc.

Knowledge Statements

- 3.1 Enterprise Governance, Corporate Governance, Governance of Enterprise IT and their relationship,
- 3.2 Using standards, Frameworks and best practices such as COBIT, COSO, ISO 27001, ISO38500, ISO 31000 etc. for Governance and Management of IT in enterprises.
- 3.3 Implementing best practices of Enterprise Goals, IT enabled goals, process and activity goals, Key Goal indicators and Key performance indicators.
- 3.4 Aligning IT strategy with business strategy and the business processes for long-term and short-term
- 3.5 IT management and monitoring of controls (e.g., continuous monitoring, QA) for compliance with the organization's policies, standards and procedures
- 3.6 Value proposition of IT investments including Capex and Opex models.
- 3.7 Key enablers of Governance and Management of IT such as relevant: principles, policies and framework, processes, organisation structure, culture, ethics and behaviours and resources (information, services, infrastructure and applications, people, skills and competencies).
- 3.8 Enterprise Risk Management, Risk management practices, Risk mitigation strategy
- 3.9 IT resource investment, use and allocation practices, including prioritization criteria, for alignment with the organization's strategies and objectives by using CAPEX and OPEX models.
- 3.10 IT operational procedures and practices, service management practices, outsourcing, end-user procedures, IT service help desk, escalation matrix, etc.
- 3.11 Performance management systems including performance measures, KGI, KPI, Balanced score cards, strategic score cards etc.
- 3.12 Internal compliance/external national and international regulatory requirements and external service providers such as SOX, Clause 49 Listing requirements, Information Technology Act, etc.

Mapping of Knowledge Statements to Task Statements

Task Statements	Knowledge Statements
3.1 Review governance mechanisms and structures in place to assess whether these are adequate to meet internal/ external stakeholder needs and facilitate value delivery and benefit optimisation.	3.1 Enterprise Governance, Corporate Governance, Governance of Enterprise IT and their relationship,
3.2 Distinguish between appropriate and inappropriate governance structures in an enterprise (e.g. tone at the top, policies, steering committees, strategies, oversight, etc.)	3.2 Using standards, Frameworks and best practices such as COBIT, COSO, ISO 27001, ISO 38500, ISO 31000 etc. for Governance and Management of IT in enterprises. 3.3 Implementing best practices of Enterprise Goals, IT enabled goals, process and activity goals, Key Goal indicators and Key performance indicators.
3.3 Assess framework for IT governance and evaluate whether the governance and management processes are meeting stakeholder needs and governance objectives.	3.2 Using standards, Frameworks and best practices such as COBIT, COSO, ISO 27001, ISO 38500, ISO 31000 etc. for Governance and Management of IT in enterprises. 3.3 Implementing best practices of Enterprise Goals, IT enabled goals, process and activity goals, Key Goal indicators and Key performance indicators.
3.4 Distinguish Governance and management processes and their objectives.	3.1 Enterprise Governance, Corporate Governance, Governance of Enterprise IT and their relationship,
3.5 Evaluate key enablers as relevant: principles, policies and framework, processes, organisation structure, culture, ethics and behaviours and resources (information, services, infrastructure and applications, people, skills and competencies) in	3.2 Using standards, Frameworks and best practices such as COBIT, COSO, ISO 27001, ISO38500, ISO 31000 etc. for Governance. 3.7 Key enablers of Governance and Management of IT such as relevant:

the areas of Governance and Management of Enterprise IT.	principles, policies and framework, processes, organisation structure, culture, ethics and behaviours and resources (information, services, infrastructure and applications, people, skills and competencies).
3.6 Review information architecture and processes to determine compliance with specified standards or criteria.	3.12 Internal compliance/external national and international regulatory requirements and external service providers such as SAS, Clause 49 Listing requirements, IT Act, etc.
3.7 Review alignment of IT strategy with the enterprise strategy so as to achieve enterprise objectives.	3.4 Aligning IT strategy with business strategy and the business processes for long-term and short-term 3.9 IT resource investment, use and allocation practices, including prioritization criteria, for alignment with the organization's strategies and objectives by using CAPEX and OPEX models.
3.8 Review risk optimisation processes and practices in place to assess whether these are appropriate to mitigate risks as per risk management strategy.	3.8 Enterprise Risk Management (ERM), Risk management practices, Risk mitigation strategy
3.9 Evaluate resource management practices to assess whether they ensure optimum utilisation	3.8 ERM, Risk management practices, Risk mitigation strategy. 3.9 IT resource investment, use and allocation practices, including prioritization criteria, for alignment with the organization's strategies and objectives by using CAPEX and OPEX models.

3.10 Review usage of IT resources considering value proposition of IT investments using CAPEX and OPEX Models.	3.6 Value proposition of IT investments including CAPEX and OPEX models. 3.9 IT resource investment, use and allocation practices, including prioritization criteria, for alignment with the organization's strategies and objectives by using CAPEX and OPEX models.
3.11 Determine the current status of the entity's use of Information Technology to support its business processes	3.9 IT resource investment, use and allocation practices, including prioritization criteria, for alignment with the organization's strategies and objectives by using CAPEX and OPEX models.
3.12 Evaluate monitoring and assurance practices and the ways to measure and manage IT performance and costs through use of Key Goal Indicators, Key Goal Indicators including balance score cards, strategic score cards etc. to ensure timely reporting and monitoring.	3.11 Performance management systems including performance measures, KGI, KPI, Balanced score cards, strategic score cards etc.
3.13 Review the process of IT Infrastructure management, IT operational procedures and practices, service management practices, outsourcing, end-user procedures, IT service help desk, problem including incidence Management, Problem Management, Change Management, Configuration Management, Capacity Management and Performance Management.	3.10 IT operational procedures and practices, service management practices, outsourcing, end-user procedures, IT service help desk, escalation matrix, etc.
3.14 Evaluate IT management and monitoring of controls (e.g., continuous monitoring, QA) for compliance with the organization's policies, standards and procedures	3.5 IT management and monitoring of controls (e.g., continuous monitoring, QA) for compliance with the organization's policies, standards and procedures
3.15 Review enterprise controls to ensure compliance with internal and external regulatory requirements and external service providers such	3.12 Internal compliance/external national and international regulatory requirements and external service

as SOX, Clause 49 Listing requirements, Information Technology Act, etc.	providers such as SAS, Clause 49 Listing requirements, Information Technology Act, etc.

Knowledge Statement Reference Guide

Each knowledge statement is explained in terms of underlying concepts and relevance of the knowledge statement to the ISA Candidate. It is essential that the candidate understand the concepts. The knowledge statements are what the IS Auditor must know in order to accomplish the tasks. Consequently, only the knowledge statements are detailed in this section. The sections identified in the matrices are described in greater detail in the following chapters.

- 3.1 Enterprise Governance, Corporate Governance, Governance of Enterprise IT and their relationship

Key Concepts	Reference
Enterprise Governance, Corporate Governance, Governance of Enterprise IT and their relationship,	Chapter 1 and 2

- 3.2 Using Standards, Frameworks and best practices such as COBIT, COSO, ISO 27001, ISO38500, ISO 31000 etc. for Governance and Management of IT in enterprises.

Key Concepts	Reference
COBIT, COSO, ISO 27001, etc.	Chapter 2

- 3.3 Implementing best practices of Enterprise Goals, IT enabled goals, process and activity goals, Key Goal indicators and Key performance indicators.

Key Concepts	Reference
Enterprise Goals, IT enabled goals, process and activity goals, Key Goal indicators and Key performance indicators.	Chapter 2 and Chapter 5

- 3.4 Aligning IT strategy with business strategy and the business processes for long-term and short-term.

Key Concepts	Reference
Aligning IT strategy with business strategy	Chapter 5

- 3.5 IT management and monitoring of controls (e.g., continuous monitoring, QA) for compliance with the organization's policies, standards and procedures

Key Concepts	Reference
Continuous monitoring, QA for compliance with the organization's policies, standards and procedures	Chapter 2, 3 and 4

- 3.6 Value proposition of IT investments including Capex and Opex models

Key Concepts	Reference
Capex and Opex models	Chapter 6

- 3.7 Key enablers of Governance and Management of IT such as relevant: principles, policies and framework, processes, organisation structure, culture, ethics and behaviours and resources (information, services, infrastructure and applications, people, skills and competencies).

Key Concepts	Reference
Key enablers of Governance and Management of IT	Chapter 1 and 2

- 3.8 Enterprise Risk Management, Risk management practices, Risk mitigation strategy

Key Concepts	Reference
Enterprise Risk Management, Risk management practices, Risk mitigation strategy	Chapter 2

- 3.9 IT resource investment, use and allocation practices, including prioritization criteria, for alignment with the organization's strategies and objectives by using CAPEX and OPEX models.

Key Concepts	Reference
IT resource investment, CAPEX and OPEX models.	Chapter 6

Module 3

- 3.10 IT operational procedures and practices, service management practices, outsourcing, end-user procedures, IT service help desk, escalation matrix, etc.

Key Concepts	Reference
Service management practices, outsourcing, end-user procedures, IT service help desk, escalation matrix, etc.	Chapter 6

- 3.11 Performance management systems including performance measures, KGI, KPI, Balanced score cards, strategic score cards etc.

Key Concepts	Reference
Performance measures, KGI, KPI, Balanced score cards, strategic score cards etc.	Chapter 5

- 3.12 Internal compliance/external national and international regulatory requirements and external service providers such as SAS, Clause 49 Listing requirements, Information Technology Act, etc.

Key Concepts	Reference
SOX, Clause 49 Listing requirements, Information Technology Act, etc.	Chapter 1, 2 and 3

SECTION 2: CONTENTS

CHAPTER 1: CONCEPTS OF GOVERNANCE AND MANAGEMENT OF INFORMATION SYSTEMS

Learning Objectives

The objective of this chapter is to provide an overview of the concepts and practice of governance and management of information systems from the perspective of corporate and business governance. Governance is built on the premise the effective enterprise risk management is implemented encompassing all key IT risks adapting a holistic approach and internal control process is used for effective risk management. Regulations require mandatory certification of such implementation by management as well as auditors. Governance also facilitates achieving enterprise objectives with much more certainty. The linkage of governance with enterprise risk management, governance of enterprise IT (GEIT) and internal controls is explained. A step by step methodology for implementing GEIT is outlined. IS Auditors need to review whether the implementation of GEIT has been done followed a structured approach and whether this has resulted in envisaged value to the enterprise.

1.1 Introduction

The need for governance and management of information systems can be assessed from the simple fact that today technology is all pervasive. Organisations are so dependent on Technology that its failure will bring all key operations to a complete halt. On the positive side, technology facilitates organisations to offer products or services to anyone across the globe. The fundamental principle in the current business environment is to use technology to enable users to access information anytime, anywhere, anyhow by anyone. The objective is to provide information access to all stakeholders online with real-time access and update. This is done using enabling technology such as the network, Internet, hardware, operating system software, database, applications and browser. Modern Technology is empowered by the cloud and internet access through wireless broadband. Technology is only an enabler but the backbone for this has to be robust systems and processes for the information systems. Hence, it is critical to ensure that organisations embed Governance and management processes and other enablers in the technology deployed. This will ensure that various stakeholder requirements are met and the management at all levels are able to use technology to perform their responsibilities. It is important to comply with the requirements of corporate governance or enterprise governance by implementing Governance of Enterprise IT, enterprise risk management using appropriate risk management strategy and internal control systems. This chapter outlines these concepts and provides overview of how to implement GEIT

1.2 Organisation of chapters

The chapters (1 to 6) in Section 2 of this module are organized in a logical sequence to enable understanding of the subject of Governance and Management of Information Systems in a simple and structured manner. It is advisable to read the chapters in the same sequence as the chapters are arranged with a logical flow and move from concepts to practice with specific examples. The objective of this module is to: “Evaluate structures, policies, procedures, practices, accountability mechanisms and performance measures for ensuring Governance and management of Information Technology, risk management and compliance as per internal and external stakeholder requirements”. It is critical to adopt and adapt best practices to cover these key areas. Hence, there is heavy reliance on best practice frameworks. As the primary focus of this module is on Governance of Enterprise IT (GEIT) and its implementation at macro to micro level covering GRC and related management practices, the best practices guidance from COBIT 5 has been extensively referenced in this module as it is only framework for GEIT.

Chapter 1 titled: “Governance and Management of Information systems” provides an overview of the concepts and practice of governance and management of information systems from the perspective of corporate and business governance and explains the relationship between corporate governance, enterprise governance, GEIT, Enterprise Risk Management, IT risk management and internal controls. It also provides generic guidance on implementing GEIT.

Chapter 2 titled: “GRC frameworks and Risk Management Practices” provides an overview of key GRC frameworks and also elaborates key concepts of risk management from strategy to operations. It explains the relationship between GEIT and GRC and how implementing GEIT will help in meeting GRC requirements. The principles and enablers of COBIT 5 with specific relevance to how it meets risk management have been explained. Understanding concepts and practice of risk management is critical for implementing any GRC framework and also to meet compliance requirements. Hence, all the key concepts of risk management have been explained.

Chapter 3 titled: “GEIT and GRC” provides an overview of the need for GEIT and how GRC requirements of compliance can be implemented using GEIT framework such as COBIT 5 and other related best practices.

Chapter 4 titled: “Key enablers of GEIT” discusses the seven key enablers of GEIT which facilitate the successful achievement of enterprise goals and IT enabled goals. Each of the seven enablers have been discussed in terms of the characteristics and components so that implementation as required is easier. The relevance and relationship of each of these enablers and how they can be implemented in an integrated manner have been explained.

Chapter 5 titled: “Performance Management Systems” provides an overview of performance management systems with specific details of goals cascade from COBIT 5 and also explains the principles of Balanced Scorecard and Strategic Scorecard. It explains the concepts of goal setting, various types of goals and linkage of goals from enterprise goals to IT related goals and process

goals. Further, principles of Balanced Scorecard have been explained. An overview of strategic scorecard, maturity model and quality management are also provided.

Chapter 6 titled: “Implementing Governance and Management practices” outlines the systematic approach to implementing GEIT detailing the phases and what is required to be done in each of the phases. Further, it highlights the distinction between Governance and Management. This chapter also explains and illustrates how to implement identified Governance and Management practices in specific areas. It also provides methodology for scoping IS assurance and consulting assignments using COBIT 5 processes.

1.3 Key Concepts of Governance

Enterprises whether they are commercial or non-commercial, exist to deliver value to their stakeholders. Delivering value is achieved by operating within value and risk parameters that are acceptable and advantageous, and by using resources including IT responsibly. In the rapidly changing environment that most enterprises operate in, swift direction setting and agility to change are essential. Senior management is responsible for ensuring that the right structure of decision-making accountabilities are shared among many people in the enterprise and when accountability is shared, governance comes into play. Governance is “the combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.” Governance should be in place to ensure IT supports the strategies and objectives of the organization. The relationship of enterprise Governance and Corporate Governance with IT governance (GEIT) is depicted below.

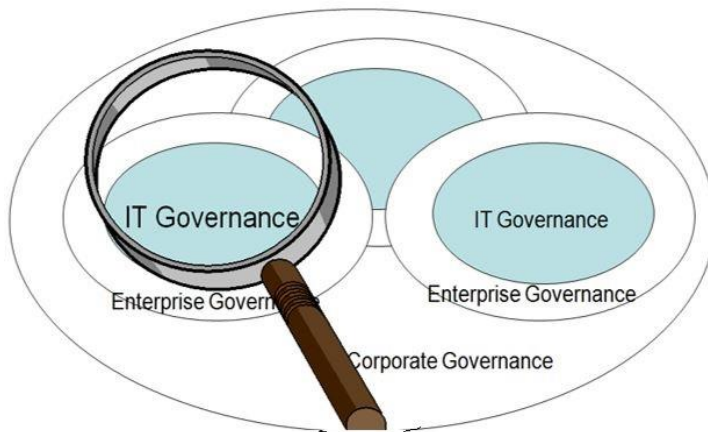


Figure 1.1: Relationship of types of Governance

1.3.1 Enterprise Governance

ISO/IEC 38500 defined Governance as: “The system by which organisations are directed and controlled”. A governance system typically refers to all the means and mechanisms that will enable multiple stakeholders in an enterprise to have an organized mechanism for evaluating options, setting direction and monitoring compliance and performance, in order to satisfy specific enterprise objectives. Enterprise governance can be defined as: ‘The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization’s resources are used responsibly.’ Enterprise governance is an overarching framework into which many tools and techniques and codes of best practice can fit. Examples include codes on corporate governance and financial reporting standards.

1.3.2 Corporate Governance

Corporate governance refers to the structures and processes for the direction and control of companies. Corporate governance is defined as the system by which a company or enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance. Corporate governance concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders. Good corporate governance contributes to sustainable economic development by enhancing the performance of companies and increasing their access to outside capital. It is about doing good business by ensuring compliance and protecting shareholders’ interest.

Good corporate governance requires sound internal control practices such as segregation of incompatible functions, elimination of conflict of interest, establishment of audit committee, risk management and compliance with the relevant laws and standards including corporate disclosure requirements. These are intended to guide companies to achieve their business objectives in a manner such that those who are entrusted with the resources or power to run the companies to meet stakeholder needs without compromising the shareholders’ interest. Legally, the directors of a company are accountable to the shareholders for their actions in directing and controlling the business, and for the actions of the company’s employees, who are in the position of trust to discharge their responsibilities in the best interest of the company. Corporate governance is thus necessary for the purpose of monitoring and measuring their performance and is mandated by regulations across the world and across various industries.

1.3.3 Need for Corporate Governance

Although Governance is not new for enterprises, a spate of frauds in the corporate sector involving large enterprises across the world including India in the last two decades have awakened regulators to the need for mandating the implementation of corporate governance integrated with Enterprise Risk Management and Internal controls. The concept of Corporate Governance has

succeeded in attracting a great deal of public interest because of its importance for the economic health of companies, protecting the interest of stakeholders including investors and the welfare of society, in general.

Corporate Governance has been defined as the system by which business corporations are directed and controlled. The corporate governance structure specifies the distribution of rights and responsibilities among different participants in the corporation, such as, the Board, management, shareholders and other stakeholders, and spells out the rules and procedures for making decisions on corporate affairs. The requirements for corporate governance are built on the principles of governance and encompass all levels of management including specific responsibility of board and senior management. Corporate Governance is focused on protecting the interests of various stakeholders and is compliance oriented. Although the terms corporate governance and enterprise governance are quite often used inter-changeably, it can be said that corporate governance is applying the principles of enterprise governance to corporate structure of enterprises. Some of the key concepts of corporate governance are:

- Clear assignment of responsibilities and decision-making authorities, incorporating an hierarchy of required approvals from individual employees to the board of directors;
- Establishment of a mechanism for the interaction and cooperation among the board of directors, senior management and the auditors;
- Implementing strong internal control systems, including internal and external audit functions, risk management functions independent of business lines, and other checks and balances;
- Special monitoring of risk exposures where conflicts of interest are likely to be particularly great, including business relationships with borrowers affiliated with the bank, large shareholders, senior management, or key decision-makers within the firm (e.g. vendors);
- Financial and managerial incentives to act in an appropriate manner offered to senior management, business line management and employees in the form of compensation, promotion and other recognition; and
- Appropriate information flows internally and to the public. For ensuring good corporate governance, the importance of overseeing the various aspects of the corporate functioning needs to be properly understood, appreciated and implemented.

1.4 Corporate Governance and Regulatory requirements

Corporate governance in India is evolving, primarily due to regulatory requirements, but also, to some extent, due to each enterprises specific needs and context. The objectives of corporate governance are fulfilled by setting up an appropriate structure and functioning mechanisms for the board of directors and audit committees, as laid down by the Companies Act, 1956. It is critical for each enterprise to establish its own specific governance system based on its own specific constraints and business culture.

The Companies Act, 2013 outlines the need for mandatory Internal Audit and reporting on Internal Financial Controls [sections 138]. The Act requires certain new aspects which need to be covered in an auditors' report which include: "whether the company has adequate internal financial controls system in place and the operating effectiveness of such controls [section 143(3) (i) of the 2013 Act]. Further, the Act deals extensively on the issue of fraud (section 447) and has for the first time defined fraud. The new regulations make it more imperative for management to implement a system of governance integrated with risk management and internal control systems. As IT is a key enabler of enterprise processes, risk management and controls has to consider technology and hence the need for implementing a holistic approach of Governance of enterprise IT (GEIT) using global best practices and frameworks.

The Information Technology Act amended in 2008 introduced new provisions which are specifically applicable to corporates, provisions relating to maintaining privacy of information and imposed compliance requirements on management with penalties for non-compliance. These requirements have to be considered as part of compliance by corporates and individuals as applicable. Please refer to module-2 for more details of these requirements. A copy of the IT Act 2000, amendments of 2008 and the related rules are provided as reference material in the DVD of the course.

Corporate Governance is a system by which companies are directed and controlled by the management in the best interest of the stakeholders and others ensuring greater transparency and better and timely financial reporting. The Board of Directors are responsible for governance of their companies. SEBI introduced a mandatory audit to ensure that this is maintained as per its norms by all listed companies as part of corporate governance and came up with an updated Clause 49 to address this requirement. Although Clause 49 primarily focuses on corporate governance, there are two key sections: Clause 49 IV (C) and Clause 49 V that make it imperative for listed companies to implement Governance of Enterprise IT.

Clause 49 IV (C) Board Disclosures on Risk Management requires every listed company to lay down procedures to inform board members about the risk assessment and minimization procedures. These procedures must be periodically reviewed to ensure that executive management controls risk through means of a properly defined framework. Indian companies often adopt a combination of home-grown, in-house practices and globally recognized frameworks for risk management. The ideal approach would be to adopt a globally accepted risk management framework such as COSO, which provides a framework for enterprise risk management, and then integrate the local practices as relevant. The amendments effected in Clause 49 V (C) and (D) clearly bring out:

- The responsibility entrusted to the CEO/CFO is in relation to establishing and maintaining internal controls for financial reporting.
- The CEO/CFO has to assert that he/she has evaluated the effectiveness of internal control systems of the company pertaining to financial reporting.

- The CEO/CFO certificate will further state the manner in which deficiencies (if any) in the design or operation of such internal controls have been disclosed to the auditors and the audit committee.
- The CEO/CFO certification will also state the steps they have taken or proposed to take to rectify these deficiencies in the design or operation of such internal control pertaining to financial reporting.

As the management is vested with responsibility of running the business, it implies that they have to take reasonable steps to ensure the implementation of the conditions of corporate governance as stipulated in clause 49 of the Listing Agreement. The auditors' responsibility in certifying conditions of corporate governance relate to verification and certifying factual implementation of conditions of corporate governance as stipulated in the above clause. Such certification is neither an audit nor an expression of opinion on financial statements of the entity. In the US, The Sarbanes Oxley Act (SOX) focuses on the implementation and review of internal controls as relating to financial audit. It highlights the importance of evaluating the risks, security and controls as related to financial statements. In an IT environment, it is important to understand whether the relevant IT controls are implemented in the relevant computerised information systems. The overall reliability of these controls would be dependent on the overall risk management strategy, risk appetite of the management, use of best practices and various other enablers.

Corporates across the world for SOX compliance have used COSO (www.coso.org) and COBIT (www.isaca.org/cobit) as the primary framework and best practices for implementing governance, risk management and internal controls. The objective of COSO is to improve the quality of financial reporting through business ethics, effective internal control and corporate governance. The COSO 2013 framework outlines 17 principles of internal controls and highlights the need for management to implement a system of risk management at the enterprise level. COBIT is a comprehensive framework for the governance and management of enterprise IT, comprising five domains, 37 IT processes and over 200 management practices and activities divided into governance and management processes. COBIT has been used as the business framework for implementing Governance of enterprise IT. Together COSO and COBIT can be used for implementing a system of enterprise risk management integrated with technology ensuring both conformance and performance. Although, there is need for implementing Governance, risk management and controls from regulatory perspective, stakeholders would be looking at performance perspective also in such implementation. The objective of the Governance of Enterprise IT is to ensure that organisations can ensure business value from their investment in IT, while managing risk.

Good corporate governance is vital for all types of enterprises big or small in view of the benefits which accrues due to its implementation. Governance helps in ensuring that control failures are mitigated appropriately. However, good corporate governance on its own cannot make an organisation successful. There is a danger that insufficient attention is paid to the need for organisations to create wealth or stakeholder value. Strategy and performance are also important. The key message of enterprise governance is that an organisation must balance the two

dimensions of conformance and performance needs to ensure long-term compliance and success. This requires that governance is ideally implemented with the right balance of conformance and performance dimensions. These two dimensions are briefly outlined here.

1.4.1 Conformance or Corporate Governance Dimension

The conformance dimension of governance provides a historic view and focuses on regulatory requirements. This covers corporate governance issues such as: roles of the chairman and CEO, role and composition of the board of directors, Board committees, Controls assurance and Risk management for compliance. Regulatory requirements and standards generally address this dimension with compliance being subject to assurance and/or audit. There are established oversight mechanisms for the board to ensure that good corporate governance processes are effective. These might include committees composed mainly or wholly of independent non-executive directors, particularly the audit committee or its equivalent in countries where the two tier board system is the norm. Other committees are usually the nominations committee and the remuneration committee. The Sarbanes Oxley Act of US and the Clause 49 listing requirements of SEBI are examples of providing for such compliances from conformance perspective.

1.4.2 Performance or Business Governance Dimension

The performance dimension of governance is pro-active in its approach. It is business oriented and takes a forward looking view. This dimension focuses on strategy and value creation with the objective of helping the board to make strategic decisions, understand its risk appetite and key performance drivers. This dimension does not lend itself easily to a regime of standards and assurance as this is specific to enterprise goals and varies based on the mechanism to achieve them. It is advisable to develop appropriate best practices, tools and techniques such as balanced scorecards and strategic enterprise systems that can be applied intelligently for different types of enterprises as required. The conformance dimension is monitored by the audit committee. However, the performance dimension in terms of the overall strategy is the responsibility of the full board but there is no dedicated oversight mechanism as comparable to the audit committee. Remuneration and financial reporting are scrutinized by a specialist board committee of independent non-executive directors and referred back to the full board. In contrast, the critical area of strategy does not get the same dedicated attention. There is thus an oversight gap in respect of strategy. One of the ways of dealing with this lacunae is to establish a strategy committee of similar status to the other board committees which will report to the board. The performance dimension in terms of how to implement performance management system is covered in more detail in chapter 5 of this module.

1.5 Enterprise governance framework

Fundamentally, enterprise governance is the entire accountability framework of the organisation, with the twin dimensions of **conformance and performance** of processes, with more emphasis on the latter. In implementing enterprise governance, it is important to use best practices developed by various professional associations and also use relevant guidelines issued by regulatory bodies. Enterprise governance in general is broader and encapsulates corporate governance, performance management, internal control and enterprise risk management. In implementing controls, it is important to adapt a holistic and comprehensive approach. Hence, ideally it should consider the overall business objectives, processes, organization structure, technology deployed and the risk appetite. Based on this, overall risk management strategy has to be adapted, which should be designed and promoted by the top management and implemented at all levels of enterprise operations as required in an integrated manner. The objective of implementing enterprise governance is to ensure that the governance objectives of benefits realisation, risk optimisation and resource optimisation are achieved considering the stakeholder needs and which leads to value creation for the enterprise. This is depicted in the figure 1.2 given here.

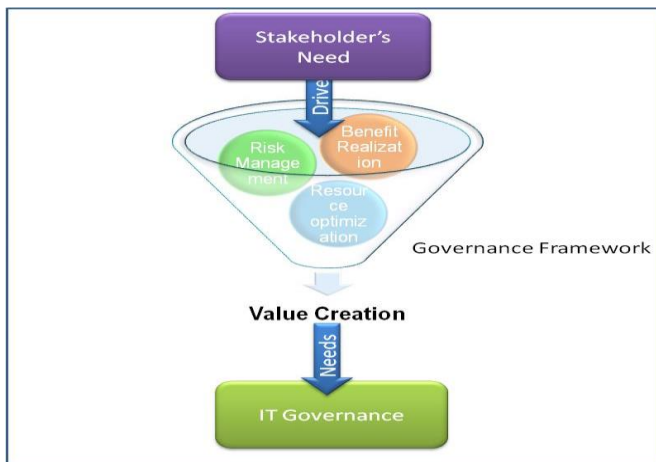


Figure 1.2: Governance framework and Drivers

Regulations require enterprises to adapt a risk management strategy, which is appropriate for the enterprise. Hence, the type of controls implemented in information systems in an enterprise would depend on this risk management strategy. There are multiple frameworks for implementing risk management. The next chapter covers details of some of the key concepts and approaches for implementing risk management in enterprises.

1.6 Enterprise Risk Management

Enterprise risk management deals with risks and opportunities affecting value creation or preservation and is defined by the Institute of Internal Auditors as: “Enterprise risk management is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.” The management to ensure that the enterprise risk management strategy considers information and its associated risks while formulating IT security and controls as relevant. IT security and controls are a sub-set of the overall enterprise risk management strategy and encompass all aspects of activities and operations of the enterprise

1.7 Governance of Enterprise IT (GEIT)

Governance of Enterprise IT is a sub-set of corporate governance and facilitates implementation of a framework of IS controls within an enterprise as relevant and encompassing all key areas. The primary objectives of GEIT are to analyze and articulate the requirements for the governance of enterprise IT, establish and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives. The key benefits of using GEIT is that it provides a consistent approach integrated and aligned with the enterprise governance approach. It ensures that IT-related decisions are made in line with the enterprise's strategies and objectives and the IT-related processes are overseen effectively and transparently.

Implementing a GEIT framework helps in better compliance with legal and regulatory requirements and ensures that the governance requirements for board members are met. A few decades back, IT was one of the wagons but now IT is the engine propelling enterprise growth. IT interfaces all aspects of the enterprise and not just transaction processing. It can be said that IT has become inseparable from the business. Hence, in a modern enterprise, IT has moved from being a mere service provider to a strategic partner which helps enterprises in achieving both competitive and strategic advantage. Considering this huge dependence on IT and the fact that internal controls are embedded in IT and effective risk management can be achieved by using IT, implementing Governance of Enterprise IT has become imperative for a modern enterprise. Regulatory agencies, professional bodies and associates issue guidelines on use of generic and specific best practices. For example, the Reserve Bank of India issues guidelines covering various aspects of secure technology deployment. These guidelines are prepared based on various global best practices such as COBIT and ISO 27001. The Information technology Rules outlines the need for maintaining secrecy of personal and sensitive information and identifies ISO 27001 as best practices framework for implementing best practices.

1.7.1 Governance Objectives

It is important to identify specific governance objective in implementing GEIT. Generally, the focus area of implementing GEIT as specified in COBIT 5 are these three governance objectives:

- **Benefit realisation:** Creating new value for the enterprise through IT, maintaining and increasing value derived from existing IT investments, and eliminating IT initiatives and assets that are not creating sufficient value for the enterprise. The basic principles of IT value are delivery of fit-for-purpose services and solutions on time and within budget, and generating the financial and nonfinancial benefits that were intended. The value that IT delivers should be aligned directly with the values on which the business is focussed and measured in a way that transparently shows the impacts and contribution of the IT-enabled investments in the value creation process of the enterprise.
- **Risk optimisation:** Addressing the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. IT-related business risk consists of IT-related events that could potentially impact the business. While value delivery focuses on the creation of value, risk management focuses on the preservation of value. The management of IT-related risks should be integrated within the enterprise risk management approach to ensure a focus on IT by the enterprise and be measured in a way that transparently shows the impacts and contribution of IT-related business risk optimisation in preserving value.
- **Resource optimisation:** Ensuring that the right capabilities are in place to execute the strategic plan and sufficient, appropriate and effective resources are provided. Resource optimisation ensures that an integrated, economical IT infrastructure is provided, new technology is introduced as required by the business, and obsolete systems are updated or replaced. It recognises the importance of people, in addition to hardware and software, and, therefore, focuses on providing training, promoting retention and ensuring competence of key IT personnel.

1.7.2 Internal Controls

Regulatory requirements and best practices framework require internal control system to be an integral part of enterprise risk management and governance system. Hence, it is important to understand how internal control requirements are generally implemented through management systems. “An effective internal control system is an essential part of the efficient management of a company” established through the governance system. Such systems should establish an adequate system of internal control to “support business requirements for effective and efficiency of operations, reliability of information and compliance with laws and regulations.” While appropriate internal control is a required outcome of sound governance and a necessary supporting element of effective governance, it does not in itself represent governance.

Any audit whether it is compliance or IS oriented would require understanding of internal control system implemented within the enterprise. Internal control is an element of the management

system rather than an aspect of the governance system. Internal control must be supported by effective risk management process with internal control arrangements determined by the enterprises level of risks. Risk management requires establishing a sound system of risk oversight and management and internal control. The Securities and Exchange Commission (SEC) of USA rules define “internal control over financial reporting” as a “process designed by, or under the supervision of, the company’s principal executive and principal financial officers, or persons performing similar functions, and effected by the company’s board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

- Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the company;
- Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company;
- Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company’s assets that could have a material effect on the financial statements.

COSO 2013 can be used as the over-arching framework for implementing risk management and internal controls and COBIT 5 framework can be used under COSO as umbrella framework for implementing Governance of Enterprise IT. Other frameworks and management policies can be implemented under these two frameworks to ensure both conformance and performance. Implementing internal controls systems is imperative for effective governance both from regulatory and management perspective. As auditors are primarily control experts, they can review the availability, adequacy and appropriateness of implemented controls and provide appropriate recommendations for mitigating control weaknesses. IS Auditors may be required to review and evaluate the system of governance, risk management and controls as embedded in IT and information systems and provide assurance on the effectiveness to meet established objectives.

1.7.3 Implementing GEIT

Governance of Enterprise IT is built on the principles of Governance but applied to IT. Hence, implementing GEIT in organizations requires understanding concepts of Governance, IT deployment and how IT can be used to implement Governance. GEIT is a blend of these concepts. Implementing GEIT requires establishing the right structures with defined roles and responsibilities, implementing relevant processes using best practices as required and establishing the relational mechanisms by active participation of relevant stakeholders as required in a collaborative effort to achieve enterprise goals.

The improvement of governance of enterprise IT is increasingly recognised by top management as an essential part of enterprise governance. Effective GEIT will result in improved business performance as well as compliance to external requirements, yet successful implementation remains elusive for many enterprises. Effective GEIT requires a range of enablers with carefully prescribed roles, responsibilities and accountabilities that fit the style and operational norms specific to the enterprise. Implementing GEIT from conformance (corporate) perspective would require viewing the enterprise at macro level and consider not only the business but also the external linkages. In case of performance (business) the enterprise has to be viewed at internal level and the focus on the processes and activities within the enterprise.

The key areas of focus in implementing GEIT are summarised in the table here.

Table 3.1: Implementing Governance from Conformance or performance perspective

Area	Conformance (Corporate)	Performance (Business)
Scope	Board Structure, Roles and Remuneration	Strategic decision making and value creation
Addressed via	Standards and Codes	Best practices, tools and techniques
Auditability	Can be audited for compliances	Not easily auditable
Oversight Mechanism	Audit Committee	Balance score cards

The COBIT framework can be used for implementing GEIT from any/both the above perspectives. The seven key enablers of GEIT which are required for effective implementation are described in next chapter. Overall, GEIT requires structures, processes and relational mechanisms.

The components and relationship of IT Governance framework are outlined in figure given below.

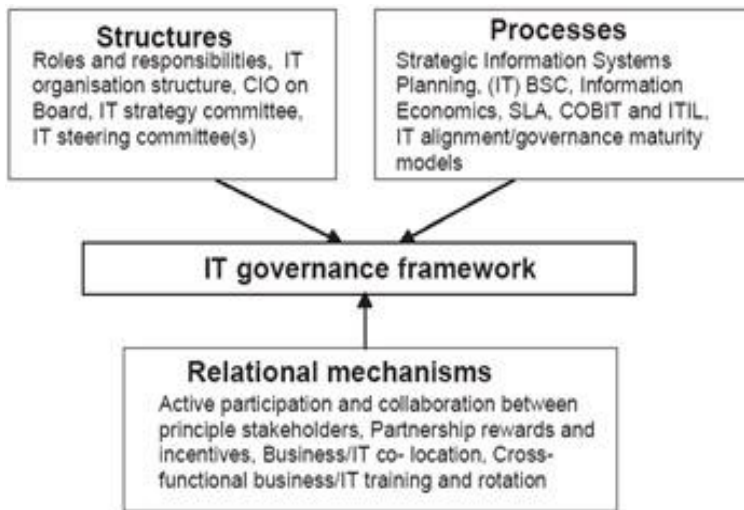


Figure 1.3: Components of Governance framework

The structures involve the organisation, and location of the IT function, the existence of clearly defined roles and responsibilities and a diversity of IT/ business committees. The processes refer to strategic decision making, strategic information systems planning (SISP) and monitoring, control, and process frameworks. The relational mechanisms finally complete the governance framework and are critical for attaining and sustaining business-IT alignment, even when the appropriate structures and processes are in place. These mechanisms include business/IT participation, strategic dialogue, training, shared learning, and proper communication. COBIT 5 which is the business framework for implementing GEIT can be used by enterprises of all sizes and types and regardless of technology deployment.

1.7.4 Guidelines for implementing GEIT

The primary objective of implementing GEIT is to ensure IT delivers value to the business and helps in mitigation of IT-related risk. This is enabled by the availability and management of adequate resources and the measurement of performance to monitor progress towards the desired goals. The COBIT 5 implementation guide provides a systematic approach with defines phases and specific roles and responsibilities for implementing GEIT. This approach can be customized and used by any organisation regardless of size, nature of business, sector or technology used.

1.7.5 Systemic approach to implementing GEIT

Research studies have established that effective implementation of GEIT maximises the contribution made by IT to organisational success. There can be multiple approaches to implementing GEIT as this varies with the needs of the enterprise and the specific framework used. It is advisable to adapt a systematic and well-proven approach as outlined in some of the best

practices and frameworks. IT solution providers and regulators also provide their own approaches for implementing GEIT. It is important to remember that the focus should be first on implementing the systems and processes first and then automating rather than expecting that automation will implement systems and processes as required. As explained earlier, frameworks such as COSO and COBIT 5 also provide a systematic approach for implementing the relevant frameworks. The technology and business frameworks can be easily integrated under these frameworks. We are giving below some general guidelines on implementing GET which can be adapted as required.

1. Aligning IT Goals with Business Goals

Achieving better governance starts with the business, and more specifically with understanding its strategy and goals. IT management should be involved early in the business strategy definition process, especially in those companies that are highly dependent on IT. The IT goals should be aligned to the business goals. The IT strategy should be an IT blueprint of the business strategy plan. The IT goals, set out in the IT strategy plan should clearly support the achievement of one or more business goals. It is the responsibility of the board and senior management to ensure that the IT strategy is aligned with the business strategy. This could be achieved through:

- Clear business goals, communicated to the entire organisation
- Early involvement of IT in business strategy process
- Align IT goals to business goals
- Derive IT strategy from business strategy

2. Formalise and implement right IT Governance Processes

After aligning the IT goals with the business goals, it is important to implement required set of efficient and effective IT governance and management processes. Using best practices such as COSO and COBIT will facilitate such implementation. It is important to select the most critical process based on business priorities, assign process owners, develop metrics and monitor the achievement of process as per set objectives.

3. Establish required IT Organisation and decision structure

Effective Governance of enterprise IT is determined by the way the IT department is organised and where the IT decision-making authority is located within the organisation. The responsibility for governance rests with the board of directors as they are responsible for evaluating, directing and monitoring the governance processes as per stakeholder requirements. They have to establish the right management structure with the C suite to ensure there is proper collaboration between business and IT department.

4. Involve Board of Directors/Executive Management in IT related matters

Governance initiatives may be initiated by IT or internal auditors but the overall responsibility vests with the board who assign specific responsibility to senior management from both business and IT. The executive management has to be aware and actively participating in the existing governance activities. IT topics and decisions should regularly appear and be discussed in executive committees or on board level, especially in organisations where IT plays a crucial role in keeping the business running. Even when the CIO is not a part of the executive committees, he should be represented by another executive member or he/she could be invited whenever an IT related topic is handled.

5. Govern and manage roles and responsibilities

The board should ensure that governance and management structures are established involving the organisation, the location of the IT function, the existence of clearly defined roles and responsibilities and a diversity of IT/business committees. The organisation structure should specify clear responsibilities defined towards the business they work for, and this throughout all levels, including the CIO and IT management. To make sure individuals adopt and execute upon their roles and responsibilities, a process of 'formal' evaluation and regular process of review has to be implemented as part of performance management system.

6. Establish IT Strategy and IT Steering Committee

Effective committees created at the right level with clearly defined roles and responsibilities play an important role in establishing ensuring alignment of IT with business which is key to successful implementation of GEIT. IT strategy committee has to operate at the board level and the IT steering committee has to operate at executive level with each committee having specific responsibility, authority and membership. The roles and responsibilities of these two key committees are explained in later chapter of this module.

7. Plan, align and manage IT enabled Investment as a Portfolio

Successful implementation of GEIT requires organisation to effectively their IT enabled investments throughout the economic life cycle of the projects using best practices of project management as required. Clear responsibility has to be allocated between IT who would be responsible for execution of IT enabled projects but business has to be responsible for analysing the anticipated benefits and making decisions.

8. Implement Performance Measurement system integrated with regular process

Measuring and monitoring the different IT processes at different levels is very important to review whether the set required service levels are met as set by the functional management. Goals have to be set at each of the levels starting from activity to process and linked to IT goals which are in turn linked to business goals. Metrics have to be set and monitored to ensure implementation and corrective action has to be taken as required. The performance management system could be integrated using the balanced scorecard technique with the complete set of metrics which is consolidated for different levels and areas as required. This is explained in detail in chapter 5.

9. Establish Sustainability through support, monitoring and regular communication

IT is most important support function to business activities as most of the service now a days are delivered through IT. Aligning business goals with IT goals requires ongoing and constant interaction between IT and business function. There has to be effective collaboration and interaction between business and IT. This requires a constant communication channel and mechanism to encourage the relationship between business and IT.

1.8 Summary

This chapter has provided an overview of concepts and practice of various aspects of Governance such as enterprise governance, corporate governance and GEIT. The interfaces between the different levels at which governance is implemented have also been highlighted. As IT is a key enabler of organisation processes, it is critical to implement GEIT as an integral part of governance. The regulatory and management requirements for implementing governance start with clearly established objectives and require using a systematic approach and use of relevant best practices frameworks as required. Corporate Governance and GEIT are closely inter-linked with enterprise risk management and internal controls. Regulatory requirement mandate the implementation of governance, enterprise risk management and internal controls. Organisations are established with the objective of value creation. Hence, they will implement governance not only from conformance perspective but also to provide value to the organisation. Hence, the two dimensions of conformance and performance have to be balanced in implementing governance in enterprises. Guidelines for implementing GEIT have been explained through a generic guidelines starting from aligning IT strategy with enterprise strategy and ending with ensuring sustainability of GEIT implementation and thus making it an integral part of day to day process.

1.9 Questions

1. Who is responsible for establishing right structure of decision-making accountabilities?
 - A. Senior management
 - B. Operational management
 - C. Chief information officer
 - D. IT steering committee
2. The MOST important benefit of implementing Governance of Enterprise IT is:
 - A. Monitor and measure enterprise performance
 - B. Provide guidance to IT to achieve business objectives
 - C. Run the companies to meet shareholders' interest
 - D. Ensure strategic alignment of IT with business
3. The primary objective of Corporate Governance is:
 - A. Reduce IT cost in line with enterprise objectives and performance.
 - B. Optimise implementation of IT Controls in line with business needs
 - C. Implement security policies and procedures using best practices.
 - D. Increase shareholder value by enhancing economic performance.
4. The ultimate objective Governance of Enterprise IT is to ensure that IT activities in an enterprise are directed and controlled to achieve business objectives for meeting the needs of:
 - A. Shareholders
 - B. Stakeholders
 - C. Investors
 - D. Regulators
5. Which of the following is a key components of Corporate Governance?
 - A. Employee rights
 - B. Security policy
 - C. Transparency
 - D. Risk assessment
6. Enterprise governance and Governance of Enterprise IT governance requires a balance between:
 - A. compliance and return on investment expected by shareholders
 - B. profit maximization and wealth maximization as decided by board
 - C. IT risks and cost of implementing IT controls as set by IT
 - D. conformance and performance goals as directed by the board.

7. Business Governance helps the Board by enabling them to understand:
 - A. enterprise functions
 - B. risk assessment
 - C. key performance drivers
 - D. Key controls
8. The effectiveness of the IT governance structure and processes are directly dependent upon level of involvement of
 - A. Heads of Business units
 - B. Internal auditor department
 - C. Technology management
 - D. Board/senior management
9. Which of the following is one of the key benefits of GEIT?
 - A. Identification of relevant laws, regulations and policies requiring compliance.
 - B. Improved transparency and understanding of IT's contribution to business
 - C. Better utilization of human resources by using automation
 - D. Increased revenues and higher Return on investments.
10. Which of the following is the primary objective for implementing ERM?
 - A. Implement right level of controls.
 - B. Better availability of information.
 - C. Tighter security at lower cost.
 - D. Implement IT best practices.

1.10 Answers and Explanations

1. A. The senior management is responsible for ensuring right structure of decision-making accountabilities. The operational management is responsible for ensuring that operations of the enterprise are run as per enterprise policy. The chief information officer is responsible for ensuring IT enabled investments provide business value and the IT steering committee is responsible for steering IT enabled projects toward successful completion of objectives.

2. D. The MOST important benefit of implementing Governance of Enterprise IT is that it helps in ensuring strategic alignment of IT with business. Alignment of IT strategy in tune with enterprise strategy ensures value delivery from IT enabled investments. The monitoring and measuring of enterprise performance is one of the key processes of GEIT. GETI does not provide guidance to IT to achieve business objectives but provides overall framework and setting for IT to achieve business objectives. Although GEIT is often implemented from a regulatory perspective and

enables enterprises to meet corporate governance requirements, it does not directly focus on running the enterprises based on shareholders' interest. Shareholders are one of the key stakeholders whose objectives are considered while formulating enterprise goals.

3. B. The primary objective of Corporate Governance is to implement security policies and procedures using best practices. Corporate governance requirements are best met by using best practices which are globally accepted. The focus of implementing corporate governance is on ensuring regulatory compliance and this does not look at cost aspects. Hence, reducing IT cost in line with enterprise objectives and performance is not an objective. Further, optimise implementation of IT Controls in line with business needs has to be considered as part of GEIT and is not directly objective of corporate governance. There are multiple stakeholders whose interests are sought to be protected by regulations of corporate governance. One of the stakeholders are shareholders. However, the regulations do not consider how to increase shareholder value by enhancing economic performance but to protect their interests.

4. B. The ultimate objective Governance of Enterprise IT (GEIT) is to ensure that IT activities in an enterprise are directed and controlled to achieve business objectives for meeting the needs of the stakeholders. There are multiple stakeholders and GEIT requires balancing the needs of these stakeholders. Shareholders, Investors and Regulators are some of the stakeholders.

5. C. One of the key components of Corporate Governance is ensuring transparency. This promotes effective governance through establishing, communication and monitoring of performance. Employee rights are not the focus of corporate governance. Security policy as prepared by the IT as applicable for the enterprise is approved by the board. Corporate governance requirements do not provide any specific details of risk assessment but only outline need for implementing risk management as appropriate for the enterprise.

6. C. Enterprise governance and Governance of Enterprise IT governance requires a balance between IT risks and cost of implementing IT controls as set by IT. Risk appetite and Risk tolerance is set by the Board and this is based on risks which are acceptable and limit to which these are acceptable. The compliance and return on investment expected by shareholders is not relevant as shareholders do not have a stake in deciding this. The last two options about: profit maximization and wealth maximization as decided by board and conformance and performance goals directed by the board are translated through the overall enterprise strategy which is then translated into business and IT strategy.

7. C The primary objective of Business Governance is to ensure performance and hence the focus by Board is to understand and implement key performance drivers. The other options are related to operational areas which are dealt by management at their level as required.

8. D. The Board/senior management play the most critical role in ensuring the effectiveness of the IT governance structure and processes. Hence, the effectiveness of Governance is directly

dependent upon their level of involvement. The head of business units work on implementing the directions of the board and are focussed on management. The internal auditor department play an important role in evaluating how well IT governance is implemented but their role is providing guidance. The technology management is responsible for aligning IT strategy in line with the enterprise strategy and implementing IT solutions which help meet enterprise objectives.

9. C. Implementing GEIT requires active collaboration between the board/senior management in directing IT towards enterprise objectives and putting a governance framework in place. Hence, the key benefit of GEIT is the improved transparency and understanding of IT's contribution to business which is reflected in the performance management system. Although identification of relevant laws, regulations and policies requiring compliance is important in implementing GEIT, this is not the primary benefit. Directly, the focus of GEIT is neither on better utilization of human resources by using automation or on increased revenues and higher return on investments although they are considered as required.

10. A. The primary objective for implementing ERM is it helps in deciding and implementing the right level of controls. The other 3 options are indirect benefits of implementing ERM.

CHAPTER 2: GRC FRAMEWORKS AND RISK MANAGEMENT PRACTICES

Learning Objectives

As IT increasingly becomes a key enabler in enterprises of all types and sizes and there is transformation of enterprises from “Technology Oriented” to “Business and Technology oriented, governance and risk management become imperative to ensure value creation and compliance. In the first chapter, we have understood how GEIT implementation can help in balancing performance with conformance. Use best practices framework helps in balancing risk vs return by implementing the right level of security. Implementing GEIT principles is critical to strive and thrive in the highly intensive IT era. Governance frameworks provide the structure within which the management can effectively operate to deliver results as per set objectives. A governance framework typically set in motion by the board of directors defines the rules under which the management system operates to translate the board strategy into specific actions. Governance is about ensuring that the required authority and responsibility is allocated appropriately within the organisation. It defines the boundaries of decision making together with mechanism that ensures that performance is monitored and risks are identified and escalated so they are managed at the appropriate level. Risk management at enterprise level encompassing all levels and all areas is critical for successful implementation of governance. Governance, Risk and Compliance is a regulatory requirement and this can be effectively implemented using well established frameworks. There are a plethora of frameworks for implementing GRC and GEIT. This chapter provides overview of some of the key GRC frameworks and also elaborates key concepts of risk management from strategy to operations.

2.1 Introduction

IT is key enabler of enterprises and forms the edifice on which the information and information systems are built. Implementing Governance, risk management and internal controls is not only a management requirement but is also mandated by law. In India, Clause 49 listing requirements seek inter alia certification of governance, risks and control by auditors. In an IT environment embedding the right level of controls within the information systems to ensure that users can access required information securely and safely and as per business requirements is critical for survival. This not only ensures business success but is also a key requirement for the continued growth of the enterprise. In implementing internal controls in an IT environment, the legacy approach of considering IT and its contents as boxes to be secured by the IT department is fraught with extreme risk as the traditional methods of securing IT from perimeter perspective is no longer relevant. Users of IT need to access and use information from anywhere, anytime. There is need to adapt a macro level and architecture perspective for securing information and information systems. Hence,

both from regulatory as well as enterprise perspective, senior management have to be involved in providing direction on how governance, risk and control are implemented using a holistic approach encompassing all levels from strategy to execution. The Board of directors have to evaluate, direct and monitor effective use of IT to achieve enterprise objectives. This governance approach will ensure harnessing the power of information and information technology for achieving business objectives in addition to meeting regulatory requirements. Best practices framework provide management with distilled knowledge of experts and this can be customized to meet stakeholder requirements which include inter alia management and regulators. Management has to choose the right mix of frameworks for implementing governance, risk, security and controls. IS Auditors can assist management in implementing these frameworks in an advisory capacity or provide assurance on how well the GRC frameworks have been implemented to meet stakeholder requirements and provide recommendations for improvement. From regulatory perspective, management have to certify whether Risk management and internal controls have been implemented as per organisation needs and auditors have to certify whether this implementation is appropriate and adequate.

2.2 GRC frameworks

2.2.1 COSO

COSO is an Enterprise Risk Management-Integrated Framework which was first published by the Committee of Sponsoring Organisations (COSO) established by Treadway commission in 1992 to define the internal control framework for business organizations, particularly listed companies where the stakeholders are common people who invest in securities. The latest update of COSO is the COSO Framework 2013. COSO has developed the framework for internal controls focusing on designing of controls based on risk assessment. According to COSO framework internal control is defined as “a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives”. The Executive Summary of Internal Control: Integrated Framework provides a high-level overview of the 2013 Framework and is intended for the CEO and other senior management, boards of directors, and regulators.

The COSO framework 2013 formalizes the principles embedded in the original more explicitly, incorporates business and operating environment changes over the past two decades, and improves the Framework's ease of use and application. The 2013 Framework also makes it easier for management to see what's covered and where gaps may exist in their current SOX 404 compliance program. The Framework set out in detail, defining internal control, describing the components of internal control and underlying principles, and providing direction for all levels of management in designing and implementing internal control and assessing its effectiveness.

The 2013 Framework has three categories of objectives: operations, reporting, and compliance and consists of five integrated components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring activities. The Framework is adaptable to a given organization's structure, allowing customisation to consider internal controls from an entity, divisional, operating unit, and/or functional level, such as for a shared services center. The key role of management judgment in designing, implementing, and maintaining internal control, as well as assessing its effectiveness, is retained. A visual representation of COSO's Internal Control: Integrated Framework (i.e., the updated COSO Cube) is given here.

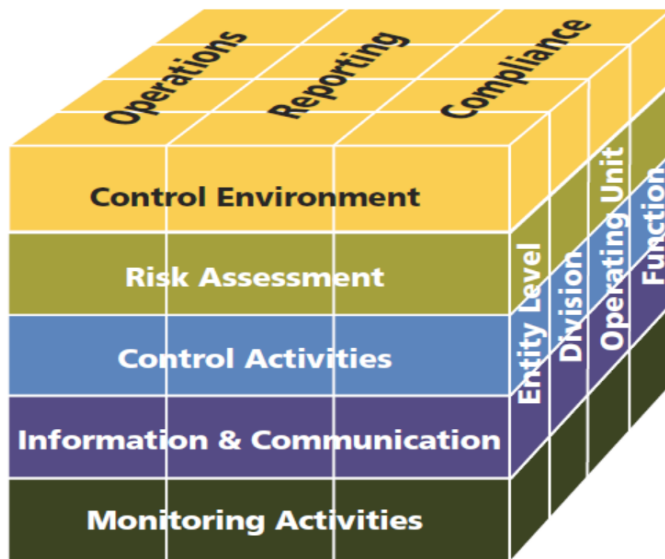


Figure 2.1: COSO 2013 Framework Cube

The COSO cube has 3 dimensions. The first dimension depicts internal controls and the 5 interrelated components. The second dimension depicts control objectives and third dimension provides controls at different levels of the enterprise. The titles of the 17 internal control principles organised by the five internal control component are given below:

Control Environment: For each business process, an organization needs to develop and maintain a control environment including categorizing the criticality and materiality of each business process, plus the owners of the business process.

- Demonstrates commitment to integrity and ethical Values
- Exercises oversight responsibility
- Establishes structure, authority, and responsibility
- Demonstrates commitment to competence
- Enforces accountability

Risk Assessment: Each business process comes with various risks. A control environment must include an assessment of the risks associated with each business process.

- Specifies suitable objectives
- Identifies and analyses risk
- Assesses fraud risk
- Identifies and analyses significant change

Control Activities: Control activities must be developed to manage, mitigate, and reduce the risks associated with each business process. It is unrealistic to expect to eliminate risks completely.

- Selects and develops control activities
- Selects and develops general controls over technology
- Deploys through policies and procedures

Information and Communication: Associated with control activities are information and communication systems. These enable an organization to capture and exchange the information needed to conduct, manage, and control its business processes.

- Uses relevant information
- Communicates internally
- Communicates externally

Monitoring: The internal control process must be continuously monitored with modifications made as warranted by changing conditions.

- Conducts ongoing and/or separate evaluations
- Evaluates and communicates deficiencies

The three main categories of Control objectives of COSO are:

1. **Operations objectives:** Relate to the achievement of the organization's mission and are based on management's choices relating to structure, industry considerations and the performance of the entity.
2. **Reporting objectives:** These are further divided into:
 - a. **External financial reporting objectives:** Relate to the organization's obligations for its financial statements.
 - b. **External non-financial reporting required objectives:** Include reporting on its internal control effectiveness and operational processes.
3. **Compliance objectives:** Relate to the laws and regulations that apply to the entity considering any foreign entities that are relevant.

Enterprises planning to implement COSO have to consider the five inter-related components and principles of internal control apply to the enterprise and adapt this as per specific requirements of the enterprise. The principles are generic and have to be customised as per stakeholder needs and as decided by the management. The involvement starts with the senior management setting the risk appetite and risk tolerance limits for the enterprise as whole.

Requirements for effective internal control

COSO 2013 clarifies requirements for effective internal control as follows:

- Effective internal control provides reasonable assurance regarding the achievement of objectives and requires that:
 - Each component and each relevant principle is present and functioning
 - The five components are operating together in an integrated manner
- Each principle is suitable to all entities; all principles are presumed relevant except in rare situations where management determines that a principle is not relevant to a component (e.g., governance, technology)
- Components operate together when all components are present and functioning and internal control deficiencies aggregated across components do not result in one or more major deficiencies
- A major deficiency represents an internal control deficiency or combination thereof that severely reduces the likelihood that an entity can achieve its objectives

COSO 2013 framework describes the role of controls to effect principles. The Framework does not prescribe controls to be selected, developed, and deployed for effective internal control. An organization's selection of controls to effect relevant principles and associated components is a function of management judgment based on factors unique to the entity. A major deficiency in a component or principle cannot be mitigated to an acceptable level by the presence and functioning of other components and principles. However, understanding and considering how controls effect multiple principles can provide persuasive evidence supporting management's assessment of whether components and relevant principles are present and functioning.

COSO is primarily a framework for implementing internal controls that IS auditor reviews for effectiveness. Identification of controls is based on level of risk mitigated by that controls, hence COSO focuses on Risk management as major area of the framework. However it does not provide how organizations should approach the risk assessment and control identification. Hence it is a high-level framework. Please visit www.coso.org for latest updates of COSO framework.

Clause 49 of the listing agreements issued by SEBI in India is on similar lines of SOX regulation and mandates inter alia the implementation of enterprise risk management and internal controls and holds the senior management legally responsible for such implementation. Further, it also provides for certification of these aspects by the external auditors. It may be noted that COSO and COBIT together have been internationally used as best practices framework for complying with SOX. The details of how IT compliance can be best implemented or reviewed by using best frameworks such as COSO and COBIT 5 is explained further in the following sections.

2.2.2 COBIT 5

COBIT 5 issued by ISACA (www.isaca.org) is the Business Framework of Governance and Management of Enterprise IT. As per COBIT 5, Information is the currency of the 21st century enterprise. Information, and the technology that supports it, can drive success, but it also raises challenging governance and management issues. COBIT 5 provides the approach and latest thinking based on global best practices. It is an umbrella framework for implementing Governance and management of information systems.

COBIT 5 can be used as a benchmark for reviewing and implementing governance and management of enterprise IT. It has a set of 5 principles and 7 enablers which are the building block of the framework. This principles and enablers make COBIT 5 an effective tool for implementing GEIT and helps enterprises in various ways such as: simplify complex issues, deliver trust and value, manage risk, reduce potential public embarrassment, protect intellectual property and maximize opportunities. As COBIT 5 is a comprehensive framework and has best practices covering all key process, its implementation can enable enterprises to adapt it as required to achieving enterprise objectives for the governance and management of enterprise IT. The best practices of COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.

COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT related interests of internal and external stakeholders. COBIT 5 helps enterprises to manage IT related risk and ensures compliance, continuity, security and privacy. COBIT 5 enables clear policy development and good practice for IT management including increased business user satisfaction. The key advantage in using a generic framework such as COBIT 5 is that it is useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

Need for Enterprises to Use COBIT 5

Enterprises depend on good, reliable, repeatable data, on which they can base good business decisions. COBIT 5 provides good practices in governance and management to address these critical business issues. COBIT 5 is a set of globally accepted principles, practices, analytical tools and models that can be customized for enterprises of all sizes, industries and geographies. It helps enterprises to create optimal value from their information and technology. COBIT 5 provides the tools necessary to understand, utilize, implement and direct important IT related activities, and make more informed decisions through simplified navigation and use. COBIT 5 is intended for enterprises of all types and sizes, including non-profit and public sector and is designed to deliver business benefits to enterprises, including:

- Increased value creation from use of IT;
- User satisfaction with IT engagement and services;

- Reduced IT related risks and compliance with laws and regulations.
- Development of more business-focused IT solutions and services; and
- Increased enterprise wide involvement in IT-related activities.

Integrating COBIT 5 with other frameworks

There is no single framework which provides all the requirements for all types of enterprises. Hence, enterprises have to select the right blend of frameworks and best practices. The main advantage of using COBIT 5 is that it provides an enterprise view and is aligned with enterprise governance best practices enabling GEIT to be implemented as an integral part of wider enterprise governance. COBIT 5 also provides a basis to integrate effectively other frameworks, standards and practices used such as ITIL, TOGAF and ISO 27001. It is also aligned with The GEIT standard ISO/IEC 38500:2008, which sets out high-level principles for the governance of IT, covering responsibility, strategy, acquisition, performance, compliance and human behaviour that the governing body (e.g., board) should evaluate, direct and monitor. Thus, COBIT 5 acts as the single overarching framework, which serves as a consistent and integrated source of guidance in a non-technical, technology-agnostic common language. The COBIT 5 Framework provides an overview of specific related frameworks in terms of breadth, depth and level of coverage. This helps in understanding and integrating different frameworks as required. The integration of framework and resulting enablers should be aligned with and in harmony with (amongst others) the:

- Enterprise policies, strategies, governance and business plans, and audit approaches;
- Enterprise risk management framework; and
- Existing enterprise governance organization, structures and processes.

Customizing COBIT 5 as per requirement

COBIT 5 can be tailored to meet an enterprise's specific business model, technology environment, industry, location and corporate culture. Enterprises can select required guidance and best practices from specific publications and processes of COBIT 5 and implement these in specific areas based on their areas of need. Because of its open design, it can be applied to meet needs related to Information security, Risk management, GEIT, Assurance activities, legislative and regulatory compliance, etc.

Five Principles of COBIT 5

COBIT 5 simplifies governance challenges with just five principles. The five key principles for governance and management of enterprise IT in COBIT 5 taken together enable the enterprise to build an effective governance and management framework that optimizes information and technology investment and use for the benefit of stakeholders. These principles are shown in Fig. 2.2 and each of the principles are explained as their understanding is critical for implementation.

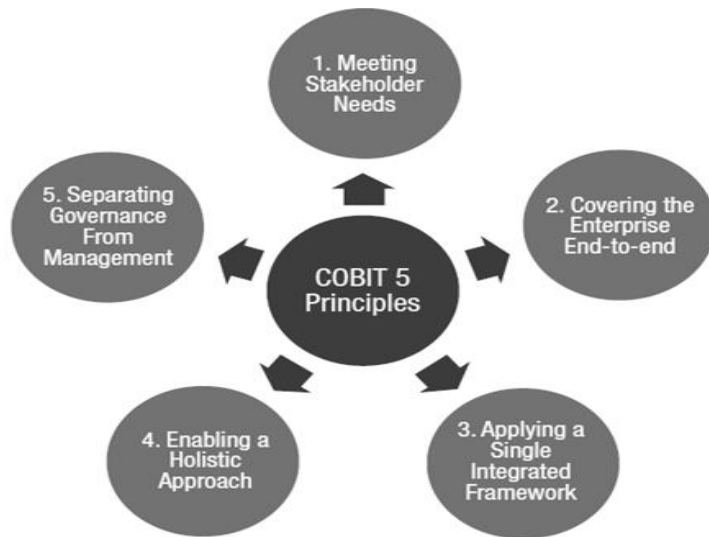


Figure 2.2: Five Principles of COBIT 5

Principle 1: Meeting Stakeholder Needs

Enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources. COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT. Because every enterprise has different objectives, an enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific, IT related goals and mapping these to specific processes and practices.

Every enterprise operates in a different context; this context is determined by external factors (the market, the industry, geopolitics, etc.) and internal factors (the culture, organization, risk appetite, etc.), and requires a customized governance and management system. Stakeholder needs have to be transformed into an enterprise's actionable strategy. The COBIT 5 goals cascade is the mechanism to translate stakeholder needs into specific, actionable and customized enterprise goals, IT related goals and enabler goals. This translation allows setting specific goals at every level and in every area of the enterprise in support of the overall goals and stakeholder requirements, and thus effectively supports alignment between enterprise needs and IT solutions and services.

Principle 2: Covering the Enterprise End-to-End

COBIT 5 integrates governance of enterprise IT into enterprise governance. It covers all functions and processes within the enterprise; COBIT 5 does not focus only on the 'IT function', but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise. It considers all IT related governance and management enablers to

be enterprise-wide and end-to-end, i.e., inclusive of everything and everyone: internal and external that is relevant to governance and management of enterprise information and related IT. The end-to-end governance approach is the foundation of COBIT 5 and covers all the key components of a governance system.

Principle 3: Applying a Single Integrated Framework

There are many IT related standards and best practices, each providing guidance on a subset of IT activities. COBIT 5 is a single and integrated framework as it aligns with other latest relevant standards and frameworks, thus allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator. It is complete in enterprise coverage, providing a basis to integrate effectively other frameworks, standards and practices used.

Principle 4: Enabling a Holistic Approach

Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components. COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise.

Principle 5: Separating Governance from Management

The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes. The interface between governance and management processes and activities at different levels is depicted here.

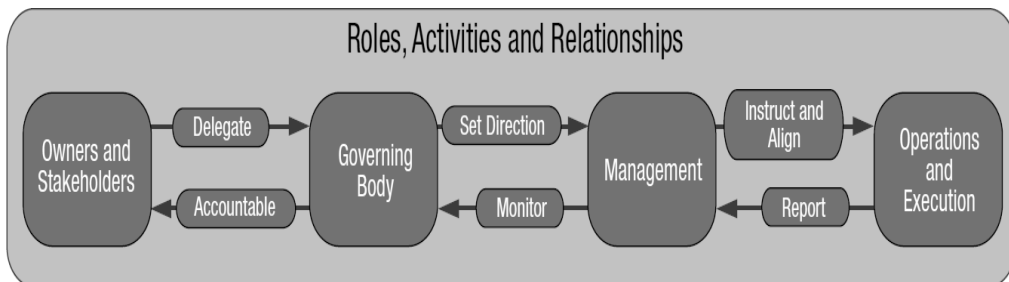


Figure 2.3: Roles, activities and relationships of Governance and management

Governance: It ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

In most of the enterprises, overall governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger, complex enterprises.

Management: It plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

In most of the enterprises, management is the responsibility of the executive management under the leadership of the Chief Executive Officer (CEO). From the definitions of governance and management, it is clear that they comprise different types of activities, with different responsibilities. The role of governance is to evaluate, direct and monitor. There is need for a set of interactions between governance and management to result in an efficient and effective governance system. The specific interfaces between Governance and management are established through governance mechanisms. These interfaces include:

- Principles and policies that define objectives, agreed plans, responsibilities, boundaries, authority, exception arrangements and reporting arrangements;
- Structure for decision making based on agreed principles and policies;
- Processes and Practices to ensure implementation; and
- Relationship Mechanism aimed at improving communication between business and IT.

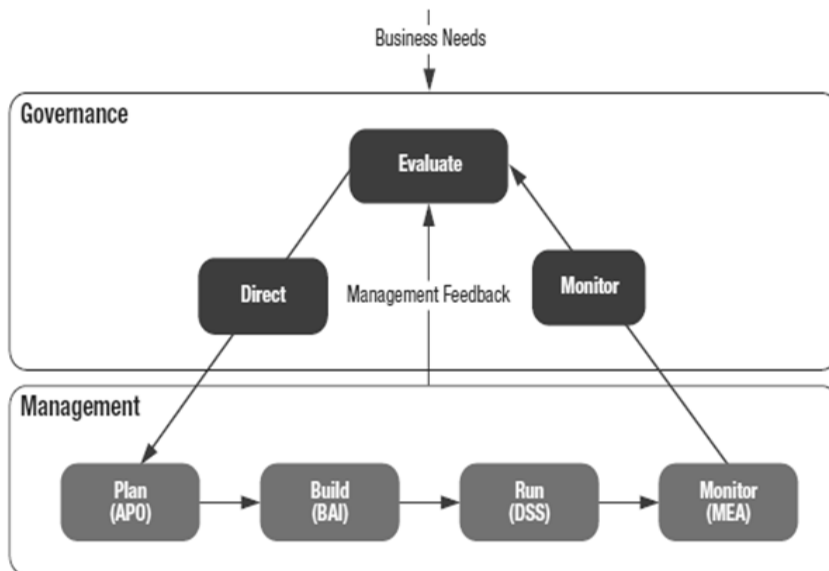


Figure 2.4: Key Areas of Governance and Management

Seven Enablers of COBIT 5

Enablers are factors that, individually and collectively, influence whether something will work; in this case, governance and management over enterprise IT. Enablers are driven by the goals cascade, i.e., higher-level IT related goals defining 'what the different enablers should achieve'. The COBIT 5 framework describes seven categories of enablers which are to be implemented as required for meeting stakeholder requirements. The seven enabler are briefly discussed here and are depicted in in Fig. 2.5.

- **Principles, Policies and Frameworks:** The vehicle to translate the desired behaviour into practical guidance for day-to-day management.
- **Processes:** Describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
- **Organizational structures:** The key decision-making entities in an enterprise.
- **Culture, Ethics and Behaviour:** of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.
- **Information:** is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
- **Services, Infrastructure and Applications:** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
- **People, Skills and Competencies:** are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

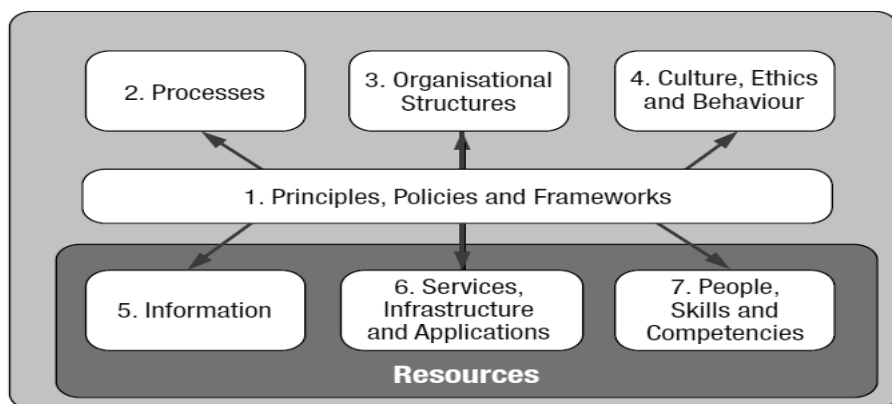


Figure 2.5: Seven Enablers of Governance

2.2.3 ISO 38500

ISO 38500 is the ISO standard for corporate governance of IT. The standard is focussed at high level and states that the board of directors should govern IT by:

1. **Evaluating** the current and future use of IT.
2. **Directing** preparation and implementation of plans and policies to ensure that the use of IT meets business objectives.
3. **Monitoring** conformance to policies and performance against the plans.

The objective of ISO 38500 is to provide a structure of principles for directors and other stake holders to use when evaluating, directing and monitoring the use of IT in their organizations. It provides a structure for effective governance of IT to assist those at the highest level of organizations to understand and fulfil their legal, regulatory and ethical obligations regarding their organizations' use of IT. The scope of the standard is to provide guiding principles for directors of organizations on the effective, efficient and acceptable use of IT within their organizations. It is applicable for all organizations, from the smallest to the largest, regardless of purpose, design or ownership structure. The standard is more of a high level expectation from management as to what should be the outcome from IT governance, however it does not provide direction or guidelines as to how it should be achieved. COBIT 5 ensures that these guidelines are available and organization implementing COBIT can be ISO 38500 compliant.

2.2.4 ISO 31000

ISO has developed a new standard for IT risk management. The standard primarily adopts AS/NZS 4360 for risk management. The modification it has made is that ISO has added processes for IT risk governance by defining IT risk committee. More details of ISO standards are provided in Chapter 3 of Module 2.

2.2.5 RIMS ERM

Standard developed by Risk and Insurance Management Society of Standards and Technology, primarily for insurance sector. RISM primarily focuses on enterprise risk management and provides all-encompassing process for risk management within organization.

- ERM-based approach:
 - Executive support covering all processes, functions, business lines, roles and geographies.
 - Integration, communication and coordination of internal audit, information technology, compliance, control and risk management.
- ERM process management:
 - Embedding the ERM Process into business processes
 - To identify, assess, evaluate, mitigate and monitor.
 - Using qualitative methods supported by quantitative methods, analysis, tools.

- Risk appetite management:
 - Understanding the risk-reward trade-offs.
 - Accountability within leadership
 - Policy to guide decision-making
 - Attack gaps between perceived and actual risk.
 - Define Risk appetite boundaries for acceptable risk and risk tolerance
- Root cause discipline:
 - Measuring a problem's root cause
 - Binding events with their process sources to drive the reduction of uncertainty
 - Collection of information and measurement of the controls' effectiveness.
 - Measure risk from people, external environment, systems, processes and relationships
- Uncovering risks:
 - Documenting risks and opportunities.
 - Collecting knowledge from employee expertise, databases and other electronic files
 - Uncover dependencies and correlation across the enterprise.
- Performance management:
 - Executing vision and strategy, working from financial, customer, business process and learning and growth perspectives using tools like BSC.
 - Exposure to uncertainty, or potential deviations from plans or expectations.
- Business resiliency and sustainability:
 - Extent of ERM Process's sustainability integrated into operational planning.
 - Evaluating how planning supports resiliency and value.
 - Ownership and planning beyond recovering technology platforms.

2.2.6 RiskIT: Risk Management framework by ITGI and ISACA

RiskIT framework is created by ISACA and ITGI. The framework is based on COBIT framework and can be mapped to most global standards. This framework is process driven framework and covers three major areas:

1. Risk Governance
2. Risk Evaluation
3. Risk Response

IT risk management as suggested by ISO 27001. It is a method based on identifying risks and vulnerabilities within IT assets and implement controls to mitigate them. However, considering the shortcomings of this method, the revised ISO 27001:2013 has revision has recommended using ISO 31000 for IT risk management. ISACA has recently released COBIT5 for Risk which integrates the principles of Risk IT, Val IT and COBIT 5. COBIT 5 for Risk which is built on the principles of COBIT 5 can be used for implementation of risk management from governance perspective.

2.3 Enterprise risk management and IT risk management

2.3.1 Risk Management

Enterprise Risk Management and IT Risk Management are key components of an effective IT governance structure of any enterprise. Effective IT governance helps to ensure close linkage to the enterprise risk management activities, including Enterprise Risk Management (ERM) and IT Risk Management. IT governance has to be an integral part of overall corporate risk management efforts so that appropriate risk mitigation strategies are implemented based on the enterprise risk appetite. The risk assessment approach adapted has to consider business impact of IS risk and different types of risks. There has to be timely and regular communication of status of residual risks to key stakeholders so that appropriate action is taken to manage the IT risk profile. This section will provide an overview of related terms like threats, vulnerabilities etc., IS Risks and exposures and risk mitigation strategies, which can be adapted by the organizations.

Risk management process is a crux of any business today and it is a day-to-day activity. Risk management processes primarily focuses on three major areas viz. Market Risk, Credit risk and Operational Risk. Most organization addresses first two risks i.e. market risk and credit risks since these are part and partial of business activities. Whereas operational risks addresses the issues and concerns related to operations of a business. Today's organizations depend heavily on information and related technology and majority operations have been automated. Hence, it is important to consider IT risks as these by themselves are very critical but in terms of impact on other risks, they can impact all areas of enterprise operations. Hence, it is important to understand how the use of technology has introduced various new types of risks and their impact specifically in organizations which are heavily dependent on technology. The Figure below describes the relationship on technology risks in overall risk scenario.



Figure 2.6: Relation of IT risks

2.3.2 Risk Management in COBIT 5

IT Risks have to be managed from holistic perspective and this approach is called risk optimisation. The COBIT framework provides excellent guidance on risk management strategy and practices from governance and management perspective. The Governance domain contains five governance processes and one of the Governance process: “EDM03: Ensure risk optimization” primarily focuses on stakeholder risk-related objectives. The objective of this process is to ensure that the enterprise’s risk appetite and tolerance are understood, articulated and communicated and that risk of IT is identified and managed. The key benefits of implementing appropriate risk optimisation process is that it ensures that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures are minimised.

The COBIT framework has management domain of “Align, Plan and Organize”, which contains a risk-related process: “APO12: Manage risk”. This process requires continually identifying, assessing and reducing IT-related risk within levels of tolerance set by enterprise executive management. The primary purpose of this process is to integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk. All enterprise activities have associated risk exposures resulting from environmental threats that exploit enabler vulnerabilities.

The combination of Governance practices of “EDM 03: Ensure risk optimization” (which ensures that the enterprise stakeholders approach to risk is articulated to direct how risks facing the enterprise will be treated) and the management practices of “APO12 Manage risk” (which provides the enterprise risk management (ERM) arrangements that ensure that the stakeholder direction is followed by the enterprise) together ensured that Risk management covers the entire life cycle and covers both governance and management perspective. Further, detailed guidance is available in the form of specific practices and activities that are designed to treat related risk (avoid, educe/mitigate/control, share/transfer/accept). In addition to activities, COBIT 5 suggests accountabilities, and responsibilities for enterprise roles and governance/management structures (RACI charts) for each process including risk-related roles at each level of management as appropriate.

Key Governance Practices of Risk Management

Implementing governance requires that governance practices covering all the aspects of governance of risk management are covered. There are three broad areas:

- **Evaluate Risk Management:** Continually examine and make judgment on the effect of risk on the current and future use of IT in the enterprise. Consider whether the enterprise's risk appetite is appropriate and that risks to enterprise value related to the use of IT are identified and managed;

- **Direct Risk Management:** Direct the establishment of risk management practices to provide reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite; and
- **Monitor Risk Management:** Monitor the key goals and metrics of the risk management processes and establish how deviations or problems will be identified, tracked and reported on for remediation.

Key Management Practices of Risk Management

Implementing Risk Management requires that the risk management practices are embedded in all the key organisational processes as required and are performed as part of the day to day tasks and activities. A process oriented approach has to be followed for implementing risk management. The key management practices of effective risk management are:

- **Collect Data:** Identify and collect relevant data to enable effective IT related risk identification, analysis and reporting.
- **Analyze Risk:** Develop useful information to support risk decisions that take into account the business relevance of risk factors.
- **Maintain a Risk Profile:** Maintain an inventory of known risks and risk attributes, including expected frequency, potential impact, and responses, and of related resources, capabilities, and current control activities.
- **Articulate Risk:** Provide information on the current state of IT- related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.
- **Define a Risk Management Action Portfolio:** Manage opportunities and reduce risk to an acceptable level as a portfolio.
- **Respond to Risk:** Respond in a timely manner with effective measures to limit the magnitude of loss from IT related events.

Metrics of Risk Management

Enterprises have to monitor the processes and practices of IT risk management by using specific metrics. Some of the key metrics are:

- Percentage of critical business processes, IT services and IT-enabled business programs covered by risk assessment;
- Number of significant IT related incidents that were not identified in risk Assessment;
- Percentage of enterprise risk assessments including IT related risks; and
- Frequency of updating the risk profile based on status of assessment of risks.

2.3.3 Risk Factors

There are unique risks for each organization, given the nature of operations, although generally organizations within the same sector will have common risk elements. The appropriate risk response will be different from organization to organization, depending on how management views the risk in terms of magnitude. Risks are represented in the external environment in which the organization chooses to operate, as well as those in the internal environment. Risk factors in the external environment and generally outside of the organization's direct control. External risk factors include political situations, the economy, regulations, natural disasters, competition. Internal risk factors includes Organization's culture, Internal environment affecting employees moral, policies , ethics and values projected by senior management, process environment, control environment and so on.

2.3.4 Categories of Risks

The risk management process begins with the identification of risk categories. An organization will have several risk categories to analyse and identify risks that are specific to the organization. Some examples of risk categories are:

- **Business risks:** Also sometimes referred as inherent risks. These are risk associated with nature of business. E.g. loss of finished product for food industry
- **Market risks:** Risks associated with fluctuations on market affecting the customer base of organization. E.g. Customer preferring smart phones over traditional phones affecting Nokia products.
- **Financial risks:** Risk associated with financial decisions and environment in which business operates. E.g. Non-availability of funds, excess expenditure etc.
- **Operational risks:** Risks associated with failure of operations of organization. E.g. failure of assembly-line for car manufacturer, non-availability of IT for banking services etc.
- **Strategic risks:** Associated with incorrect and inappropriate strategy selection and implementation. Eg. Planning for implementing IT application that is outdated, selecting application for automation that may not satisfy future growth expectations. Not-considering effect of smart phones by Nokia management.
- **IT risks:** How the company's IT infrastructure relates to business operations and their impact on business in case risk materializes. E.g. failure of networks affecting communications, failure of applications impacting operations and service delivery.
- **Compliance risks:** Risk when an organization does not comply with legal, regulatory, contractual or internal compliance requirements E.g. failure of complying with privacy laws, labour laws, software license agreement.

2.3.5 Elements of Risk Management

Before establishing a strategy for information risk management, the following elements must be in place to permit effective risk management:

- **Top Management support:** The need for risk management must start and be supported at the highest level within the company. This includes the governance level and the CEO.
- **Proactive approach:** Risk management efforts must be proactive. This involves the active identification, measurement and management of the risks, scanning of changes in the risk profile and reports on managing the risk profile.
- **No ambiguity:** There needs to be a clear definition of the risks, and these must be understood across the organization.
- **Accountability:** Responsibility for responding to and managing the risks must be clearly understood and individuals held accountable for fulfilling the roles.
- **Resource allocation:** Appropriate resources including people and tools need to be deployed and available to help managers, executive and the governance level conduct their obligations within the risk management framework.
- **Cultural change:** The organization's culture must provide for the active management of risk.

2.4 Risk Management strategies

When risks are identified and analyzed, it is not always appropriate to implement controls to counter them. Some risks may be minor, and it may not be cost effective to implement expensive control processes for them. Risk management strategy is illustrated below in Figure 2.7:



Figure 2.7: Risk Mitigation strategies

The risk mitigation strategy is explained for each of the options.

- **Tolerate/Accept the risk.** One of the primary functions of management is managing risk. Some risks may be considered minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.
- **Terminate/Eliminate the risk.** It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.
- **Transfer/Share the risk.** Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization. Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.
- **Treat/mitigate the risk.** Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.
- **Turn back.** Where the probability or impact of the risk is very low, then management may decide to ignore the risk.

2.4.1 Developing Strategies for Information Risk Management

Some organisations have adopted a centralized model for risk management, while others are using a decentralized model. The approach depends on:

- a. An organization's particular operations,
- b. The significant risks,
- c. The culture of the organization,
- d. The management style and
- e. The control environment i.e. the degree of centralization or the delegation of authority and the infrastructure of the business.

In a centralized model it is the Information Risk Management team that develops policies for the board to consider. Other organizations have decentralized model requiring the involvement of front line staff in managing the inherent risks of the company, of the business unit or of the process.

2.4.2 Risk Register and control catalogue

It is a collective record of all identified and evaluated risk along with risk owner and risk response. The structure of risk register may vary organization to organization, however it must:

1. Contain risk scenario, likelihood, assets impacted, overall impact on business (assessment), owner, risk response decision, reference to control catalogue, review date.
2. It must be maintained based on updating process.
3. Generally it is used to develop risk profile for reporting to management and approval.

IS auditor should use this risk register to review and audit the risk management process and also ensure that appropriate controls are identified, designed and implemented. Control catalogue is collective register of all controls designed and implemented within organization with reference to risk register.

2.5 Risk management process

The Objective of risk management process is to ensure that the organization can manage risks with acceptable limits. These acceptable limits are decided by Risk Appetite and Risk tolerance.

Risk Appetite: It is ability of organization to sustain losses due to materialization of risk. It also represents the ability of organization to take risk while considering new business initiatives.

Risk Tolerance: It is the limit up to which organization can tolerate to sustain loss of business in case risk materializes. In other words, in case any risk materializes the organization must recover from it within specified time decided by risk materialization.

Information Risk Management process involves a continuous cycle to identify, assess, measure, decide response, assign responsibility and monitor information risk. Organization may adopt any standard or framework discussed earlier for implementing Information risk management. Although different framework describe different processes for managing IT risks, typically IT risk management process follows following steps:

1. Risk identification
2. Risk evaluation
3. Risk prioritization
4. Risk response
5. Risk mitigation
6. Risk monitoring

2.5.1. Risk Identification

As name suggest it is process to identify risks for organization. Organization may deploy one or more methods to identify risks. Some methods are:

1. Workshop and brainstorming sessions with stakeholders and process owners: In this method the process owners and risk practitioners (IS Auditors) meet and discuss the possible causes for process failures affecting desired outcome. This workshops typically covers risk identification, risk evaluation, control definition steps. In case process owners does not agree a method called Delphi technique we used to assess the risks.

2. Use of generic risk scenarios based on industry experience and historical data: Generic scenarios are the list of possible incidents affecting desired outcome of business process objectives.
3. Review and audit of processes and technology. This includes vulnerability assessment: Audit findings, lessons learned from Incident response, vulnerability assessments helps organization in identifying possible threats that can impact the normal functioning of business processes.

Organizations may adopt various methods for identifying and recording risks some of them are discussed here.

Threat profile/ Inventory

It is a list of all possible threats that might have impact on organization. Organization may prefer to categorize them based on nature.

- **Physical and Environmental** for example fire, theft, humidity, temperature
- **External** threats that are not in control of organization like hackers, Denial of service, virus, sabotage, targeted attacks
- **Internal** threats are those are initiated within organization for example disgruntled employee, unauthorized access by authorised users, confidential data leakage by employee, misuse of management override. Majority breaches are due to internal threats
- **Natural** threats like earthquake, floods, and tsunami

Organization may prepare a list of threats and try to evaluate how they affect organization.

Vulnerability Assessment

A vulnerability assessment is one of the process of identifying, the vulnerabilities in a system. Vulnerability assessment is a one process in risk identification. The Vulnerability Assessment is an evaluation to identify gaps and vulnerabilities in your network, servers, etc. help you validate your configuration and patch management, and identify steps you can take to improve your information security. The assessment helps you meet your minimum compliance mandates and security assessment needs. Assessments are typically performed according to the following steps:

- a. Cataloguing assets and resources in a system.
- b. Assigning quantifiable value or rank and importance to those resources
- c. Identifying the vulnerabilities or potential threats to each resource

Vulnerabilities that may exist across your systems and applications can create an easy path for hackers to gain access to and exploit your environment. With dozens and even hundreds of applications and systems across your environment with access to the Internet, maintaining and updating system operating systems and applications to eliminate vulnerabilities is paramount - especially when those applications and systems are tied to sensitive customer, patient or cardholder information.

Asset Inventory

Risks when materialize affect the functioning of organization. The impact of a risk can be different for different business function depending upon the various factors like time of incident, functions affected etc. For example in case on a Bank failure of connectivity might affect ATM network as well as branch network, however if the failure happens after business hours impact of non-availability of ATM could be higher. In other words providing protection for connectivity to ATM shall be different as compared to branch networks. In order to provide appropriate security organizations may focus on implementing controls over assets that supports business processes. ISO27001:2005 also recommends to implement controls around assets by prioritizing them based on results of risk evaluation. (ISO27001:2013 recommend ISO31000 for Risk management and also states that risk management need not be asset based.)

Risk components

Risk to be managed effectively have to be understood in totality. Hence, it important to understand all the specific components of all identified risks and these are:

- **Risk Scenario** : A possible event due to materializing of one or more risks for example Failure of connectivity might be caused due to one or more reasons like physical damage to cables / devices, malfunction of devices, virus / malware attack, Denial of service attack, failure of service provider.
- **Threat** : Reason for risk materialization for example theft of equipment, fire, natural disaster, non-availability of human resources, Virus
- **Vulnerability**: Weakness that gets exploited due to threat. For example absence of antivirus is a vulnerability that will enable a virus to infect the system or improper physical security leading to theft
- **Likelihood / Probability**: Judgment of possibility that threat shall exploit vulnerability. For example there is always a possibility of earthquake, however it may not take place every day. The possibility can be worked out based on historical data and seismic zone in which facility is located. Or possibility of virus attacking systems can happen multiple times in a day.
- **Impact / Consequences**: When threat materializes, it will affect normal functioning which might result in loss of business, interruption of services. A calculation of possible loss expressed in monetary terms.
- **Response**: Action Plan designed by organization to minimize impact or likelihood of risk materializing. There are four types of responses and organization may choose one or more for each risk. The four types are: Accept, Transfer, Avoid and Mitigate. For example Management may have process to monitor virus by maintaining antivirus tool updated and also run a schedule scan. In case cost of process and tool is higher than impact organization may decide to do nothing and accept the risk.

- **Controls / Mitigation:** In order to mitigate risk management implements controls. For example Access controls reduces the likelihood of unauthorized access, Fire suppression system reduces the impact due to fire.
- **Inherent Risk:** Total risk without any controls is inherent risk.
- **Residual risk:** Controls cannot mitigate the risk completely. It may reduce likelihood and/or impact. There is a small portion of risk still remains that is known as residual risk. It also includes accepted risk.
- **Risk aggregation:** A risk faced by organization may have different impact on different business function/ locations. However from organization's perspective it is necessary to present them as total risk for organization. For example a location on sea shore may have higher risk of flooding as compared to another location away from seashore.
- **Risk profile:** Collective view of all risks an organization likely to face.
- **Heat Map:** Graphical representation of risk profile.
- **Risk Register:** A document that is maintained to provide information on identified risks and contents details of components.
- **Risk Owner:** Person or entity that is responsible for evaluation and decision of response for identified risk

2.5.2. Risk Evaluation

Also called risk assessment. It is a process for assessing likelihood and impact of identified risk. There are two methods used for risk evaluation

1. **Quantitative risk analysis** refers to expressing total risk in monetary terms
2. **Qualitative risk analysis** refers to expressing total risk with qualification like high, medium, low etc. However the challenge is perception of these terms differs from person to person, hence it is necessary to define the meaning of terms high, medium and low so that there are interpreted uniformly across organization.

Determine likelihood of risk

Once risks are identified, the next step is to determine the likelihood that the potential vulnerability can be exploited. Several factors need to be considered when determining this likelihood.

- a. Consider source of the threat, motivation behind the threat, and capability of the source.
- b. Determine the nature of the vulnerability and,
- c. The existence and effectiveness of current controls to deter or mitigate the vulnerability. The likelihood that a potential vulnerability could be exploited can be described as high, medium, or low.

Most of the time the likelihood is judgment of analysts hence it is best estimated by risk owners who are the business process owners as they are likely to be affected due to risk materialization. This helps in arriving at likelihood.

2.5.3. Risk prioritization

Based on evaluation of risks, have to be prioritised into high, medium or low or ranked on scale of 1 to 5. This risk ranking will help enterprises to decide the priority in which the risks will be mitigated. Based on the decisions taken in this process/stage, the next step of risk response is implemented. The organizations generally use Risk profile and Heat map to prioritize evaluated risks based on criticality of risks and priorities of business objectives.

Likelihood	Consequence				
	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophe 5
Almost Certain 5	5	10	15	20	25
Likely 4	4	8	12	16	20
Possible 3	3	6	9	12	15
Unlikely 2	2	4	6	8	10
Rare 1	1	2	3	4	5

Figure 2.8: Risk prioritisation

2.5.4. Risk Response

With the potential impact assessment in hand, the next step is to determine what the appropriate response is to prudently manage the risk. The risk responses are given here:

Response	Description
Avoid	Eliminate the risk by eliminating the cause e.g. where feasible, do not implement processes that would incur risk.
Accept	This response is to accept the level of risk and monitor.
Transfer/Share	This response is to transfer the risk to someone else, e.g. purchase insurance or share with outsourcing service provider
Mitigate	Refers to define controls to reduce the likelihood or impact or both so as to bring the residual risk within the acceptable limits defined by risk appetite and risk tolerance.

For each risk identified, the risk response can be articulated the objective is to bring the estimated risk below the Risk appetite and risk tolerance of the organization. For example, where the risk response is to accept the risk, this becomes part of the organization's risk tolerance, means the business must recover from impact before tolerance limits.

2.5.5. Risk Mitigation

Defining controls to reduce likelihood and/or impact of risk is referred as risk mitigation. The controls are designed based on the nature and type of process after considering process objectives. Controls are selected based on the cost benefit analysis. The cost of control covers cost for tools, impact on process efficiency, resource requirements, training requirements and cost associated with monitoring of control. Total cost is compared against the total impact reduced due to controls i.e. difference between evaluation of inherent risk and residual risk. In case of positive difference controls are implemented. In case of negative results organization may select another response like accept or avoid the risk.



Figure 2.9: Relationship of Risks and Controls

2.5.6. Risk Monitoring

Once the controls are implemented what remains is residual risk i.e. risk remaining after implementing controls and risk accepted. For example Organization may implement fire resistant material to reduce the likelihood of risk. They also implement policies regarding use of inflammable material and safe electrical design using circuit breakers. Still if the fire breaks out smoke detectors

are implemented to get early warning so that the incident can be responded to contain damage. Depending upon the level of impact organization may install fire suppression system that will automatically activated based on temperature levels and response time and hence damage is further reduced. However there still remains risk of fire and hence it needs to be monitored by including processes for testing control equipment, processes etc. Risk monitoring is process consists of following activities:

1. Periodic review identified and evaluated risks to confirm that the evaluation is appropriate. This might change due to various factors like changes in environment, business strategy and focus, Market changes and so on.
2. Review of risks associated with changes in infrastructure, processes and IT. Change might have effect on risks, for example organization has implemented uninterruptible power supply system. Subsequently it might have added more equipment and hence the capacity of UPS may not be sufficient in future. Identifying evaluating this risk in time shall reduce impact of failure.
3. Incident response and lessons learned is another area that prompts for review of risks that materialized.
4. Audit findings also requires review of risks since non-effective controls might provide false comfort of compliance to management.

2.6 IS Risks and Risk Management

There are numerous changes in IT and its operating environment that emphasizes the need to better manage IT related risks. Dependency on electronic information and IT systems is essential to support critical business processes. In addition, the regulatory environment is mandating stricter control over information. Increasing disclosures of information system disasters and increasing electronic fraud, in turn, drive this. The management of IT related risks is now being understood as a key part of enterprise governance.

Risk is the possibility of something adverse happening, resulting in potential loss/exposure. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Risk management involves identifying, measuring, and minimizing uncertain events affecting resources. Any Information system based on IT has its inherent risks. These risks cannot be eliminated but they can be mitigated by appropriate security. This security has to be implemented as per required control system envisaged by the management of the enterprise. The risks in IT environment are mitigated by providing appropriate and adequate IS Security. IS security is defined as "procedures and practices to assure that computer facilities are available at all required times, that data is processed completely and efficiently and that access to data in computer systems is restricted to authorized people".

IS Auditors are required to evaluate whether the available controls are adequate and appropriate to mitigate the risks. If controls are unavailable or inadequate or inappropriate, then there would be

a control weakness, which has to be reported to auditee management with appropriate recommendations to mitigate them.

2.7 Summary

This chapter has provided an overview of various types of Governance and risk management frameworks which can be used by organisations for implementing. There is no single framework which meets all requirements. Hence, it is important to understand the scope and coverage of each of these frameworks so that they can adapted as required for implementation. Risk management is an integral aspects of governance and management. Risks have both positive and negative attributes. Risks provide challenges but they also provide opportunities. Risk management requires effective mitigation of risks by adapting the risk management process strategy thereby balancing risk versus benefits.

2.8 Questions

1. The most important requirement for IT governance function to be effective is:
 - A. Monitoring
 - B. Evaluation
 - C. Directing
 - D. Managing
2. The primary objective of implementing principles, policies and framework within an organization is to:
 - A. communicate stakeholder's intent.
 - B. benchmark performance against competitors.
 - C. confirm with regulatory compliance.
 - D. implement corporate governance.
3. The MOST important benefit of implementing IT risk management process is that it helps in:
 - A. optimizing internal control framework.
 - B. ensuring residual risk is at acceptable level.
 - C. prioritizing business functions for audit planning.
 - D. complying with regulatory requirements.
4. Which of the following is a major risk factor?
 - A. Existence of inflationary trends.
 - B. Vendor launches new software.
 - C. Board of directors elects new chairman.
 - D. Change in government post elections.

Module 3

5. The level to which an enterprise can accept financial loss from a new initiative is:
 - A. Risk tolerance
 - B. Risk management
 - C. Risk appetite
 - D. Risk acceptance
6. Designing and implementing a control to reduce the likelihood and/or impact of risk materializing is a:
 - A. Risk acceptance
 - B. Risk transfer
 - C. Risk treatment
 - D. Risk transfer
7. Which of the following is a valid risk statement?
 - A. Network service provider is unable to meet bandwidth.
 - B. Hacker attempts to launch attack on web site.
 - C. Application server crash due to power failure.
 - D. Delay in servicing customers due to network congestion.
8. Which of the following is primary reason for periodic review of risk? The changes in:
 - A. risk factors
 - B. risk appetite
 - C. budget
 - D. risk strategy
9. Which of the following is a strategic IT risk?
 - A. IS audit may not identify critical non-compliance.
 - B. Non-availability of networks impacting services to customers.
 - C. New application may not achieve expected benefits.
 - D. Defer replacement of obsolete hardware.
10. Which of the following is the most essential action after evaluation of inherent risks?
 - A. Evaluate implemented controls.
 - B. Update risk register.
 - C. Prepare heat map.
 - D. Prioritized evaluated risk.

2.9 Answers and Explanations

1. **C.** Directing is the most critical of the Governance function which can be performed by the Board. **Although**, governance has three critical functions: Evaluate, direct and monitor, evaluation and monitoring can be performed against directions.
2. **A.** Principles, policies and framework have to be implemented within organizations primarily to communicate the intent of management (Stakeholders) so that management can implement or translate this into specific action.
3. **B.** The primary function of IT risk management process is to support value creation by reducing the risk to an acceptable level. The other options are secondary benefits of IT risk management.
4. **D.** Risk factors are conditions that affect the risk profile of organization. Change in government is one of major risk factor as compared with other options.
5. **C.** Risk appetite denotes the level of risk acceptable by management. Risk tolerance is the time up to which an organization can afford to accept the risk. Risk management is a process of risk mitigation and risk acceptance is decision of the management and is considered as risk response.
6. **C.** Implementing control is a risk treatment.
7. **D.** Options A, B and C are threats and not risks.
8. **A.** Changes in risk factors is the primary reason for reviewing changes in risk levels for an organization. The other options are secondary reasons.
9. **D.** Deferring replacement of obsolete hardware is strategic decision and hence it is a strategic IT risk. Others are operational IT risks.
10. **A.** Once risks are evaluated it is necessary to find out the current state of risk mitigation (gaps in controls) by evaluating the existing controls. This help in identifying gaps and implementing controls so as to reduce the total exposure within acceptable limits. Other activities are required but not as essential as identifying gaps in controls.

CHAPTER 3: GEIT AND GRC

Learning Objectives

Governance, Risk and Compliance (GRC) has been at the fore-front of corporate world due to the increasing emphasis on implementing this to meet regulatory requirements of Corporate Governance. Failures of some large enterprises in the last two decades due to lack of adequate level of Enterprise Risk Management (ERM) has compelled regulators to mandate its enforcement thus necessitating GRC implementation. Effective implementation of ERM requires consideration of multiple factors such as using a: holistic approach which encompasses enterprise from end-to-end, top down approach, best practices framework, technology deployment, related regulatory requirements and business needs. As IT is a key enabler for most enterprises, it makes good economic sense to implement IT GRC as a sub-set of overall GRC under the regulatory umbrella of corporate governance. This chapter provides an overview of the need for GEIT and how GRC requirements of compliance can be implemented using GEIT framework such as COBIT 5 and other related best practices.

3.1 Introduction

Modern enterprises are required to comply with a plethora of regulations covering not only business and regulatory aspects but also social and environment aspects. Most of the enterprises today are increasingly dependent on IT extensively for providing business services. The pervasiveness of technology in the current era can be gauged from the fact that the cost of Technology in a modern car is significantly higher than the cost of steel and the car can be considered as a mobile data centre as it has multiple processors which work together to provide safer and comfortable experience to the user. Technology provides the capability to deliver products and services at speeds hitherto unknown and also in a uniform and structured manner which is dynamically scalable. Enterprises using IT recognize that value is not derived miraculously from technology but is only realized when the capability of technology is applied and managed for enabling the required changes in delivering services of core business processes. This technology enablement process has its own inherent risks which coupled with compliance requirements make it imperative to implement an effective system of risk management encompassing both business and IT. There is a growing need to balance risk vs. value, benefits vs. cost and convenience vs. controls by implementing the right level of controls from the holistic perspective of enterprise risk management (ERM). As business processes and related controls get embedded into technology it is critical to implement IT risk management as strategic and integral part of ERM.

This ERM-enabled technology deployment provides a robust platform for enterprises to service customers empowering them to not only survive but also thrive in a dynamic competing environment. The principles of GRC can be used even in Small and Medium Enterprises (SME) as

they provide the benefit of a safe and secure environment. However, the scope and level of ERM would be lesser for SMEs. This has led to an increasing demand for GRC related services which is being provided by vendors and solution providers ranging from consulting firms to large IT vendors. This chapter provides overview of regulatory need for GRC and how a GRC program can be implemented or reviewed using COBIT 5.

3.2 What is GRC?

GRC has been given multiple interpretations by different vendors who have varied solutions to offer. GRC in general is the umbrella term which encompasses corporate governance, enterprise risk management (ERM) and compliance with applicable laws and regulations. GRC gained prominence globally after enactment of Sarbanes Oxley Act (SOX) in the US and similar legislations across the world. In India, Clause 49 of the listing agreements applicable for listed companies inter alia includes all the key aspects of SOX and covers corporate governance requirements which include GRC. Some key definitions of GRC which need to be understood while implementing/reviewing GRC are:

- **Corporate Governance:** The systems and processes, by which enterprises **are directed, controlled and monitored**.
- **Compliance:** The systems and processes that ensure conformity with business rules, policy and regulations.
- **Governance:** ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; **setting direction** through prioritisation and decision making; and **monitoring performance and compliance against agreed-on direction and objectives**. In most enterprises, overall governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organisational structures at an appropriate level, particularly in larger, complex enterprises.
- **Management:** **Plans, builds, runs and monitors activities in alignment with the direction** set by the **governance body** to achieve **the enterprise objectives**. In most enterprises, management is the responsibility of the executive management under the leadership of the chief executive officer (CEO).
- **Governance of Enterprise IT (GEIT):** Concerned with IT value delivery to the business and the mitigation of IT-related risks. This is enabled by the availability and management of adequate resources and the measurement of performance to monitor progress towards the desired goals.
- **Risk Management:** The culture, processes and structures that are directed to the effective management of potential opportunities and adverse effects
- **Risk:** The potential for an event to occur that could have an effect on the Enterprise objectives or operations

- **Framework:** Set of controls and/or guidance organized in categories, focused on a particular topic. It is a structure upon which to build strategy, achieve objectives and monitor performance.
- **Control:** refers to the policies, procedures, practices and organization structure which are designed to provide reasonable assurance that business objectives are achieved and undesired events are prevented or detected and corrected.

3.2.1 GRC from Corporate Governance perspective (Clause 49)

Specific provisions highlighting the regulatory requirements for implementing GRC in enterprises as per Clause 49 listing requirements are:

Risk Management

Section 49 (C) outlines the need for Board Disclosures relating to Risk management and states: "The Company shall lay down procedures to inform Board members about the risk assessment and minimization procedures. These procedures shall be periodically reviewed to ensure that executive management controls risk through means of a properly defined framework.

CEO/CFO Certification

Section 49 (V) deals with CEO/CFO certification and states that the CEO, i.e. the Managing Director or Manager appointed in terms of the Companies Act, 1956 and the CFO i.e. the whole-time Finance Director or any other person heading the finance function discharging that function shall certify to the Board and includes **inter alia** the following:

(c) **They accept responsibility for establishing and maintaining internal controls and that they have evaluated the effectiveness of the internal control systems of the company** and they have disclosed to the auditors and the Audit Committee, deficiencies in the design or operation of internal controls, if any, of which they are aware and the steps they have taken or propose to take to rectify these deficiencies.

(d) They have indicated to the auditors and the Audit committee

(i) **Significant changes in internal control during the year;**

(ii) Significant changes in accounting policies during the year and that the same have been disclosed in the notes to the financial statements; and

(iii) **Instances of significant fraud** of which they have become aware and the involvement therein, if any, of the management or an employee having a significant role in the company's internal control system

Internal Control

Internal control is a formal system of safeguards established by top management to provide a feedback on the way a financial institution, industrial organization, or any other entity observes the board's and senior management's policies, plans, directives, and rules as well as the law of the land and regulatory requirements. It should be seen as a process:

- Promoting transparency,
- Enhancing communications, and
- Affecting all levels of personnel.

The competitive advantage of internal control is that it enables board members to supervise, and senior executives to manage, by tracking exposure to deviations from guidelines, programs, established courses of action, and regulations. Such deviations may increase in credit risk, market risk, operations risk, settlement risk, legal risk, or other exposures relating to transactions, assets, and liabilities as well as to fraud and other events due to breaches of security. Beyond risks, internal control goals include the preservation of assets, account reconciliation, and compliance. Without any doubt, laws and regulations impact on IC, whose able management requires policies, organization, technology, open communications channels, reliable information, access to all transactions, quality control, experimentation, and corrective action. The major objectives of implementing internal control are:

- Promote personnel accountability and
- Keep open the arteries of corporate communications.

The development, implementation, and proper functioning of an internal control system require the existence of clearly stated internal bylaws and directives; a rigorous sense of supervisory activity; compliance with government regulations; and an organization that is flexible, dynamic, and appreciative of the need for management control

Auditor Certification

Section 49 (VII) deals with compliance aspects and states that the company shall obtain a certificate from either the auditors or practicing company secretaries regarding compliance of conditions of corporate governance as stipulated in this clause and annex the certificate with the directors' report, which is sent annually to all the shareholders of the company. The same certificate shall also be sent to the Stock Exchanges along with the annual report filed by the company. Based on the above, it is clear that implementing GRC requires implementing enterprise risk management and internal control system as required to meet the compliance requirements.

3.2.2 GRC program implementation

Although a GRC program (project) can be implemented primarily from a compliance perspective, it is advisable to consider business requirements also so as to optimise the investments made in

implementing relevant processes, control structures and systems. GRC program Implementation requires:

- Defining clearly what GRC requirements are applicable
- Identifying the regulatory and compliance landscape
- Reviewing the current GRC status
- Determining the most optimal approach
- Setting out key parameters on which success will be measured
- Using a process oriented approach
- Adapting global best practices as applicable.
- Using uniform and structured approach which is auditable.

Successful implementation of GRC in enterprise can be measured in general by the assurance provided to the senior management on the adequacy of controls implemented. However, specific success of a GRC program can be measured by using the following goals and metrics:

1. Reduction of redundant controls and related time to execute (audit, test and remediate)
2. The reduction in control failures in all key areas.
3. The reduction of expenditure relating to legal, regulatory and review areas.
4. Reduction in overall time required for audit for key business areas.
5. Improvement through streamlining of processes and reduction in time through automation of control and compliance measures.
6. Improvement in timely reporting of regular compliance issues and remediation measures.
7. Dashboard of overall compliance status and key issues to senior management on a real-time basis as required.

3.2.3 Using COBIT 5 for effective GRC program

GRC is about compliances. However, the focus of GEIT is on benefit realization, risk optimization and resource optimization. Hence, implementing GEIT will help in implementing GRC. Benefit realization focusses on creating new value for the enterprise through IT, maintaining and increasing value derived from existing IT investments, and eliminating IT initiatives and assets that are not creating sufficient value for the enterprise. Risk optimization addresses the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. IT-related business risk consists of IT-related events that could potentially impact the business. Resource optimization focusses on ensuring that the right capabilities are in place to execute the strategic plan and sufficient, appropriate and effective resources are provided. Implementing a GRC program using GEIT framework will help in ensuring that GRC not only facilitates conformance but also helps in ensuring performance.

3.2.4 Responsibility of Senior Management in GRC

The responsibility of senior management in implementing and monitoring functioning of requisite GRC measures is not only a regulatory requirement but it also makes business sense as effective GRC implementation helps in meeting not only compliance but business requirements as well. Using best practices frameworks such as COBIT 5 can help in discharging this responsibility by ensuring that all aspects of GRC are implemented. It is advisable that the board should mandate adaption of a GEIT framework such as COBIT5, as an integral part of enterprise governance development. COBIT 5 framework would provide the overall approach and based on this, relevant guidance can be selected from specific standards and good practices for designing specific policies, processes, practices and procedures. This ensures that appropriate governance processes and other enablers are developed and optimized so that GEIT operates effectively as part of normal business practice and becomes a supporting culture as demonstrated by top management. Alignment with COBIT 5 best practices would also result in faster and more efficient external audits since COBIT is widely accepted as a basis for IT audit procedures.

3.3 IT Compliance Review

Failures of some large enterprises in the last decade due to lack of adequate level of ERM has compelled regulators to mandate its enforcement thus necessitating compliance with Governance, Risk Management and Compliance (GRC). Effective implementation of ERM requires consideration of multiple factors such as using a holistic approach, which encompasses enterprise from end-to-end, top down approach, best practices framework, technology deployment, related regulatory requirements and business needs. As IT is a key enabler for most enterprises, it makes good economic sense to implement IT GRC as a sub-set of overall GRC under the regulatory umbrella of corporate governance.

3.3.1 SOX requirements

As discussed earlier, In the US, Sarbanes Oxley Act has been passed to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes. In India, Clause 49 of listing agreement issued by SEBI mandates similar implementation of enterprise risk management and internal controls as appropriate for the enterprise. Further, the Information Technology Act, which was passed in 2000 and amended in 2008 provides legal recognition for electronic records and also mandates responsibilities for protecting information. The Act also identifies various types of cyber-crimes and has imposed specific responsibilities on corporate. Hence, it can be rightly said that implementing Governance, Risk, security and controls is not only a management requirement but is mandated by law, too. Hence, it is important for enterprises to be aware of and be well conversant of IT compliances and accordingly implement processes and practices to manage these compliances both from conformance and performance perspective.

3.3.2 Clause 49 Requirements

All listed Companies in India have to enter into an agreement with the Stock Exchange and this agreement is called the Listing Agreement. This agreement is more or less defined by SEBI and all Stock Exchanges have similar wordings. Apart from other clauses in the agreement some of the clauses in the listing agreement require additional disclosures from the listed companies and compliance with corporate governance and other requirements. One such clause is Clause 49 of the Listing Agreement that prescribes certain additional disclosure requirements and also corporate governance requirements. This requirement is similar to the requirement of the Sarbanes Oxley Act of the USA and there are similar legislations in Australia, Japan and other countries. In USA, the PCAOB has come out with detailed guidelines on Compliance by Auditors and Companies under the Act. In India, no such guidance is available for Companies and Auditors other than limited guidance from the ICAI to its members, which focuses primarily on audit requirements.

3.3.3 Risk management

Every enterprise should have a risk management function and process to meet both management and regulatory requirements. The scope of process of "Manage Risk" is to continually identify, assess and reduce IT-related risks within levels of tolerance set by enterprise executive management. This helps in integrating the management of IT-related enterprise risk with overall ERIM, and balance the costs and benefits of managing IT-related enterprise risk.

3.3.4 Internal control requirements and Clause 49

The Internal control requirements of Clause 49 are similar to SOX requirements. Section 302 of the SOX requires CEOs and CFOs to certify the dependability of their firms' financial statements, including whether their entities have:

- (a) Effective systems of internal control related to external financial disclosures and
- (b) Procedures capable of notifying both external auditors and their audit committees when significant control deficiencies are detected in these systems.

Section 404 of SOX demands that a firm's external auditor must report on the reliability of management's assessment of internal controls. Similar to SOX, under section F.I.6, the clause 49 listing agreement requires the Directors to cover their internal controls systems and their adequacy in the Management Analysis and Discussion. Under section V (c), the agreement requires the CEO/CFO to accept responsibility for establishing and maintaining internal controls for financial reporting and that they have evaluated the effectiveness of internal control systems of the company pertaining to financial reporting and they have disclosed to the auditors and the Audit Committee, deficiencies in the design or operation of such internal controls, if any, of which they are aware and the steps they have taken or propose to take to rectify these deficiencies.

Reporting on Internal control requirements are also mandated by the Indian Companies Act, 1956 for all companies and a separate annexure to the audit report has to be provided by auditors as per Companies (Auditor's Report) Order, 2003 (CARO). Hence, implementing internal controls is mandated by law not only for listed companies but for all companies. The recently passed Companies Act 2013 also similar audit reporting requirements in addition to reporting of fraud by auditors. This reinforces the need for implementing internal control system and risk management to meet regulatory requirements as well as stakeholder needs.

3.3.5 Compliance in COBIT 5

As discussed in earlier chapters, COSO and COBIT are two most popular frameworks which have been used for ensuring compliance. In this section, we will discuss how compliance is facilitated in COBIT 5 and the specific processes which provide the best practices for implementing compliance process in the organisation. The Management domain of "Monitor, Evaluate and Assess" has a compliance focused process titled: "MEA03 Monitor, Evaluate and Assess Compliance with External Requirements". This process is designed to evaluate that IT processes and IT supported business processes are compliant with laws, regulations and contractual requirements. This requires that the enterprise has processes in place to obtain assurance and that these requirements have been identified and complied with, and integrate IT compliance with overall enterprise compliance. The primary purpose of this process is to ensure that the enterprise is compliant with all applicable external requirements.

Legal and regulatory compliance is a key part of the effective governance of an enterprise. Hence, its inclusion in the GRC term and in the COBIT 5 Enterprise Goals and supporting enabler process structure (MEA03). In addition to MEA03, all enterprise activities include control activities that are designed to ensure compliance not only with externally imposed legislative or regulatory requirements but also with enterprise governance-determined principles, policies and procedures. In addition to activities, COBIT 5 suggests accountabilities, and responsibilities for enterprise roles and governance/management structures (RACI charts) for each process, which also include a compliance-related role.

The COBIT 5 framework includes the necessary guidance to support enterprise GRC objectives and supporting activities. The Governance activities related to GEIT are covered in the five processes of the Governance domain. The risk management process and supporting guidance for risk management spread across the GEIT space meet the compliance need of regulations such as SOX and other similar regulations across the world. COBIT has a specific focus on compliance activities within the framework and explains how they fit within the complete enterprise picture. Inclusion of GRC arrangements within the business framework for GEIT helps enterprises to avoid the main issue with GRC arrangements as silos of activity but instead provides a comprehensive and holistic approach for ensuring compliance.

3.4 Key Management Practices of IT Compliance

COBIT 5 provides key management practices for ensuring compliance with external compliances as relevant to the enterprise. These practices can be adapted as required:

- **Identify External Compliance Requirements:** On a continuous basis, identify and monitor for changes in local and international laws, regulations, and other external requirements that must be complied with from an IT perspective.
- **Optimize Response to External Requirements:** Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated. Consider industry standards, codes of good practice, and best practice guidance for adoption and adaptation
- **Confirm External Compliance:** Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements
- **Obtain Assurance of External Compliance:** Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.

3.4.1 Key Metrics for Assessing Compliance Process

Implementing compliance practices requires monitoring of metrics. A list of sample metrics for reviewing the process of evaluating and assessing compliance are given here for both areas of compliance with external laws and regulations and IT compliances with internal policies:

Compliance with External Laws and Regulations:

- Cost of IT non-compliance, including settlements and fines;
- No. of IT related non-compliance issues reported to board or causing public comment or embarrassment;
- No. of non-compliance issues relating to contractual agreements with IT service providers;
- Coverage of compliance assessments.

IT Compliance with Internal Policies:

- Number of incidents related to non-compliance to policy;
- Percentage of stakeholders who understand policies;
- Percentage of policies supported by effective standards and working practices; and
- Frequency of policies review and updates.

3.5 Using COBIT 5 Best Practices for GRC

Although a GRC program (project) can be implemented primarily from a compliance perspective, it is advisable to consider business requirements also in such a project so as to optimize the investments made in implementing relevant processes, control structures and systems. Implementing GRC requires:

- Defining clearly what GRC requirements are applicable;
- Identifying the regulatory and compliance landscape;
- Reviewing the current GRC status;
- Determining the most optimal approach;
- Setting out key parameters on which success will be measured;
- Using a process oriented approach;
- Adapting global best practices as applicable; and
- Using uniform and structured approach which is auditable.

The responsibility of senior management in implementing and monitoring functioning of requisite GRC measures is a regulatory requirement. However, it also makes business sense to focus not only on compliance but business requirements as well. Using best practices frameworks such as COBIT 5 can help in discharging this responsibility by ensuring that all aspects of GRC are implemented covering both conformance and performance perspectives as required. It is advisable that the board should mandate adaption of a GEIT framework such as COBIT 5, as an integral part of enterprise governance development.

COBIT 5 framework provides the overall approach and based on this, relevant guidance can be selected from specific standards and good practices for designing specific policies, processes, practices and procedures. This ensures that appropriate governance processes and other enablers are developed and optimized so that GEIT operates effectively as part of normal business practice and becomes a supporting culture as demonstrated by top management. Alignment with COBIT 5 best practices would also result in faster and more efficient external audits since COBIT is widely accepted as a basis for IT audit procedures.

Successful implementation of GRC in enterprise can be measured in general by the assurance provided to the senior management on the adequacy of controls implemented. However, specific success of a GRC program can be measured by using the following goals and metrics:

- The reduction of redundant controls and related time to execute (audit, test and remediate);
- The reduction in control failures in all key areas;
- The reduction of expenditure relating to legal, regulatory and review areas;
- Reduction in overall time required for audit for key business areas;
- Improvement through streamlining of processes and reduction in time through automation of control and compliance measures;
- Improvement in timely reporting of regular compliance issues and remediation measures;

- Dashboard of overall compliance status and key issues to senior management on a real-time basis as required.

3.6 Summary

Implementing GRC is mandatory requirement as per law and using the right type of GEIT framework helps in meeting regulatory and management requirements. COBIT 5 is a globally accepted GEIT framework and includes the necessary guidance to support enterprise GRC objectives and supporting activities. The Governance activities related to GEIT are covered in the 5 processes of the Governance domain. The Risk management process and supporting guidance for risk management cut across the GEIT space. Compliance is a specific focus on compliance activities within the GEIT framework and they fit in well to provide the complete enterprise GRC perspective. There is a specific process in COBIT 5 on ensuring compliance. Further, there are specific best practices provided in COBIT 5 which facilitate in meeting compliance requirements. The inclusion of GRC arrangements within the business framework for GEIT helps enterprises to avoid the main issue with GRC arrangements which is silos of activity which are not integrated. Implementing GRC using GEIT framework will help in meeting both conformance and performance requirements. Implementing compliance has considered as project of GRC implementation. Outline of steps to be followed for such implementation have been outlined in this chapter.

The COBIT 5 framework is available to all as a free download from ISACA at www.isaca.org/cobit.

3.7 Questions

1. Which of the following scenarios has the highest impact?
 - A. Absence of business continuity plan.
 - B. Absence of Security operations center.
 - C. Absence of monitoring of SLA.
 - D. Absence of risk management process.
2. Which of the following is the best strategy to address the risk of non-compliance?
 - A. Maintain inventory compliance requirements.
 - B. Embedding risk of non-compliance in operations.
 - C. Appointing chief compliance officer.
 - D. Implement IT governance framework.
3. Implementing IT risk management process is essential for implementing IT governance because IT risk management primarily helps enterprise in:
 - A. Protecting and securing IT resources.
 - B. Arriving at likelihood and impact of risk.
 - C. Optimizing cost of control based on risk.
 - D. Monitoring performance of resources.

4. Which of the following is most important requirement of compliance with governance?
 - A. Monitoring performance
 - B. Whistle blower policy
 - C. Independent directors
 - D. Assurance on controls.
5. Which of the following is main benefit of implementing GRC framework with organization?
 - A. Reduction in compliance expenditure
 - B. Assurance on compliance and controls
 - C. Reduction in internal audit cycles over year
 - D. Availability of compliance status dashboard
6. Which type of non-compliance does situation of an organization using evaluation version of software provided by vendor beyond specified number of days without paying for it?
 - A. Regulatory
 - B. Legal
 - C. Contractual
 - D. Internal
7. Overall reduction in regulatory non-compliances within the organization over a period of time indicates that:
 - A. Governance practices implemented are effective
 - B. The risk response policy adopted is to avoid risk
 - C. Legal framework provides for heavy penalties
 - D. Increase in number of internal audits performed
8. Which of the following is first step in implementing GRC framework with organization?
 - A. Perform IT risk assessment
 - B. Identify internal policy requirements
 - C. Determining critical success factors
 - D. Perform control gap analysis
9. Primary objective of implementing legal and regulatory requirement framework like SOX or clause 49 is to:
 - A. Make management accountable
 - B. Protect stakeholder's interest
 - C. Get assurance on internal controls
 - D. Facilitate trading on stock exchanges

10. GRC compliances were made mandatory because of:
- A. Management override of controls
 - B. Frauds committed by staff members
 - C. Reduction in market value of shares
 - D. Adoption of open economic policy

3.8 Answers and Explanations

1. **A.** Of the options absence of BCP shall have highest impact when incident results in disaster.
2. **B.** Embedding compliance requirements in operations controls in best strategy to mitigate the risks related to on-compliance.
3. **C.** Risk management helps in selecting cost beneficial controls based on exposure. This in turn helps in value creation for organization.
4. **D.** Most important requirement of Governance compliance is assurance on internal controls implemented within organization. Other requirements are important but secondary.
5. **B.** Main benefit of implementing GRC framework is to provide assurance to stakeholders on compliance and internal controls. Others are secondary and subjective.
6. **C.** It is a breach of contract between vendor and organization. Depending on provisions it can be regulatory and internal non-compliance also. It will be legal non-compliance if the software is used without paying and informing to vendor.
7. **A.** Reduction in non-compliances indicates that the governance framework is effective. Others may or may not be concluded.
8. **D.** The first step in implementing GRC framework is to perform control gap analysis in order to achieve the desired state. Identifying policy requirements is performed based on gap analysis. Performing risk assessment also uses the input from control gaps. Deciding critical success factors is done after plan is defined.
9. **B.** Protecting stakeholder's interest has been primary objective of compliance requirements.
10. **A.** Management of some organization's committed financial frauds jeopardizing existence of organizations and hence stakeholder's investments.

CHAPTER 4: KEY ENABLERS OF GEIT

Learning Objectives

An enabler can be defined as capabilities, forces, and resources that contribute to the success of an entity, program, or project. An enabler has a positive impact on the initiative and supports the achievement of the goals and objectives. Enablers represent the heart and lifeblood of any initiative. A key enabler has a significant positive impact on the initiative and compensates to some extent for other factors that may be less positively ranked. Key enablers can also be called as the critical success factors that provide the vision, direction, energy and resources to initiate, sustain and realize their promised benefits. COBIT 5 which is based on seven key enablers can be used for implementing Governance of Enterprise IT (GEIT). This chapter discusses the key enablers of GEIT which facilitate the successful achievement of enterprise goals and IT enabled goals.

4.1 Introduction

Organizations which wish to implement GEIT for achieving enterprise objectives have to consider various key aspects such as goals, objectives, benefit and value for the organisation. However to ensure these are achieved, an appropriate GEIT framework must be implemented. Implementing GEIT does not occur in a vacuum but has to consider the specific environment applicable to the enterprise. We have discussed in earlier chapters how implementation of GEIT can be focussed both on conformance and performance. GEIT implementation has to be taken as a project with an empowered project champion vested with responsibility for results. Selecting and implementing the right type of enablers as required is the key to successful implementation of a GEIT framework. This implementation takes place in different conditions and circumstances determined by numerous factors impacting both internal and external environment and these could be pertain to:

- Ethics and culture of the organisation
- Laws, regulations and policies
- Applicable standards
- Industry practices
- Competitive environment

Implementing GEIT requires consideration of specific aspects applicable to the enterprise and these could pertain to:

- Mission, vision, goals and values
- Governance policies and practices
- Culture and management style
- Models for roles and responsibilities
- Business plans and strategic intentions
- Operating model and level of maturity

4.2 Overview of Seven Enablers of COBIT 5

The best approach to implement GEIT is to build on and enhance the existing approaches so as to be inclusive of IT rather than developing a new approach just for GEIT. Implementing any new initiative requires implementation of required enablers to the required extent as applicable. Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise. They are also the factors that, individually and collectively, influence whether something will work for example: implementing GEIT. In COBIT 5, enablers are driven by the goals cascade, i.e., higher-level IT related goals defining 'what the different enablers should achieve'. There are seven enablers of COBIT 5 which have been described briefly earlier in chapter 2. In this chapter, we will discuss the key characteristics of each of these seven enablers. The step to step approach to implementing Governance and management practices including specific aspects of performance management system using seven enablers are explained in next two chapters.

4.2.1 Principles, policies and framework

The first enabler of COBIT 5 is: "Principles, policies and framework". It may be noted that these enablers although provided in COBIT 5 from a GEIT perspective can be equally applicable and adaptable for any new project or initiative.

The purpose of principles policy and framework is to convey the governing body's and management's direction and instructions. They are instruments to communicate the rules of the enterprise, in support of the governance objectives and enterprise values as defined by the board and executive management. The primary reason for implementing principles, policies and frameworks is to translate the desired strategy into practical guidance for day-to-day management. The key difference between principles and policies are that principles need to be limited in number. The characteristics of good policies are that they should:

- **Be effective:** achieve their purpose
- **Be efficient:** especially when implementing them
- **Non-intrusive:** Should make sense and be logical to those who have to comply with them.

Policies should have a mechanism (framework) in place where they can be effectively managed and users know where to go. Specifically they should be:

- Comprehensive, covering all required areas
- Open and flexible allowing for easy adaptation and change.
- Current and up to date

The purpose of a policy life cycle is that it must support a policy framework in order to achieve defined goals and express clearly as possible the core values of the enterprise. Policies are more detailed guidance on how to put principles into practice. The good practice requirements for policies

and frameworks have to be approved by the Board and senior management. These are important and should specifically cover the following:

- Scope and applicability.
- Consequences of failing to comply with the policy.
- Means of handling exceptions.
- How they will be monitored.

The links and relationships between principles, policies and frameworks and other enablers are:

- Principles, policies and frameworks reflect the cultures, ethics and values of the enterprise.
- Processes are the most important vehicle for executing policies.
- Organizational structures can define and implement policies.
- Policies are part of information which has to be documented and communicated.

4.2.2 Processes

The second enabler of COBIT 5 is “Processes”. COBIT 5 has a specific publication titled: “COBIT 5: Enabling process” which provides specific guidance for the governance and management domains. Let us look at some of the key components and what they cover:

- **A process is defined** as ‘a collection of practices influenced by the enterprises policies, and procedures that takes inputs from a number of sources (including other processes) manipulates the inputs and produces outputs (e.g. products and services).
- **Process practices** are defined as the ‘guidance’ necessary to achieve process goals.
- **Process activities** are defined as the ‘guidance’ to achieve management practices for successful governance and management of enterprise IT.
- **Inputs and Outputs** are the process work products/artefacts considered necessary to support operation of the process.

Process model of COBIT 5 focuses on generic processes required by organization to implement within organization. It clearly distinguishes between Governance processes and management processes. The Governance domain contains five governance processes; within each process, evaluate, direct and monitor (EDM) practices are defined. The four management domains are in line with responsibility areas of plan, build, run and monitor (PBRM). The four management domains are: “Align, Plan and Organise (APO)”, “Build, Acquire and Implement (BAI)”, “Deliver, Support and Service (DSS)” and “Monitor, Evaluate and Assess (MEA)”. There are 32 processes covering the management domain. Each process provides:

- Process description
- Process purpose statement
- IT-related Goals
- Each IT-related goal is associated with a set of generic related metrics
- Process Goals (also from the Goals cascade mechanism and is referred to as Enabler Goals).

- Each process goal is associated or related with a set of generic metrics.
- Each Process contains a set of Management Practices.
- These are associated with a generic RACI chart (Responsible, Accountable, Consulted, Informed)
- Each management practices contains a set of inputs and outputs (called work products)
- Each management Practice is associated with a set of activities.

In addition COBIT 5 identifies the goals for each process and also defines the metrics to measure the performance of each process.

4.2.3 Organisation Structures

The third enabler of COBIT 5 is “Organisation structure”. Establishing accountability mechanisms through appropriate organisation structure is the corner-stone of governance implementation. Deployment of IT requires involvement not only from management (management processes) but also from the Board of directors (governance processes). Hence, the organisation structure has to include establishing specific responsibility for both governance and management. The key role and responsibilities for most of the typical functions in an organisation from governance and management perspective is identified for each of the 200+ management practices covering all the 37 COBIT processes. This is provided in the RACI chart which will help in defining roles, responsibilities covering risks and controls for all critical areas as per COBIT processes and practices. Using these practices will help organisations to establish a number of good practices of organizational structure such as:

- **Operating principles:** The practical arrangements regarding how the structure will operate, such as meeting frequency documentation and other rules
- **Span of control:** The boundaries of the organization structure’s decision rights.
- **Level of authority:** The decisions that the structure is authorized to take.
- **Delegation of responsibility:** The structure can delegate a subset of its decision rights to other structures reporting to it.
- **Escalation procedures:** The escalation path for a structure describes the required actions in case of problems in making decisions.

Implementing right organisation structure from governance perspective requires creation of the right accountability mechanisms and decision-making system. This requires establishing committees at different levels covering all areas right from strategy to execution. Two important committees which are required for implementing effective GEIT are the IT Strategy committee and the IT Steering Committee. The roles and responsibilities of each of these committees is explained in this chapter. Further, clear job definitions have to be provided for all key IT positions so as to ensure that the required IT organisation structure is established. It is also important to understand the roles, responsibilities and risks of key IT personnel. Hence, roles, risks and controls for some of the key IT roles are outlined in this chapter. Understanding of the roles and responsibilities and

customizing these as per requirements of the organisation is critical for implementing GEIT. In establish the right organisation structure for GEIT, it is important to get the distinction between governance and management. This is summarized in the table here.

Table 3.1: Distinction between Governance and Management

Governance	Management
• Evaluate: Stakeholder needs, conditions and options	• Plan, build, run and monitor activities
• Determine: Agreed on enterprise objectives	• Align with: direction set by the governance body
• Set direction: Prioritisation and decision making	• Achieve: Enterprise objectives
• Monitor: Performance and compliance	• Monitor and Report: Performance and conformance
• Responsibility: Board of directors	• Responsibility: Management at all levels

IT Strategy Committee

Governance of enterprise IT should be an integral part of corporate governance, and in this way a primary concern of the board of directors. Boards may carry out their governance duties through committees and they can consider the criticality of IT through an IT strategy committee. The IT strategy committee is composed of board and non-board members. They should assist the board in governing and overseeing the enterprise's IT-related matters. This committee should ensure that IT is a regular item on the board's agenda, where it must be addressed in a structured way. The IT strategy committee should work in close relationship with the other board committees and with management in order to provide input to, and to review and amend the aligned enterprise and IT strategies. The implementation of the IT strategy must be the responsibility of executive management assisted by one or more IT steering committees. Typically, such a steering committee has the responsibility for overseeing major projects and managing IT priorities, IT costs, and IT resource allocation. While the IT strategy committee operates at the board level, the IT steering committee is situated at executive level, which implies that they have different responsibility, authority and membership

IT Steering Committee

Planning is essential for determining and monitoring the direction and achievement of the enterprise goals and objectives. As enterprises are dependent on the information generated by information systems, it is important that planning relating to information systems is undertaken by senior management or by the steering committee. Depending on the size and needs of the enterprise, the senior management may appoint a high-level committee to provide appropriate

direction to IT deployment and information systems and to ensure that the information technology deployment is in tune with the enterprise business goals and objectives. This committee called as the IT Steering Committee is ideally led by a member of the Board of Directors and comprises of functional heads from all key departments of the enterprise including the audit and IT department.

The role and responsibility of the IT Steering Committee and its members must be documented and approved by senior management. As the members comprise of function heads of departments, they would be responsible for taking decisions relating to their departments as required. The IT Steering Committee provides overall direction to deployment of IT and information systems in the enterprises. The key functions of the committee would include:

- To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives;
- To establish size and scope of IT function and sets priorities within the scope;
- To review and approve major IT deployment projects in all their stages;
- To approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc.;
- To review the status of IS plans and budgets and overall IT performance;
- To review and approve standards, policies and procedures;
- To make decisions on all key aspects of IT deployment and implementation;
- To facilitate implementation of IT security within enterprise;
- To facilitate and resolve conflicts in deployment of IT and ensure availability of a viable communication system exists between IT and its users; and
- To report to the Board of Directors on IT activities on a regular basis.

Appointment: The IS Steering Committee is appointed by the Board in order to oversee the IS Department's processes, and it operates at the executive level.

Responsibilities: The duties, responsibilities, authority and accountability of the Steering Committee should be defined in a formal charter, which should be approved by the Board. Members should know IS department policies, practices and procedures. Each member should have the authority to make decisions within the group for his or her respective areas.

Objective: The primary objective of the Steering Committee is to ensure that the IS department is aligned with the organization's mission and objectives. It provides planning and control for the organization's IS function.

Chairman: It should preferably be chaired by a member of the board of directors who understands information technology risks and issues.

Representation: The membership of the committee should be broad-based and should include a cross-section of senior business managers including legal and finance, senior management, user management and IS department.

4.2.4 Roles, Responsibilities and Risks of IT department

Implementing Governance of Enterprise IT requires establishing the right organisation structure with proper accountability mechanism. COBIT 5 provides the RACI chart for each of the process for each of the management practices. In implementing specific processes or management practices, these can be used as a model and adapted as required. Implementing internal control and risk management requires implementing appropriate segregation of duties through job definition of each of the key roles and designations for all key functions in the IT department. The risks and controls of the various roles performed by personnel in the IS Department are briefly outlined here.

Chief Information Officer (CIO)

The CIO reports to the Chief Operating Officer or the Board of Directors and is the overseer of all IT activities in most organizations. He is responsible for the alignment of strategic business goals with the IT processes. Instead of routine day-to-day functions, he focuses on business, IT planning and strategy. The IT processes cover delivery and support of:

- Traditional computer data processing services
- Internet technology
- Telecommunications
- Network services
- User support etc.

Risks

- Inadequate interface with the top management may result in loss of alignment with business and IT processes.
- This position may give him unrestricted access to the system.
- Inadequate background checking and performance review may bring in uncontrollable risks

Controls

In view of the importance of this function the following internal controls may be employed:

- Regular interface with the board of directors.
- Training and other appropriate HR controls in order to ensure competency and trustworthiness.
- Work should be documented and subject to regular reviews.
- Access should be granted on a “need to know”, “need to do” basis.

Application Systems Development Manager (ASDM)

The main role of the ASDM is to oversee the work of

- a) Application systems analysts and
- b) Application programmers, who design, develop and maintain new or existing application programs.

Risks

- Inadequate communication with the CIO may result in loss of effectiveness and efficiency of this important function.
- Work may not be documented and subject to regular reviews.
- Access may have been granted without reference to his job needs.

Controls

- Employ a competent and trusted person by using HR controls.
- Regular interface with the CIO.
- Work should be documented and subject to regular reviews.
- Access should be granted on a “need to know”, “need to do” basis.

Application Systems Analysts

Such persons are responsible for designing application systems based on user specifications, resulting in the development of functional specifications and other high level systems design documents required by the application programmers.

Risks

- Inadequate HR controls may introduce an undesirable person in the company.
- Work may not have been documented and subject to regular reviews.
- Access may have been granted without reference to his job needs.

Controls

- Employ a competent and trusted person by using HR controls.
- Work should be documented and subject to regular reviews.
- Access should be granted on a “need to know”, “need to do” basis.

Application Systems Programmers (ASP)

The main role of the ASP is to develop new application systems and maintain the existing production systems based on the design made by the application systems analyst.

Risks

The main risks are manipulation of live programs and data in order to perpetrate a fraud.

Controls

- Employ a competent and trusted person by using HR controls.
- Should not have access to live programs and data.
- Should work in a test-only environment.
- Should not be allowed to have any change control duties that would enable him to say, modify a program and launch it in the live environment without going through change controls like quality control, security and end user signoff.

Data Administrator (DA)

This role may only be found in large IT environments only, while in smaller IT environments, the functions of the DA may be merged with those of the database administrator. The DA is responsible for the long term planning of the data architecture and management of data. It is basically a policy making and administrative role.

- Undertake strategic data planning, determining user needs
- Specifying validation criteria for data
- Specifying new conceptual and external schema definitions
- Specifying retirement policies for data
- Determining end-user requirements for database tools; testing and evaluating end-user database tools

Database Administrator (DBA)

The DBA performs a technical role, and is responsible for short term planning, design, definition, maintenance and integrity of the database systems in an organization.

- Define, manage, create and retire data
- Specify and change the physical data definition
- Make the database available to users
- Service the users' needs
- Maintain database integrity
- Monitor database operations
- Set up new installation, perform upgrades and migrations
- Select and implement database optimization tools
- Test and evaluate programmer and optimization tools
- Implement database definition controls, access controls, update controls and concurrency controls
- Monitor database usage, collect performance statistics and tune the database
- Define and initiate backup and recovery processes and procedures
- Ensure security of data

Quality management

Quality management is the means by which IS department based processes are controlled, measured and improved. Processes in this context are defined as a set of tasks that when properly performed, produce the desired results. These processes may be split between assurance and control functions. These processes which impact all IT related functions, also follow the PDCA cycle, namely:

- Formulate quality goals
- Implement standards
- Monitor processes, report and train users
- Suggest programs for obtaining improvement in the processes

Quality Assurance Manager

This function deals with assuring adherence to prescribed quality processes in all IT related functions like programming, data entry etc., e.g. ensuring that programs and allied documentation adhere to the prescribed standards and computer naming conventions adopted by the organization.

Quality Control Manager

This function deals with applying quality control procedures, e.g. conducting tests in order to verify and ensure that the software and other allied processes are free from defects before they are transferred to live operations and that it meets the needs and expectations of the end users.

Risks

There will be impairment in quality processes if:

- A person is allowed to carry out a quality review of his own work.
- Incompetent persons are recruited due to inadequate HR controls.
- Quality management do not have independence in their reporting function

Controls

- Employ a competent and trusted person by using HR controls.
- Should be given appropriate training in the latest quality management systems.
- Should not have any application programming responsibilities because QC manager is the “checker” not the “maker” of a system.
- Should report to the CIO to maintain independence.

Security management

Top management should demonstrate their commitment to security by developing an information security management policy considering the nature of business, its assets, technology and the organization structure. This includes the development of business continuity and disaster recovery plans related to IS functions. The approved policy should state the:

- Framework for setting objectives that gives a sense of direction to information security
- Business, legal, regulatory and contractual requirements that apply
- Alignment of the policy with the organization's strategic risk management process
- Criteria for determining how risk will be evaluated

Security Manager

- Maintains the access rules for data and other IS resources.
- Ensures security and confidentiality for the issuance and maintenance of authorised user IDs and passwords.
- Monitors activities for security breaches and take appropriate corrective actions.
- Reviews the security policy and suggest necessary changes.
- Provides appropriate training and awareness programs to users.
- Tests the security processes in order to determine their strengths and weaknesses and detect possible threats.
- Implements new or better security software.

Risks

There will be impairment in the security management processes if:

- Allowed to carry out conflicting work like application programming.
- Incompetent or dishonest persons may be recruited due to inadequate HR controls.
- The security manager may not have independence due to the reporting structure.

Controls

- Should report directly to the CIO in order to maintain independence. In small organizations where this is not possible, the security manager may report to the operations manager, in which case some compensating controls like monitoring and awareness have to be implemented.
- Employ a competent and trusted person by using HR controls.
- Should be given appropriate training in the latest security management systems.
- Should not have any conflicting duties like application programming responsibilities because security manager is the “checker” not the “maker” of a system.

Technical support manager

This function is responsible for overseeing the following technical support functions:

- Systems Analyst
- Systems Programmer
- Systems Administrator
- Network Administrator
- End User Support Manager

Risks

- Incompetent or dishonest persons may be recruited due to inadequate HR controls.

Controls

- Employ a competent and trusted person by using the HR controls.

Systems Analyst

System Analyst is responsible for designing systems software and therefore may have complete access to the system libraries. They interpret the user needs and develop requirements and functional specifications, as well as high-level design documents; which enable programmers to create the particular application.

Risks

- Inappropriate HR controls may lead to employment of persons who may be incompetent or untrustworthy.
- If the computer logs are not enabled, any breach of security will remain undetected.

Controls

- Employ competent and trusted persons by deploying the HR controls.
- Activities should be recorded in the computer logs in order to detect access breaches.
- Access to the system libraries should be granted on a “need to know”, “need to do” basis.

Systems Administrator

This is generally applicable where a network of computers are used. The responsibilities of this function include:

- Creation and deletion of user accounts.
- Installation and maintenance of systems software e.g. the operating system.
- Taking proactive virus prevention measures.

- Allocating storage space for data and programs.
- The addition and configuration of client machines.
- Maintenance of major multi-user computer systems, including local area networks as well as mainframe systems.
- Initiating backups at the end of or during the day.

Risks

- Inappropriate HR controls may lead to employment of persons who may be incompetent or untrustworthy.
- If the computer logs are not enabled, any breach of security will remain undetected.

Controls

- Employ competent and trusted persons by using HR controls.
- Activities should be recorded in the computer logs in order to detect access breaches.
- Access to the system libraries should be granted on a “need to know”, “need to do” basis.
- Should not have any application programming duties.

Network Administrator

They are responsible for the entire network of the organization which may include LANs, WANs and wireless communication and voice networks. The infrastructure of the network may include routers, hubs, switches, firewalls, network segmentation through e.g. VLANs etc. They are also responsible for network performance management, network maintenance, remote access etc. This position is responsible for technical and administrative control over the LAN. This includes ensuring that transmission links are functioning correctly, backups of the system are occurring, and software/hardware purchases are authorized and installed properly.

Risks

- Inappropriate HR controls may lead to employment of persons who may be incompetent or untrustworthy.
- Breach confidentiality, integrity and availability of data by eavesdropping on communication between two nodes on the network or by launching denial-of-service attack.

Controls

- Employ competent and trusted persons by using HR controls.
- Should not have any application programming responsibilities.
- Activities should be recorded in the computer logs in order to detect access breaches.

End User Support Manager

This function is responsible for liaison between the end users and the IS department, including the management of the help desk. The function of the help desk is to resolve the users' hardware and software technical problems through e-mail, telephone or the fax machine. All the reported problems are recorded and the user is given a reference number for his complaint. The help desk will send this complaint to the appropriate engineers who will resolve the problem by telephone, fax, e-mail or by personal visit to the user. The help desk may also acquire hardware or software and train users in order to enable the user to function effectively and efficiently. In very large organizations this function is becoming more and more important. The function may be performed in-house or outsourced.

Risks

- Inappropriate HR controls may lead to employment of persons who may be incompetent or untrustworthy.
- If the computer complaint logs are not enabled, the resolution, frequency and nature of complaints will remain undetected.

Controls

- All user complaints should be logged and allotted a complaint number.
- Depending on the severity of the complaint, the complaint should be forwarded to the appropriate engineer.
- All unresolved problems should be followed up and closed by an independent person.
- Competent and trusted staff should be employed.
- Complaints should be periodically summarised and reviewed for the nature and frequency of the complaints.

Operations Manager

The operations manager's functions include responsibility for computer operations personnel including computer operators, librarians, data entry personnel and maintenance operators. They are also responsible for physical and data security of the department.

Risks

- Inappropriate HR controls may lead to employment of persons who may be incompetent or untrustworthy.
- Unauthorised access to the operations centre may result in breach of security.

Controls

- A competent and trusted person should be employed based on the HR controls.

- Only operations personnel should have access to the operations department, based on the “need to know”, “need to do” access principle.
- All operations and programming functions should always be separated.

4.2.5 Culture, Ethics and Behaviour

The fourth enabler of COBIT 5 is “Culture, ethics and Behaviour”. The principles of this enabler are inbuilt in the processes and other guidance. Organizational Ethics determine the values by which the enterprise want to live (its code). Individual ethics determined by each person’s personal values and dependent to some extent on external factors not always under the enterprise’s control. Individual behaviours which collectively determine the culture of the enterprise and is dependent on both organizational and individual ethics. In governance terms, culture is significantly influenced but what is referred to as “The Tone from the Top”. In other words, the spoken and unspoken messages sent from the IT executive leadership, which in turn influences managerial behaviour and directly influences company plans, policies, and organizational direction. In short, culture is shaped and transformed by consistent patterns of senior management action. Some examples are:

- Behaviour towards risk taking
- Behaviour towards the enterprise’s principles and policies
- Behaviour towards negative outcomes, e.g. loss events

Good practices for creating, encouraging and maintaining desired behaviour throughout the enterprise include:

- Communication throughout the enterprise of desired behaviours and corporate values. (This can be done via a code of ethics)
- Awareness of desired behaviour, strengthened by senior management example. This is one of the keys to a good governance environment when senior management and the executives ‘walk the talk’ so to speak. It is sometimes a difficult area and one that causes many enterprises to fail because it leads to poor governance. (Typically this will be part of a training and awareness sessions based around a code of ethics)
- Incentives to encourage and deterrents to enforce desired behaviour. There is a clear link to HR payment and reward schemes.
- Rules and norms which provide more guidance will typically be found in a Code of Ethics

4.2.6 Information

Information is the fifth and most enabler of COBIT 5. Information is processed using information technology. The success of an enterprise in the digital world depends on how well information is harnessed for achieving enterprise objectives. Information is the most valuable asset and success of an enterprise is determined by how well information is processed and made available to all the stakeholders with the requisite level of security. Ensuring the right type of information using

information systems in safe and secure environment is the most critical aspects of technology deployment. As per COBIT 5, Information is currency of the 21st century. Process requires information and management at all levels require information for decision making and monitoring performance. IT maintains information and hence the attributes of information are most important for business and management. IT supports business process by generating and processing data. The information is then transformed into knowledge that creates value for management and helps in decision which affects the business process. There is a specific publication titled: "COBIT: information" which is designed on the principles of COBIT and provides additional guidance on implementing this most important enabler. The attributes required to assess the context and quality of information to the user which need to be considered, specifically are:

- **Relevancy:** The extent to which information is applicable and helpful for the task at hand
- **Completeness:** The extent to which information is not missing and is of sufficient depth and breath for the task at hand
- **Appropriateness:** The extent to which the volume of information is appropriate for the task at hand.
- **Conciseness:** The extent to which the information is compactly represented.
- **Consistency:** The extent to which the information is presented in the same format.
- **Understandability:** The extent to which the information is easily understandable
- **Ease of Manipulation:** The extent to which information is easy to manipulate and apply to different tasks.

4.2.7 Services, Infrastructure and Applications

The sixth enabler of COBIT 5 is: "Services, infrastructure and Applications". This refers to the services provided by IT to business and stakeholders to meet internal as well as external requirements. Application helps in providing services by processing information. Application is hosted using IT infrastructure. Application software are at the heart of processing of transaction processing and encompass all mission critical processes. In a modern enterprise where services are provided on an on-line, real-time basis, services, infrastructure and applications provide the most critical foundation for providing services to customers. Hence all these three aspects: services, infrastructure and applications must be considered together. Modern applications are complex and interact with various technologies, for example core banking application is hosted on server that processes and provide data in real time to various delivery channels like ATM, Mobile banking, Internet banking, Branch banking. All delivery channels are set of applications focusing on providing services to customers. Hence a bank must consider all these three objects together. COBIT 5 does not have specific publication for this enabler but this is integrated in all the best practices provided by COBIT for all the processes. Further, ITIL framework which is focused on service management can be integrated with COBIT 5.

There are five architecture principles that govern the implementation and use of IT-Related resources. This is part of the good practices of this enabler. Architecture principles are overall

guidelines that govern the implementation and use of IT-related resources within the enterprise. Examples of such principles are:

- **Reuse:** Common components of the architecture should be used when designing and implementing solutions as part of the target or transition architectures.
- **Buy vs. build:** Solutions should be purchased unless there is an approved rationale for developing them internally.
- **Simplicity:** The enterprise architecture should be designed and maintained to be simple as possible while still meeting enterprise requirements.
- **Agility:** The enterprise architecture should incorporate agility to meet changing business needs in an effective and efficient manner.
- **Openness:** The enterprise architecture should leverage open industry standards.

The services, infrastructure and applications as an enabler is also designed and built based on the IT strategic plan which in turn is derived from the enterprise strategic plan. For most enterprises, the investment and cost of this enabler would be the highest and hence needs to be managed both as a one-time projects and as on-going maintenance projects as relevant. Any new business initiative would require IT enabled change which has to be supported by required services, infrastructure and applications and once deployed, there is a need for on-going maintenance to ensure that the required level of services are provided.

4.2.8 People, Skills and Competencies

People, Skill and competencies are the most valuable asset of an enterprise. In an increasingly digital world where most of the routine transaction processing is automated. It is the people with the required skills and competencies who are the key differentiator. IT is only enabler and by itself provide value. Value is derived by how IT is harnessed through right blend of people, process and technology. It is the employees of an enterprise who as knowledge workers use the power of IT to provide services to customers. In the service industry, the human resources are the most valuable asset. Technology can be bought but effective implementation requires people to be trained with the requisite skills and competencies to provide services. Nothing can move unless supported and managed by people who use their intrinsic capacity to analyze information and take decisions. Without people organizations will not exist. People, however possess different skills and organization need people with different skills. In order to ensure appropriate skills organization follow various people management practices like training, motivational programs, career progressions, job rotation.

While defining organization structure organizations also define job description, roles and responsibilities along with competencies required to perform the job. For example IT related activities likes business analysis, system design, development and coding, testing. Organizations also consider outsourcing to ensure appropriate skill and competencies are available to achieve performance and service delivery objectives. For implementing GEIT, organizations require skills

for developing and executing IT Policy formulation, IT strategy, enterprise architecture, innovation, financial management, portfolio management and many such related processes as relevant.

The seven enablers of COBIT 5 have to be implemented in enterprises of all sizes regardless of nature of business or sector or technology deployment. However, the relevance of each these enablers would vary across enterprises. For example, in a software company, the enabler: people, skills and competencies is extremely important whereas in the case of highly regulated industry, the enabler: culture, ethics and behaviour is most important. For successful implementation of GEIT, selecting the right blend of these enablers customised as required is most critical. The enablers also have the openness of integrating across various frameworks.

4.3 Summary

The seven key enablers for implementing GEIT are the building blocks for any technology deployment. This chapter has provided details of key characteristics of each of the seven enablers. These seven enablers are: Principles, policies and framework, Processes, Information, Organisation structure, Services, infrastructure and applications, People, skills and competencies and Culture, ethics and behavior. Each of these enablers is critical. However, information is most valuable for most of the enterprises. Each of these enables have their own characteristics that have to be considered while implementing GEIT. Organization need to ensure that these enablers are implemented as appropriate depending on the requirements of the organisation.

In implementing GEIT, it is most important to note that Governance and management are different concepts. Governance is providing direction and monitoring performance, whereas management is about implementing, executing and monitoring activities as per the strategy to ensure that enterprise objectives are achieved. How well these enablers are effective would also depend on the involvement of senior management with the governance perspective of providing direction and channelizing use of technology from strategic perspective. COBIT 5 provides generic guidance for each of these enablers and in case of processes and information, there are specific publications which provide detailed guidance. However, implementation of these seven enablers requires integration and use of detailed guidance from other relevant frameworks as required. However, considering that COBIT 5 is an umbrella framework, it provides the overall framework for integration of best practice guidance from all frameworks.

4.4 Questions

1. Which of the following is most important resource of the organization?
 - A. Policies and procedures
 - B. IT infrastructure and applications
 - C. Information and data
 - D. Culture, ethics and behaviour

2. Which of the following is most important characteristic of policies?
 - A. Must be limited in number.
 - B. Requires framework to implement.
 - C. Reviewed periodically.
 - D. Non-intrusive and logical.
3. Primary function of a process is to:
 - A. Act on input and generate output.
 - B. Define activities to be performed.
 - C. Focus on achieving business goals.
 - D. Comply with adopted standards.
4. Effective organization structure focuses on:
 - A. Defining designations.
 - B. Delegating responsibility.
 - C. Defining escalation path.
 - D. Deciding span of control.
5. Implementing GEIT is a primary responsibility of which of the following?
 - A. IT steering committee
 - B. IT strategy committee
 - C. IT risk committee
 - D. IT portfolio management
6. Prioritization of IT initiatives within organization is primarily based on:
 - A. Results of risk assessments
 - B. Expected benefit realization
 - C. Recommendations of CIO
 - D. Rate of obsolescence of IT
7. Primary objective of IT steering committee is to:
 - A. Align IT initiatives with business
 - B. Approve and manage IT projects
 - C. Supervise IT and business operations
 - D. Decide IT strategy for organization
8. A data administrator is primarily a:
 - A. Data base administrator
 - B. Data owner
 - C. Data custodian

- D. Data integrator
9. Which of the following is a function of information security manager?
- A. Implement firewalls in organization
 - B. Perform IT risk assessment
 - C. Approve information security policy
 - D. Define rules for implementing ID
10. Which of the following is best control for building requisite skills and competencies within organization?
- A. Hiring only highly qualified people
 - B. Outsourcing the critical operations
 - C. Conducting skill enhancement training
 - D. Defining skill requirements in job description

4.5 Answers and Explanations

1. **C.** Entire GEIT implementation focuses on Information and data. Policies are defined based on nature of information and data, culture and behaviour. IT infrastructure and applications stores, process and communicates information.
2. **D.** Policies are vehicle to communicate intent of management and hence must be clear and easy to implement that will make them effective. B and D are requirements to maintain policies and A is characteristic of principles.
3. **A.** Primary function of process is to process received inputs and generate output to achieve process goals. Process is a set of activities but it is not primary function to define activities. Although processes are defined to achieve business goals, these are broken down to arrive at process goals. Compliance with standards may need certain processes but the primary function is to process input.
4. **B.** Effectiveness of organization structure depends on right level of delegation of responsibilities. Defining designation is only naming of specific role which is not directly relevant. Other options depend upon level of delegation.
5. **B.** IT strategy committee is appointed at board level and they are responsible for implementing GEIT. Other committees are more tactical and operational in nature.
6. **B.** Although the IT steering committee considers all inputs, the primary consideration is expected benefits to the organization.
7. **A.** The primary objective of appointing IT steering committee is to ensure that IT initiatives are in line with business objectives. D is objective of IT strategy committee. B and C are secondary objectives derived from A.

- 8. C. Data administrator is primarily a data custodian.
- 9. D. Information security manager does not perform A, B and C. A is performed by network manager, B is performed by department heads, security manager is facilitator, information security policy is defined by security manager and approved by management.
- 10. C. The best control for building requisite skills and competencies within organization is to ensure skill enhancement training is provided.

CHAPTER 5: PERFORMANCE MANAGEMENT SYSTEMS

Learning Objectives

The Governance processes of ISO 38500 and COBIT 5 primarily focus on “Evaluate, Direct and Monitor”. Governance is an oversight function and evaluates the business environment in terms of the business strategy and objectives, the technology environment, market conditions, competitive environment, regulatory requirements and emerging innovations that could significantly impact and influence the business strategic and operating models of the organisation.

The governance function thus provides the direction that the IT operation should integrate to maximise the support and involvement to the business. The governance function also monitors the performance of the IT operation in terms of its direction and the goals achieved. The ‘direct’ function provides what is expected from management, whereas ‘monitor’ function focuses on whether what was expected has been achieved or not. The challenge is to ‘evaluate’ what is actually achieved and validate whether it is as per set objectives. This evaluation should help enterprise to make a realistic assessment of what was achieved, what are the gaps and how to monitor the performance not only on reactive but proactive basis. This chapter provides an overview of key concepts and models of performance management system.

5.1 Introduction

An effective performance management system is the corner-stone for meeting this challenge and implementing effective governance. This requires setting goals and metrics which are integrated across all the key areas and are measured and monitored. The system of performance measurement can be implemented by use of relevant governance and performance frameworks such as balanced scorecards, maturity models, and quality systems. This chapter provides an overview of performance management systems with specific details of goals cascade from COBIT 5 and also explains the principles of Balanced Scorecard and Strategic Scorecard.

5.2 Performance Measurement

Performance measurement is the process of collecting, analyzing and/or reporting information regarding the performance of an individual, group, organization, system or component. It can involve studying the processes and strategies within organizations or studying enterprise processes, parameters and phenomena, to evaluate whether the results are in line with what was intended or should have been achieved. An important principle of good governance is that management should provide direction using clearly defined and communicated objectives, and then manage adherence to objectives by applying appropriate practices. Monitoring of performance using metrics enables

management to ensure that goals are achieved. In developing a performance management system, it is important to identify the enterprise goals and then obtain understanding of the connection between the entity's mission, vision and strategies and its operating environment.

The board phases of performance measurement system are:

- Establishing and updating performance measures
- Establishing accountability for performance measures
- Gathering and analysing performance data
- Reporting and using performance information

5.3 Performance measurement system

As per COBIT 5: Enterprises exist to create value for their stakeholders. Consequently, any enterprise whether commercial or not, will have value creation as a governance objective. Value creation means realising benefits at an optimal resource cost while optimising risk. Benefits can take many forms, e.g., financial for commercial enterprises or public service for government entities. To assess performance against set objectives, it is important to implement a performance management system which assesses performance against goals by setting right key goals indicators (KGI) and also implementing key process indicators (KPI) to monitor performance of process. Performance measurement system is one of the ways of monitoring and evaluating the business achievements. Getting business value from IT and measuring that value are, therefore, important governance domains. They are responsibilities of both the business and IT and should take both tangible and intangible costs and benefits into account. In this way, good IT performance management should enable both the business and IT to fully understand how IT is contributing to the achievement of business goals, in the past and in the future. IT performance management is aimed at identifying and quantifying IT costs and IT benefits. There are different monitoring instruments available, depending on the features of the costs and benefits.

The ability of enterprise to manage organizational performance is based on how well they the design governance processes that address short-term and long-term management information needs, decisions and control frameworks. Further, enterprise has to identify specific roles, responsibilities, expectations, policies and procedures to be followed for decision-making and accountability. The performance management system has to consider various reward and recognition systems that are implemented and how they might impact performance. Performance is evaluated at various levels such as: at organization level against goals and objectives, resource level against set performance goals by defining key performance indicators (KPI), risk level based on key risk indicators (KRI). There are two approaches for performance measurements:

1. Proactive approach where management implements measure to provide assurance on achieving goals by implementing best practices and using lead indicators.
2. Reactive approach where achievements are compared with goals using lag indicators.

5.4 Goal Setting

Goal setting is the first pre-requisite of performance management. This could be done at different levels of enterprise and each of these need to be integrated and linked together at all levels of the enterprise. At a macro level, the Board of directors set the enterprise direction and goals to be achieved. These are the overall enterprise goals and are derived from the enterprise strategy. The enterprise goals could be set from a top-down or bottom-up or combination of these two approaches. Typically, the top management sets the goal considering the views of the business units. Once the goals are set, the top level goals need to be allocated to function/business units and specific goals set for each of them. From a governance perspective, the enterprise goals will have to be shared by the IT department which will prepare the IT strategy in alignment with the enterprise strategy. Based on the enterprise, the IT department will prepare the IT strategic plan and IT related goals. These IT goals facilitate achievement of enterprise goals. There are various models or frameworks which could be used for implementing performance management system. For example: COBIT 5 goals cascade which is based on the Balanced Scorecard principles. In a manufacturing industry, six sigma or quality management system may be implemented and in a software development company, the Capability Maturity model may be used.

A performance measurement system will broadly have two types of goals. These are:

- **Outcome:** These are called as goals and are evaluated through KGI (key goal indicators). The focus is on achieving the set results. These are also called lag indicators as the measurement of achievement is after the event or period.
- **Performance:** These refer to performance and are evaluated through KPI (key performance indicators). These are also called lead indicators as they measure the performance.

There are many approaches to performance management. In this chapter, we will understand some of the performance management practices based on COBIT 5, Balanced Scorecard and Quality management.

5.5 Performance measurement in COBIT 5

Enterprises exist to create value for their stakeholders. Consequently, any enterprise: commercial or not—will have value creation as a governance objective. Value creation means realising benefits at an optimal resource cost while optimising risk. Benefits can take many forms, e.g., financial for commercial enterprises or public service for government entities. COBIT 5 provides an effective way to understand business and governance priorities and requirements and then use this knowledge when implementing improved governance and management enablers. This approach also enhances the preparation of business cases for governance improvements, obtaining the support of stakeholders, and the realisation and monitoring of the expected benefits. The relationship can be summarised in this top-down flow. COBIT 5 helps ensure strategic alignment and drive what to do, supported by the selected enterprise goals mapped to relevant IT related goals to identified IT

processes and cascaded further into prioritised governance or management practices and activities. COBIT 5 framework provides multiple approaches to setting goals. These could start from identifying stakeholder needs or the governance objectives or directly selecting relevant processes as required.

Enterprises have many stakeholders, and 'creating value' means different—and sometimes conflicting—things to each of them. Governance is about negotiating and deciding amongst different stakeholders' value interests. By consequence, the governance system should consider all stakeholders when making benefit, risk and resource assessment decisions. For each decision, the following questions can and should be asked:

- For whom are the benefits?
- Who bears the risk?
- What resources are required?

Stakeholder needs have to be transformed into an enterprise's actionable strategy. The COBIT 5 goals cascade is the mechanism to translate stakeholder needs into specific, actionable and customised enterprise goals, IT-related goals and enabler goals. This translation allows setting specific goals at every level and in every area of the enterprise in support of the overall goals and stakeholder requirements.



Figure 5.1: The Governance Objective: Value Creation

5.5.1 Goal setting and stakeholder needs

Understanding of current stakeholder needs relating to *GEIT* and current enterprise goals and how they impact *GEIT* is very helpful for three reasons:

- The stakeholder needs and enterprise objectives influence the requirements and priorities of *GEIT*. For example, there could be a focus on cost reduction, compliance or launching a

new business product, each of which could put a different emphasis on current governance priorities.

- The stakeholder needs and enterprise objectives help to focus where attention should be given when improving *GEIT* and
- It assists the business and IT functions to do better forward *planning* of opportunities to add value to the enterprise.

COBIT5 provides useful guidance and examples for defining enterprise and IT related objectives and how they relate to each other. A generic set of 17 enterprise goals and 17 IT related goals is presented as a cascade in the COBIT 5 Framework and Process Reference Guide. These sample goals are provided with relevant metrics. Further, there are mapping tables for stakeholder needs to enterprise goals, enterprise goals to IT goals and IT goals to IT processes which help in easy selection and customisation of the goals as required. This enables users to relate their enterprise's current business and IT environment to specific objectives, and then map them onto the processes that are likely to be relevant in successfully achieving these goals.

5.5.2 Category of Enterprise Goals

Goals to be effective need to be covering all levels of operations of the enterprise. They also need to be linked and automated and used as a measure of evaluating how well the department or employees have performed. Enterprise goals could be categorised as per the table given below.

Table 5.1: Categories of Enterprise goals

Enterprise Goal Category	Relates to ...
Strategic	High-level goals, aligned with and supporting the enterprise's mission or vision
Operational	Effectiveness and efficiency of the enterprise's operations, including performance and profitability goals, which vary based on management's choices about structure and performance
Reporting	The effectiveness of the enterprise's reporting, including internal and external reporting and involving financial or nonfinancial information
Compliance	The enterprise's compliance with applicable laws and regulations

5.5.3 COBIT 5 enterprise and IT relates goals

The COBIT 5 enterprise and IT related goals are used as the basis for setting IT objectives and for establishing a performance measurement framework. IT objectives are expressed as goals and need to be aligned with enterprise goals. COBIT 5 provide structures for defining goals at three levels: for the enterprise, for IT overall, for IT processes. These goals are supported by metrics known as outcome measures because they measure the outcome of a desired goal. The metrics at a specific level also act as performance drivers for achieving higher-level goals. These goals and metrics can be used to set objectives and monitor performance by establishing scorecards and performance reports as well as for driving improvements. COBIT 5 provides guidance on how to define and break down business objectives and create monitoring metrics based on the balanced scorecard.

5.5.4 Requirements for Measures

Measures and performance information need to be linked to strategic management processes. An effective performance management system produces information that provides following benefits:

- It is an early warning indicator of problems and the effectiveness of corrective action.
- It provides input to resource allocation and planning. It can help enterprises prepare for future conditions that are likely to impact program and support function operations and the demands for products and services, such as decreasing personnel or financial resources or changes in work load. Use of measures can give organizations lead times for needed resource adjustments, if these conditions are known in advance.
- It provides periodic feedback to employees, customers and stakeholders about the quality, quantity, cost and timeliness of products and services.

The most important benefit of setting measures is that it builds a common results language among all decision makers. Selected measures define what is important to an enterprise, what it holds itself accountable for, how it defines success and how it structures its improvement efforts.

5.5.5 Performance Measurement processes / indicators

This is considered to be an important part of the IT governance processes. They say that what cannot be measured cannot be improved on. Therefore metrics should be generated for e.g. all products and processes, financial measurement, benchmarking and external party evaluation, satisfaction of customers, internal staff and stakeholders, in order to ensure that they are achieving the desired results. Performance measurement is used to:

- Measure and manage products and services
- Assure accountability

- Make budgeting decisions and
- Optimise performance i.e. improve the productivity of IS to its highest possible level without making unnecessary added investments in the IS infrastructure.

Phases of performance measurement

Performance measurement typically has the following phases:

- Plan, establish and update performance measures
- Plan and establish the accountability of persons for the performance measures
- Collect and analyse data on performance
- Report on performance information and
- Take corrective action

Performance indicators or metrics will determine how well the process is performing in enabling the goals to be achieved. They are also indicators of capabilities and skills of IS personnel.

Examples of performance measures

- Better use of communications bandwidth and computing power
- Lower number of non-compliance with prescribed processes reported
- Better cost and efficiency of the process
- Lower numbers of complaints made by stakeholders
- Better quality and increased innovation etc.
- Lower number of errors and rework
- Improved staff productivity

5.5.6 Measures defined in COBIT

In the context of GEIT, goals and metrics are defined by the COBIT framework at three levels:

1. **Enterprise goals as metrics:** Define the organizational context and objectives and how to measure them
2. **IT-related goals and metrics:** Define what the business expects from IT and how to measure it
3. **Process goals and metrics:** Define what the IT-related process must deliver to support IT's objectives and how to measure it

In these three levels, it is important to make a distinction between outcome measures and performance drivers. Outcome measures indicate whether goals have been met. These can be measured only after the fact and, therefore, are sometimes called lag indicators. Using the COBIT framework, outcome measures inform management whether an IT function, process or activity has achieved its goals.

5.5.7 Enterprise Goals

Enterprise goals are set by the board of directors based on the strategy and objectives. The list of enterprise goals from COBIT 5 are given here. These need to be customised by selecting by what is relevant for the enterprise and adding specific dates, values and number to the identified goals:

1. Stakeholder value of business investments
2. Portfolio of competitive products and services
3. Managed business risk (safeguarding of assets)
4. Compliance with external laws and regulations
5. Financial transparency
6. Customer-oriented service culture
7. Business service continuity and availability
8. Agile responses to a changing business environment
9. Information-based strategic decision making
10. Optimisation of service delivery costs
11. Optimisation of business process functionality
12. Optimisation of business process costs
13. Managed business change programmes
14. Operational and staff productivity
15. Compliance with internal policies
16. Skilled and motivated people
17. Product and business innovation culture

Sample metrics for enterprise goal

1. Stakeholder value of business investments	▪ Percent of investments where value delivered meets stakeholder expectations ▪ Percent of products and services where expected benefits are realised ▪ Percent of investments where claimed benefits are met or exceeded

5.5.8 IT related Goals

COBIT 5 provides IT related goals which are mapped to the enterprise goals. As discussed earlier, the selected IT goals need to be customised as required by adding values, number and dates to make them practically relevant. It may be noted that the IT related goals are closely linked to the

enterprise goals and as per the goals cascade an identified list of IT related goals would be required to achieve enterprise goals. Please refer to COBIT Framework for more details.

1. Alignment of IT and business strategy
2. IT compliance and support for business compliance with external laws and regulations
3. Commitment of executive management for making IT-related decisions
4. Managed IT-related business risk
5. Realised benefits from IT-enabled investments and services portfolio
6. Transparency of IT costs, benefits and risk
7. Delivery of IT services in line with business requirements
8. Adequate use of applications, information and technology solutions
9. IT agility
10. Security of information, processing infrastructure and applications
11. Optimisation of IT assets, resources and capabilities
12. Enablement and support of business processes by integrating applications and technology into business processes
13. Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards
14. Availability of reliable and useful information for decision making
15. IT compliance with internal policies
16. Competent and motivated business and IT personnel
17. Knowledge, expertise and initiatives for business innovation.

Sample metrics for IT related is given below:

01 Alignment of IT and business strategy	▪ Percent of enterprise strategic goals and requirements supported by IT strategic goals ▪ Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services ▪ Percent of IT value drivers mapped to business value drivers

5.5.9 Sample goals and metrics for Resource optimisation

We have discussed earlier that COBIT 5: enabling process publication provides specific guidance for each of the processes. We are giving below an extract for one process to highlight how COBIT 5 specifically provides guidance on performance measures for each process in terms of IT related goals with metrics and process goals with metrics. This demonstrates how goals and metrics can be set in an integrated manner by using and adapting best practices as required.

Process: EDM04 Ensure Resource Optimisation	Area: Governance Domain: Evaluate, Direct and Monitor
Process Description: Ensure that adequate and sufficient IT-related capabilities (people, process and technology) are available to support enterprise objectives effectively at optimal cost.	
Process Purpose Statement: Ensure that the resource needs of the enterprise are met in the optimal manner, IT costs are optimised, and there is an increased likelihood of benefit realisation and readiness for future change.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	Related Metrics
09 IT agility	• Level of satisfaction of business executives with IT's responsiveness to new requirements • Number of critical business processes supported by up-to-date infrastructure and applications • Average time to turn strategic IT objectives into an agreed-on and approved initiative
11 Optimisation of IT assets, resources and capabilities	• Frequency of capability maturity and cost optimisation assessments • Trend of assessment results • Satisfaction levels of business and IT executives with IT-related costs and capabilities
16 Competent and motivated business and IT personnel	• Percent of staff whose IT-related skills are sufficient for the competency required for their role • Percent of staff satisfied with their IT-related roles • Number of learning/training hours per staff member
Process Goals and Metrics	
Process Goal	Related Metrics
1. The resource needs of the enterprise are met with optimal capabilities.	• Level of stakeholder feedback on resource optimisation • Number of benefits (e.g., cost savings) achieved through optimal utilisation of resources

Process: EDM04 Ensure Resource Optimisation	Area: Governance Domain: Evaluate, Direct and Monitor
	• Number of deviations from the resource plan and enterprise architecture strategies
2. Resources are allocated to best meet enterprise priorities within budget constraints.	• Number of deviations from, and exceptions to, resource management principles • Percent of projects with appropriate resource allocations
3. Optimal use of resources is achieved throughout their full economic life cycles.	• Percent of re-use of architecture components • Percent of projects and programmes with a medium- or high-risk status due to resource management issues • Number of resource management performance targets realised

5.6 Balanced scorecard (BSC)

A Balanced Scorecard, as defined by Robert S. Kaplan and David P. Norton, groups objectives, measures, targets, and initiatives into four perspectives: financial, customer, learning and growth, and internal processes. However, some organizations create their own perspectives that align more closely with the way they run their business. Most executives quickly discover that the BSC methodology is more than a performance measurement system. It is also a strategic management system that they can be used to execute strategy and manage organizational performance. BSC is described as a tool to create a "strategy-focused organization"—in which strategy becomes the driving force of organizational activity and communication. The BSC focuses the energy of an organization into achieving strategic goals and objectives that are represented by key performance indicators (KPIs) customized to every group or business unit of the organisation. BSC is a methodology to solve challenges in balancing the theories of a strategy with its execution. BSC has the following characteristics:

- The methodology is suitable for managing business strategy.
- Uses a common language at all levels of the organisation.
- Uses a common set of principles to manage day-to-day operations as well as to framework the organisation's strategy.
- Designed to identify and manage business purposes.
- Provides a balance between certain relatively opposing forces in strategy:
 - Internal and external influences
 - Leading and lagging indicators and measures

- Financial and non-financial goals
- Organizational silos focused on their own goals and an over-arching framework of goals
- Finance priorities and operations
- Aligns strategic goals with objectives, targets, and metrics.

5.6.1 BSC perspectives

The four perspectives of BSC with examples are explained here.

Financial Perspective. The Financial perspective contains measures that indicate whether a strategy is achieving bottom-line results. Financial metrics are classic lagging indicators. The more common ones are:

- Profitability
- Revenue growth
- Economic value added

Customer Perspective. The Customer perspective defines the organization's target customers and the value proposition it offers them, whether it is efficiency (low price, high quality), innovation, or exquisite service. Most customer metrics are lagging indicators of performance, as follows:

- Customer satisfaction
- Customer loyalty
- Market share, "share of wallet"

Internal Process Perspective. Delivering value to customers involves mastering numerous internal processes, including product development, production, manufacturing, delivery, and service. Organizations may need to create brand new processes to meet goals outlined in the Customer perspective. Common metrics are:

- Patents pending, ratio of new products to total products
- Inventory turnover, stock-outs
- Zero defects, on-time deliveries

Learning and Growth Perspective. This perspective measures the internal resources needed to drive the other three perspectives. These include employee skills and information technology. Typical metrics are:

- Employee satisfaction, turnover rate, absenteeism
- Training hours, leadership development programs
- Number of cross-trained employees, average years of service

5.6.2 BSC as a Management tool

The BSC is an invaluable management tool to translate strategy into action and to bring non-financial performance indicators into better focus. BSC is considered to be less effective where uncertain and complex decisions are required to formulate the strategy during times of transformational change. The BSC is used to solve a “measurement problem” but it is also a management system. Traditional financial measurements do not capture the value creating activities in an organisation like skills, competencies, IT etc. It provides a prescription as to what enterprises should measure in order to ‘balance’ the financial perspective. If something cannot be measured, it cannot be improved upon. Metrics allow managers to view their enterprise from many perspectives and therefore, make better decisions. BSC attempts to move businesses from monitoring to measurement; from measurement to management and from management to direction setting:

- **Monitoring:** The art and science of observing employee behaviour and coaching.
- **Measurement:** The art and science of gauging, using numbers and metrics, performance to a task.
- **Management:** The art and science of motivating, coaching, and enabling individuals and teams in the achievement of an objective.
- **Direction setting:** Discovering strategic directions that are unique and differentiating in the marketplace, communicating this to all levels in the organization in the form that they can identify and co-relate their day-to-day actions to the goals.

Successful organisations who are goal-oriented can get a complete perspective of where they are compared to where they want to be. This requires that they have to measure “where we are and how far we have to go”. This assessment helps in identifying the gaps and designing and implementing the roadmap to bridge the gaps. The basis for any action plan is knowledge. Knowledge, using BSC is purposeful and focused on strategic action and this helps in translating strategy into day-to-day action plans and initiatives.

As BSC provides a view of organisation from four perspectives, it is important to develop metrics, collect data and analyse it in relation to these perspectives. BSC has been used in some enterprises to translate strategy into action while others have used it to measure non-financial performance indicators. The BSC is useful in making strategy actionable. BSC is also designed to ensure that performance metrics and strategic themes are balanced with financial and nonfinancial, operational and financial, leading and lagging indicators. A diagrammatic representation of the four perspectives of BSC is given in figure 5.1 here. This clearly highlights how the overall vision and strategy are linked to each of the perspectives with specific objectives, measures, targets and initiatives for each of the four perspectives.

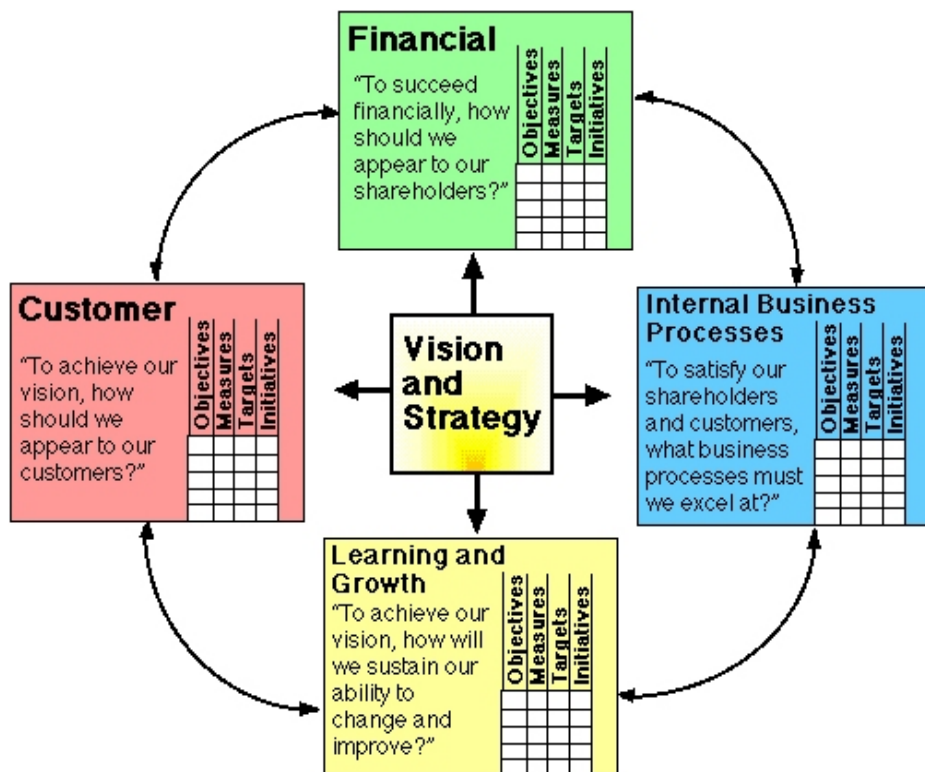


Figure 5.2: The Balanced Scorecard

5.6.3 IT Balanced Scorecard

BSC cascades to all levels of the organization and can be linked with IT. Use of an IT BSC is one of the most effective means to aid the board and management to achieve IT and business alignment. The IT BSC provides a balanced view of the total value delivery of IT to the business. It provides a snapshot of where the IT organization is at a certain point in time. The user orientation perspective represents the user evaluation of IT. The operational excellence perspective represents the IT processes employed to develop and deliver the applications. The future orientation perspective represents the human and technology resources needed by IT to deliver its services over time. The business contribution perspective captures the business value created from the IT investments. Each of these perspectives must be translated into corresponding metrics and measures that assess the current situation. As noted previously, the cause-and-effect relationships between measures are essential components of the IT BSC, and these relationships are articulated by two types of measures: Outcome measures and performance drivers

Outcome measures: Such as programmers' productivity (e.g., number of function points per person per month), need performance drivers, such as IT staff education (e.g., number of education days per person per year) communicate how the outcomes are to be achieved.

Performance drivers: Need outcome measures to ensure a way to determine whether the chosen strategy is effective, especially important in cases where a significant investment is made. These cause-and-effect relationships must be defined throughout the entire scorecard: more and better education of IT staff (future orientation) is an enabler (performance driver) for a better quality of developed systems (operational excellence perspective) that in turn is an enabler for increased user satisfaction (user perspective) that eventually will lead to higher business value of IT (business contribution). The starting point is the vision which leads to the mission and based on the mission, specific strategies are formulated. The chosen strategies should be implemented through appropriate initiatives which have their own milestones and deliverables. The table below illustrates how to implement BSC covering mission and strategies.

Table 5.2: Implementing BSC covering mission and strategies

User Orientation <i>How do the users view the IT department?</i>	Corporate Contribution <i>How does management view the IT department?</i>
Mission To be the preferred supplier of information systems	Mission To obtain a reasonable business contribution of IT investments
Strategies ▪ Preferred supplier of application ▪ Preferred supplier of operations ▪ Partnership with users ▪ User-satisfaction	Strategies ▪ Control of IT expenses ▪ Provide new business capabilities ▪ Business value of new IT projects
Operational excellence <i>How effective and efficient are the IT processes?</i>	Future orientation <i>How well is IT positioned to answer future challenges?</i>
Mission To deliver effective and efficient deliver IT applications and services	Mission To develop opportunities to answer future challenges
Strategies ▪ Efficient an effective software development ▪ Efficient an effective operations	Strategies ▪ Training and education of IT staff ▪ Expertise of IT staff ▪ Age of the application portfolio ▪ Research into emerging IT

5.7 Strategic scorecard

The CIMA (Chartered Institute of Management Accountants) Strategic Scorecard was developed in response to the key findings that emerged from a project led by the International Federation of Accountants (IFAC) and CIMA to develop the framework of enterprise governance. By providing a continuous process with standard progress reporting with which directors become familiar, the CIMA Strategic Scorecard can address all three issues and thus makes for a more effective board. The scorecard approach forms a key element of what has been termed the enterprise governance framework.

The scorecard is a pragmatic and flexible tool that is designed to help boards to fulfil their responsibilities to contribute to and oversee strategy effectively. It is the responsibility of the management team to develop and propose the strategy. However, it is not for the board to undertake the detailed strategic planning. The board's focus should be to challenge the strategy constructively, endorse it and monitor its implementation. The implementation of the scorecard assumes that the organisation has already determined its broad strategic direction and has a strategic plan in place. The scorecard represents a process for developing and moving this strategy forward in a dynamic way.

The enterprise governance framework helps understand the importance of both conformance and performance to the organisation's long-term success. What the scorecard does is to give the board a simple, but effective process that helps it to focus on the key strategic issues and – most importantly – to ask the right questions. This means that the board can work constructively with management to promote the future success of the organisation. The uniqueness of the scorecard lies in the fact that it:

- Summarises the key aspects of the environment in which an organisation is operating to ensure that the board is aware of changing competitor, economic and other factors.
- Identifies the (key) strategic options that could have a material impact on the strategic direction of the organisation and helps the board to determine which options will be developed further and implemented.

Enterprise governance encapsulates two dimensions of corporate governance processes i.e. conformance and performance that need to be kept in balance. This has been discussed earlier in detail in the first chapter: Governance and Management of information systems.

- **Conformance dimension:** Covers issues such as board structures and roles as well as executive remuneration. Codes and/or standards can generally address this dimension with compliance being subject to assurance/audit.
- **Performance dimension:** Focuses on strategy and value creation. The focus is on helping the board to make strategic decisions, understand its appetite for risk and the key drivers of performance. This dimension does not lend itself easily to a regime of standards and audit.



Figure 5.3: Enterprise Governance framework

The enterprise governance framework given above outlines clearly the focus, scope and responsibilities of each of these dimensions. Management has to balance these dimensions.

The primary objectives of using the strategic scorecard are:

- Assist the board in the oversight of a strategic process
- Deal with the strategic choice and transformational change
- Give a true and fair view of the company's strategic position and progress
- Track the actions into and out from the strategic process
- At the heart of the framework is the argument that good corporate governance can help to prevent failure, but it does not guarantee good business performance.

The Strategic Scorecard has four basic elements (Figure 5.3) aimed at helping the board to ensure that all strategic aspects are covered by making the board aware of what work is being done.



Figure 5.4: Strategic Scorecard

1. Strategic Position deals with information on:

- The micro environment e.g. market, competition and customers
- The macro environment e.g. political, economic and regulatory factors
- Threats from changes e.g. strategic inflexion points
- Business position e.g. market share, pricing, quality, service
- Capabilities e.g. core competencies and SWOT analysis which deals with Strengths, Weaknesses, Opportunities and Threats
- Stakeholders e.g. vendors, employees, shareholders

2. Strategic Options deals with what options are available with respect to:

- Scope change e.g. area, product, market sector
- Direction change e.g. high or low growth, price and quality offers

3. Strategic Implementation deals with:

- Project milestones and timelines
- Pursue or abandon the plan etc.

4. Strategic Risks deals with what can go wrong and what must go right with respect to:

- Informing the board on risks and how they are being managed
- Measurement of risks
- Internal controls

Goal Accomplishment processes / indicators: These are used in order to determine the effectiveness of a system by comparing actual performance with predefined business and IT goals. This can be done by using manual or automated logs in order to issue early warnings, for various processes such as:

- Productivity improvements like lower data entry time taken and errors
- Meeting customer requirements for quality
- Lower hardware or software errors
- Lower IS risks
- Standardised processes
- Lower security violations etc.

These goal indicators will determine whether the targets are being met for the processes.

5.8 Methods to report on IT resource performance

In any modern enterprise using IT extensively, the Investment in IT projects is a major investment and the expenditure on IT operations is one of the major revenue items. Hence, it is important to ensure that the metrics are set for this not only at the operational level but at strategic level.

5.8.1 Strategic Metrics for IT Projects

For IT projects, there should be metrics in place to measure IT project effectiveness in terms of timeliness of delivery, budget vs. actual spending, and whether the solutions delivered contributed to the achievement of organizational objectives as noted in their cost benefit analysis. Cost benefit analysis for each potential IT investment should include ROI analysis, transformation costs, and benefits. It also is important to note the distinction between output and outcome and measure each. While output metrics might be useful and possibly the only means of measurement, the internal auditor should analyze these in relation to actual outcomes. In addition, performance-based agreements and incentives should be reviewed to ensure the organization is exercising intended governance. Post-implementation reviews are a useful tool for learning and increasing knowledge of what works and what does not.

5.8.2 Strategic Metrics for IT Operations

Metrics should be in place to measure the effectiveness of the day-to-day operational aspects of the IT function. From an internal perspective, IT management will require more technical metrics such as system uptime/ downtime, helpdesk ticket open-to-closed ratio, peak usage time periods, capacity, and utilization. To enable easier measurement of IT's impact on the achievement of strategic organization goals, it could be helpful to break down these goals into lower level operational component objectives and use various metrics such as SLAs and operations level agreements (OLAs).

5.9 Maturity Model

Capability Maturity Model Integration (CMMI) is a process improvement approach that provides enterprise with the essential elements of effective processes. It can be used to guide process improvement across a project, division or entire organizational CMMI helps integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality processes and a point of reference for appraising current processes.

The COBIT 5 product set includes a process capability model, based on the internationally recognized ISO/IEC 15504 Software Engineering: Process Assessment standard. This model provides a means to measure the performance of any of the governance (Evaluate, Direct and Monitor [EDM]-based) processes or management (Plan, Build, Run and Monitor [PBRM]-based) processes and will allow areas for improvement to be identified.

The ISO/IEC 15504 standard specifies that process capability assessments can be performed for various purposes and with varying degrees of rigor. Purposes can be internal, with a focus on comparisons between enterprise areas and/or process improvement for internal benefit, or they can be external, with a focus on formal assessment, reporting and certification.

5.10 Total Quality Management

Total quality management (TQM) is a management strategy aimed at embedding awareness of quality in all organizational processes. It is a set of systematic activities carried out by the entire enterprise to effectively and efficiently achieve company objectives and provide products and services with a level of quality that satisfies customers at the appropriate time and price. At the core of TQM is a management approach to long-term success through customer satisfaction. In a TQM effort, all members of an enterprise participate in improving processes, products, services and the culture in which they work. Quality management for IT services is a systematic way of ensuring that all the activities necessary to design, develop and implement IT services that satisfy the requirements of the organization and of users take place as planned and that the activities are carried out in a cost-effective manner.

5.11 Quality Management

The scope of the process of "Manage Quality" is to define and communicate quality requirements in all processes, procedures and the related enterprise outcomes, including controls, ongoing monitoring and the use of proven practices and standards in continuous improvement and efficiency efforts. This helps in ensuring the consistent delivery of solutions and services to meet the quality requirements of the enterprise and satisfy stakeholder needs.

The development and maintenance of defined and documented processes by the IS department is evidence of effective governance of information resources. Observance of documented

processes and use of related process management techniques is key to the effectiveness and efficiency of the IS organization. Various standards have emerged to assist IS organisations in achieving these results. Quality standards are increasingly being used to assist IS organisations in achieving an operational environment that is predictable, measurable, repeatable and certified for their IT resources. Quality has to be monitored by setting of appropriate goals and metrics both at strategic and operational level.

Quality management is the means by which IS department-based processes are controlled, measured and improved. Processes in this context are defined as set of tasks that, when properly performed, produce the desired results. Areas of control for quality management may include the following:

- Software development, maintenance and implementation
- Acquisition of hardware and software
- Day-to-day operations
- Service management
- Security
- HR management
- General administration

5.12 Summary

The purpose of performance measurement is to uncover, communicate and evolve organizational performance drivers. The choice of measures communicates to stakeholders what is important, and this affects what gets done. Choosing measures that answer critical management questions improves management's visibility into key processes. This chapter has provided an overview of performance management system with specific details from COBIT 5 using enterprise goals, IT related goals with examples of specific process with IT related goals with related metrics and process goals with related metrics. Further, the key concepts of Balanced scored card with the four perspectives with example of IT BSC have been illustrated. Other examples of performance measurement such as strategic scorecard, maturity model, TQM and total Quality management have been covered in brief.

The key to success is setting goals and monitoring them to ensure success with corrective steps to be taken as required. Use of frameworks helps in setting the right goals with the metrics to measure and monitor successful achievement of the goals. Performance measurement is critical for successful implementation of Governance or GEIT. Performance management helps management in keeping on track towards meeting stakeholder requirements and also in complying with regulatory requirements on time. IS Auditors with knowledge of performance management system can provide assurance or advisory services on the performance management system in place and provide recommendations for improving the effectiveness.

5.13 Questions

1. Which of the following is best approach for monitoring the performance of IT resources?
 - A. Compare lag indicators against expected thresholds
 - B. Monitor lead indicators with industry best practices
 - C. Define thresholds for lag indicators based on long term plan
 - D. Lead indicators have corresponding lag indicator.
2. Performance monitoring using balance score card is most useful since it primarily focuses on:
 - A. Management perspective
 - B. Product and services
 - C. Customer perspectives
 - D. Service delivery processes
3. Which of the following is considered as an example of a lead indicator?
 - A. Number of gaps with respect to industry standard.
 - B. Comparative market position of organization.
 - C. Percentage of growth achieved over three years.
 - D. Improvement in customer satisfaction survey.
4. The **PRIMARY** objective of base lining IT resource performance with business process owners is to:
 - A. define and implement lead and lag indicators.
 - B. ensure resource planning is aligned with industry.
 - C. assess cost effectiveness of outsourcing contracts.
 - D. benchmark expected performance measurement.
5. Which of the following is **BEST** measure to optimize performance of skilled IT human resources?
 - A. Include personal development plan in job description.
 - B. Document personal expectations during exit interviews.
 - C. Implement 'Bring Your Own Device (BYOD)' policy.
 - D. Monitor performance measure against baseline.
6. IT resource optimization plan should primarily focus on:
 - A. Reducing cost of resources
 - B. Ensuring availability
 - C. Conducting training programs

- D. Information security issues
7. The PRIMARY objective of implementing performance measurement metrics for information assets is to:
- A. decide appropriate controls to be implemented to protect IT assets.
 - B. compare performance of IT assets with industry best practices.
 - C. determine contribution of assets to achievement of process goals.
 - D. determine span of control during life cycle of IT assets.
8. Which of the following is the PRIMARY purpose of optimizing the use of IT resources within an enterprise?
- A. To increase likelihood of benefit realization.
 - B. To ensure readiness for future change.
 - C. To reduce cost of IT investments.
 - D. To address dependency on IT capabilities.
9. While monitoring the performance of IT resources the PRIMARY focus of senior management is to ensure that:
- A. IT sourcing strategies focus on using third party services.
 - B. IT resource replacements are approved as per IT strategic plan.
 - C. key goals and metrics for all IT resources are identified.
 - D. resources are allocated in accordance with expected performance.
10. Organization considering deploying application using cloud computing services provided by third party service provider. The MAIN advantage of this arrangement is that it will:
- A. minimize risks associated with IT
 - B. help in optimizing resource utilization.
 - C. ensure availability of skilled resources.
 - D. reduce investment in IT infrastructure.

5.13 Answers and Explanations

1. **B.** Lead indicators are proactive approach for ensuring performance shall be as expected and hence are defined using industry best practices. Lag indicators are useful after the fact (A), Thresholds based on long term plane may not provide input on performance during execution. (C). All lead indicators may not have lag indicator.
2. **C.** The Balance score card (BSC) focuses on Financial, Customer, internal and learning perspective.

3. **A.** Lead indicators are proactive in nature and helps management in planning. Identification of gaps with respect to industry standard is beginning of process of implementing best practices. Other indicators are result of past performance.
4. **D.** In order to plan resources performance of resource must be determined and compared with business expectation from IT. This will help management in implementing performance measures against expected performance. Other options uses baselines.
5. **A.** Motivation helps human resources in performing better. Career progression planning including in job description along with performance norms shall help in motivating human resources.
6. **B.** Resource optimization plan primarily focus on availability of right resources at right time. Other requirements are secondary.
7. **C.** Resource performance is essential to measure the performance of business and IT processes so as to monitor the level of contribution in achieving process goals and hence business objectives. Performance measurement is performed to measure this contribution.
8. **A.** IT resource optimization within an enterprise must primarily focus on increasing benefit realization from IT so as to deliver value to business. **B.** Ensuring readiness for future change is essential to meet the growing IT service delivery and is part of resource optimization requirements, but not the primary purpose. **C.** Resource optimization may or may not reduce IT costs, however it will help in increasing return on IT investment. **D.** Business dependency on IT depends on capabilities of IT to deliver services to business. Resource optimization is one of the processes to address this dependency not objective.
9. **D.** Management must monitor the performance of IT resources to ensure that the expected benefits from IT are being realized as per planned performance. This is done by allocating IT resources in accordance to the planned performance of business process cascaded down to IT resources supporting business processes.
10. **B.** Outsourcing shall help organization in optimizing use of existing IT resources by outsourcing, which in turn shall help in focusing on more critical business requirements and hence improving benefit realization. However outsourcing may or may not minimize risks associated with IT. i.e. it may minimize risks associated with own investment but may introduce risks associated with outsourcing. Although outsourcing helps in ensuring availability of skilled resources, it is not main advantage. Outsourcing may or may not reduce investment in IT, i.e. it may reduce need for acquisition of IT infrastructure, but there is cost associated with outsourcing and there is additional cost for SLA monitoring.

CHAPTER 6: IMPLEMENTING GOVERNANCE AND MANAGEMENT PRACTICES

Learning Objectives

Implementing Governance is about implementing key Governance practices with responsibility set right at the top with Board and executive management involved in all key areas of IT and evaluating, directing and monitoring the use of technology to achieve enterprise goals. COBIT 5 clarifies the distinction between governance and management practices with the addition of a new Governance domain. The design of specific processes and procedures based on COBIT 5 should always fit the needs of the enterprise's culture, management style and IT environment. The guidance in COBIT 5 must be tailored appropriately. It is important to select and adopt the best practices that are recommended but adapt them so that they will be practical and appropriate to each specific enterprise's objectives and needs. The activities provide guidance on what needs to be implemented to achieve a specific management practice. The COBIT 5 practices and activities are based on current relevant standards and best practices which should be used and integrated to obtain more detailed and specific guidance. This chapter briefly describes systematic approach to implementing GEIT and illustrates how to implement GEIT practices in specific areas. It also provides methodology for scoping IS assurance and consulting assignments using COBIT 5 processes.

6.1 Introduction

One of the primary reasons for implementing GEIT is to alleviate pain points. Another reason could be trigger events. Some examples of trigger events could be acquisition/merger, new market conditions or new regulations. Some examples of the pain points faced by enterprises could be:

- Complicated IT assurance efforts due to entrepreneurial nature of many of the organisations.
- Complex IT operating models due to the internet service based business models in use.
- Geographically dispersed entities, made up of diverse cultures and languages.
- The Federated and largely autonomous business control model employed within the group.
- Implementing reasonable levels of IT management, given a highly technical, and at times, volatile IT workforce.
- IT's balancing of the enterprise's drive for innovation capabilities and business agility, with the need to manage risks and have adequate control.
- The setting of risk and tolerance levels for each business unit.
- Increasing need to focus on meeting regulatory (Privacy) and contractual (PCI), compliance requirements.
- Regular audit findings about poor IT controls and reported IT quality of service problems.
- Delivering new and innovative services in a highly competitive market successfully on time.

6.2 Stakeholders in implementing GEIT

There are many stakeholders who need to collaborate to achieve the overall objective of improved IT performance. COBIT5 is based on stakeholder needs and the approach provided in this guide will help to develop an agreed-upon and common understanding of what needs to be achieved to satisfy specific stakeholder concerns in a coordinated and harmonised way. The most important stakeholders and their specific role and responsibilities are outlined here:

- **Board and executive management:** How do we set and define enterprise direction for the use of IT and monitor that relevant and required *GEIT* enablers are established so that business value is delivered and IT-related risks are mitigated?
- **Business management and business process owners:** How do we enable the enterprise to define/align IT-related goals to ensure that business value is delivered from the use of IT and IT-related risks are mitigated?
- **Chief information officer (CIO), IT management and IT process owners:** How do we plan, build, deliver and monitor information and IT solutions and service capabilities as required by the business and directed by the board?
- **Risk, compliance and legal experts:** How do we ensure that we are in compliance with policies, regulations, laws and contracts, and risks are identified, assessed and mitigated?
- **Internal audit:** How do we provide independent assurance on value delivery and risk mitigation?

6.3 Critical Success factors of GEIT implementation

There are many factors which help in successful implementation of GEIT in an enterprise and these vary across enterprises. However, in generally, the critical success factors for a successful GEIT implementation are:

- Top management provides the direction and mandate
- All stakeholders understand the enterprise and IT-related objectives
- Effective communication mechanism and channels are established
- Enablement of the necessary organisational and process changes.
- Frameworks and good practices to fit the purpose and design of the organisation are identified, adapted and used.
- The initial focus is on quick wins and the prioritisation of the most beneficial improvements that are easiest to implement to demonstrate benefit and build confidence for further improvement.
- Benefits of implementation are communicated regularly to all stakeholders.
- Implementation of GEIT is taken as a project with a project champion who is empowered with the requisite responsibility and authority for execution.
- The project implementation is monitored with specific milestones and deliverables.
- On closure of the project, the processes are integrated as part of day to day activities to ensure sustainability.

6.4 Using systematic approach for implementing GEIT

COBIT 5: Implementation provides a systematic approach for implementing GEIT project within an enterprise with specific phases, tasks and activities and roles and responsibilities and deliverables of each of these phases. One of the key enablers of GEIT implementation is “Culture, ethics and behaviour”. This is set by the tone at the top with the senior management establishing and enforcing the right culture. In implementing GEIT, this is most critical. The COSO framework also highlights this. The overall enterprise environment should be analysed to determine the most appropriate change enablement approach. This will include aspects such as the management style, culture (ways of working), formal and informal relationships, and attitudes. It is also important to understand other IT or enterprise initiatives that are ongoing or planned, to ensure that dependencies and impacts are considered. It should be ensured from the start that the required change enablement skills, competencies and experience are available and utilised: for example, by involving resources from the HR function or by obtaining external assistance. As an outcome of this phase, the appropriate balance of directive and inclusive change enablement activities required to deliver sustainable benefits can be designed. A systematic approach for implementing GEIT is provided in the publication: “COBIT 5: Implementation”. This is based on the Kotter model. Brief overview of each of the phases of a GEIT implementation is provided. This approach has to be adapted as per requirements of the project.

6.4.1 Phase 1: Establish the desire to change

The purpose of this phase is to understand the breadth and depth of the envisioned change, the various stakeholders that are impacted, the nature of the impact on and involvement required from each stakeholder group, as well as the current readiness and ability to adopt the change. Current pain points and trigger events can provide a good foundation for establishing the desire to change. The ‘wake-up call’, an initial communication on the programme, can be related to real-world issues that the enterprise may be experiencing. Also, initial benefits can be linked to areas that are highly visible to the enterprise, which creates a platform for further changes and more widespread commitment and buy-in. While communication is a common thread throughout the implementation or improvement initiative, the initial communication or wake-up call is one of the most important and should demonstrate the commitment of senior management—therefore, it should ideally be communicated by the executive committee or CEO.

6.4.2 Phase 2: Form an effective implementation team

Dimensions to consider in assembling the right core implementation team include involving the appropriate areas from business and IT as well as the knowledge and expertise, experience, credibility, and authority of team members. Obtaining an independent, objective view as provided by external parties, such as consultants and change agent, could also be highly beneficial and aid the implementation process or could address skill gaps that may exist within the enterprise. Therefore,

another dimension to consider is the appropriate mix of internal and external resources. The essence of the team should be a commitment to:

- A clear vision of success and ambitious goals
- Engaging the best in all team members, all the time
- Clarity and transparency of team processes, accountabilities and communications
- Integrity, mutual support and commitment to each other's success
- Mutual accountability and collective responsibility
- Ongoing measurement of its own performance and the way it behaves as a team
- Living out of its comfort zone, always looking for ways to improve, uncovering new possibilities and embracing change

It is important to identify potential change agents within different parts of the business that the core team can work with to support the vision and cascade changes down.

6.4.3 Phase 3: Communicate desired vision

A high-level change enablement plan should be developed in conjunction with the overall programme plan. A key component of the change enablement plan is the communication strategy, which should address who the core audience groups are, their behavioural profiles and information requirements, communication channels, and principles. The desired vision for the implementation or improvement programme should be communicated in the language of those affected by it. The communication should include the rationale for and benefits of the change, as well as the impacts of not making the change (purpose), the vision (picture), the road map to achieving the vision (plan) and the involvement required of the various stakeholders (part). Senior management should deliver key messages (such as the desired vision). It should be noted in the communication that both behavioural/cultural and logical aspects should be addressed, and that the emphasis is on two-way communication. Reactions, suggestions and other feedback should be captured and acted upon.

6.4.4 Phase 4: Empower role players and identify quick wins

As core improvements are designed and built, change response plans are developed to empower various role players. The scope of these may include:

- Organisational design changes such as job content or team structures
- Operational changes such as process flows or logistics
- People management changes such as required training and/or changes to performance management and reward systems

Any quick wins that can be realised are important from a change enablement perspective. These could be related to the pain points and trigger events discussed in chapter 2. Visible and unambiguous quick wins can build momentum and credibility for the programme and help to address any scepticism that may exist. It is imperative to use a participative approach in the design

and building of the core improvements. By engaging those impacted by the change in the actual design, e.g., through workshops and review sessions, buy-in can be increased.

6.4.5 Phase 5: Enable operation and use

As initiatives are implemented within the core implementation life cycle, the change response plans are implemented. Quick wins that may have been realised are built on and the behavioural and cultural aspects of the broader transition are addressed (issues such as dealing with fears of loss of responsibility, new expectations and unknown tasks). It is important to balance group and individual interventions to increase buy-in and engagement and to ensure that all stakeholders obtain a holistic view of the change.

Solutions will be rolled out and during this process, mentoring and coaching will be critical to ensure uptake in the user environment. The change requirements and objectives that had been set during the start of the initiative should be revisited to ensure that they were adequately addressed. Success measures should be defined and should include both hard business measures and perception measures that track how people feel about a change.

6.4.6 Phase 6: Embed new approaches

As concrete results are achieved, new ways of working should become part of the enterprise's culture and rooted in its norms and values ('the way we do things around here') - for example, implementing policies, standards and procedures. The implemented changes should be tracked, the effectiveness of the change response plans should be assessed and corrective measures taken as appropriate. This might include enforcing compliance where still required. The communication strategy should be maintained to sustain ongoing awareness.

6.4.7 Phase 7: Sustain

Changes are sustained through conscious reinforcement and an ongoing communication campaign, and they are maintained and demonstrated by continued top management commitment. Corrective action plans are implemented, lessons learned are captured and knowledge is shared with the broader enterprise

6.5 Implementing Governance and Management practices

Implementing Governance and management practices is essential for every enterprise to meet management and regulatory requirements. However, the specific practices which need to be implemented vary depending on various factors such as requirements, current maturity level, management style, regulatory environment, etc. One of the guiding principles in COBIT is the distinction made between governance and management. In line with this principle, every enterprise would be expected to implement a number of governance processes and a number of

management processes to provide comprehensive governance and management of enterprise IT. When considering processes for Governance and management in the context of the enterprise, the difference between types of processes lies within the objectives of the processes.

6.5.1 Governance Processes and Practices

Governance processes

Governance processes deal with the stakeholder governance objectives—value delivery, risk optimisation and resource optimisation—and include practices and activities aimed at evaluating strategic options, providing direction to IT and monitoring the outcome (Evaluate, direct and monitor [EDM])—in line with the ISO/IEC 38500 standard concepts). The relationship between Governance and management is clearly established with Governance being based on the principles of “Evaluate, Direct and Monitor”. COBIT 5 has five Governance processes.

Governance practices

The generic governance practices provided in COBIT 5 to implement Governance are:

- **Evaluate the Governance System:** Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and make judgment on the current and future design of governance of enterprise IT;
- **Direct the Governance System:** Inform leadership and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of IT in line with agreed governance design principles, decision-making models and authority levels. Define the information required for informed decision making; and
- **Monitor the Governance System:** Monitor the effectiveness and performance of the enterprise's governance of IT. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of IT.

6.5.2 Key Management Processes and Practices

Management processes

In line with the definition of management, practices and activities in management processes cover the responsibility areas of PBRM enterprise IT, and they have to provide end-to-end coverage of IT. Although the outcome of both types of processes is different and intended for a different audience, internally, from the context of the process itself, all processes require ‘planning’, ‘building or implementation’, ‘execution’ and ‘monitoring’ activities within the process. The guidance for implementing processes and practices has structure and contents provided in a

consistent manner which can be applied across the enterprises. The processes also have inbuilt PDCA (Plan, Do, Check, Act) cycle for ensuring continuous quality improvement.

Management practices

COBIT 5 has four domains covering all areas of management. There are 32 processes in the four domains of: Align, Plan and Organise (APO), Build, Acquire and Implement (BAI), Deliver, Service and Support (DSS) and Monitor, Evaluate and Assess (MEA). Each of these processes has a set of management practices and there are more than 200 management practices covering all the processes. Further, each of the management practices has a set of activities which can be implemented to achieve the management practices and thus ensure that the required process structure is in place. Please refer to COBIT 5: Process for more details of the process.

6.6 Implementing GEIT in specific areas

Chapter 1 provides generic guidelines on implementing GEIT. Further, in the first section of this chapter we have reviewed the systematic approach with specific phases for implementing GEIT. The most critical factors in implementing GEIT is to identify the scope and objectives of such implementation and based on this prioritise which of the 37 processes the organisation has to select and focus on for making implementation achieve the objectives. The ideal implementation approach would be to take a top-down perspective and obtain understanding of the business' strategic goals through discussions with business-unit management and executives. This will help in understanding of pain points and identifying relevant best practice guidance to adapt and implement. Another critical aspect of implementing GEIT is identifying and setting the outcomes and performance measures for specific goals and activities by using the pragmatic approach of adopt and adapt so as to make these relevant for the organisation. Some specific examples of implementing GEIT in specific areas are explained in the next section of this chapter. These cover key areas such as: Strategic alignment, value optimisation, resource optimisation, outsourcing and capacity management.

6.6.1 Strategic alignment of IT with Business

Strategic alignment and performance measurement are important and apply overall to all the Governance and management activities to ensure that IT goals are aligned with the enterprise goals and there are process goals are set for the IT goals and metrics are designed for these. IT is a key enabler of corporate business strategy. Chief Executive Officers (CEO), Chief Financial Officers (CFO) and Chief Information Officers (CIO) agree that strategic alignment between IT and business objectives are a critical success factor for the achievement of business objectives. Corporate governance drives the corporate information needs to meet business objectives. IT has to provide critical inputs to meet the information needs of all the required stakeholders or it

can be said that enterprise activities require information from IT activities in order to meet enterprise objectives. Hence, corporate governance drives and sets IT governance.

Management Strategy determines at the macro level the path and methodology of rendering services by the enterprise. Strategy outlines the approach of the enterprise and is formulated by the senior management. Based on the strategy adapted, relevant policies and procedures are formulated. From business strategy perspective, IT is affecting the way in which enterprises are structured, managed and operated. One of the most dramatic developments affecting enterprises is the fusion of IT with business strategy. Enterprises can no longer develop business strategy separate from IT strategy and vice versa. Accordingly, there is a need for the integration of sound IT planning with business planning and the incorporation of effective financial and management controls within new systems. Management primarily is focused on harnessing the enterprise resources towards achievement of business objectives. This would involve the managerial processes of planning, organizing, staffing, directing, coordinating, reporting and budgeting.

Objective of IT Strategy

The primary objective of IT strategy is to provide a holistic view of the current IT environment, the future direction, and the initiatives required to migrate to the desired future environment by leveraging enterprise architecture building blocks and components to enable nimble, reliable and efficient response to strategic objectives. Alignment of the strategic IT plans with the business objectives is done by clearly communicating the objectives and associated accountabilities so they are understood by all and all the IT strategic options are identified, structured and integrated with the business plans as required.

IT organizations should define their strategies and tactics to support the organization by ensuring that day-to-day IT operations are delivered efficiently and without compromise. Metrics and goals are established to help IT perform on a tactical basis and also to guide the efforts of personnel to improve maturity of practices. The results will enable the IT function to execute its strategy and achieve its objectives established with the approval of enterprise leaders. Internal audit can determine whether the linkage of IT metrics and objectives aligns with the organization's goals, adequately measure progress being made on approved initiatives, and express an opinion on whether the metrics are relevant and useful. Additionally, auditors can validate that metrics are being measured correctly and represent realistic views of IT operations and governance on a tactical and strategic basis.

IT Strategy Planning

IT strategic plans provide direction to deployment of information systems and it is important that key functionaries in the enterprise are aware and are involved in its development and implementation. Management should ensure that IT long and short-range plans are communicated to business process owners and other relevant parties across the enterprise. Management should

establish processes to capture and report feedback from business process owners and users regarding the quality and usefulness of long and short-range plans. The feedback obtained should be evaluated and considered in future IT planning.

IT Strategic Planning Process

The strategic planning process has to be dynamic in nature and IT management and business process owners should ensure a process is in place to modify the IT long-range plan in a timely and accurate manner to accommodate changes to the enterprise's long-range plan and changes in IT conditions. Management should establish a policy requiring that IT long and short-range plan are developed and maintained. IT management and business process owners should ensure that the IT long-range plan is regularly translated into IT short-range plans. Such short-range plans should ensure that appropriate IT function resources are allocated on a basis consistent with the IT long-range plan. The short-range plans should be reassessed periodically and amended as necessary in response to changing business and IT conditions. The timely performance of feasibility studies should ensure that the execution of the short-range plans is adequately initiated.

Aligning IT Strategy with Enterprise Strategy

The key management practices, which are required for aligning IT strategy with enterprise strategy, are highlighted here:

- **Understand enterprise direction:** Consider the current enterprise environment and business processes, as well as the enterprise strategy and future objectives. Consider also the external environment of the enterprise (industry drivers, relevant regulations, basis for competition).
- **Assess the current environment, capabilities and performance:** Assess the performance of current internal business and IT capabilities and external IT services, and develop an understanding of the enterprise architecture in relation to IT. Identify issues currently being experienced and develop recommendations in areas that could benefit from improvement. Consider service provider differentiators and options and the financial impact and potential costs and benefits of using external services.
- **Define the target IT capabilities:** Define the target business and IT capabilities and required IT services. This should be based on the understanding of the enterprise environment and requirements; the assessment of the current business process and IT environment and issues; and consideration of reference standards, best practices and validated emerging technologies or innovation proposals.
- **Conduct a gap analysis:** Identify the gaps between the current and target environments and consider the alignment of assets (the capabilities that support services) with business outcomes to optimize investment in and utilization of the internal and external asset base. Consider the critical success factors to support strategy execution.

- **Define the strategic plan and road map:** Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT- related goals will contribute to the enterprise's strategic goals. Include how IT will support IT-enabled investment programs, business processes, IT services and IT assets. IT should define the initiatives that will be required to close the gaps, the sourcing strategy, and the measurements to be used to monitor achievement of goals, then prioritize the initiatives and combine them in a high-level road map.
- **Communicate the IT strategy and direction:** Create awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprise.

The success of alignment of IT and business strategy can be measured by reviewing the percentage of enterprise strategic goals and requirements supported by IT strategic goals, extent of stakeholder satisfaction with scope of the planned portfolio of programs and services and the percentage of IT value drivers, which are mapped to business value drivers.

Role of IS Auditors

IS auditors could be involved in providing assurance requiring review of Information Systems as implemented from control perspective. However, auditors may also be required to provide consulting before, during or after implementation of information systems strategy. It becomes imperative for the auditor to understand the concepts of the enterprise strategy as relevant. Hence, auditors must have good understanding of management aspects as relevant to deployment of IT and IT strategy. This would include understanding of the IS Strategy, policies, procedures, practices and enterprise structure, segregation of duties, etc.

6.6.2 Value optimization

Business value from use of IT is achieved by ensuring optimization of the value contribution to the business from the business processes, IT services and IT assets resulting from IT-enabled investments at an acceptable cost. The benefit of implementing this process will ensure that enterprise is able to secure optimal value from IT-enabled initiatives services and assets, cost-efficient delivery of solutions and services, and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.

Key Governance practices

The key management practices, which need to be implemented for evaluating 'whether business value is derived from IT', are highlighted as under:

- **Evaluate Value Optimization:** Continually evaluate the portfolio of IT enabled investments, services and assets to determine the likelihood of achieving enterprise

objectives and delivering value at a reasonable cost. Identify and make judgment on any changes in direction that need to be given to management to optimize value creation.

- **Direct Value Optimization:** Direct value management principles and practices to enable optimal value realization from IT enabled investments throughout their full economic life cycle.
- **Monitor Value Optimization:** Monitor the key goals and metrics to determine the extent to which the business is generating the expected value and benefits to the enterprise from IT-enabled investments and services. Identify significant issues and consider corrective actions.

The success of the process of ensuring business value from use of IT can be measured by evaluating the benefits realized from IT enabled investments and services portfolio and the how transparency of IT costs, benefits and risk is implemented.

Metrics for value optimisation

Some of the key metrics, which can be used for such evaluation, are:

- Percentage of IT enabled investments where benefit realization monitored through full economic life cycle;
- Percentage of IT services where expected benefits realized;
- Percentage of IT enabled investments where claimed benefits met or exceeded;
- Percentage of investment business cases with clearly defined and approved expected IT-related costs and benefits;
- Percentage of IT services with clearly defined and approved operational costs and expected benefits; and
- Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of IT financial information.

6.6.3 Resource Optimization

The process of Resource optimisation has to be implemented to ensure that adequate and sufficient IT related capabilities (people, process and technology) are available to support enterprise objectives effectively at optimal cost. The primary objectives of implementing this process is to ensure that the resource needs of the enterprise are met in the most optimal manner, IT costs are optimised, and there is an increased likelihood of benefit realization and readiness for future change. A key to successful IT performance is the optimal investment, use and allocation of IT resources (people, applications, technology, facilities, data) in servicing the needs of the enterprise. Most enterprises fail to maximize the efficiency of their IT assets and optimize the costs relating to these assets. *GEIT* is concerned with IT value delivery to the business and the mitigation of IT-related risks. This is enabled by the availability and management of adequate resources and the measurement of performance to monitor progress towards the desired goals. ISACA's COBIT 5

introduces a “resource governance” process to “Ensure that the resource needs of the enterprise are met in the optimal manner, IT costs are optimized and there is an increased likelihood of benefit realization and readiness for future change”.

Key Governance practices

The key Governance practices of this process are defined as follows:

- **EDM04.01 Evaluate resource management:** Continuously examine and make judgment on the current and future need for IT-related resources, options for resourcing (including sourcing strategies), and allocation and management principles to meet the needs of the enterprise in the optimal manner.
- **EDM04.02 Direct resource management:** Ensure the adoption of resource management principles to enable optimal use of IT resources throughout their full economic life cycle.
- **EDM04.03 Monitor resource management:** Monitor the key goals and metrics of the resource management processes and establish how deviations or problems will be defined, tracked and reported for remediation.

6.6.4 Sourcing processes

Sourcing is managed through suppliers and appropriate service agreements. COBIT 5 has specific processes: Manage Services and Manage Suppliers which provide specific guidance. The scope of the process of “Manage service agreements” is to align IT-enabled services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of IT services, service levels and performance indicators. This helps in ensuring that IT services and service levels meet current and future enterprise needs.

The scope of process of "Manage Supplier" is to ensure that IT-related services provided by all types of suppliers meet enterprise requirements, including the selection of suppliers, management of relationships, management of contracts, and reviewing and monitoring of supplier performance for effectiveness and compliance. This helps in minimizing the risk associated with non-performing suppliers and ensure competitive pricing.

Sourcing processes refer to the procurement practices of an organization in order to find, evaluate and engage vendors of goods and services are called sourcing processes. The purchasing processes should ensure that the processes are defined and capable of meeting organizational needs. This involves several activities like:

- Timely identification of needs.
- Evaluation of product cost, performance and delivery and installation logistics.
- Method of evaluating that quality needs have been met.
- Contract administration, guarantee replacement or warranty, access to the vendors premises, vendor development and
- Reduction of vendor related risks.

6.6.5 Outsourcing

Outsourcing is a strategic decision for management in order to achieve long-term improvement in business performance, by utilising the vendor's core competencies. Outsourcing is the order of the day for many organizations today. IT is one of the key areas which is outsourced in part or in totality depending on the criticality of the processes. There are many service providers who provide a range of outsourcing services. Although IT outsourcing has many benefits, it has inherent risks which need to be mitigated. The risks are much more when IT outsourcing covers strategic use of IT. Hence, mitigating these risks require all the service provider are managed through an appropriate structure. This vendor management process should not only monitor performance but also include specific functional heads who have the appropriate level of authority to hold the service providers accountable. Some of the important tools which are used to manage and monitor IT service providers are performance targets, service level agreements (SLAs), and scorecards. It is critical to note that senior management cannot abdicate its ultimate responsibility for IT service delivery just because it has been outsourced as the responsibility for compliance and ensuring performance vests with the enterprise. The key principles and guidelines as explained earlier relating to sourcing are applicable to outsourcing as this is also a form of sourcing.

6.6.6 Capacity Management & Growth Planning processes

Capacity management is the process of planning, sizing and continuously optimising IS capacity in order to meet long and short term business goals in a cost effective and timely manner. Its primary goal is to ensure that IT capacity meets current and future business requirements in a cost-effective manner. Capacity management is covered in COBIT in the process of "Manage Configuration." The scope of this process is to define and maintain descriptions and relationships between key resources and capabilities required to deliver IT-enabled services, including collecting configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository. This helps in providing sufficient information about service assets to enable the service to be effectively managed, assess the impact of changes and deal with service incidents.

Capacity management to be effective has to be supported by an effective process of monitoring and evaluating Performance and Conformance. The scope of this process is to collect, validate and evaluate business, IT and process goals and metrics. Monitor that processes are performing against agreed performance and conformance goals and metrics and provide reporting that is systematic and timely. This helps in providing transparency of performance and conformance and drive achievement of goals. Capacity management or configuration management process is used in order to assess the effectiveness and efficiency of the IS operations. Capacity includes:

- Storage space
- Network throughput
- Human resources

- Electronic messaging
- Customer Relationship Management
- Quantum of data processed, etc.

The ITIL framework provides a set of best practices in service delivery and views capacity management from three dimensions:

1. Business Capacity Management
2. Service Capacity Management and
3. Component or resource Capacity Management

The success of capacity management depends on factors like:

- The availability of precise and timely business forecasts
- Having a thorough understanding of present and future technologies
- Proper communication with service management processes
- Planning and acquiring appropriate levels of resources in order to meet business needs

The benefits of good capacity management are:

- Enhanced customer satisfaction
- Better justification of spending on IS resources
- Avoiding incorrect capacity sizing which may lead to inappropriate utilisation of IS resources and insufficient capacity to process the production workloads
- A reduction in capacity failures
- Better alignment of business needs and IS resources
- Better service level management

6.6.7 Capex and Opex

Outsourcing and capacity management requires effective utilisation of resources thereby resulting in business value from investments. There are various options for procuring IT assets. In the current era, IT is being regarded increasingly as a utility and there are vendors providing all types of IT outsourcing services. Use of IT through outside vendors reduces capital expenditure but increases revenue expenditure or it can be said that Capex is converted to Opex. It is important for management to understand the key concepts of Capex and Opex as they impact the funds outflow and ROI on usage of such IT resources. These concepts are briefly explained here.

Capex stands for Capital Expenditures and is the money spent of generating physical assets. Opex stands for Operating Expenditures and refers to day to day expenses required to maintain physical assets. Capex and Opex are necessary to be measured to arrive at the valuation of any organization. Capex is a business expense incurred to create future benefit i.e. acquisition of assets that will have a useful life beyond the tax year. For example expenditure on assets like building, machinery, equipment or upgrading existing facilities so their value as an asset increases. Since capital expenses acquire assets that have a useful life beyond the tax year, these expenses cannot be fully deducted in the year in which they are incurred. Instead, they are capitalized and either

amortized or depreciated over the life of the asset. Intangible assets like intellectual property (e.g. patents) are amortized and tangible assets like equipment are depreciated over their lifespan.

Capex refers to all assets, whether tangible or intangible, that is made use of, to generate more business and thus, revenues. Capex is an investment in the business. It adds to shareholders value. These are expenditures made keeping in mind the future benefits. These investments could be on machinery, equipment, property or upgrade of apparatus. It is usually shown in the financial statement as cash flow or investment in plant, machinery or similar head. Depreciation of such assets takes place every year until it becomes zero. Opex refers to expenses that are incurred on maintenance and running of assets generated through Capex. Day to day running expenses for sales and administration and R&D are taken as Opex. Thus Opex are expenses that are necessary to maintain capital assets. On the other hand, those expenditures required for the day-to-day functioning of the business, like salaries, administrative expenses, maintenance, repairs, etc. These fall under the category of Opex. Opex is the money the business spends in order to turn inventory into throughput. Operating expenses also include depreciation of plants and machinery which are used in the production process or official work. Operating expenditure, on the other hand, can be fully deducted. "Deducted" means subtracted from the revenue when calculating the profit/loss of the business. Most companies are taxed on the profit that they make; so what expenses you deduct impacts your tax bill.

In general, Capex is what needs to be avoided, while Opex is something to be kept under tight control. Opex can be considered to be (in) efficiency of any business. It has a direct relation with the value of the business. If you can reduce Opex without hurting day to day operations, you eventually increase valuation of any business. The concept of Capex and Opex is critical to consider in making IT enabled investment decisions. The distinction between Capex and Opex has become important as most of the organisations now look at outsourcing as the preferred option for all non-core activities. Further, in cloud computing environment, critical activities are outsourced by organisations considering the benefits of converting Capex into Opex. IS Auditors who are required to evaluate such alternatives have to consider not only the cost benefit analysis but also the associated risks and how these risks have been mitigated through implementation of appropriate controls.

6.7 Auditing Governance and Management practices

Technology will keep on evolving on a regular basis. We have seen IT moving from main frame to desktops to laptops to tablets. Similarly, the networking has moved from wired/cabled to wireless and computing is moving from fixed location to cloud computing to mobile computing. Each phase of technology evolution brings with its own benefits and inherent risks. The risks need to be mitigated by implementing appropriate controls and independent assurance is required by management. CA firms with the right Technology skills can exploit this opportunity to provide assurance and consulting services to clients. There are no ready-made solutions/training courses

which can meet all the requirements of CA firms. CA firms have to perform their own SWOT analysis and chalk out the strategy for updating skills to remain relevant with the times. IT strategic planning and IT planning could enable CA firms to successfully ride the technology wave and become thought leaders in the dynamic IT arena.

Auditors whether internal or external, whether general or specialists, have to understand business processes and assess how controls are implemented for any assurance engagement. However, understanding of business process and assessment of controls in an IT environment requires understanding technology and how controls are implemented using technology to mitigate risks. The old approach of putting “ticks” by using checklists is no longer relevant; auditors need to learn how to “click”. It is said auditing was and always will be a thinking person's profession and no software will ever replace that but building relevant IT competencies and skill-sets to harness the power of technology is a must.

Using global best practices can help in developing standard approach for providing IT enabled services. For example, a good understanding of the COBIT 5 Concepts and COBIT 5 Enabling process documents (available at www.isaca.org/cobit) will enable auditors to provide different types of IT enabled services by using a combination relevant processes from the list of 37 processes. These processes have detailed management practices, input-output matrix, RACI chart and activities which can be used as a benchmark and customised for scoping assignments as required. By reading the contents of each of the process, one can get good idea of what is covered in each of these processes. The contents from each of these processes or a combination of selected processes as relevant can be made for preparing the proposal which becomes starting point from discussion regarding scope and objective of the assurance/consulting assignment. Once the scope is agreed upon, the extracted contents from these processes can be customised and used as a benchmark for providing the required services. This annexure provides a list of IT enabled services with title of the assignment, sample scope and objectives of the assignment. This list can be used as the starting point for identifying current competencies and building capabilities to provide services in identified areas of services which can be provided by CAs.

6.8 Summary

Successful implementation of GEIT requires use of systematic approach. This chapter has provided outline of approach for implementing GEIT with specific phases, milestones and deliverables. GEIT implementation requires differentiating governance and management so that senior management has the responsibility with the Board and executive management involved in all key areas of IT and evaluating, directing and monitoring the use of technology to achieve enterprise goals. Management has to understand the governance setting and accordingly work on operationalising these into specific actionable items for implementation.

The definition of Governance and Management from COBIT 5 have been provided. The key principles of Governance and management with detailed list of practices under each of them have

been outlined. Further, specific examples on how to implement governance and management practices in key areas such as strategic alignment, value optimisation, resource optimisation, outsourcing and capacity management have been explained. Finally, IS Auditors have an important role to play in implementing and evaluating GEIT. An overview of the specific role of IS Auditors with examples of how to scope such assignments using COBIT processes have been provided in the appendix.

6.9 Questions

1. Which of the following is MOST critical for implementing GEIT?
 - A. Obtaining financial budget for IT
 - B. Building business case for implementation.
 - C. Creating the right environment.
 - D. Documenting the enterprise architecture
2. Which of the following principles are MOST relevant for Governance domain?
 - A. Plan, Do, Check and Act
 - B. Evaluate, Direct and Monitor
 - C. Plan, Build, Run and Monitor
 - D. Four dimensions of Balanced Scorecard
3. The primary objectives of implementing Resource optimisation process is to ensure:
 - A. resource needs of the enterprise are minimised.
 - B. return on IT investments is ensured
 - C. increased monitoring of benefit realization
 - D. making enterprise IT infrastructure resilient.
4. Which of the following is MOST critical for ensuring sustained alignment of IT strategic plans? The IT strategic plans provide:
 - A. direction to IT department on deployment of information systems
 - B. key functionaries are involved in development and implementation.
 - C. IT long and short-range plans are communicated to stakeholders.
 - D. feedback is captured, reported and evaluated for inclusion in future IT planning.
5. The primary objective of value optimisation process is to ensure:
 - A. IT-enabled investments are made at the lowest cost.
 - B. appropriate IT-enabled initiatives are selected.
 - C. cost-efficient delivery of solutions and services
 - D. Quantification of IT costs and likely benefits

6. Which of the following is the key benefit of capacity management?
 - A. Meet long-term business goals in a cost effective and timely manner
 - B. Meets current and future business requirements in a cost-effective manner
 - C. Define and maintain relationships between key resources and capabilities
 - D. Assess the impact of changes and deal with service incidents.
7. In order to ensure that IT strategic plan is successful, the organization first ensure that the plan:
 - A. focuses on optimization of cost.
 - B. is aligned with business strategy
 - C. provides direction for IT deployment
 - D. consists of long and short term goals
8. Which of the following indicators assurance that IT strategy is focuses on benefit realization?
 - A. Low percentage of IT enabled investments where claimed benefits met or exceeded;
 - B. High percentage of IT services approved based on reduction in operational costs
 - C. High percentage of business cases approved based on costs and benefits
 - D. Satisfaction survey of key stakeholders is neutral on IT service delivery.
9. Which of the following is most important to be included in SLA, while considering the outsourcing of IT operation to cloud service provider?
 - A. Ownership of information
 - B. Periodic audit reports
 - C. Logical access controls
 - D. Reduction in operational costs
10. Which of the following is primary input for IT resource capacity management planning?
 - A. Annual financial budget for IT
 - B. IT resource acquisition plan
 - C. Number of databases in use
 - D. Expected growth of business

6.10 Answers and Explanations

1. C. Creating the right environment is the most critical for implementing GEIT. Obtaining financial budget for IT is an operational activity. Building business case for implementation is done for all

projects and not just for GEIT. Documenting the enterprise architecture may help to some extent in implementing GEIT but is not a critical factor.

2. B. Governance domain is built on the three principles of Evaluate, Direct and Monitor. PDCA is pertaining to continuous improvement initiatives. PBRM is pertaining to management domain. The four dimensions of Balanced Scorecard are useful in translating strategy into action. They are useful aid in implementing Governance as measure of performance management but they are not principles of Governance.

3. C. The primary objectives of implementing Resource optimisation process is to ensure increased monitoring of benefit realization. The resource needs of the enterprise are to be optimised and not minimised. Implementing resource optimisation process does not ensure return on IT investments. In implementing resource optimisation the focus is on utilisation considering the investments and benefits. Resilience of IT infrastructure is considered in the process of maintaining business continuity.

4. D. Capturing, reporting and evaluating feedback for inclusion in future IT planning is MOST critical for ensuring sustained alignment of IT strategic plans as this provides metrics for monitoring and also ensuring that the performance is maintained not only for the current but also for the future. Top management shares the enterprise strategy based on which IT strategy is prepared by the IT department. There is no direction to IT department on deployment of information systems provided as part of IT strategic planning. The involvement of key functionaries in development and implementation is critical to ensure success but it is required in the initial stages. However, this does not guarantee the sustainability of the initiative. The communication of IT long and short-range plans is important to get buy-in and to keep all stakeholders informed but this is only a reporting process.

5. B. The primary objective of value optimisation process is to ensure cost-efficient delivery of solutions and services. The focus of value optimisation process is not on ensuring lowest cost but optimal cost of all IT-enabled investments. Selection of appropriate IT-enabled initiatives is one of the operational activities of value optimisation. Although it is critical but it is not the primary objective. All IT investments benefits cannot be quantified. Hence, the option of quantification of IT costs and likely benefits is not correct. Further, this is not the objective but a mechanism of performance monitoring.

6. B. The key benefit of capacity management is to ensure that not just the current but the future business requirements are met in a cost-effective manner. Capacity management looks at both long-term as well as short-term business goals in a cost effective and timely manner. Defining, describing and maintaining relationships between key resources and capabilities is a primary requirement of capacity management and not a benefit. Assessing the impact of changes and deal

with service incidents is one of the benefits of capacity management but compared to option A, this is not a key benefit.

7. B. IT strategic plan must be aligned with business strategic plan in order to maximize benefit realization, optimize cost, provide direction to management and consist of long term and short term goals.

8. C. Most IT initiatives are approved based on cost and benefits indicates that the IT strategy is focused on benefit realization. B Indicated focus in on cost reduction. A indicates that IT initiatives does not achieve expected benefits and D indicates that IT services are just enough.

9. A. Establishing ownership of assets deployed on infrastructure owned by third party is most essential. Other aspects are required and must be addressed in SLA.

10. D. Expected growth of business is primary input for capacity planning of IT resources. IT resources must fulfil the business requirements. Other options depends on expected business growth.

6.11 References

www.icai.org

www.cit.icai.org

www.isaca.org/cobit

www.ifac.org

www.aicpa.org

www.sox.org

www.theiia.org

<https://cloudsecurityalliance.org/>

<http://www.cag.gov.in/>

<http://deity.gov.in/>

www.coso.org

www.rbi.org.in

SECTION 3: APPENDIX

IT enabled Services in Governance, Management, Assurance and Control using COBIT 5

P.No	Area	Details
1	Process	Ensure Governance Framework Setting and Maintenance
1	Scope	Analyse and articulate the requirements for the governance of enterprise IT, and put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.
1	Objectives	Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT--related decisions are made in line with the enterprise's strategies and objectives, IT--related processes are overseen effectively and transparently, compliance with legal and regulatory requirements are confirmed, and the governance requirements for board members are met.
2	Process	Ensure Benefits Delivery
2	Scope	Optimise the value contribution to the business from the business processes, IT services and IT assets resulting from IT--enabled investments at an acceptable cost.
2	Objectives	Secure optimal value from IT--enabled initiatives services and assets, cost-efficient delivery of solutions and services, and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.
3	Process	Ensure Risk Optimisation
3	Scope	Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and risks to enterprise value related to the use of IT are identified and managed
3	Objectives	Ensure that IT--related enterprise risks do not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimised.
4	Process	Ensure Resource Optimisation
4	Scope	Ensure that adequate and sufficient IT--related capabilities (people, process and technology) are available to support enterprise objectives effectively at optimal cost.
4	Objectives	Ensure that the resource needs of the enterprise are met in the most optimal manner, IT costs are optimised, and there is an increased likelihood of benefit realization and readiness for future change

P.No	Area	Details
5	Process	Ensure Stakeholder Transparency
5	Scope	Ensure that enterprise IT performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and the necessary remedial actions
5	Objectives	Make sure that the communication to stakeholders is effective and timely and the basis for reporting is established in order to increase performance, identify areas for improvement, and confirm that IT--related objectives and strategies are in line with the enterprise's strategy
6	Process	Manage the IT Management Framework
6	Scope	Clarify and maintain the governance of enterprise IT mission and vision. Implement and maintain mechanisms and authorities to manage information and the use of IT in the enterprise in support of governance objectives in line with guiding principles and policies.
6	Objectives	Provide a consistent management approach to enable the enterprise governance requirements to be met, covering management processes, organisational structures, roles and responsibilities, reliable and repeatable activities, and skills and competencies
7	Process	Manage Strategy
7	Scope	Provide a holistic view of the current IT environment, the future direction, and the initiatives required to migrate to the desired future environment, leveraging enterprise architecture building blocks and components to enable nimble, reliable and efficient response to strategic objectives.
7	Objectives	Align strategic IT plans with business objectives. Clearly communicate the objectives and associated accountabilities so they are understood by all, with the IT strategic options identified, structured and integrated with the business plans.
8	Process	Manage Enterprise Architecture
8	Scope	Establish a common architecture consisting of business process, information, data, application and technology architecture layers for effectively and efficiently realising enterprise and IT strategies by creating key models and practices that describe the baseline and target architectures. Define requirements for taxonomy, standards, guidelines, procedures, templates and tools, and provide a linkage for these components. Improve alignment, increase agility, improve quality of information and generate potential cost savings through initiatives such as re--use of building block components.

P.No	Area	Details
8	Objectives	Represent the different building blocks that make up the enterprise and their inter--relationships as well as the principles guiding their design and evolution over time, enabling a standard, responsive and efficient delivery of operational and strategic objectives.
9	Process	Manage Innovation
9	Scope	Maintain an awareness of information technology and related service trends, identify innovation opportunities, and plan how to benefit from innovation in relation to business needs. Analyse what opportunities for business innovation or improvement can be created by emerging technologies, services or IT--enabled business innovation, as well as through existing established technologies and by business and IT process innovation. Influence strategic planning and enterprise architecture decisions
9	Objectives	Achieve competitive advantage, business innovation, and improved operational effectiveness and efficiency by exploiting information technology developments.
10	Process	Manage Portfolio
10	Scope	Execute the strategic direction set for investments in line with the enterprise architecture vision, and the desired characteristics of the investment and related services portfolio, and consider the different categories of investments and the resources and funding constraints. Evaluate, prioritize and balance programmes within resource and funding constraints, based on their alignment with strategic objectives, enterprise worth and risk. Move selected programmes into the active services portfolio for execution. Monitor the performance of the overall portfolio, of services and programmes, proposing adjustments to it as necessary in response to programme performance or changing enterprise priorities.
10	Objectives	Optimise the performance of the overall portfolio of programmes in response to programmer performance and service performance and changing enterprise priorities and demands.
11	Process	Manage Budget and Costs
11	Scope	Manage the IT--related financial activities in both the business and IT functions, covering budgeting, cost and benefit management, and prioritisation of spending through the use of formal budgeting practices and a fair and equitable system of allocating costs to the enterprise. Consult stakeholders to identify and control the total costs and benefits within the context of the IT strategic and tactical plans, and initiate corrective action where needed.

P.No	Area	Details
11	Objectives	Foster partnership between IT and enterprise stakeholders to enable the effective and efficient use of IT--related resources and provide transparency and accountability of the cost and business value of solutions and services. Enable the enterprise to make informed decisions regarding the use of IT solutions and services
12	Process	Manage Human Resources
12	Scope	Provide a structured approach to ensure optimal structuring, placement, decision rights and skills of human resources. This includes communicating the defined roles and responsibilities, learning and growth plans, and performance expectations, supported with competent and motivated people.
12	Objectives	Optimise the human resource capabilities to meet enterprise objectives.
13	Process	Manage Relationships
13	Scope	Manage the relationship between the business and IT in a formalized and transparent way that ensures a focus on achieving a common and shared goal of successful enterprise outcomes in support of strategic goals and within the constraint of budgets and risk tolerance. Base the relationship be based on mutual trust, using open and understandable terms and common language and a willingness to take ownership and accountability for key decisions.
13	Objectives	Create improved outcomes, increased confidence, and trust in IT and effective use of resources.
14	Process	Manage Service Agreements
14	Scope	Align IT--enabled services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of IT services, service levels and performance indicators
14	Objectives	Ensure that IT services and service levels meet current and future enterprise needs.
15	Process	Manage Supplier
15	Scope	Ensure that IT--related services provided by all types of suppliers meet enterprise requirements, including the selection of suppliers, management of relationships, management of contracts, and reviewing and monitoring of supplier performance for effectiveness and compliance.
15	Objectives	Minimize the risk associated with non--performing suppliers and ensure competitive pricing.
16	Process	Manage Quality

P.No	Area	Details
16	Scope	Define and communicate quality requirements in all processes, procedures and the related enterprise outcomes, including controls, ongoing monitoring and the use of proven practices and standards in continuous improvement and efficiency efforts.
16	Objectives	Ensure the consistent delivery of solutions and services to meet the quality requirements of the enterprise and satisfy stakeholder needs
17	Process	Manage Risk
17	Scope	Continually identify, assess and reduce IT--related risks within levels of tolerance set by enterprise executive management
17	Objectives	Integrate the management of IT--related enterprise risk with overall ERIM, and balance the costs and benefits of managing IT-related enterprise risk.
18	Process	Manage Security
18	Scope	Define, operate and monitor a system for information security management.
18	Objectives	Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels
19	Process	Manage Programmes and Projects
19	Scope	Manage all programmes and projects from the investment portfolio in alignment with enterprise strategy and in a co--ordinated way. Initiate, plan, control, and execute programmes and projects, and close with a post--implementation review.
19	Objectives	Realize business benefits and reduce the risk of unexpected delays, costs and value erosion by improving communications to and involvement of business and end users, ensuring the value and quality of project deliverables, and maximizing their contribution to the investment and services portfolio
20	Process	Manage Requirements Definition
20	Scope	Identify solutions and analyse requirements before acquisition or creation to ensure that they are in line with enterprise requirements covering business processes, applications, information/data, infrastructure and services. Co-ordinates with affected stakeholders the review feasible options including relative costs and benefits, risk analysis, and approval of requirements and proposed solutions.
20	Objectives	Create feasible optimal solutions that meet enterprise needs while minimizing risks.
21	Process	Manage Solutions Identification and Build

P.No	Area	Details
21	Scope	Establish and maintain identified solutions in line with enterprise requirements covering design, development, procurement/sourcing, configuration, test preparation, testing, requirements management and maintenance of business processes, applications, information/data, infrastructure and services.
21	Objectives	Establish timely and cost--effective solutions capable of supporting enterprise strategic and operational objectives.
22	Process	Manage Availability and Capacity
22	Scope	Balance current and future needs for availability, performance and capacity with cost--effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements.
22	Objectives	Maintain service availability, efficient management of resources and optimisation of system performance through prediction of future performance and capacity requirements
23	Process	Manage Organisational Change Enablement
23	Scope	Maximise the likelihood of successfully implementing sustainable enterprise wide organisational change quickly and with reduced risk covering the complete life cycle of the change and all affected stakeholders in the business and IT
23	Objectives	Prepare and commit stakeholders for business change and reduce the risk of failure.
24	Process	Manage Changes
24	Scope	Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure and documentation
24	Objectives	Enable fast and reliable delivery of change to the business and mitigation of the risks of negatively impacting the stability or integrity of the changed environment.
25	Process	Manage Change Acceptance and Transitioning
25	Scope	Formally accept and make operational new solutions, including implementation planning, system and data conversion, acceptance testing, communication, release preparation, promotion to production of new or changed business processes and IT services, early production support, and a post--implementation review.
25	Objectives	Implement solutions safely and in line with the agreed--upon expectations and outcomes

P.No	Area	Details
26	Process	Manage Knowledge
26	Scope	Maintain the availability of relevant, current, validated and reliable knowledge to support all process activities and to facilitate decision making, and plan for the identification, gathering, organising, maintaining, use and retirement of knowledge
26	Objectives	Provide the knowledge required to support all staff in their work activities and for informed decision making and enhanced productivity
27	Process	Manage Assets
27	Scope	Manage IT assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational (fit for Objectives), they are accounted for and physically protected, and those assets that are critical to support service capability are reliable and available. Manage software licenses to ensure that the optimal number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with license agreements.
27	Objectives	Account for all IT assets and optimise the value provided by these assets.
28	Process	Manage Configuration
28	Scope	Define and maintain descriptions and relationships between key resources and capabilities required to deliver IT-enabled services, including collecting configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository.
28	Objectives	Provide sufficient information about service assets to enable the service to be effectively managed, assess the impact of changes and deal with service incidents.
29	Process	Manage Operations
29	Scope	Co-ordinate and execute the activities and operational procedures required to deliver internal and outsourced IT services, including the execution of pre-defined standard operating procedures and the required monitoring activities.
29	Objectives	Deliver IT operational service outcomes as planned.
30	Process	Manage Service Requests and Incidents
30	Scope	Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents.
30	Objectives	Achieve increased productivity and minimise disruptions through quick resolution of user queries and incidents.

P.No	Area	Details
31	Process	Manage Problems
31	Scope	Identify and classify problems and their root causes and ensure timely resolution to prevent recurring incidents providing recommendations for improvements
31	Objectives	Increase availability, improve service levels, reduce costs, and improve customer convenience and satisfaction, by reducing the number of operational problems.
32	Process	Manage Continuity
32	Scope	Establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain availability of information at a level acceptable to the enterprise
32	Objectives	Continue critical business operations and maintain availability of information at a level acceptable to the enterprise in the event of a significant disruption
33	Process	Manage Security Services
33	Scope	Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access privileges and perform security monitoring.
33	Objectives	Minimise the business impact of operational information security vulnerabilities and incidents
34	Process	Manage Business Process Controls
34	Scope	Define and maintain appropriate business process controls to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements. Identify the relevant information control requirements and manage and operate adequate controls to ensure that information and information processing satisfy these requirements
34	Objectives	Maintain information integrity and the security of information assets handled within business processes in the enterprise or outsourced
35	Process	Monitor and Evaluate Performance and Conformance
35	Scope	Collect, validate and evaluate business, IT and process goals and metrics. Monitor that processes are performing against agreed performance and conformance goals and metrics and provide reporting that is systematic and timely.
35	Objectives	Provide transparency of performance and conformance and drive achievement of goals.
36	Process	Monitor, Evaluate and Assess the System of Internal Control

P.No	Area	Details
36	Scope	Continuously monitor and evaluate the control environment, including self--assessments and independent assurance reviews. Enable management to identify management deficiencies and inefficiencies and to initiate improvement actions. Plan, organise and maintain standards for internal control assessment and assurance activities
36	Objectives	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risks.
37	Process	Monitor, Evaluate and Assess Compliance with External Requirements
37	Scope	Evaluate that IT processes and IT--supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with and integrate IT compliance with overall enterprise compliance.
37	Objectives	Ensure that the enterprise is compliant with all applicable external requirements.