

Background Material

On

Information Systems Audit 2.0 Course

Volume II



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

© The Institute of Chartered Accountants of India

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 well 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 II

INTRODUCTION TO BACKGROUND MATERIAL	xi
MODULE 4: PROTECTION OF INFORMATION ASSETS	11
SECTION 1: OVERVIEW	11
SECTION 2: CONTENTS.....	17
Chapter 1: Information Risk Management and controls.....	17
Chapter 2: Information Security Management	31
Chapter 3: Information Assets and their Protection	53
Chapter 4: Physical and environmental controls	67
Chapter 5: Logical Access Controls	97
Chapter 6: Network Security Controls.....	135
SECTION 3: APPENDIX	177
MODULE 5: SYSTEMS DEVELOPMENT: ACQUISITION, MAINTENANCE AND IMPLEMENTATION.....	205
SECTION 1: OVERVIEW	205
SECTION 2: CONTENTS.....	213
Chapter 1: System Development Life Cycle (SDLC) introduction and Concepts	213
Chapter 2: Initiating SDLC	239
Chapter 3: Project Management for SDLC	253
Chapter 4: Different models and methods for SDLC.....	281
Chapter 5: System acquisition framework.....	305
Chapter 6: Implementation and Maintenance.....	317
Chapter 7: Trends in technology impacting SDLC.....	339
Chapter 8: SDLC Reviews and Audit	351
SECTION 3: APPENDIX	357
MODULE 6: BUSINESS APPLICATION SOFTWARE AUDIT	371
SECTION 1: OVERVIEW	371
SECTION 2: CONTENTS.....	379
Chapter 1: Business Process and Business Application.....	380

Part 1: Enterprises business models.....	380
Part 2: Business Application Software as per Enterprises Business Model	387
Part 3: Case Studies	391
Chapter 2: Application Control	397
Part 1: Application controls review.....	397
Part 2: Application controls review.....	405
Part 3: Cases of Application controls.....	411
Chapter 3: Auditing Application Control.....	423
Part 1: Audit Program for review of application software.....	423
Part 2: Compliance testing and Substantive testing.....	439
Part 3: Impact of Business application software on Business processes / controls	441
Part 4: User Controls.....	443
Part 5: Database controls	447
Part 6: Financial Reporting and Regulatory requirement in Information Systems	453
Part 7: System Audit Report format as per best practices	459
SECTION 3: APPENDIX	465
Appendix 1: Checklist for Application Controls	465
Appendix 2: ATM Audit Checklist	471
Appendix 3: Application Software Checklist.....	471
Appendix 4: User Rights Creation Checklist.....	471
Appendix 5: Review of business application's impact on controls	475
Appendix 6: System Audit Report.....	476
Appendix 7: Sample Audit Report Of Application Software	479
MODULE 7: BUSINESS CONTINUITY MANAGEMENT (6%)	491
SECTION: OVERVIEW	491
SECTION 2: CONTENTS.....	499
Chapter 1: Business Continuity Management, Business Continuity Planning and Disaster Recovery Planning.....	499
Chapter 2: Strategies for Development of Business Continuity plan	515

Chapter 3: Audit of business Continuity plan	571
SECTION 3: APPENDIX	595
Checklists and control matrix.....	595

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 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-4

Protection of Information Assets

TABLE OF CONTENTS

MODULE 4: PROTECTION OF INFORMATION ASSETS	11
SECTION 1: OVERVIEW	11
Objective.....	11
Learning Objectives.....	11
Task Statements	11
Knowledge Statements	12
Relationship of Task Statements with Knowledge Statements	13
Task and Knowledge Statements Mapping	13
Knowledge Statement Reference Guide	14
SECTION 2: CONTENTS.....	17
Chapter 1: Information Risk Management and controls.....	17
1.1 Introduction	17
1.2 Risk Management	17
1.3 Introduction to Information Systems Controls	18
1.3.1 Need for control and audit of Information systems	18
1.3.2 Objectives of Control.....	20
1.3.3 Internal Controls	21
1.3.4 Types of Internal Controls.....	22
(i) Preventive Controls	22
(ii) Detective Controls	23
(iii) Corrective Controls	23
1.4 Risk and control ownership	24
1.5 Periodic Review and monitoring of risk and controls	25
1.5.1 Controls assessment	25
1.5.2 Control self-assessment	25
1.6 Role of IS Auditor in Information Risk Management	25
1.7 Summary	26
1.8 Questions	26

1.9 Answers and Explanations	28
Chapter 2: Information Security Management	31
2.1 Introduction	31
2.2 Senior management commitment and support	31
2.3 Critical Success Factors to Information Security Management	32
2.4 IT Security Policies, procedures, standards and guidelines	33
2.4.1 What should the policy contain?	33
Data classification and Privacy Policies	33
Acceptable use of information assets policy	34
Physical access and Security Policy	34
Asset Management Policy	34
Business Continuity Management Policy	35
Network Security Policy	35
Password policy	35
2.4.2 Controls over Policy	35
Exceptions	35
2.5 Tools to Implement Policy: Standards Guidelines and Procedures	36
2.6 Information Security Organization	36
2.6.1 Clearly defined duties	37
Segregation of Duties	37
The 'Four Eyes' (Two-person) Principle	37
The Rotation of Duties	38
'Key Man' Policies	38
2.6.2 The Concept of Responsibility in Security	38
Ownership	38
Custodianship	39
Controlling	39
2.7 Role and responsibilities	39
2.7.1 Steering Committee	40
2.7.2 Information Owner	40

2.7.3 Information custodian.....	40
2.7.4 System Owner	40
2.7.5 Process owner.....	41
2.7.6 System Administrator	41
2.7.7 User manager.....	41
2.7.8 Super User.....	41
2.7.9 Security Manager	41
2.8 Human Resources Security	42
2.9 Training and Education.....	42
2.10 Systems Configuration	43
2.11 Information Security and external parties	44
2.12 Issues and challenges of IS Management	44
2.13 Computer crimes and exposures.....	45
2.14 Incident handling and response.....	46
2.15 Implementing Information security policies.....	48
2.15.1 Increasing Awareness	48
2.15.2 Communicating Effectively	48
2.15.3 Simplify enforcement	49
2.15.4 Integrating Security with the corporate culture	49
2.16 Summary.....	49
2.17 Questions	50
2.18 Answers and Explanations	51
Chapter 3: Information Assets and their Protection	53
3.1 Introduction	53
3.2 Why Information classification?	54
3.3 Benefits from information classification	55
3.4 Information Classification policy	56
3.5 Classification schema.....	57
3.6 Data Privacy.....	58

3.7 Compliance requirements for Private data.....	58
3.8 Data Protection.....	59
3.8.1 Data Protection automation and challenges in automation	60
3.9 Classification of other Information Assets.....	61
3.10 Privacy management issues and role of IS Auditors.....	62
3.11 Summary.....	64
3.12 Questions.....	64
3.13 Answers and Explanations	66
Chapter 4: Physical and environmental controls	67
4.1 Introduction	67
4.2 Physical Security controls	67
4.2.1 Objectives of physical access controls	68
4.2.2 Physical Security Threats and Exposures.....	69
4.2.3 Sources of Physical security threats	70
4.2.4 Physical access exposures to assets	70
4.2.5 Physical Security Control Techniques	71
Choosing and designing a secure site.....	71
Security Management.....	72
Emergency Procedures	72
Human resource controls	72
Perimeter security	73
Smart Cards	76
4.2.6 Biometric devices	77
Understanding Biometrics	77
4.2.7 Auditing Physical Access Controls.....	78
4.3 Environmental Controls.....	80
4.3.1 Objectives of Environmental Controls.....	81
4.3.2 Environmental Threats and Exposures.....	81
Natural Threats.	81
Man-made Threats.....	82

Exposures.....	82
4.3.3 Techniques of Environmental Controls.....	83
i. Choosing and designing a safe site	83
ii. Facilities Planning	85
iii. Documentation	85
iv. People Responsibility and Training	85
v. Emergency Plan	86
vi. Vendors/Suppliers (Third Party)	86
vii. Maintenance Plans	86
viii. MTBF and MTTR	86
ix. Fire-resistant walls, Floors and Ceilings	87
x. Concealed Protective Wiring	87
xi. Ventilation and Air Conditioning	87
xii. Power Supplies	87
xiii. Smoke Detectors and Fire Detectors	88
xiv. Fire Alarms	88
xv. Emergency Power Off	88
xvi. Water detectors.....	88
xvii. Fire Suppression Systems	89
a. Water Based Systems	89
b. Gas Based Systems.....	90
4.3.3 Integration and fine-tuning of environmental controls	90
4.3.4 Audit and evaluation of Environmental Controls	90
Documentation of findings.....	91
Examples of environmental controls and their Audit procedures.....	91
4.4 Summary	93
4.5 Questions	93
4.6 Answers and Explanations	95
Chapter 5: Logical Access Controls	97

5.1 Introduction	97
5.2 Objectives of Logical Access Controls	97
5.3 Paths of Logical Access	98
5.4 Logical Access attacks	99
Social Engineering	101
5.5 Logical Access Controls policy and procedures	104
5.5.1 User management.....	104
User registration.....	104
Privilege management.....	105
Password management.....	105
Review of user access rights.....	105
Default Users.....	105
5.5.2 User responsibilities User responsibilities primarily include:	106
5.5.3 Network access control.....	106
Policy on use of network services	106
Segregation of networks	106
Network connection and routing control	106
Enforced path	107
Clock synchronization.....	107
5.5.4 Application and monitoring system access control	107
Sensitive system isolation	107
Event logging.....	107
Monitor system use.....	107
5.5.5 Database access controls.....	108
5.5.6 Operating system access control	108
5.6 Audit Trail.....	109
5.7 Access controls and mobile computing	109
5.8 Access control Mechanism	110
5.8.1 Identification Techniques	110
5.8.2 Authentication Techniques	112

One-Time Passwords	113
Challenge Response	113
5.8.3 Weaknesses of Logon mechanism	113
Recommended practices for strong passwords	114
5.8.4 Attacks on logon/password systems	114
Token Based Authentication	115
5.8.5 Biometric Security	116
5.8.6 Authorization Techniques: Operating Systems	118
5.8.7 Pluggable authentication modules	118
5.8.8 File permissions	119
5.9 Access Control Lists (ACL).....	119
5.10 Identity Management and Access Controls	120
5.11 Privileged logons	121
5.12 Bypass Security Procedures	122
5.13 The Access control Matrix	122
User of Generic / Group IDs:	122
5.14 Single Sign-On (SSO)	123
Active Directory (AD).....	123
Kerberos	124
Weakness of Single sign-on.....	124
Authorization	124
5.15 Access Controls in Operating Systems.....	125
5.16 Database Controls	125
5.16.1 Database Roles and Permissions	126
5.16.2 Application Software Controls in a Database	127
5.17 Audit of Access Controls	128
5.17.1 Audit Test Procedures	129
5.17.2 Logical access: Audit considerations	129
5.17.3 Systems Configuration.....	129
5.17.4 Logical Access mechanisms	130

User account management and password management.....	130
Privileged logons and special user accounts	130
Access to file directories and application logic and system instruction sets	131
5.17.5Bypass Security Procedures.....	131
5.18 Summary.....	131
5.19 Questions.....	131
5.20 Answers and Explanations	133
Chapter 6: Network Security Controls.....	135
6.1 Introduction	135
6.2 Network Characteristics	135
6.3 Threats and Vulnerabilities	136
6.3.1 Information Gathering	137
6.3.2 Exploiting communication subsystem vulnerabilities	138
6.3.3 Protocol Flaws	139
6.3.4 Impersonation.....	139
6.3.5 Message Confidentiality Threats	140
6.3.6 Message Integrity Threats	140
6.3.7 Web Site Defacement	141
6.3.8 Denial of Service	141
6.3.9 Distributed Denial of Service	142
6.3.10 Threats from Cookies, Scripts and Active or Mobile Code	142
6.3.11 Malicious Code.....	143
Viruses.....	143
Logic Bomb/Time Bomb	144
6.3.12 Virus / Malicious Code protection mechanisms:	144
6.4 Current Trends in attacks.....	145
6.4.1 Exploiting application vulnerabilities	145
6.4.2 Advanced persistent threat (APT)	146
6.5 Network Security Controls	146
6.5.1 Architecture	147

6.5.2 Cryptography/Encryption	148
Link Encryption.....	148
End-to-End Encryption.....	149
PKI and Certificates	150
SSL Encryption	151
IPSec	151
Signed Code.....	152
Encrypted E-Mail.....	152
6.5.3 Content Integrity	152
Error Correcting Codes.....	152
Message Digests (Cryptographic Checksums)	153
6.5.4 Strong Authentication.....	153
6.5.5 Remote Access Security.....	154
Virtual Private Networking (VPN)	154
Dial back procedures	154
Other controls.....	155
Authentication Servers.....	155
6.5.6 Firewalls	155
Intranet.....	155
Extranets	156
Securing a Firewall	156
6.5.7 Intrusion Detection Systems	157
6.6 Monitoring Controls	158
6.7 End-point security	159
6.8 Wireless Security threats and Risk Mitigation	160
6.9 Voice-over IP	162
6.9.1 Security Threats to VOIP	162
6.9.2 VOIP Security	163
6.10 Penetration Testing	163
6.10.1 Types of Penetration Testing	164

6.10.2 Risks associated with Penetration Testing	165
6.11 Auditing Network Security	169
6.12 Summary	172
6.13 Questions	172
6.14 Answers and Explanations	174
6.15 References	174
a. Publication:	174
b. Websites:	175
SECTION 3: APPENDIX	177
1. Audit Checklist: Risk Management Process	177
2. Audit of Security management	179
3. Audit of information and asset classification	180
4. Audit checklist for physical and environmental security	181
Some key tips	183
5. Audit Checklist on Logical Access Controls	185
6. Audit Checklist for Network Administration and Security Auditing	187
7. Network Infrastructure Auditing Checklist	192
Network Server	192
Router	192
Firewalls	193

MODULE 4: PROTECTION OF INFORMATION ASSETS

SECTION 1: OVERVIEW

Objective

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.

Learning Objectives

This module focuses on different methods for protecting information assets. This primarily covers following:

- Risk response and definition of controls for protection of information assets
- Essentials of information security management like objectives, processes, policies and procedures and compliance.
- Information asset protection based on information classification
- Essentials of Physical and environmental security
- Logical access controls
- Network and related security processes.
- Audit guidelines for information protection controls

Task Statements

By completing the module, DISAs will be able to perform the following tasks:

- 4.1. Review Risk Management strategy of the enterprise so as to ensure Information security (Confidentiality, Integrity and Availability) and mapping of related risks and controls
- 4.2. Assess IT security management with reference to IT policies, procedures and methodologies that support the entity's strategic plan, IT organization related to system components, IT human resource policies and changes to IT organization and policies with focus on Corporate Security Policy.
- 4.3. Review information security policies of the organization and ensure they are communicated to all relevant stakeholders. Ensure that policies are reviewed, updated and maintained current.
- 4.4. Assess the procedures the entity utilizes to achieve and maintain its objectives in accordance with its established policies and standards and to protect the IT architecture and system assets including information assets against potential risks

Module 4

- 4.5. Review the asset protection mechanism with reference to risk management and ensure that information and other assets are classified and protected in line with security policies and procedures.
- 4.6. Review environmental controls, protection devices and supporting practices
- 4.7. Review the physical access controls for the identification, authentication and restriction of users to authorized facilities
- 4.8. Review logical access controls for the identification, authentication and restriction of users to authorized functions and data.
- 4.9. Evaluate system software configuration and user management such as user rights and administration as per enterprise policies relating to segregation of duties by reviewing user rights granted to specific roles and responsibilities.
- 4.10. Review network security controls with respect to threats and vulnerabilities associated with network and network based infrastructure.
- 4.11. Review the processes and procedures used to encrypt, communicate, store, retrieve, transport and dispose of confidential information assets
- 4.12. Review intrusion detection tools and control techniques (e.g., firewalls, virus detection, spyware)

Knowledge Statements

By completing this module, DISAs will be able to gain knowledge of the following topics:

- 4.1. Best practices of Risk response and control definition strategy and practices.
- 4.2. Principles/Concepts of Information security (threats, vulnerabilities, controls; risk; confidentiality, integrity, availability; security policies, security mechanisms; assurance; prevention, detection,
- 4.3. IT Security Policies, procedures, standards, guidelines and best practices
- 4.4. Human resource policies and changes to IT organization and policies.
- 4.5. IT infrastructure and its relationship to other IT assets like applications, data and information
- 4.6. IT assets and Data classification policy and protection methods including Regulatory requirements of information security, Privacy, etc.
- 4.7. Physical access controls
- 4.8. Environmental controls
- 4.9. Logical access controls at different layers of technology such as Operating System Software and Database Management Software including setting of parameters and user administration and management by using baseline security procedures as relevant.
- 4.10. Security issues in a networked environment. Types of attacks on Information Technology such as cyber-attacks, mobile technology attacks, etc.
- 4.11. Communication controls and encryption (Cryptography, PKI Controls in the Telecommunication sub system including Firewall/IDS, VPN)
- 4.12. Intrusion detection tools and intrusion prevention tools.

Relationship of Task Statements with 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 is DISA 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 and Knowledge Statements Mapping

Task Statements	Knowledge Statements
4.1 Review Risk Management strategy of the enterprise so as to ensure Information security (Confidentiality, Integrity and Availability) and mapping of related risks and controls	4.1 Best practices of Risk response and control definition strategy and practices. 4.2 Principles/Concepts of Information security (threats, vulnerabilities, controls; risk; confidentiality, integrity, availability; security policies, security mechanisms; assurance; prevention, detection,
4.2 Assess IT security management with reference to IT policies, procedures and methodologies that support the entity's strategic plan, IT organization related to system components, IT human resource policies and changes to IT organization and policies with focus on Corporate Security Policy.	4.2 Principles/Concepts of Information security (threats, vulnerabilities, controls; risk; confidentiality, integrity, availability; security policies, security mechanisms; assurance; prevention, detection, 4.3 IT Security Policies, procedures, standards, guidelines and best practices 4.4 Human resource policies and changes to IT organization and policies.
4.3 Review information security policies of the organization and ensure they are communicated to all relevant stakeholders. Ensure that policies are reviewed, updated and maintained current.	4.3 IT Security Policies, procedures, standards, guidelines and best practices
4.4 Assess the procedures the entity utilizes to achieve and maintain its objectives in accordance with its established policies and standards and to protect the IT architecture and system assets including information assets against potential risks	4.3 IT Security Policies, procedures, standards, guidelines and best practices 4.5 IT infrastructure and its relationship to other IT assets like applications, data and information

4.5 Review the asset protection mechanism with reference to risk management and ensure that information and other assets are classified and protected in line with security policies and procedures.	4.6 IT assets and Data classification policy and protection methods including Regulatory requirements of information security, privacy, etc.
4.6 Review environmental controls, protection devices and supporting practices	4.8 Environmental controls
4.7 Review the physical access controls for the identification, authentication and restriction of users to authorized facilities	4.7 Physical access controls
4.8 Review logical access controls for the identification, authentication and restriction of users to authorized functions and data.	4.9 Logical access controls at different layers of technology such as Operating System Software and Database Management Software including setting of parameters and user administration and management by using baseline security procedures as relevant.
4.9 Evaluate system software configuration and user management such as user rights and administration as per enterprise policies relating to segregation of duties by reviewing user rights granted to specific roles and responsibilities.	4.9 Logical access controls at different layers of technology such as Operating System Software and Database Management Software including setting of parameters and user administration and management by using baseline security procedures as relevant.
4.10 Review network security controls with respect to threats and vulnerabilities associated with network and network based infrastructure.	4.10 Security issues in a networked environment. Types of attacks on Information Technology such as cyber-attacks, mobile technology attacks, etc.
4.11 Review the processes and procedures used to encrypt, communicate, store, retrieve, transport and dispose of confidential information assets	4.11 Communication controls and encryption (Cryptography, PKI Controls in the Telecommunication sub system including Firewall/IDS, VPN)
4.12 Review intrusion detection tools and control techniques (e.g., firewalls, virus detection, spyware)	4.12 Intrusion detection tools and intrusion prevention tools.

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 described in greater detail in the forthcoming part of this module.

Knowledge Statements	Chapter / Section
Best practices of Risk response and control definition strategy and practices.	Chapter 1 - 1.2 to 1.7
Principles/Concepts of Information security (threats, vulnerabilities, controls; risk; confidentiality, integrity, availability; security policies, security mechanisms; assurance; prevention, detection,	Chapter 2 – 2.1 to 2.3, 2.6, 2.11 to 2.14
IT Security Policies, procedures, standards, guidelines and best practices	Chapter 2 - 2.4 to 2.6, 2.15
Human resource policies and changes to IT organization and policies.	Chapter 2 – 2.7 to 2.9
IT infrastructure and its relationship to other IT assets like applications, data and information	Chapter 3 – 3.1 to 3.11,
IT assets and Data classification policy and protection methods including Regulatory requirements of information security, Privacy,	Chapter 3 – 3.1 to 3.11
Physical access controls	Chapter 4 – 4.1 and 4.2
Environmental controls	Chapter 4 – 4.1 and 4.3
Logical access controls at different layers of technology such as Operating System Software and Database Management Software including setting of parameters and user administration and management by using baseline security procedures as relevant.	Chapter 5 – 5.1 to 5.18
Security issues in a networked environment. Types of attacks on Information Technology such as cyber-attacks, mobile technology attacks, etc.	Chapter 6 – 6.1 to 6.4
Communication controls and encryption (Cryptography, PKI Controls in the Telecommunication sub system including Firewall/IDS, VPN)	Chapter 6 – 6.3 to 6.10
Intrusion detection tools and intrusion prevention tools.	Chapter 6 – 6.5 to 6.11

SECTION 2: CONTENTS

CHAPTER 1: INFORMATION RISK MANAGEMENT AND CONTROLS

1.1 Introduction

Use of information technology has become way of life and organizations have adapted the business methodologies by adopting changes in technology. Technology is said to be a double-edged sword. It can help organisations to lead or it may lead to organisations to bleed. Hence, it is important to be at the leading edge of IT but avoid being at its bleeding edge. Technology has inherent risks and hence has to be adequately protected with the right level of controls. In order to reap the benefits of technology organizations must establish processes for protecting the interest of stakeholders to avoid the losses to business due to misuse of technology.

We have seen in earlier modules (module 3) the process for risk management covering the identification and assessment of relevant risk due to technology and how these can impact the organization. Once the risks are assessed they must be responded so as to ensure that possible losses in case of risk materialization are within acceptable limits of risk appetite and risk tolerance.

1.2 Risk Management

There are typically four types of risk responses:

1. **Avoid:** Organization may consider this response by deciding not to use technology for select business operation.
2. **Transfer:** Where organization try to pass on the risk to another entity. For example insuring against financial losses with insurance company by paying suitable premium. Another example could be using outsourcing option, however in this organization transfers technological risk but in turn introduces managerial risks, hence it may be considered as risk sharing.
3. **Accept:** If the risk assessed is within the risk appetite, management may decide not to implement control and accept the risk.
4. **Mitigate:** Where organization decide to implement controls, sometimes by incurring additional cost (like delay in process, acquiring tool, adding manpower etc.) so as to reduce the assessed impact to bring it within acceptable limits. Organization may choose to accept remaining risk.

It is possible that organization may select more than one response to manage a risk, for example organization may choose to implement control (Mitigate) and also insure against losses/damage

(Transfer). Risk mitigation primarily focuses on designing and implementing controls to prevent incidents due to risk materialization and/or detect when incident happens or likely to happen and define process to recover from incidence. We will understand in this chapter the concepts associated with identification, selection and implementation of controls.

1.3 Introduction to Information Systems Controls

Control is defined as a mechanism that provides reasonable assurance that business objectives will be achieved and undesired events are prevented or detected and corrected. Control includes policies, procedures, practices and enterprise structure and activities that ensure the desired outcome from business process is not affected. Thus an information systems auditing includes reviewing the implemented system or providing consultation and evaluating the reliability of operational effectiveness of controls.

1.3.1 Need for control and audit of Information systems

Technology has impacted what can be done in business in terms information and as a business enabler. It has increased the ability to capture, store, analyse and process tremendous amounts of data and information by empowering the business decision maker. With the advent of affordable hardware, technology has become a critical component of business. Today's dynamic global enterprises need information integrity, reliability and validity for timely flow of accurate information throughout the organization. Safeguarding assets to maintain data integrity to achieve system effectiveness and efficiency is a significant control process.

The factors influencing an organization toward control and audit of computers and the impact of the information systems audit function on organizations are depicted in the Figure 1.1 below.

- i. **Organisational Costs of Data Loss:** Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in a changing environment.
- ii. **Incorrect Decision Making:** Management and operational controls taken by managers involve detection, investigations and correction of out-of-control processes. These high level decisions require accurate data to make quality decision rules.
- iii. **Costs of Computer Abuse:** Unauthorised access to computer systems, computer viruses, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets (hardware, software, documentation etc.).

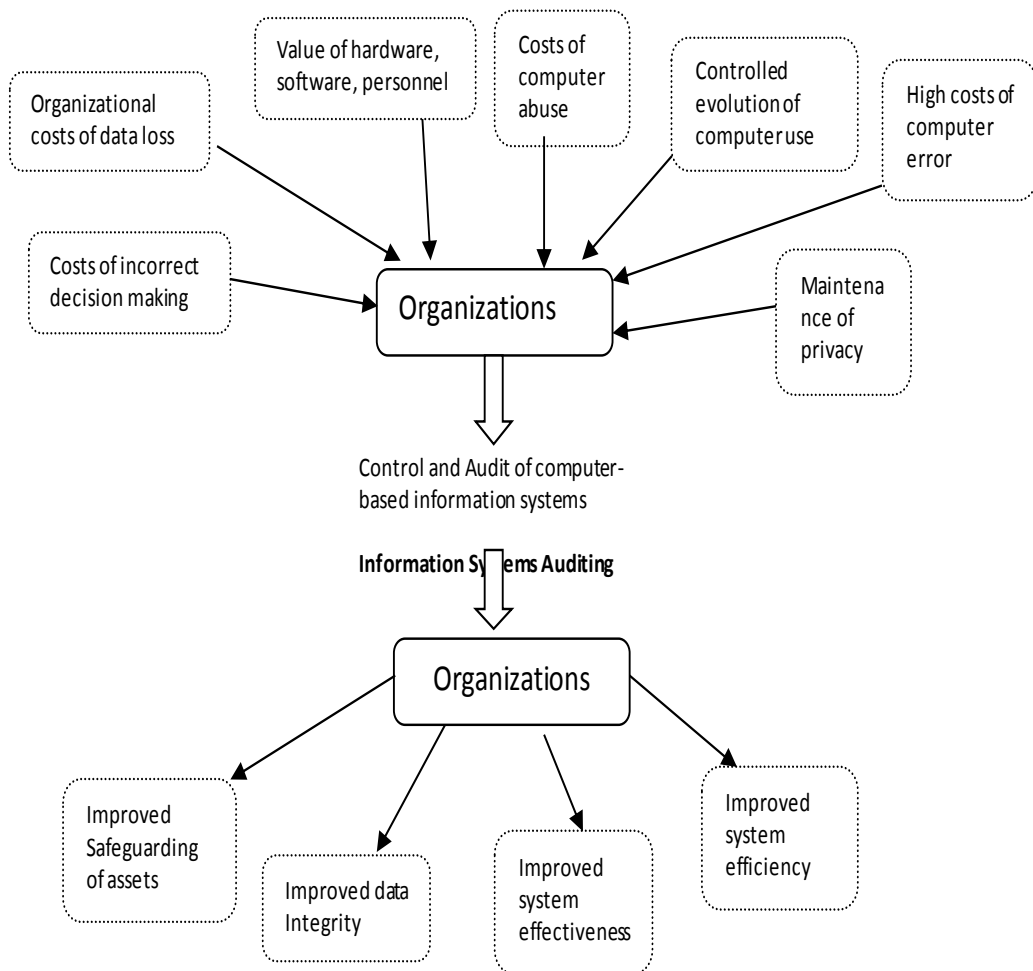


Figure 1.1: Need for control and audit of Information Systems

- iv. **Value of Computer Hardware, Software and Personnel:** These are critical resources of an organisation which has a credible impact on its infrastructure and business competitiveness.
- v. **High Costs of Computer Error:** In a computerised enterprise environment where many critical business processes are performed a data error during entry or process would cause great damage.
- vi. **Maintenance of Privacy:** Today data collected in a business process contains details about an individual on medical, educational, employment, residence etc. These data were also collected before computers but now there is a fear that privacy has eroded beyond acceptable levels.

- vii. **Controlled evolution of computer Use:** Technology use and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.
- viii. **Information Systems auditing:** is the process of attesting objectives (those of the external auditor) that focus on asset safeguarding and data integrity, and management objectives (those of the internal auditor) that include not only attest objectives but also effectiveness and efficiency objectives.
- ix. **Asset Safeguarding Objectives:** The information system assets (hardware, software, data files etc.) must be protected by a system of internal controls from unauthorised access.
- x. **Data Integrity Objectives:** is a fundamental attribute of IS Auditing. The importance to maintain integrity of data of an organisation depends on the value of information, the extent of access to the information and the value of data to the business from the perspective of the decision maker, competition and the market environment.
- xi. **System Effectiveness Objectives:** Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet substantial user requirements.
- xii. **System Efficiency Objectives:** To optimize the use of various information system resources (machine time, peripherals, system software and labour) along with the impact on its computing environment.

1.3.2 Objectives of Control

Control objective is defined as “A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT process or activity”. Control objectives describe what is sought to be accomplished by implementing the control and the purpose thereof. It serves two main purposes:

- (i) Outline the policies of the organization as laid down by the management.
- (ii) A benchmark for evaluating whether control objectives are met.

The objective of controls is to reduce or if possible eradicate the causes of the exposure to probable loss. All exposures have causes and are potential losses due to threats materializing. Some categories of exposures are:

- Errors or omissions in data, procedure, processing, judgment and comparison.
- Improper authorizations and improper accountability with regards to procedures, processing, judgment and comparison.
- Inefficient activity in procedures, processing and comparison.

Some of the critical control considerations in a computerized environment are:

- Lack of management understanding of IS risks and lack of necessary IS and related controls.
- Absence or inadequate IS control framework.

- Absence of or weak general and IS controls.
- Lack of awareness and knowledge of IS risks and controls amongst the business users and even IT staff.
- Complexity of implementation of controls in distributed computing environments and extended enterprises.
- Lack of control features or their implementation in a highly technology driven environments.
- Inappropriate technology implementations or inadequate security functionality in technologies implemented.

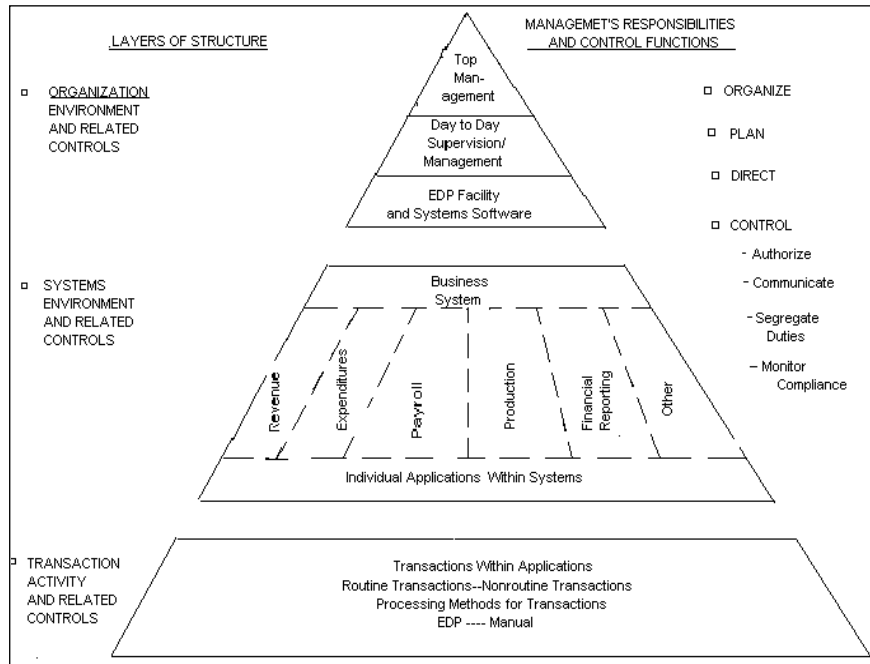


Figure 1.2: Structure of the Control environment

1.3.3 Internal Controls

The basic purpose of an internal control in an organization is to ensure that the business objectives are achieved and undesired risk events are prevented or detected and corrected. This is achieved by designing an effective internal control framework, which comprises policies, procedures, practices, and organizational structure that gives reasonable assurance to achieve the business objectives. Ultimately, all these policies, procedures etc. are broken into discrete activities and supporting processes, which can be either manual or automated. Control is not solely a policy or a procedure which is performed at a certain point of time; rather it is an ongoing activity, based on the risk assessment of the organization.

1.3.4 Types of Internal Controls

Controls can be preventive, detective, or corrective (reactive) and have administrative, technical and physical implementations. Examples of administrative implementations are items such as policies and processes. Technical implementations are the tools and software that logically enforce control (such as passwords) and physical implementations include controls such as guard and locked rooms.

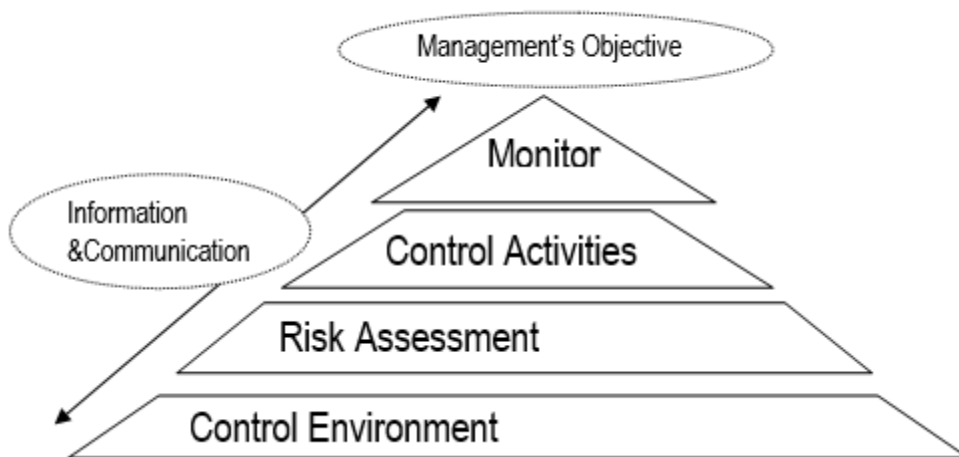


Figure 1.3: Elements of the Internal Control Environment

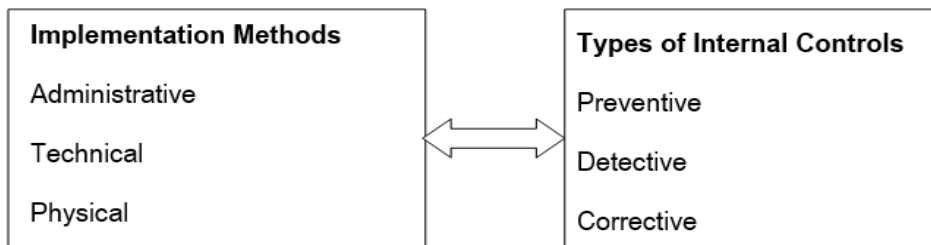


Figure 1.4: Internal Controls and Implementations

(i) Preventive Controls

These controls are those inputs, which are designed to protect the organization from unauthorized activities. This attempts to predict the potential problems before they occur and make necessary adjustments. The broad classifications of preventive controls are:

- A clear cut understanding about the vulnerabilities of the asset.
- Understanding possible threats.
- Provision of necessary controls for probable threats from materializing.

Examples of preventive controls include – employing qualified personnel, segregation of duties, access control, documentation etc.

Table 1.1: Preventive Controls

Purpose	Manual Control	Computerized Control
Restrict unauthorized entry into the premises	Build a gate and post a security guard.	Use access control software, smartcard, biometrics, etc.
Restrict unauthorized entry into the software applications	Keep the computer in a secured location and allow only authorized person to use the applications	Use access control, viz. User ID, password, smart card, etc.

(ii) Detective Controls

These controls are designed to detect errors, omissions of malicious acts that occur and reporting the occurrence. An example of a detective control would be, audit logs, smoke and fire detectors, or from business perspective use of automatic expenditure profiling where management gets regular reports of spend to date against a profiled spend. The main characteristics of such controls are:

- Clear understanding of legalized activities so that anything which deviates from these is reported as unlawful, malicious, etc.
- An established mechanism to refer the reported unlawful activity to the appropriate person/group.
- Interaction with the preventive control to prevent such acts from occurring.
- Surprise checks by administrator.

Examples of detective controls include: Hash totals, check points in production jobs, error message, duplicate checking of calculations, past-due accounts report etc.

(iii) Corrective Controls

These controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. A business continuity plan is considered to be a significant corrective control. The main characteristics of the corrective controls are:

- Minimize the impact of the threat.
- Identify the cause of the problem.
- Remedy for problems are discovered by detective controls.
- Get feedback from preventive and detective controls.
- Correct error arising from a problem.
- Modify the processing system to minimize future occurrences of the problem.

Examples of Corrective Controls are - contingency planning, backup and restoration procedure, rerun procedure, procedure for treating error, etc.

For an auditor to effectively evaluate the efficiency of the objectives of these controls, the following key **Table 1.2** might be used keeping in mind the minimum redundancy in the levels of control. The controls rating by an auditor are:

- **High-** Controls implemented over a cause of exposure/error type and should be highly effective.
- **Moderate-** Controls implemented over a cause of exposure/error type and is moderately effective.
- **Low-** Controls implemented over a cause of exposure/error type but have low effectiveness.
- **Blank-** Controls not implemented or does not exist to that cause or exposure or error type.

Table 1.2: Effectiveness and Efficiency of Internal Controls

Methods of Control Implementation	Type of Internal control		
	Preventive	Detective	
		With Corresponding Corrective	Without Corrective
Manual Control	Blank or Low	Moderate	Blank
	Least effective, generally manual controls applied at front-end of processing; moderately efficient	Moderately effective manual controls; probably least efficient	Least effective and possibly dangerous since users rely on them improperly; very inefficient
Computerized Control	Low or Moderate	High	Blank
	Moderately effective, generally Application controls, applied at front-end of processing; probably most efficient	Most effective, generally controls that are computerized and applied before processing can take place; moderately efficient	May have some effectiveness but probably little; highly inefficient

1.4 Risk and control ownership

Each risk needs to have an owner who can take a decision on risk response. Generally owner is a person or position within the organization that has close interest about the processes affected due to risk. The person responsible needs to ensure that the risk response is translated into actual day-to-day actions that will prevent and/or detect the risk. It will be this person's responsibility to ensure and manage the effectiveness of an insurance program, an outsourced arrangement, a policy statement, exception reporting, assignment of authorities, etc.

1.5 Periodic Review and monitoring of risk and controls

After implementation of the risk responses and management techniques, the managers need to monitor the actual activities to ensure that the identified risk stays within an acceptable threshold. To ensure that risks are reviewed and updated organizations must have a process that will ensure the review of risks. The best processes are:

1. Periodic review: the risk assessment exercise may be conducted after predefined period say annual.
2. All incidents and lesson learned must be used to review the identified risk
3. Change management processes proactively review the possible risks and ensure they are part of organization's risk register.
4. New initiatives and Projects must be considered only after risk assessment.

1.5.1 Controls assessment

The first step in control's assessment is to review the control catalogue (which is a collective record of all controls implemented) and ensure that associated risk is mitigated either by reducing likelihood or reducing impact or both. Based on this the auditor shall be able to prioritize the controls to be tested. The next step is to review control procedure documents the organisation's control processes with the aim of identifying suitable ways of measuring or testing each control.

1.5.2 Control self-assessment

In case organization has implemented control self-assessment, the actual testing of the controls is performed by staff whose day-to-day role is within the area of the organisation that is being examined as they have the greatest knowledge of how the processes operate. The two common techniques for performing the evaluations are:

- Workshops, that may be but do not have to be independently facilitated, involving some or all staff from the business unit being tested;
- Surveys or questionnaires completed independently by the staff.

On completion of the assessment each control may be rated based on the responses received to determine the probability of its failure and the impact if a failure occurred. It is critical to note that both these methods can be used for risk identification, risk assessment and control design.

1.6 Role of IS Auditor in Information Risk Management

The role of auditor with regard to Information Risk Management can be:

1. Facilitator for conducting risk assessment workshops as risk professional and also guide the process owner of designing of controls.

2. As Auditor, to provide objective assurance to the board on the effectiveness of an organisation's Risk Management framework to help ensure that key business risks are being managed appropriately and the system of internal controls is operating effectively.
3. As internal auditor, plan the audit cycle according to the perceived risk, i.e. plan for higher frequency for high-risk area business processes.

Key roles that an auditor can perform are:

- 1) To give assurance on risk management process
- 2) To give assurance that the risks are being evaluated correctly
- 3) Evaluate Risk Management process
- 4) Review the management of key risks.

There are some roles which an auditor should not perform, to maintain his independence:

- 1) Setting the risk appetite
- 2) Imposing risk management process
- 3) Taking decision on risk responses
- 4) To implement risk response on management's behalf.

1.7 Summary

Information Security is a paramount risk management concern. Information Risk Management follows information as it is created, distributed, stored, copied, transformed and interacted with throughout its lifecycle. It includes understanding what information is critical to key business initiatives, such as growth through acquisitions or expanding partnerships, where it exists across the organization, where the points of vulnerability are, and what events could put the business at risk. Investments are prioritized based on the amount of risk a given activity entails relative to the potential business reward, and in keeping with the organization's appetite for risk. Once enterprise information has been located and a risk assessment performed, next step is to implement controls — including policies, technologies, and tools — to mitigate that risk.

1.8 Questions

1. Which of the following shall **BEST** help in deciding upon the protection level for information asset?
 - A. Location of asset.
 - B. Impact of risk.
 - C. Vulnerabilities in asset.
 - D. Inventory of threats
2. Which of the following is a risk response option?
 - A. Determine likelihood of threat
 - B. Determine probability of risk

- C. Deciding amount of insurance cover
 - D. Prepare risk profile report
3. After a Tsunami, a business decides to shift the location of data centre from coastal area to mid land? Which type of risk response option it has exercised?
- A. Accept
 - B. Avoid
 - C. Mitigate
 - D. Transfer
4. Organizations capacity to sustain loss due to uncertainty and expressed in monetary terms is best known as:
- A. Risk appetite
 - B. Risk tolerance
 - C. Risk acceptance
 - D. Risk mitigation
5. Main use of maintaining and updating risk register is to:
- A. Define controls
 - B. Identify risk owner
 - C. Built risk profile
 - D. Maintain evidence
6. Of the following who is accountable for deciding and implementing controls based on risk mitigation plan?
- A. Chief risk officer
 - B. Risk owner
 - C. IT operations manager
 - D. Board of directors
7. Which of the following is a risk factor that may have impact on organization?
- A. Management decides to acquire new application software.
 - B. A new application required by organization is released.
 - C. Vendor decides to stop supporting existing application.
 - D. Organization retires old application that is not in use.
8. While auditing risk monitoring process which of the following IS auditor should review FIRST?
- A. Risk assessment process
 - B. Risk management framework
 - C. Alignment with business risks
 - D. Annual review of risk register

9. The quantum of risk after enterprise has implemented controls based on risk mitigation plan is:

- A. Accepted risk
- B. Residual risk
- C. Inherent risk
- D. Current risk

10. Which of the following shall best help in aligning IT risk with enterprise risk?

- A. Presenting IT risk results in business terms.
- B. Conducting business impact analysis.
- C. Making Chief risk officer accountable.
- D. Align IT strategy with business strategy.

1.9 Answers and Explanations

1. **B.** Other options i.e. location of asset, existing vulnerabilities in asset shall be covered during risk assessments. Inventory of threats only will not help, impact due to threat must be assessed.

2. **C.** Of the four main risk response options accept, avoid, mitigate and transfer, Insurance cover is a risk response option of risk transfer

3. **B.** BY shifting location the business has avoided the risk associated with Tsunami.

4. **A.** It is the definition of risk appetite. Risk tolerance is capacity to tolerate down time due to risk materialization. Risk acceptance and risk mitigation are risk response decision based on risk appetite.

5. **C.** Main use of risk register is to develop risk profile of the organization for management's review and enable risk informed decisions.

6. **B:** Risk owner is primarily accountable for deciding and implementing on nature of controls. Generally risk owner is process owner. Chief risk office guides risk owner, IT head is responsible for responding to risk owned by IT head. Although board of directors is ultimately accountable, for specific risk, risk owners are responsible.

7. **C.** Vendor decides to stop supporting existing software changes the market situation that will affect organization, since it has to take decision on replacing application. Release of new application though changes market, it may not affect the organization immediately as the organization may not need to take action. Options A and D are internal decisions and will be done after risk assessment and hence these are not risk factors.

8. **D.** Risk monitoring refers to review of identified and asessed risks based on changes, incidents, and periodically. Other options are part of risk management framework.

9. B. Accepted risk is where controls are not implemented is part of residual risk, Inherent risk is total risk before implementing controls. Current risk is residual risk at a point in time during control implementation.

10. A. Expressing IT risk in business terms i.e. as impact on business will help business in understating relevance of IT risks. Business impact analysis may be useful however it may or may not help depending upon scope of project. Making chief risk officer accountable may help but best is A. Aligning IT strategy with business strategy shall help in defining better IT plan, but it is at higher level.

CHAPTER 2: INFORMATION SECURITY MANAGEMENT

2.1 Introduction

Protection of information assets includes the key components that ensure confidentiality, integrity and availability (CIA) of information assets. There are three key objectives of Information Security Management viz.: **Confidentiality, Integrity and Availability** also called **CIA Triad**.

- **Confidentiality:** No data or information is made available to any person within or outside the organization, other than the persons who are authorized to use that data.
- **Integrity:** No data/information or programs shall be allowed to be modified by anyone without proper authority.
- **Availability:** All Information Systems including hardware, communication networks, software applications and the data they hold, is available to authorized users to carry out business activities.

Controls to protect the assets are designed, developed, selected and implemented based on risk evaluation and cost-benefit analysis. The primary control for implementing protection strategy is defining and implementing information security policy. Organization need to focus on ensuring that information security practices are followed to meet the security objectives of organization derived from the stakeholder's expectations. This requires implementing processes for information security management. The key elements of information security management include:

- Senior management commitment and support,
- Policies and procedures,
- Organization structure and roles and responsibilities,
- Security awareness and education,
- Monitoring
- Compliance,
- Incident handling and response.

2.2 Senior management commitment and support

Commitment and support from senior management are important for successful establishment and continuance of an information security management program. The tone at the top must be conducive to effective information protection and security management. It is unreasonable to expect lower-level personnel to abide by security measures if they are not exercised by senior management. Executive management endorsement of intrinsic security requirements provides the basis for ensuring that security expectations are met at all levels of the enterprise. Penalties for non-compliance must be

defined, communicated and enforced from the board level down. The senior management's support for security initiatives is evident from activities and decisions. Some of the key indicators are:

1. Providing support for defining organization structure that supports implementation of information security initiatives by establishing Information Security Organization (ISO) and steering committee and assigning responsibility for security operations
2. Regularly reviewing security projects, reports and activities as part of agenda item on board meetings.
3. Approving risk response decisions and security policies.
4. Practicing security practices
5. Ensuring adequate budget
6. Review of audit reports

2.3 Critical Success Factors to Information Security Management

Information Security can be a business enabler if following five suggested actions are adopted by Information Security Management:

- a) **Alignment with business objectives:** Management views Information Security as another support function and not primary business function although an important function. The Management need to establish security policy in line with business objectives, to ensure that all Information Security elements are strategically aligned.
- b) **Organizational culture:** Ensure that the framework followed to implement, maintain, monitor and improve Information Security is consistent with the organisational culture.
- c) **Establish and enforce an Information Security Program:** Information Security program focuses on protecting information present in business processes. Establish a program to improve Information Security management enterprise-wide and enforce it.
- d) **Adoption of standard:** Adopting an internationally recognized reference framework to establish an Information Security framework is useful in providing assurance that all required aspects of information security are covered. It also helps in benchmarking the security levels. Adopting an information security standard seems to demonstrate to staff, customers and trading partners that their data is safe, and that there is an independent verification of this fact. Rules formulated under IT (Amendment) act 2008 defines reasonable security as implementation of ISO 27001 or equivalent certifiable standard so as to establish that reasonable security practices are being followed.
- e) **Spend resources wisely and transparently:** Prioritise expenditures to mitigate risks and avoid spending more resources in assessing risks than those that would be spent if the problems really occurred.

2.4 IT Security Policies, procedures, standards and guidelines

Information Security policy will define management's intent on how the security objectives must be achieved. It will also encompass the view on risk and will define a security framework to meet business objectives. Security policies, guidelines and procedures affect the entire organization and, as such, should have the support and suggestions of end users, executive management, auditors, security administration, IS personnel and legal counsel. After policies are outlined, standards are defined to set the mandatory rules that will be used to implement the policies. Some policies can have multiple guidelines, which are recommendations as to how the policies can be implemented. Finally, information security management, administrators, and engineers create procedures from the standards and guidelines that follow the policies.

A security policy is a document that defines the scope of security needed by the organization and discusses the information assets that need protection and the extent to which protection is required. The Information Security Policy is an overview or generalization of an organization's security needs. It should clearly define why security is important and what assets are valuable. The formulations of policies are based on outcome of risk management process. Organizations can have policies depending upon culture of organization, nature of business, compliance requirements, geographical and regional environment within which organization is operating.

2.4.1 What should the policy contain?

The policy should have a number of different statements covering each of the major aspects of information security. Each policy statement should be derived from a major business objective, as this is the fundamental justification for any security requirement. The relationship between objectives (sometimes called Business Principles), policies, the resulting standards and procedures is best illustrated by an example below.

Example of Business Objective Policy: To be recognized as a good employer staff safety and security come before the security of company assets.

Every organization may have different policies depending upon nature and focus of business and result of risk management process, however some of the common policies are discussed here.

Data classification and Privacy Policies

It is the policy of the Organization to protect against the unauthorized access, use, corruption, disclosure, and distribution of non-public personal information in its possession, and to comply with all applicable laws and regulations regarding such information. It generally covers:

- The organization shall hold non-public personal information in strict confidence and shall not release or disclose such information to any person except as required or authorized by law and only to such persons who are authorized to receive it.

- The organization shall adopt procedures for the administrative, technical and physical safeguarding of all non-public personal information.
- The organization shall ensure that an entity controlled by it, or any other entity that utilizes information provided by the organization to carry out its responsibilities, shall have signed and agreed to abide by the terms of the data privacy and security policy or shall have adopted a data privacy and security policy that is substantially similar to the organization policy.

Acceptable use of information assets policy

An acceptable use policy (AUP), also known as an Acceptable Usage policy or Fair Use policy, is a set of rules applied by the owner or manager of a network, website or large computer system that restrict the ways in which the network, website or system may be used. AUP documents are written for corporations, businesses, universities, schools, internet service providers, and website owners, often to reduce the potential for legal action that may be taken by a user, and often with little prospect of enforcement.

Acceptable use policies are an integral part of the framework of information security policies; it is often common practice to ask new members of an organization to sign an AUP before they are given access to its information systems. For this reason, an AUP must be concise and clear, while at the same time covering the most important points about what users are, and are not, allowed to do with the IT systems of an organization. It should specifically cover Acceptable Use of Internet. For e.g. it may state that no user of company's Internet facility will connect to pornographic, child abuse, or racial discrimination sites and so on.

Physical access and Security Policy

Physical security describes security measures that are designed to restrict unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks). Physical security involves the use of multiple layers of interdependent systems which include CCTV surveillance, security guards, Biometric access, RFID cards, access cards protective barriers, locks, access control protocols, and many other techniques.

Asset Management Policy

This policy defines the requirements for Information Asset's protection. It includes assets like servers, desktops, handhelds, software, network devices etc. Besides, it covers all assets used by an organization- owned or leased.

Business Continuity Management Policy

This policy defines the requirements to ensure continuity of business critical operations. It is designed to minimize the impact of an unforeseen event (or disaster) and to facilitate return of business to normal levels.

Network Security Policy

A network security policy defines the overall rules for organisation's network access, determines how policies are enforced and lays down some of the basic architecture of the company security/ network security environment.

Password policy

This policy defines high-level configuration of password to be used within organization to access the information assets. For example:

- Password length must be more than 8 characters
- Password must be complex containing upper case, lower case, numeric and special characters
- Password must be changed regularly
- Password should not be used again for minimum period
- Password should not be changed in consecutive sequence

2.4.2 Controls over Policy

Information security policies need to be maintained and updated regularly. This is required due to changes in environment, IT technology, threat scenarios, business processes, business strategy, and organizational structures. This might need to revisit the security requirements and hence policies. Hence, it is necessary to review the security policies periodically to ensure that they are in line with the management's intent. Typically security policies are reviewed:

- Periodically, generally annually
- After incident
- As a part of change management process

Exceptions

Policies are generic and sometimes cannot be enforced in specific situations, a process for defining and approving exceptions must be defined. In such situations it is necessary to ensure there are suitable compensating controls so that the risks mitigated by enforcement of policy are within acceptable limits. Such exceptions are for predefined period and must be removed over the period of time or reviewed periodically. For example: legacy application does not provide for implementing

password policy. An exception may be approved with additional strong compensating control over access granting process or application accesses. This exception may be approved for a specific period of time, during which application may be changed to be compliant with password policy.

2.5 Tools to Implement Policy: Standards Guidelines and Procedures

The next level down from policies is three elements of policy implementation as given here:

Standards: Specify the uniform way for the use of specific technologies in an organization. This standardization of operating procedures can be a benefit to an organization by specifying the uniform methodologies to be used for the security controls. Standards are usually compulsory and are uniformly implemented throughout organization.

Guidelines: Guidelines are similar to standards; they refer to the methodologies of securing systems, but they are only recommended actions and are not compulsory. Guidelines are more flexible than standards.

Procedures: Procedure contains the detailed steps that are followed to perform a specific task. Procedures are the detailed actions that must be followed. They are considered the lowest level in the policy chain. Their purpose is to provide detailed steps for implementing the policies, standards, and guidelines previously created.

2.6 Information Security Organization

Information security is responsibility of entire organization and accountability of senior management and board of director. Information security officer is facilitator in implementing security across organization. The Information Security Organization (ISO) plays a critical role in ensuring an Organization's information and its information assets are properly protected, managing vulnerabilities within the infrastructure, managing threats and incidents impacting resources, ensuring policies are in place and employees comply with them, and educating employees about their information security and privacy protection responsibilities.

The position must be strategically placed within the Organization and visibly supported by top management while carrying out the duties in an effective and independent manner. Possessing both a broad range of business management and technical security skills, and a clear understanding of the Organization's business is critical to an ISO's success.

There is no easy solution to implementing an effective information security program within an Organization. An effective program cannot be established overnight and will be a continuous ongoing function once established. Appointing a skilled ISO who has the full support of executive management is the first important step necessary to implementing the program. To ensure that information security is implemented across organization ISO requires creation of the information

security organization. This can be best done by defining security responsibilities for every person and position as part of his/her role within organization and documented in their job description. While defining roles and responsibilities following aspects must be considered.

2.6.1 Clearly defined duties

The first fundamental security rule is that each individual should be aware of what the organization expects from them. These expectations are communicated through various important documents such as company policies and individual job descriptions duties, responsibilities and the level of authority they have. It is difficult (and unjust) for an organization to accuse an individual of carrying out activities or tasks which they have no right to do, if the individual's job was not clearly possible for an organization to put into place other personnel security procedures including the following:

- Segregation of duties
- Four eyes (the two person principle)
- Rotation of duties
- Key man policies

Segregation of Duties

No individual, of whatever seniority in the organization, should have the ability to carry out every step of a sensitive business transaction. For example, a salesman should not be able to enter a customer's order in the order book and have access to the stock control/delivery system and settlement part of the sales ledger. Access to too many functions enables staff to carry out a fraudulent transaction and hide their tracks.

- A programmer should not be allowed to operate a computer system, or to gain access to production systems or data. Similarly, operators, should not act as programmers although, in practice, this rule is becoming undermined by the use of personal computers and small office systems. It is also a difficult rule to apply to an on-line computing environment.
- System security features should be introduced by staff completely independent of programming or operations.
- Devolution of authority from an owner to a custodian of any classified or sensitive material should include the ability to authorize its reproduction, issue or destruction. Independent checks of this person's work must be carried out at random times.

The 'Four Eyes' (Two-person) Principle

To reduce the opportunities for any person to breach security, those responsibilities and duties which would afford particularly powerful access to the system, or which act at key control points, should not be carried out by one person alone. Examples of this include: two signatories required for a cheque, and two people always being present in a critical computer room.

It must be noticed that there is a possibility of collusion between the staff members. To avoid this, steps should be taken to vary shift rotas and working practices so that the same people are not always working together. Vital functions should also be well dispersed amongst staff members. Although this can be seen as a mistrust of staff it can also provide a protection, as individual with the ability to act alone may be in danger of coercion.

The Rotation of Duties

No one person should be kept in one particular post for too long, especially if that appointment involves any particular security responsibilities opportunities for dishonesty. Job rotation can also help avoid the errors which occur from boredom and over familiarity, and place a limit on any fraudulent activities. The replacement of an individual may well reveal any dishonesty or inefficiency which has been continuing over a period of time.

A similar rule should insist that staff take at least two consecutive weeks; holiday in any year, as experience has shown that many frauds need continual masking by the perpetrator and may surface when the individual is away.

'Key Man' Policies

Organizations should avoid situations where an individual becomes indispensable to the business. A 'key man' policy identifies areas of operational activities where such situation may occur and seeks, where possible to enable cover by other individuals to be established. In cases where it is unavoidable that a single individual is pivotal, insurance policies may be taken out to cover losses resulting from his or her death or incapacity. Key man policies also cover issues such as the protection of groups of key staff such as senior managers and lays down rules under which they will not travel in the same vehicle (aircraft and cars) to limit the impact on the organization, should there be an accident.

2.6.2 The Concept of Responsibility in Security

Responsibilities are the defined duties of individual within an organization, once a responsibility is assigned it is usual for an individual to be held to be accountable for satisfactory performance. The main types of role for individuals within a security structure are described below.

Ownership

Organization has acquired a number of assets required for business operations. The organization is legal owner of these assets. However for security and control the ownership is delegated to an employee or group of employees who need to use these assets. In other words, users have right to not only use the assets but are also responsible for the safe-keeping of assets.

This fundamental rule of organizational control also applies to corporate security, where ownership must be defined in order for control to be applied. Thus every corporate asset, building, item of equipment, bank account and item of information hood have a clearly defined 'owner'. The owner should then have a defined set of responsibilities.

- Ensuring that computer rooms are kept clean and tidy
- Ensuring that equipment is well maintained and kept operational
- Ensuring that an item of data used by the organization is accurate and up to date.

Owners of a particular asset generally have authority over it, thus an owner may have the authority to update an item of data. Where too much power may be put into the hands of an individual more than one owner may be appointed (although there can be problems where there is unclear authority). Bad management practice will put an individual in a position where they have no real authority to influence something for which they have been given responsibility. Authorization is the essential statement where an owner gives their assent to an activity happening. Authority and ownership are generally synonymous.

Custodianship

In some instances an owner is not able to manage a particular asset on a day to day basis, perhaps for logical or technical reasons. In this case responsibility may be passed on by the owner to a custodian. The owner should clearly state the requirements, the responsibilities and associated levels of authority of the custodian and final management responsibility will always reside with the owner. Examples of custodian include a data center operations functions controlling access to production data, and a computer bureau running an application for a client.

Controlling

In all security systems there are key tasks which can be called control points. It is at these control points that the actual security mechanism has its application. For example, a security administrator acts as a control on who has access to computer resources. They carry out the task of adding and deleting user identifiers from the system or modifying the task of adding available to them, and therefore effectively control the activities of the owner, or other designated authority.

2.7 Role and responsibilities

To have an effective information security program, the roles and responsibilities of all participants must be clearly defined. Besides, segregation of duties plays an important role in the effective application of information classification and related controls. Some of the key roles and responsibilities are explained here.

2.7.1 Steering Committee

To some extent security affects all aspects of an organization. To be effective, security must be pervasive throughout the enterprise. To ensure that all stakeholders impacted by security considerations are involved, many organizations use a steering committee comprised of senior representatives of affected groups. This facilitates achieving consensus on priorities and trade-offs. It also serves as an effective communications channel and provides an ongoing basis for ensuring the alignment of the security program with business objectives. It can also be instrumental in achieving modification of behaviour toward a culture more conducive to good security. The committee discusses issues related to protecting information assets, and establishes and approves security practices. The committee should be formally established with appropriate terms of reference

2.7.2 Information Owner

Information Owner (also called **Data Owners**) is responsible for a company information asset. The responsibilities are generally assigned to person/position that owns business process. Primary responsibilities are:

- Assign appropriate information classification and periodically review the classification to ensure it still meets the business requirements.
- Ensure security controls have been implemented in accordance with the information classification.
- Review and ensure currency of the access rights associated with the information assets they own.

2.7.3 Information custodian

Information custodian is assigned the task of implementing the prescribed protection defined by the security procedure and top level/Senior management decisions. He is usually an information technology or operations person, and is the system administrator for the Information Owner.

Among other activities, information custodian also performs following activities:

- Ensuring safe keeping of information on behalf of information owner
- Providing access to users that are approved by owners
- Running regular backups and routinely testing from backup data
- Performing data restoration activity from the backups when necessary

2.7.4 System Owner

The system owner is responsible for one or more systems, each of which may process and store data owned by different information owners. Here a system refers to group of assets required for hosting one or more applications that support a business function. E.g. Human resource data

management system is owned by the HR department including Hardware, OS, database, Middleware, application and data. A system owner is responsible for:

- Integrating security considerations into application and system purchasing process and decisions.
- Ensuring that adequate security is built or defined once the applications and systems have been acquired and are ready for use in production environment.
- Ensuring that the systems are properly assessed for vulnerabilities and report any to the incident response team and information owner.

2.7.5 Process owner

This person is responsible for the implementation, management and continuous improvement of a process that has been defined to meet a business requirement.

2.7.6 System Administrator

System Administrator is the one with administrative / root level privileges of the Operating systems like Windows, Unix etc. This means that they can add and remove permissions and set security configurations. A system administrator is responsible for:

- Creating new system user accounts,
- Changing permissions of existing user accounts,
- Implementing new security software,
- Testing security patches and updates, and
- Resetting user passwords.

2.7.7 User manager

User manager is the immediate manager or reporting manager of an employee. They have ultimate responsibility for all user IDs and information assets owned by company employees. In the case of non-employee individuals such as contractors, consultants, etc., user manager is responsible for the activity and for the company assets used by these individuals.

2.7.8 Super User

The person with the highest level of authorization access, who can make any transaction and master setup activity immediately and sets the conditions for transaction approvals, financial daily limits of each transaction type, and classifies and authorizes other Users.

2.7.9 Security Manager

Security manager is responsible for defining security strategy and policies for the organization. The manager also ensures defining roles and responsibilities.

2.8 Human Resources Security

Employees handling personal data in an organization need to receive appropriate awareness training and regular updates in an effort to safeguard the data entrusted to them. Appropriate roles and responsibilities assigned for each job description need to be defined and documented in alignment with the organization's security policy.

The management of human resources security and privacy risks is necessary during all phases of employment association with the organization. Training to enhance awareness is intended to educate individuals to prevent data disclosure, recognize information security problems and incidents, and respond according to the needs of their work role. Safeguards include the following:

- Job descriptions and screening,
- User awareness and training,
- A disciplinary process, and
- An orderly exit process must exist to equip employees to operate securely and use information appropriately, and ensure that access privileges change when a user's relationship with the organization changes.

The objective of human resources security is to ensure that all employees and 3rd parties (having access to sensitive data) are qualified for and understand their roles and responsibilities of their job duties and that access is removed once employment is terminated. The three areas of Human Resources Security are:

- a) **Pre-employment:** It includes defining roles and responsibilities of the job, defining appropriate access to sensitive information for the job, and determining depth of candidate's screening levels - all in accordance with the company's information security policy.
- b) **During employment:** Employees and 3rd parties with access to sensitive information in an organization should receive periodic reminders of their responsibilities and receive ongoing, updated security awareness training to ensure their understanding of current threats and corresponding security practices to mitigate such threats.
- c) **Termination or change of employment:** To prevent unauthorized access to sensitive information, access must be revoked immediate upon termination/separation of an employee and 3rd parties with access to such information. This also includes the return of any assets of the organization that was held by the employee.

2.9 Training and Education

Since the terrorist attacks, corporations and government organizations alike have brought security training, awareness, and education into the spotlight. Once thought of as "just filling a mandatory requirement" or "I have to do this because my boss told me too," is not the perception now. Various computer crime studies show that the threat from insiders ranges from 60% to 90%. This does not mean that more than 60% of the employees in an organization are trying to hack into the system; it

does mean that employees, whether intentionally or accidentally, may allow some form of harm to the system. This includes having weak passwords, sharing their passwords with others, installing illegal copy of screensaver software or downloading shareware from the Internet. Thus, employees need to be made aware of the information security policies of the company and how to practice good computer security skills.

An integrated security training, awareness, and education program must be based on a validated training strategy and include a formal course curriculum in addition to other learning interventions designed to deliver the appropriate security information and messages to all levels of employees. To do this, a broad program that includes training, education, awareness, and outreach must be developed to deliver a multitude of security messages through various means to all employees. Formal, instructor led training, computer or Internet-based training, videos, conferences, forums, and other technology based and traditional delivery methods are all examples of what must be part of the integrated security training, education, and awareness program. Important considerations for security awareness training program are:

- a) **Mandatory Security Awareness:** Ensure that security awareness training is mandatory for all staff (including management).
- b) **Training for Third Parties:** Ensure that all third parties with access to an organization's information receive the same security awareness training, or training to an equivalent level.
- c) **Training is required before access is granted:** Security awareness training commences with a formal induction process designed to introduce the organization's security policies and expectations before access to information or services is granted.
- d) **Acknowledge Policy:** Ensure that all employees are required to acknowledge that they have read and understood the organization's information security / acceptable use policy.
- e) **Training at Least Annually:** Ensure that all employees and third parties (having access to company information and information systems) are given security awareness training at least once per year.

2.10 Systems Configuration

Configuration management is the process of tracking and approving changes to a system. It involves identifying, controlling, and auditing all changes made to the system. It can address hardware and software changes, networking changes, or any other change affecting security. Configuration management can also be used to protect a trusted system while it is being designed and developed. The primary security goal of configuration management is to ensure that changes to the system do not unintentionally diminish security. For example, configuration management might prevent an older version of a system from being activated as the production system. Configuration management also makes it possible to accurately roll back to a previous version of a system in case a new system is found to be faulty. Another goal of configuration management is to ensure that system changes are

reflected in current documentation to help mitigate the impact that a change might have on the security of other systems, while in either the production or planning stages.

Configuration management is a discipline applying technical and administrative direction to do the following:

- Identify and document the functional and physical characteristics of each configuration setting
- Manage all changes to these characteristics
- Record and report the status of change processing and implementation

Configuration management involves process monitoring, version control, information capture, quality control, bookkeeping, and an organizational framework to support these activities. The configuration being managed is the verification system plus all tools and documentation related to the configuration process.

2.11 Information Security and external parties

In order to bring efficiencies and economies of scale, many organizations resort to outsourcing and are allowing more and more vendors, customers and other 3rd parties to access the information assets of organization. This trend has its own operational merits but brings significant information security challenges specifically with regard to confidentiality and integrity of the organisation's information. As a result, many organisations these days are asking all 3rd parties, having access to the organisation's information and information systems, to sign a Non-Disclosure Agreement (NDA). A non-disclosure agreement (NDA), also known as a confidentiality agreement (CA), is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to or by third parties. It's a contract through which the parties agree not to disclose information covered by the agreement. An NDA creates a confidential relationship between the parties to protect any type of confidential and proprietary information or trade secrets. As such, an NDA protects non-public business information.

2.12 Issues and challenges of IS Management

An organization may face various challenges in Information Security Management. Some common challenges are:

1. **Organization's strategic drivers:** The strategic drivers and needs of the organization may conflict with the actions required to ensure that assets and processes remain productive. Finding the right balance between protecting the organization's core assets and processes and enabling them to do their job becomes a challenge for security management—and a significant barrier to effectiveness.

2. **Regulatory Requirements:** Another consideration for security management is the organization's regulatory environment. Just as the organization must expose itself to its environment to operate, so must it be willing to accept some of the limitations imposed on like organizations that operate in its competitive space. This brings another level of challenges that affects the organization's ability to be effective at security management.
3. **Information Security as an afterthought:** The problem of information security being considered as an afterthought dates back to the era of checklists. Once a system has been implemented, it was a norm to follow a checklist to address whether any of the security 'holes' remained unplugged. While the information security community has recognized the inadequacy of checklists as a means to address security concerns, the checklist culture has, however, prevailed. Therein resides the problem of information security being considered as an afterthought.
4. **Lack of Integration in System Design and Security Design:** Development duality is a phenomenon where systems and security design are undertaken in parallel rather than in an integrated manner. This largely occurs when systems developers fail to recognize the security requirements at the onset of the development process.

2.13 Computer crimes and exposures

A computer crime, also called **cyber-crime**, is any unlawful activity that is done using a computer. Computer crime is one of the fastest-growing types of illegal activity, both in the India and internationally. While the Internet links people together like never before, it also provides endless opportunity to criminals seeking to exploit the vulnerabilities of others. These types of crime are notoriously hard to solve and sometimes occur without the victim ever knowing anything illegal has taken place. There are several different types of computer crime, many of which overlap. Some of the most commonly reported computer crimes are:

- a. **Denial of Service (DoS):** A Denial-of-Service attack (DoS) is an attempt to make a machine or network unavailable to its intended users. This causes legitimate users to not be able to get on the network and may even cause the network to crash.
- b. **Network Intrusions:** Network Intrusion refers to unauthorized access to an organisation's internal network.
- c. **Software Piracy:** The illegal copying of software.
- d. **Spoofing of IP Addresses:** IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system
- e. **Eavesdropping:** Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, and video-conference or fax transmission.

- f. **Phishing:** Phishing is the act of trying to obtain information like user ID and password for bank accounts, credit card pin etc. using electronic communication means like emails, fake websites etc.
- g. **Social Engineering:** It is the act of obtaining or attempting to obtain otherwise secure data by conning an individual into revealing secure information. Social engineering is successful because its victims innately want to trust other people and are naturally helpful. The victims of social engineering are tricked into releasing information that they do not realize will be used to attack a computer network. For example, an employee in an enterprise may be tricked into revealing an employee identification number to someone who is pretending to be someone he trusts or representing someone he trusts.
- h. **Hacking:** Hacking is the process of exploiting vulnerabilities of a system to gain unauthorized access to system or resources like a website, bank accounts etc.
- i. **Dumpster diving:** Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) It is a technique used to retrieve information that could be used to carry out an attack on an organisation. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network.
- j. **Data-Diddling:** Data diddling is the changing of data before or during entry into the computer system. Examples include forging or counterfeiting documents used for data entry and exchanging valid disks and tapes with modified replacements
- k. **Targeted attacks:** The new trend in cyber (computer related) crimes is targeted attacks. These are the attacks that are specifically targeted to selected organization. It is combination of attacks like malware (a virus or program that is written with specific objective e.g. Stuxnet), social engineering to introduce malware in system, data diddling and scavenging (malware once activated initiated these attacks and sends information outside in small proportions so as not to detect).
- l. **Advanced persistent Threat (APT):** This is a type of targeted attack that continues for a sustained period for about a year or more. A malware launched starts sending confidential information masking it and in small proportions so as not to cross monitoring thresholds.
- m. **Botnets:** Acronym for robotic network. An underground network established by hackers by sending malware. This malware goes undetected since it is part of targeted attack. Hackers build a virtual network of such compromised computers and uses as and when required to launch attacks.

2.14 Incident handling and response

A computer security incident is an event adversely affecting the processing of computer usage. This includes loss of confidentiality of information, compromise of integrity of information, denial of service,

unauthorized access to systems, misuse of systems or information, theft and damage to systems. Other incidents include virus attacks and intrusion by humans within or outside the organization. It defines requirements for handling information security incidents. Information security incidents include virus, worm, and Trojan horse attack, unauthorized use of company information systems, and Acceptable Use Policy violations. This policy applies to all Employees and Third Parties who have access to Company information and information systems. Incident Handling should address:

- a. What constitutes an incident
- b. How should an incident be reported
- c. To who should an incident be reported
- d. What action should be taken if an incident occurs
- e. Who should handle the response to the incident
- f. Are recovery procedures required
- g. What type of follow up or review is required
- h. Should additional safeguards be implemented

To minimize damage from security incidents and to recover and to learn from such incidents, a formal incident response capability should be established, and it should include the following phases:

- Planning and preparation
- Detection
- Initiation
- Recording
- Evaluation
- Containment
- Eradication
- Escalation
- Response
- Recovery
- Closure
- Reporting
- Post-incident review
- Lessons learned

The organization and management of an incident response capability should be coordinated or centralized with the establishment of key roles and responsibilities. This should include:

- A coordinator who acts as the liaison to business process owners
- A director who oversees the incident response capability
- Managers who manage individual incidents
- Security specialists who detect, investigate, contain and recover from incidents
- Non-security technical specialists who provide assistance based on subject-matter expertise
- Business unit leader liaisons (legal, human resources, public relations, etc.)

Incidents occur because of weaknesses or vulnerabilities that are not addressed properly. A post-incident review phase should determine which vulnerabilities were exploited and why. Analysing the cause of incidents may reveal errors in the risk analysis or point out need for risk review due to unidentified threat, indicating that the residual risks are higher than the calculated values and inappropriate countermeasures have been taken to reduce inherent risks. In establishing this process, employees and contractors are made aware of procedures for reporting the different types of incidents (e.g., security breach, threat, weakness or malfunction) that might have an impact on the security of organizational assets.

2.15 Implementing Information security policies

Appropriate implementation of information security policy helps in minimizing internal security breaches that are accidental and unintentional. Educating employees about the importance of observing security policies is one of most important process. In addition following guidelines can help to enforce security policies.

2.15.1 Increasing Awareness

A security policy is only successful if employees understand and regularly observe the procedures. Those in charge of corporate security must understand the level of employee awareness in order to determine whether security policies are effective. Conducting a survey can help you determine this level and take steps to raise awareness, if necessary. Some of the questions such a survey might include are:

- Do employees know that there are security policies?
- Do they know where to find them?
- Are the policies easily accessible?
- Have all the employees read the policies?
- Do the employees understand the policies?

2.15.2 Communicating Effectively

Whether explaining security policies to new hires or sharing updates with employees, clear communication through established channels is critical. Making sure that employees understand why they are being asked to comply with security policies is also an important aspect of communication. Additional communications guidelines include:

- Target communications for various user communities.
- Provide a list of policy updates in your annual training.
- Supplement primary communications vehicles with website and newsletter articles.

2.15.3 Simplify enforcement

Convince employees to comply with every policy. Generating a higher level of compliance by creating realistic, workable policies shall help.

- **Creating a manageable number of policies:** Keeping the number of policies manageable so users can more easily find the policy that they need.
- **Making policies understandable for all audiences:** Using language that is suited for all users with examples to illustrate how the user can comply with the policy.
- **Making it easy to comply:** Including employees in policy review process to get some sense of the ease of compliance.
- **Integrating security with business processes:** Integrating security policy compliance into business processes, so employees won't need to bypass security procedures in the process of doing their jobs.
- **Aligning policies with job requirements:** Even well-intentioned policies can get in the way of job requirements.

2.15.4 Integrating Security with the corporate culture

Integrating security into the corporate culture helps to convince employees and harried executives that security is central to business success. This approach can foster a feeling of community and encourage everyone to feel that their support of security policies is important.

- **Making employees a partner in the security challenge:** Employees will be more likely to support security initiatives if they feel that the security team is there to help them instead of to police them. Establish good relationships and use the awareness program to encourage business leaders to drive security within their organizations.
- **Making security policy part of a larger compliance initiative:** Work with human resources, legal, and other compliance teams so that there is importance, credibility, and urgency attached to any policy training or communication.
- **Tying security policies to company's code of business conduct:** Educate employees to understand that their compliance with security initiatives is integral to overall appropriate behaviour and critical to business success.

2.16 Summary

Information Security is a business issue and it needs to be properly integrated into the organization's overall business goals and objectives because security issues can negatively affect the resources an organization depends upon. Security management has become more important over the years because networks have evolved from centralized environments to distributed environments. The objectives of Information Security are to provide confidentiality, integrity and availability to data and resources.

2.17 Questions

1. The Primary objective of implementing Information security management is to:
 - A. Ensure reasonable security practices.
 - B. Comply with internal audit requirements.
 - C. Adopt globally recognized standards.
 - D. Protect information assets.
2. Which of the following is primary function of information security policies?
 - A. Align information security practices with strategy.
 - B. Communicate intent of management to stakeholders.
 - C. Perform risk assessment of IT operations and assets.
 - D. Ensure compliance with requirements of standards.
3. IT security policies are set of various policies addressing different IT areas based on the IT infrastructure of organization. Which of the following policy is most common in all organizations?
 - A. Acceptable use policy
 - B. BYOD policy
 - C. Data encryption policy
 - D. Biometric security policy
4. Data-Diddling refers to:
 - A. Data manipulation.
 - B. Data entry.
 - C. Data processing.
 - D. Data backup
5. Protecting integrity of data primarily focuses on:
 - A. Intentional leakage of data.
 - B. Accidental loss of data.
 - C. Accuracy and completeness.
 - D. Data backup procedures.
6. Primary function of information security steering committee is to:
 - A. Manage information security
 - B. Select security projects
 - C. Define security policies
 - D. Direct IT security strategy
7. Which of the following is primary reason for periodic review of security policy?
 - A. Compliance requirements.
 - B. Changes on board of directors
 - C. Changes in environment

- D. Joining of new employees.
8. Main benefit of Control self-assessment is:
- A. Replacement of internal audits
 - B. Implement strong controls
 - C. Removal of redundant controls
 - D. User awareness of controls
9. Which of the following is best evidence indicting support and commitment of senior management for information security initiatives?
- A. Directive for adopting global security standard.
 - B. Higher percentage of budget for security projects.
 - C. Assigning responsibilities for security to IT head.
 - D. Information security is on monthly meeting agenda.
10. Which of the following is a concern for compliance with information security policy?
- A. Decrease in low risk findings in audit report
 - B. High number of approved and open policy exceptions
 - C. Security policy is reviewed once in two years
 - D. Security policy is signed by chief information officer

2.18 Answers and Explanations

1. **A.** The primary objective of information security management is to provide adequate level of protection to information security assets.
2. **B.** Policies are vehicle to communicate management's intent to all stakeholders. Information security practices are aligned with business objectives and not the strategy. Security policies are defined as outcome of risk assessment. Compliance with standard is not primary function of policies.
3. **C.** Acceptable use policy that address the use of IT assets by users is most common in all organizations that depends upon IT. Policies in other option depend upon organization's use of BYOD or Encryption or Biometric.
4. **A.** Data Diddling is the changing of data before or during entry into the computer system with malicious intent.
5. **C.** Integrity primarily refers to reliability that is achieved by implementing controls to ensure accuracy and completeness of data.
6. **D.** Primary function of IT security steering committee is to direct and guide IT security within organization. Other functions can be delegated.

7. C. Changes in environment introduce new risks. In order to address them it is necessary to review the security policy based on assessment of new risks. Other options are secondary reasons

8. D. Main benefit of control self-assessment is process owners are aware of risks and threats impacting desired outcome of process since they are asked to select and evaluate the controls.

9. D. Without senior management's support security cannot be a success. There are many activities senior management is involved in effective security initiative. Reviewing progress of security in monthly meeting is one of them. Other options may or may not indicate unless there is more evidence to conclude.

10. B. Policy exceptions are temporary and must be reviewed and closed as per plan. Increasing number of exceptions indicates that the policy provisions may not be appropriate and hence need to be reviewed. Other options are not concerns.

CHAPTER 3: INFORMATION ASSETS AND THEIR PROTECTION

3.1 Introduction

Effective control requires a detailed inventory of information assets. Such a list is the first step in classifying the assets and determining the level of protection to be provided to each asset. The inventory record of each information asset should include:

- Specific identification of the asset: Server, printer, network device etc.
- Relative value to the organization (based on the impact on business in case of compromise. Many times this value is determined based on the class of information processes/stored by the asset)
- Location: Where the asset is located? Depending on class of information location and protection might be decided.
- Security/risk classification
- Asset group (where the asset forms part of a larger information system)
- Owner
- Designated custodian

Information is the major business driver for almost all organizations. Dependence on information technology to collect, process and store this information to execute business operations requires that the information must be appropriately protected. Organizations cannot think of protecting entire data and information within organization uniformly. The reason is there are set of information that organization want to: 1. Publish 2. Share with select entities and business partners 3. Made available to internal users and stakeholders 4. Should not be known for more than select few. A uniform protection may introduce unnecessary delay and sometimes create challenges for operations. The solution organization adopt is known identify the information that needs various levels of protection and put them in appropriate "bucket". Now the bucket can be protected as per nature of information it contains.

Information Asset and protection guideline helps information owners in developing and implementing a comprehensive risk-based strategy for information assets protection. Key strategies are:

- defining policy, schema and guidelines for classifying and labelling information,
- defining levels of protection during every stage of information life cycle i.e. collecting, storing, using, processing, transmitting, and disposing,
- educating users and owners of information on classification schema and protection levels
- including information breach incidents in incident management process
- Review, audit/compliance processes.

The most secure environment for using restricted data files is a standalone workstation: a computer with no wired, wireless, or dial-in/out network connectivity. However in certain circumstances a user might need to connect his workstation to a network in order to access a shared resource such as a secure server, or common database or global information. This chapter covers procedures generally used for improving protection of information assets including data. Users should be aware that maintaining security in a network environment is complex and can require a systemic approach that can provide a “defence in depth” for organizational information assets. This requires considerable technical knowhow, skill and experience.

3.2 Why Information classification?

‘Data’ means information held by the company on its own behalf and/or that entrusted to it by others. It is a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. It is also information (original or derived) organized for analysis or used to reason or make decisions. The following are examples of the media which may contain or comprise information/data.

- Databases
- Data files
- Back-up media
- On-line magnetic media
- Off-line magnetic media
- Paper
- System documentation
- User manuals
- Training material
- Operational or support procedures
- Continuity plans
- Fall-back arrangements

Information classification can provide organizations with a systematic approach to protecting information consistently across all parts of organization and for all versions of information (original, copies, discarded, outdated etc.). Information follows a life cycle consisting of one or more of stages such as: origination, draft, approved/signed, received, stored, processed, transmission, archived, discarded, destruction etc. The organization is expected to protect information, during each stage of its lifecycle in a consistent manner. The state in which information exists can also influence how a piece of information should be protected.

3.3 Benefits from information classification

Table 3.1: Benefits of Information classification

Determines the level of protection to apply to information	
Description	Information classification can help in determining the risk associated in case of loss and thus prevent 'over-protecting' and/or 'under-protecting', ensuring that information is adequately protected (e.g. against unauthorized disclosure, theft and information leakage)
Example	Information classification is used on a joint project with multiple third parties. Classifying information ensures that it is adequately protected during transmission between the third parties and sent only to authorized individuals
Helps to meet compliance requirements	
Description	Information classification can be used to demonstrate that the organization is meeting particular compliance requirements (e.g. Data Protection and Privacy directives) and regulation (e.g. RBI)
Example	Internal audit uses information classification to identify documents containing Personally Identifiable Information (PII) and determine whether it has been adequately protected
Reduces operational costs	
Description	Information classification helps to ensure that security controls are only applied to information that requires such protection. This can help reduce the demand on resources and staff and ultimately reduce the cost of protecting information
Example	IT operational costs are reduced by encrypting a smaller amount of information, e.g. only information that has been classified and identified as being secret
Enables access control technologies to function more effectively	

Description	Information classification can help enforce access control policies by using the classification label to determine if an individual can gain access to a piece of information (e.g. information labelled as Secret can only be accessed by individuals that have been granted a security clearance of Secret)
Example	The Exchange may choose to deploy an information classification scheme to help ensure that users gain appropriate access to protected files. • Digital Rights Management Solution (DRM): Information classification can be used to control access and privileges for each DRM object according to individuals' security clearance (e.g. individuals assigned to work on a particular project may access files classified as secret) • Records management: Information classification can be used in records management by facilitating the organization of information, e.g. according to a particular client, date information was created or specified retention period. • E-Discovery investigation: Information classification can be used to identify electronic information in storage that is relevant to a business transaction that has resulted in, or can be expected to give rise to, legal action.

Factors that should be considered when determining the level of confidentiality of information are:

- Changes to the content of information
- Changes to external conditions over time
- Aggregation of individual pieces of information.

3.4 Information Classification policy

An information classification policy is one of the critical components of Information Security. An information security classification policy addresses the following:

- Structure of classification schema (categories of classes)
- Information owners and custodians
- Protection levels for each class of information defined by schema
- Classification method using risk management process i.e. depending upon impact on business if information is breached or not available and possibility (Likelihood) of breach.

Policy also determines the accountability of Information owners, custodians and users. Generally owners are responsible for assigning classifications to information assets according to the standard information classification system (schema and method) adopted by the organisation. Where practicable, the information category shall be embedded in the information itself.

3.5 Classification schema

All organizational information and all information entrusted to Company from third parties may fall into one of the following four classifications, presented in order of increasing sensitivity. Most organization may follow following classes: Top secret, confidential, sensitive, internal and public. The table describes the general description of classification schema, however organization may adopt different schema depending upon requirement, nature of business, compliance requirements etc.

Information Category	Description	Examples
Unclassified/ Public	Information is not confidential and can be made public without any implications for Company.	• Product brochures widely distributed • Information widely available in the public domain, including publicly available Company web site areas • Sample downloads of Company software that is for sale • Financial reports required by regulatory authorities • Newsletters for external transmission
Sensitive	• Requires special precautions to ensure the integrity and confidentiality of the data by protecting it from unauthorized modification or deletion. • Requires higher than normal assurance of accuracy and completeness.	• Passwords and information on corporate security procedures • Know-how used to process client information • Standard Operating Procedures used in all parts of Company's business • All Company-developed software code, whether used internally or sold to clients
Client Confidential Data	Information received from clients in any form for processing in production by Company. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Client media • Electronic transmissions from clients • Product information generated for the client by company

Company Confidential Data	Information collected and used by Company in the conduct of its business to employ people, to log and fulfil client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Salaries and other personnel data • Accounting data and internal financial reports • Confidential customer business data and confidential contracts • Company business plans

3.6 Data Privacy

Data privacy, also called **Information Privacy**, is generally refers to personal information. This personal information can be related to any person or stake holders who need to provide this information to organization. For example Banks may have to collect identification proofs, PAN card details, address, telephone numbers from the customers, and generates information like credit cards details, bank account numbers for customers. Or retail stores may collect credit card information from customers. If such information is leaked it may result into identity theft or impersonation by another person with malicious intent. Organizations must take care of protecting such information. Many countries have enacted laws to fix the accountability and organizations must comply with these laws. These laws specifically mandate that organization must secure personally identifiable information (PII) while processing, sharing with third parties and business associates, users etc.

3.7 Compliance requirements for Private data

There are various compliance requirements related to Personally Identifiable Information or also referred as PII.

1. **PCIDSS: Pay-card industry data security standard:** De-facto standard for card related information. Must be complied by all those deals with credit or debit cards which include banks, merchants, intermediately. Although there may not be regulatory or legal requirements as of now for compliance with PCIDSS, it has been accepted by industry.
2. **Information technology Act 2000, (Amendment 2008):** Provides that any organization is collecting PII shall be liable in case absence of reasonable security of such information results in identify theft.
3. **Reserve Bank and other regulatory authorities like CERT-In, Ministry of IT:** The regulations have mandated processes for collecting, storing, securing data and information including PII. For example one time password (OTP) for online credit card transactions, implementing security processes as per ISO27001 or equivalent certifiable information security standard etc.

4. Organisations that deals with internationally and collects privacy related information also need to comply with international legislations such as:
 - **Gramm-Leach-Bliley Act:** Mandates how financial institutions must deal with the private information of individuals.
 - **Video Privacy Protection Act:** Prevents wrongful disclosure of an individual's personally identifiable information stemming from their rental or purchase of audio-visual material.
 - **Children's Online Privacy Protection Act (COPPA):** Gives parents control over what information websites can collect from their kids.
 - **Health Insurance Portability and Accountability Act (HIPPA):** Ensures patient confidentiality for all healthcare-related data.
 - **Electronic Communications Privacy Act (ECPA):** Extends government restrictions on wire taps to include transmissions of electronic data.
- a. **Medical Information:** A person may not wish for their medical records to be revealed to others. Revealing medical or psychological conditions or treatments which would be embarrassing. Revealing medical data could also reveal other details about one's personal life.
- b. **Location Information:** As location tracking capabilities of mobile devices are increasing, problems related to user privacy arise. Location data is among the most sensitive data currently being collected.
- c. **Information on World Wide Web:** The ability to control the information one reveals about oneself over the Internet, and who can access that information, has become a growing concern. These concerns include whether email can be stored or read by third parties without consent, or whether third parties can continue to track the web sites someone has visited. Another concern is web sites which are visited collect, store, and possibly share personally identifiable information about users.

3.8 Data Protection

In order to ensure that appropriate protection is provided to information assets organization must first identify and classify all information assets. Information assets must take place at all levels described below:

- For paper documents, including output from systems, classification will apply to each individual document;
- For server-based systems, classification will be done at the file or data level;
- For information in a database, the classification will normally apply to the entire database;
- For critical databases, classification may apply to column level, at the discretion of the information owner;

- For distributed systems, classification will normally apply to all information supported by the system – in this case the classification is determined by the highest category of information supported;
- CD, DVD, diskettes, tapes, memory cards, USB sticks and any other information carriers should be classified at the highest category of information carried.

Protection policy must be defined based on class of information and type of information described above. Protection level for each class of information shall be determined based on the risk to organization due to breach of such information. While formulating data protection levels organizations need to consider these key points:

1. Physical security to all assets involved in information lifecycle:
 - a. Desktops / Laptops
 - b. Servers / storage area networks (SAN)
 - c. USB, tapes, DVDs and other Potable storages
 - d. Documents
2. Physical security of back-up media during transition depending upon the criticality of contents
3. Strong room / Safe, lock and key, fireproof cupboards for paper documents and other portable storages based on class of information.
4. Strong access controls based on principle of "Need to know and need to do". Information asset owner/custodian may consider defining access control matrix for approving and granting accesses to information based on class.
5. Encryption of information during transmission, processing and storing.
6. Content management process for data being published (printed, advertisement, website), transmitted, communicated, mailed.
7. Information communication policies and approval process, if required, before accessing/processing/transmitting classified information.
8. Consider automating data protection process based on cost-benefit analysis
9. Monitoring outgoing traffic particularly for classified information.

Note: Various protection controls mentioned here are discussed in respective modules/chapters e.g. Network security and encryption is discussed in Module 1, access controls are discussed on chapter 5 and physical and environmental security is discussed in chapter 4.

3.8.1 Data Protection automation and challenges in automation

Organization considering protecting data using automated tools finds it difficult to get appropriate information due to confusion in the marketplace(vendor) regarding DLP (data loss prevention) controls. Although there are many factors, most notable are a general lack of understanding in the vendor community about what constitutes risk to a business and bottlenecks due to impractical processes.

Organizations want to protect confidential data and also have to comply with laws and regulations look for technology to offer quick solution. However most important thing to realize is that it's not the technology, it's the methodology and execution strategy that governs the results. Organization's requirements for data protection can be categorized as:

1. Protecting data from leaking out of organization through mail and internet (Network)
2. Controlling leakage of data using removable media (End Point)
3. Protecting data stored on storage networks (NAS/SAN)

Considering these requirements organizations may have to look for multiple technological solutions. The solutions generally referred under popular acronym DLP (Data leak prevention/ Data loss prevention/ Data leak protection) provide few capabilities to be implemented independently e.g. there are solutions that focuses on protecting data passing through networks based on the rule-set and classification. Another component that focuses on endpoint controls based on rules and classification.

In addition there are solutions referred by acronym DRM (Digital rights Management) that can be applied to data files. The solutions expects creator of data file to decide who shall access the data and need to add in central user list. Sometimes this becomes impractical when such files are meant for users out of organization and they need to be authenticated by DRM server. Another challenge is that not all products support all types of data files. (E.g. Microsoft format, PDF, JPG etc.)

The third solution has acronym DAM (Digital access management) that works at data base level and manages the access rights while providing data to applications, based on rules and classification. A prerequisite for successful implementation of these tools is appropriate rule set and data classification based on impact of risks associated with data leak. Following steps might be useful:

- Create an information risk profile based on impact severity
- Create awareness about risk associated with data leak
- Define and establish process for data classification
- Identify information resources and determine classification
- Determine rule set for data usage and movement based on class of data
- Identify solutions that meets organization's requirements
- Integrate controls into the rest of the organization

3.9 Classification of other Information Assets

Classification of Information Assets helps an organization address their most significant risks, by affording them the appropriate level of security. As all information does not have the same value or use, or is subject to the same risks their protection mechanisms, recovery processes, etc., are different, with differing costs associated with them. Information assets other than data can be, categorized into following types:

1. **Servers:** Servers are the most physically secure class of systems. This is due to the common practice of placing them in a location that has better access and environmental control. Although this class may be the most physically secure, their overall security is dependent on the physical security of the workstations and portable devices that access them.

2. **Workstations:** Usually located in more open or accessible areas of a facility. Because of their availability within the workplace, workstations can be prone to physical security problems if used carelessly.

3. **Portable devices:** Can be an organization's security nightmare. Although issuing laptops and PDAs to employees facilitates flexibility and productivity in an organization, it poses several serious risks with regard to physical security. Besides, more and more organizations are adopting Bring Your Own Device (BYOD) policy which further makes the portable device and the corporate network vulnerable. With users accessing the company's internal information systems from anywhere, a breach in physical security on one of these devices could undermine an organization's information security. Extreme care must be taken with this class.

4. **Printers:** Although the data is stored on electronic for the purpose. The reports, letters, communications etc. have to be printed. Organizations deploy printers. In order to optimize use of printer most organization deploy network based printers shared among group of users. In such situation it is necessary to control the number of copies printed particularly if the information is classified and the owner is not attending the printer, there is possibility that unauthorized users may access such reports.

5. **Network devices:** devices deployed for establishing communication which includes routers, switches, firewalls, cables, wireless devices and other network monitoring tools.

Unattended equipment: Special care must be taken to protect the unattended devices. For example telecom companies may install towers to facilitate mobile communication that are not attended. Or Bank installing ATM without security guards.

3.10 Privacy management issues and role of IS Auditors

One of the many challenging and formidable risk management issues faced by organizations today is protecting the privacy of customers and employees personal information. The organization's customers, suppliers, and business partners want assurances that personal information collected from them is protected and used only for the purposes for which it was originally collected. When privacy is managed well, organizations earn the trust of their customers, employees, and other data subjects. When it's managed poorly, trust and confidence quickly erode. Privacy definitions in the business environment vary widely depending on country, culture, political environment, and legal framework. In many countries, privacy is closely linked to data protection. It can mean freedom from unwanted attention from others or freedom from observation or surveillance. And in today's business

context, privacy often refers to the privacy of personal information about an individual and the individual's ability to:

- Know how his or her personal information is handled.
- Control the information collected.

It is important that the organization implements an effective privacy program that includes:

- Privacy governance and accountability.
- Written policies and procedures.
- Controls and processes.
- Roles and responsibilities.
- Training and education of employees.
- Monitoring and auditing.
- Incident response plans.
- Plans for responding to detected problems and corrective action.

An organization's governing body is responsible for establishing an appropriate privacy framework, and internal auditing can evaluate that framework, identify significant risks, and make appropriate recommendations.

When evaluating an organization's privacy framework, internal auditors should consider the following:

- Laws and regulations in all jurisdictions in which business is conducted.
- Internal privacy policies and guidelines.
- Liaising with in-house legal counsel to understand legal implications.
- Liaising with information technology specialists and business process owners to understand information security implications.
- The maturity of the organization's privacy controls.

The auditor's role includes conducting privacy risk assessments and providing assurance over privacy controls across the organization.

Typical areas that internal auditing may review include:

- Management oversight.
- Privacy policies and controls.
- Systems that process personal information.
- Data collection methodologies.
- Uses of personal information according to stated intent, applicable laws, and other regulations.
- Security practices covering personal information.

Privacy Management audit normally includes the following:

- Is private information being disposed of according to policy and procedures?
- Is the privacy program supported by the corporate culture?

- Are workstations locked when unattended?
- Are documents stored securely prior to disposal or shredding?
- Are working documents with private data stored securely?
- How effective are the organization's privacy awareness and training programs?

3.11 Summary

Information security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, or disruption or distribution. The never ending process of information security involves ongoing training, assessment, protection, monitoring & detection, documentation, and review. This makes information security an indispensable part of all the business operations across different domains. The objective of security is to ensure confidentiality, integrity and availability company information. Information Security Policies can be issue-specific and system-specific. Security management should work from the top down, from senior management down to the staff.

3.12 Questions

1. Which of the following is Primary purpose of Information classification?
 - A. Comply with regulatory requirement
 - B. Assign owner to information asset
 - C. Provide appropriate level of protection
 - D. Reduce costs of data protection
2. Data base administrator (DBA) is:
 - A. Information Custodian
 - B. System Administrator
 - C. End User
 - D. Data Owner
3. Effectiveness of information Security awareness training program is best indicated by increase in:
 - A. percentage of classified and labelled information.
 - B. number of mails with attachments.
 - C. number of incidents reported by users.
 - D. percentage of contract employees.
4. Classification of information is primarily based on:
 - A. Where the information is stored?
 - B. Who has access to information?
 - C. What will happen if information is not available?
 - D. Why attachments to mail are encrypted?

5. Which of the following best helps in classifying the information within organizations?
- A. Using minimum classes in classification schema.
 - B. Conducting training on classification schema.
 - C. Labelling all information based on classification schema.
 - D. Determining storage based on classification schema.
6. A business application is hosted on a server. Being a small application the database required the application is also on the same server. Which of the following is best way to determine the class of the server?
- A. All servers are critical assets for organization
 - B. Based on classification of application hosted
 - C. Same as class of database decided by business
 - D. As decided by data base administrator(DBA)
7. Which of the following is a major threat related to private data of customers collect by the organization?
- A. Loss of data
 - B. Integrity of data
 - C. Data diddling
 - D. Identify theft
8. Which of the following controls can be implemented effectively due to classification of data?
- A. Input validation
 - B. Access controls
 - C. Scanning for viruses
 - D. Internal audit
9. While determining appropriate level of protection to information asset, IS auditor should **PRMARILY** focus on which of the following evidence?
- A. Results of risk assessment
 - B. Relative value to business
 - C. List of users having access
 - D. Classification of asset
10. Which of the following is **PRIMARY** consideration for classifying information assets?
Assets to be classified based on:
- A. level of protection provided.
 - B. inputs by data owner.
 - C. result of risk analysis.
 - D. requirements of security policy.

3.13 Answers and Explanations

1. **C** Primary purpose of information classification is to provide appropriate level of protection to information assets.
2. **A**. DBA is an Information custodian as DBA is responsible for maintaining database but do not have right to modify the data.
3. **A**. Security awareness program helps users and employees to understand reason for security and help in implementing it effectively. Options B, C and D do not provide information on improvement aspect.
4. **C**. It helps in assessing the risks associated and determine the protection level i.e. class of information. A, B and C are determined based on classification.
5. **B**. Training users on how to classify information as per definition provided in classification schema shall best help users in classifying the information. A. Number of classes shall depend upon organization's objectives. C and D are performed after classification of information.
6. **C**. The primary asset in this case is data that is being stored and process by the application. The server supports the data and hence must be classified as per the classification of database owned by business function.
7. **D**. Misuse of customer's private data can result in identity theft resulting in making organization liable for losses and might affect reputation adversely. A, B and C are threats can be managed by internal controls.
8. **B**. Information classifications help management in implementing better access controls for sensitive information. Other controls are not related to data classification.
9. **A**. Appropriate level of protection to asset is determined based on risk associated with asset based on vulnerabilities. Results of risk assessment, therefore is primary information IS auditor should review. Relative value of asset to business is considered while assessing impact of risk associated. Access to asset is determined based on classification of asset and need to do basis which is determined based on risk associated. Assets are classified based on result of risk assessment.
10. **C**. Assets must be primarily classified based on risk associated. Level of protection is to be decided based on result of risk analysis and not the other way round. Inputs from the owner are useful in assessing risk for the organization. Security policy provides intent of management however the policies are based on result of risk analysis.

CHAPTER 4: PHYSICAL AND ENVIRONMENTAL CONTROLS

4.1 Introduction

Prior to use of computers and communications technology most business assets were in physical form and securing them was primarily controlled manually. However technology has also enabled attackers to launch successful attack without being physically near the victim organization. Apart from traditional requirement of security organization's assets, physical security also focuses on securing technology assets physically. Physical security of computers and related resources was not as challenging in earlier days as it is today, because computers were mostly mainframes that were locked away in server rooms, and only a few people knew what to do with them anyway. Today, there is a computer on almost every desk, and access to devices and resources is spread throughout the environment. Besides, organizations have several remote and mobile users. Properly protecting these computer systems, networks, facilities, and employees has become an overwhelming task to many organizations.

Use of technology has also added a requirement to ensure that the environmental controls are in place so that the technology deployed can perform as expected. For example computer uses electrical energy to process, store and transmit data. In the process they generate heat. This heat can affect the small electronic circuits within computers resulting in failure of technology to perform. This means the environment must be able to provide sustain climatic conditions like uniform low temperature, dust free air with lower level of humidity.

Physical security should be implemented as part of layered approach to security so that if one layer fails there are other layers to protect the information and other valuable assets. A physical security program should comprise **safety** and **security** mechanisms. Safety mechanisms should cover the protection of life and assets against fire, natural disasters, and devastating accidents. Security mechanisms should cover theft, vandalism and attacks by individuals.

4.2 Physical Security controls

Physical security is a term in computer security that refers to the ability of people to physically gain access to a computer system. These can be enforced by personnel such as a border guard, a doorman, a ticket checker, etc., or with a device such as a turnstile (a gate which ensures one-way traffic of people). There may be fences to avoid circumventing this access control. An alternative of access control in the strict sense (physically controlling access itself) is a system of checking authorized presence, see e.g. Ticket controller (transportation).

Physical control can be achieved by a human (a guard, bouncer, or receptionist), through mechanical means such as locks and keys, or through technological means such as access control systems like

the Access control vestibule. Within these environments, physical key management may also be employed as a means of further managing and monitoring access to mechanically keyed areas or access to certain small assets.

Access control is the ability to permit or deny the use of a particular resource by a particular entity. Access control mechanisms can be used in managing physical resources (such as a movie theatre, to which only ticketholders should be admitted), logical resources (a bank account, with a limited number of people authorized to make a withdrawal), or digital resources (for example, a private text document on a computer, which only certain users should be able to read).

4.2.1 Objectives of physical access controls

Physical access control is a matter of who, where, and when. An access control system determines who is allowed, where they are allowed, and when they are allowed to enter or exit. Physical Access controls seek to safeguard the IS resources from physical access exposures. However designing, acquiring and implementing these controls is an expensive proposition.

- i. Physical access controls encompass securing physical access to computing equipment as well as facilities housing the IS computing equipment and supplies. The choice of safeguard should be such that they prevent unauthorized physical access but at the same time cause the least inconvenience to authorized users.
- ii. Physical access controls restrict physical access to resources and protect them from intentional and unintentional loss or impairment. Assets to be protected could include:
 - Primary computer facilities
 - Cooling system facilities
 - Microcomputers
 - Telecommunications equipment and lines, including wiring closets Sensitive areas such as buildings, individual rooms or equipment.
- iii. Physical access controls may include – manual door or cipher key locks, photo Ids and security guards, entry logs, perimeter intrusion locks etc. The effectiveness of these controls is to:
 - Grant/discontinue access authorizations.
 - Control passkeys and entry during and after normal business hours.
 - Handle emergencies.
 - Control the deposit and withdrawals of tapes and other storage media to and from the library.
- iv. Physical controls should also include:
 - Pre-planned appointments.
 - Identification checks.
 - Controlling the reception area.
 - Logging in visitors.
 - Escorting visitors while in sensitive areas etc.

4.2.2 Physical Security Threats and Exposures

One of the most important steps in any risk management procedure is to identify the threats to any organization. A threat is defined as an event (for example- a theft, fire accident etc.), the occurrence of which can have an adverse impact on the well-being of an asset. Physical threats to information system assets comprises of threats to computing equipment, facilities which house the equipment, media and people. This section deals with the security of the physical equipment and infrastructure and the environment in which they operate. The focus of the IS Auditor is to examine all factors that adversely bear on the confidentiality, integrity and availability of the information, due to improper physical access. Confidentiality, Integrity and Availability (CIA Triad) are the core principles of information safety.

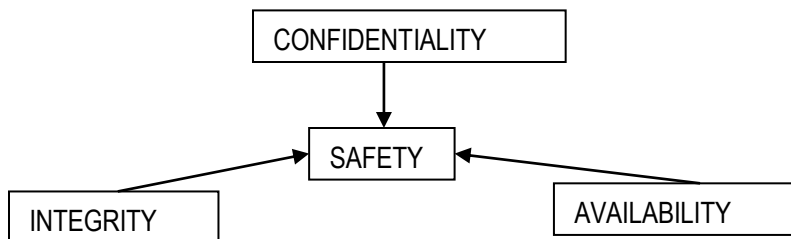


Figure 4.1: Principles of Information Safety

Confidentiality: Preventing disclosure of information to unauthorized individuals or systems.

Integrity: Prevent modification of data by unauthorized personnel.

Availability: Information must be available when it is needed.

Physical security threats can be placed into four major categories:

- i. **Electrical:** Electrical vulnerabilities are seen in things such as spikes in voltage to different devices and hardware systems, or brownouts due to an insufficient voltage supply. Electrical threats also come from the noise of unconditioned power and, in some extreme circumstances like total power loss.
- ii. **Environmental:** Not only do you need to secure your systems from human interference, but also need to secure them from the interference of natural disasters such as fires, hurricanes, tornados, and flooding, which fall under the realm of environmental threat. Extreme temperature and humidity are also environmental issues.
- iii. **Hardware:** It has the threat of physical damage to corporate hardware or its theft.
- iv. **Maintenance:** These threats are due to poor handling of electronic components, which cause ESD (electrostatic discharge), the lack of spare parts, poor cabling, poor device labelling, etc.

4.2.3 Sources of Physical security threats

The sources of physical access threats can be broadly divided into the following based on the nature of access. The perpetrators or source of physical threats can be as follows:

- Physical access to IS resources by unauthorized personnel.
- Authorized personnel having pre-determined rights of access, misusing their rights in a manner prejudicial to the interests of the organization.
- Authorized personnel gaining access to Information Systems resources in respect of which they are not authorized access. (i.e. gaining access to resources beyond their rights of “need to know; need to do”)
- Interested or Informed outsiders such as competitors, thieves, organized criminals and hackers
- Former Employees/ outsourced agencies former employees
- Accidental/Ignorant who unknowingly perpetrates a violation
- Discontented or disgruntled employees. Outsourced agencies employees
- Employees on strike or issues at outsourced agency
- Employees under termination or suspended and pending termination
- Addicted to substances or gamblers
- Experiencing financial or emotional problems

Threats from improper physical access usually are human-induced. Some examples are:

- Unauthorized persons gaining access to restricted areas. Examples are prospective suppliers gaining access to computer terminal of purchases department, thereby viewing list of authorized suppliers and rates being displayed on the screen during data entry.
- Employees gaining access to areas not authorized, e.g. sales executives gaining access to server room.
- Damage, vandalism or theft of equipment or other IS resources.
- Abuse of data processing resources, e.g. employees using internet for personal purposes.
- Damage due to civil disturbances and war.
- Embezzlement of computer supplies, e.g. floppies, cartridges, printer consumables.
- Public disclosure of sensitive information, e.g. Information regarding location of servers, confidential or embarrassing information.

4.2.4 Physical access exposures to assets

(i) **Unintentional or Accidental:** Authorized personnel or unauthorized personnel unintentionally gaining physical access to IS resources result in accidentally or inadvertently causing loss or damage to the organization.

(ii) **Deliberate:** Unauthorized personnel may deliberately gain access or authorized personnel may deliberately gain access to IS resources, for which they are not permitted or possess rights of access. This may result in the perpetrator achieving his objective of causing loss or damage to the organization or gain personal monetary benefits or otherwise.

(iii) **Losses:** Improper physical access to IS resources may result in losses to organization which can result in compromising one or any of the following:

- **Confidentiality** of organizational information or knowledge of protected organizational resources. Example: unauthorized access to systems containing sensitive information may be viewed or copied by visitors accidentally gaining access to such systems.
- **Integrity** of information by improper manipulation of information or data contained on systems or media. Example: Unauthorized access to record rooms or databases may result in modification or deletion of file content.
- **Availability** of information. Improper access to IS resources may be used to adversely impact availability of IS resources' ultimately preventing or delaying access to organizational information and business applications. Example: A disgruntled bank employee may switch off power to information servers thus sabotaging operations.

4.2.5 Physical Security Control Techniques

In order to provide physical security organization must plan security controls. This can include:

- Selection of location for hosting infrastructure and technology facilities
- Planning areas for high security requirements (e.g. data center, executive wing), Medium security requirements (e.g. employee work areas), Low security requirements (e.g., public area, receptions) and other areas where risk cannot be determined but may be prone for launching attack (e.g. parking, loading/unloading areas) Organization may have more layers based on their specific requirements.
- Define physical security controls and protection levels for each layer

Choosing and designing a secure site

Organizations may consider various controls to implement physical security. In the choice of the location during initial planning for a facility the following concerns are to be addressed.

- **Local considerations:** What is the local rate of crime (such as forced entry and burglary)?
- **External services:** The relative proximity of local emergency services, such as police, fire, and hospitals or medical facilities is to be factored in while choosing a site.
- With respect to designing the site the following considerations apply:
- **Visibility:** Facilities such as data centres should not be visible or identifiable from the outside, that is, no windows or directional signs.

- **Windows:** Windows are normally not acceptable in a data centre to avoid data leakage through electromagnetic radiation emitted by monitors. If they do exist, however, they must be translucent (semi-transparent, i.e. allowing light without being able to view things clearly) and shatterproof or monitors should not be facing them.
- **Doors:** Doors in the computer centre must resist forcible entry and have a fire rating equal to the walls. Emergency exits must be clearly marked and monitored or alarmed. Electric door locks on emergency exits should revert to a disabled state if power outages occur to enable safe evacuation. While this may be considered a security issue, personnel safety always takes precedence, and these doors should be manned in an emergency.

Security Management

- **Controlled user registration procedure:** It should be ensured that rights of physical access are given only to persons entitled thereto and to the extent necessary, based on the principles of least privileges.
- **Audit Trails.** With respect to physical security, audit trails and access control logs are vital because management needs to know where access attempts occurred and who attempted them. The audit trails or access logs must record the following:
 - The date-and time of the access attempt
 - Whether the attempt was successful or not
 - Where the access was granted (which door, for example)
 - Who attempted the access
 - Who modified the access privileges at the supervisor level
- **Reporting and incident handling procedure:** Once an unauthorized event is detected, appropriate procedures should be in place to enable reporting of such incidents and effectively handling such incidents to mitigate losses. The security administrator should be kept notified of such incidents. He may use such history to effect modifications to the security policy.

Emergency Procedures

The implementation of emergency procedures and employee training and knowledge of these procedures is an important part of administrative physical controls. These procedures should be clearly documented, readily accessible (including copies stored off-site in the event of a disaster), and updated periodically.

Human resource controls

These includes identification of employees and visitors, providing identity cards, assigning responsibilities, provided training in physical security, monitoring behaviour, escort terminated or resigned / retired employees. Human resources controls may be implemented by various departments including human resource, physical security, facility management etc.

One of most important control is process of providing access cards to employees, vendor personnel working onsite and visitors. The process should aim in preventing generation of false cards, modifying contents of cards, accounting for lost cards and reconciliation of cards to detect missing/lost cards. In addition a process to grant, change and revoke access must be in place.

Perimeter security

- i. **Guards:** Guards are commonly deployed in perimeter control, depending on cost and sensitivity of resource to be secured. While guards are capable of applying subjective intelligence, they are also subject to the risks of social engineering. They are useful whenever immediate, discriminating judgment is required.
- ii. **Dogs:** Dogs are used in perimeter security, they are loyal, reliable, and have a keen sense of smell and hearing. However, they cannot make judgment calls the way humans can.
- iii. **Compound walls and perimeter fencing:** A common method of securing against unauthorized boundary access to the facility. It helps in deterring casual intruders but is ineffective against a determined intruder.
- iv. **Lighting:** Lighting is also one of the most common forms of perimeter or boundary protection. Extensive outside lighting of entrances or parking areas can discourage casual intruders.
- v. **Deadman Doors:** Also called as Mantrap systems. These are typically used to secure entrance to sensitive computing facilities or storage areas. This technique involves a pair of doors and the space between the doors is enough to accommodate just one person. When a person is to be admitted to the premises, the second or inner door is closed while the first or outer door opens, thus admitting one person in the space between the doors. Once within that space the first door closes and then the second or inner door opens. Such doors reduce the risk of piggybacking, in which an unauthorized person could enter the secured facility by closely following an authorized person which may or may not be monitored by a guard.
- vi. **Bolting door locks:** This is the most commonly used means to secure against unauthorized access to rooms, cabins, closets. These use metal locks and keys and access can be gained by any person having physical possession of the key. This is cheap yet a reasonably effective technique, however control over physical custody and inventory of keys is required.
- vii. **Combination or Cipher locks:** The most common kind of cipher lock consists of a push button panel that is mounted near the door outside of the secured area. There are ten numbered buttons on the panel. To gain entry, a person presses a four digit number in a particular pre-determined sequence which disengages the levers for a pre-set interval of time. Cipher locks are used where large number of entrances and exits must be usable frequently. Such locks (both cipher and combination) enable resetting the unlocking sequence periodically or as per requirement. One of the most common application of combination locks is the number locks on briefcases.

- viii. **Electronic Door Locks:** Such locks may use electronic card readers, smart cards readers or optical scanners. The readers or scanners read the cards and upon the information stored on the card matching with the information pre-stored internally in the reader device, the device disengages the levers securing the door, thus enabling physical access. The advantages of such locks include:
- This technique provides a higher level of security over the previous discussed devices.
 - The same device can be used to distinguish between various categories of users.
 - Individual access needs can be restricted through the special internal code and sensor devices.
 - Restrictions can be assigned to particular doors or to particular hours.
 - Duplication of such cards is difficult.
 - Card entry can be easily deactivated from a central electronic control mechanism. This is useful in case of cards being lost or for disabling access to terminated employees etc. This also enables easy implementation of changes to security policy.
 - The devices may also include various features such as “card swallow” after pre-set number of failed attempts, activating audible alarms, engaging other access areas thus securing sensitive areas or trapping the unauthorized entrant.
- ix. **Biometric Door Locks:** These are some of the most secure locks since they enable access based on individual features such as voice, fingerprint, hand geometry, retina or iris. These are similar to the electronic door locks but more sophisticated since in this case the mechanical component securing the physical door is engaged/disengaged is controlled by an electronic device. In this case the device has a scanner/reader which reads the fingerprint or such other biometric and matching the individuals features with that internally stored.

While these devices are considered highly secure, they suffer from the following disadvantages:

- Relatively high cost of acquisition, implementation and maintenance, hence they are used mainly to secure sensitive installations.
- Time consuming process of user registration.
- Privacy issues relating to use of devices like retina and fingerprint scanners.
- High error rates compared to other devices since they may result in a false rejection or more critically a false acceptance.

Biometric devices can be used for logical access also more about biometric devices is discussed in next section.

- (i) **Perimeter intrusion detectors** - The two most common types of physical perimeter detectors are based either on photoelectric sensors or dry contact switches.
- **Photoelectric sensors** - Photoelectric sensors receive a beam of light from a light-emitting device, creating a grid of either visible white light, or invisible infrared light.

An alarm is activated when the beams are broken. The beams can be physically avoided if seen; therefore, invisible infrared light is often used.

- **Dry contact switches** - Dry contact switches and tape are probably the most common types of perimeter detection. This can consist of metallic foil tape on windows or metal contact switches on doorframes to detect when a door or window has been opened.
- x. **Video Cameras: Cameras** provide preventive and detective control. Closed-Circuit Television (CCTV) cameras have to be supplemented by security monitoring and guards for taking corrective action. The location of such cameras and recording/retention of tapes/images for future playback should be decided based on security strategy.
- xi. **Identification badges:** Special identification badges such as employee cards, privileged access pass, visitor passes etc. enable tracking movement of personnel. These can also be cards with signature and/or photo identity. These are physically examined by security staff to permit/deny access and detect unauthorized access.
- xii. **Manual Logging:** All visitors to the premises are prompted to sign a visitor's log recording the date and time of entry/exit, name of entrant, organization, purpose etc. The visitor may also be required to authenticate his identity by means of a business card, photo identification card, driver's license etc.
- xiii. **Electronic Logging:** Electronic card users may be used to record the date and time of entry/exit of the card holder by requiring the person to swipe the card both time of entry and exit. This is a faster and more reliable method for restricting access to employees and pre-authorized personnel only. These devices may use electronic/biometric security mechanisms.
- xiv. **Controlled single point access:** Physical access to the facility is granted through a single guarded entry point. Multiple entry points may dilute administration of effective security. This involves identifying and eliminating or disabling entry from all entry points except one.
- xv. **Controlled Visitor access:** A pre-designated responsible employee or security staff escorts all visitors such as maintenance personnel, contract workers, vendors, consultants for a specified time period (unless they are long-term, in which case guest access may be provided) and auditors.
- xvi. **Bonded Personnel:** This is useful in situation where physical access to sensitive facilities is given to employees or outsiders such as contract employees. Bonding (contractors or employees being required to execute a financial bond) such personnel does not improve physical security but only reduces financial impact due to improper access/misuse of physical access.
- xvii. **Wireless Proximity Readers.** A proximity reader does not require physical contact between the access card and the reader. The card reader senses the card in possession of a user in the general area (proximity) and enables faster access.
- xviii. **Alarm Systems/Motion detectors.** Alarm systems provide detective controls and highlight security breaches to prohibited areas, access to areas beyond restricted hours, violation of

direction of movement e.g. where entry only/exit only doors are used. Motion detectors are used to sense unusual movement within a predefined interior security area and thus detect physical breaches of perimeter security, and may sound an alarm.

Device level security: Organizations may also consider security controls that are implemented at device levels:

- xix. **Secured Distribution Carts:** One of the issues in batch output control is to get the printed hardcopy reports (which may include confidential materials) securely across to the intended recipients. In such cases distribution trolleys with fixed containers secured by locks are used, the keys to the relevant container are held by the respective user team.
- xx. **Cable locks:** A cable lock consists of a plastic-covered steel cable that chains a PC, laptop or peripherals to the desk or other immovable objects.
- xxi. **Port controls:** Port controls are devices that secure data ports (such as a floppy drive or a serial or parallel port) and prevent their use.
- xxii. **Switch controls:** A switch control is a cover for the on/off switch, which prevents a user from switching of the file server's power.
- xxiii. **Peripheral switch controls:** These types of controls are lockable switches that prevent a keyboard from being used.
- xxiv. **Biometric Mouse:** The input to the system uses a specially designed mouse, which is usable only by pre-determined/pre-registered person based on the fingerprint of the user.
- xxv. **Laptops Security:** Securing laptops and portables represent a significant challenge, especially since, loss of laptops create loss of confidentiality, integrity and availability. Cable locks, biometric mice/fingerprint/iris recognition and encryption of the file system are some of the means available to protect laptops and their data.

Smart Cards

A smart card used for access control is also called a security access card. This card comprises the following types:

- Photo-image cards: Photo-image cards are simple identification cards with the photo of the bearer for identification.
- Digital-coded cards: Digitally encoded cards contain chips or magnetically encoded strips (possibly in addition to a photo of the bearer). The card reader may be programmed to accept or deny entry based on an online access control computer that can also provide information about the date and time of entry. These cards may also be able to create multi-level access groupings.
- Wireless proximity readers: A proximity reader does not require the user to physically insert the access card. This card may also be referred to as a wireless security card. The card reader senses the card in possession of a user in the general area (proximity) and enables access.

4.2.6 Biometric devices

Biometric access control devices are technical applications in physical security. Biometric technologies can be used for identification or authentication. The following are typical biometric characteristics used to uniquely identify or authenticate an individual:

- Fingerprints
- Retina scans
- Iris scans
- Facial scans
- Palm scans
- Hand geometry
- Voice
- Handwritten signature dynamics

Understanding Biometrics

Biometrics is used for identification in physical access control, and for authentication in technical (logical) access control. In biometrics, identification is a one-to-many search of an individual's characteristics from a database of stored images. Authentication in biometrics is a one-to-one search to verify a claim to an identity made by a person. The three main performance measures in biometrics are:

1. **False rejection rate (FRR), or Type I error:** The percentage of valid subjects that are falsely rejected
2. **False acceptance rate (FAR), or Type II error:** The percentage of invalid subjects that are falsely accepted. FAR is more critical than FRR.
3. **Crossover error rate (CER):** The percent at which the FRR equals the FAR. In most cases, the sensitivity of the biometric detection system can be increased or decreased. If the system's sensitivity is increased, such as in an airport metal detector, the system becomes increasingly selective and has a higher FRR. Conversely, if the sensitivity is decreased, the FAR will increase.

Other important factors that must be evaluated in biometric systems are *enrolment time*, *throughput rate*, and *acceptability*.

- *Enrolment time* is the time it takes to initially register with a system by providing samples of the biometric characteristic to be evaluated.
- An acceptable enrolment time is around two minutes.
- The *throughput rate* is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a system. Acceptable throughput rates are in the range of 10 subjects per minute.
- *Acceptability* refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system.

4.2.7 Auditing Physical Access Controls

Auditing physical access requires that the auditor to review the physical access risks and controls to form an opinion on the effectiveness of these controls. This involves risk assessment, review of documentation and testing of controls.

- i. **Risk Assessment:** The auditor should satisfy himself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures.
- ii. **Controls Assessment:** The auditor based on the risk profile evaluates whether physical access controls are in place and adequate to protect the IS assets against the risks.
- iii. **Review of Documentation:** Planning for review of physical access controls requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list, cabling diagrams.
- iv. **Testing of Controls:** IS auditor should review physical access controls for their effectiveness. This involves:
 - Tour of organizational facilities including outsourced and offsite facilities.
 - Physical inventory of computing equipment and supporting infrastructure.
 - Interviewing personnel can also provide information on the awareness and knowledge of procedures.
 - Observation of safeguards and physical access procedures. This would also involve inspection of:
 - Core computing facilities.
 - Computer storage rooms.
 - Communication closets.
 - Backup and Off-site facilities.
 - Printer rooms.
 - Disposal yards and bins.
 - Inventory of supplies and consumables.

Some special considerations also involve the following:

- All points of entry/exit
- Glass windows and walls
- Moveable and modular cubicles
- Ventilation/Air-conditioning ducts
- False Ceiling and flooring panels.

Review of Physical access procedures including user registration and authorization, special access authorization, logging, periodic review, supervision etc. Employee termination procedures should provide withdrawal of rights such as retrieval of physical devices such as smart cards, access tokens, deactivation of access rights and its appropriate communication to relevant constituents in the organization. Examination of physical access logs and reports includes examination of incident reporting logs and problem resolution reports.

Some examples of Physical Control Techniques and their suggested audit procedures are given in the table here.

Control Activities	Control Techniques	Audit Procedures
Physical safeguards to commensurate with the risks of physical damage or access.	Identify facilities housing sensitive and critical resources. Identify all threats to physical well-being of sensitive and critical resources are being adequately secured using keys, alarm systems, security devices and other access control devices, including- - Use of badges. - Display and output devices. - Data transmission lines. - Power equipment and power cabling. - Mobile or portable systems. All deposits and withdrawals of tapes and other storage media from the library are authorized and logged. Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after fire drills, etc.	Review the physical layout diagram of computer, telecommunications and cooling system facilities. Walk through facilities. Review risk analysis. Review procedures for the removal and return of storage media from and to the library. Review of written emergency procedures. Observe a fire drill. Review the knowledge and awareness of emergency procedures by employees with respect to facilities using interviews, questionnaires etc.
Establish adequate security at entrance and exits based on risk	All employee access is authorized and credentials (badges, ID cards, smart cards) are issued to allow access. Management conducts regular reviews of	Review procedures and logs of employee entry and exits during and after normal business hours. Review Procedures used by management to ensure that individuals having access to sensitive facilities are

Control Activities	Control Techniques	Audit Procedures
	individuals with physical access to sensitive facilities. Visitors to the sensitive areas, such as the main computer room and tape/ media library, are formally signed in and escorted. Entry codes are changed periodically.	adequately restricted and possess physical access authorization. Review visitor entry logs. Interview guards at the facility entry. Review documentation on logs of entry, code changes and system maintenance.
Perimeter Security	Control/restrict vehicle and pedestrian traffic with measures like fences, gates, locks, guard posts and inspections. Installation of closed circuit system with recording and warning alarms - 24 hours.	Assess vehicle and pedestrian traffic around high risk facility. Inspect guard procedures and practices for controlling access to facility grounds. Inspect the facility surveillance system to assess its capability in protecting the facility.
Security control policies and procedures are documented, approved and implemented by management.	Security control policies and procedures at all levels- -Are document -Address purpose, scope, roles, responsibilities and compliance. -Ensure users can be held accountable for their actions. -are approved by management and - Periodically reviewed and updated.	Review security policies and procedures at the enterprise level, system level and process level are aligned with business/enterprise stated objectives.

4.3 Environmental Controls

This section examines the risks to IS resources arising from undesired changes in the environment. Environmental threats to information assets include threats primarily relating to facilities and supporting infrastructure, which house and support the computing equipment, media and people. IS

Auditor should review all factors that adversely bear on the confidentiality, integrity and availability of the information, due to undesired changes in the environment or ineffective environmental controls.

4.3.1 Objectives of Environmental Controls

The objects to be protected in an environment are much the same as discussed in the section on physical access controls. However from the perspective of environmental exposures and controls, information systems resources may be categorized as follows, with the focus primarily on facilities which house:

- i. **Hardware and Media:** Includes Computing Equipment, Communication equipment, and Storage Media
- ii. **Information Systems Supporting Infrastructure or Facilities:** This typically includes the following:
 - Physical Premises, like Computer Rooms, Cabins, Server Rooms/Farms, Data Centre premises, Printer Rooms, Remote facilities and Storage Areas
 - Communication Closets
 - Cabling ducts
 - Power Source
 - Heating, Ventilation and Air Conditioning (HVAC)
- iii. **Documentation:** Physical and geographical documentation of computing facilities with emergency excavation plans and incident planning procedures.
- iv. **Supplies:** The third party maintenance procedures for say air-conditioning, fire safety, and civil contractors whose entry and assess with respect to their scope of work assigned are to be monitored and logged.
- v. **People:** The employees, contract employees, visitors, supervisors and third party maintenance personnel are to be made responsible and accountable for environmental controls in their respective information processing facility (IPF). Training of employees and other stake holders on control procedures is a critical component

4.3.2 Environmental Threats and Exposures

Undesired or unintentional or intentional alteration in the environment in which computing resources function can result in threats to availability of information systems and integrity of information. Exposures from environmental threats include total or partial loss of computing facilities, equipment, documentation and supplies causing loss or damage to organizational data and information and more importantly people. The threats can be broadly classified as Natural and Man-made.

Natural Threats.

Threats to facilities and environment from natural causes can significantly and adversely impact the availability, integrity and confidentiality of information. Examples include:

- Natural disasters such as earthquakes, floods, volcanoes, hurricanes and tornadoes
- Extreme variations in temperature such as heat or cold, snow, sunlight, etc.
- Static electricity
- Humidity, vapours, smoke and suspended particles
- Insects and organisms such as rodents, termites and fungi
- Structural damages due to disasters

Man-made Threats

Human induced threats again can be unintentional or intentional, examples of which are:

- Fire due to negligence and human action
- War Action and Bomb threats
- Power – uncontrolled/unconditioned power, spikes, surges, low voltage
- Equipment failure
- Failure of Air-conditioning, Humidifiers, Heaters
- Food particles and residues, undesired activities in computer facilities such as smoking.
- Structural damages due to human action/inaction and negligence
- Electrical and Electromagnetic Interference (EMI) from Generators, motors.
- Radiation
- Chemical/liquid spills or gas leaks due to human carelessness or negligence

Exposures

Some examples of exposures from violation of environmental controls:

- A fire could destroy valuable computer equipment and supporting infrastructure and invaluable organizational data. Usually the use/ storage of thermo coal or Styrofoam (technically called Expanded Polystyrene) material, inflammable material used for construction of the server cabin, false ceiling aggravate the probability of fire and loss due to fire.
- Magnetic tapes use materials which are inflammable.
- Poor quality of power cables can over-heat and cause fire.
- Lightening may burn up communication devices and computing equipment due to improper earthing or grounding.
- Continuous process systems bear the risk of internal component damage due to improper air conditioning or high humidity.
- Damage of keyboards and other computing devices due to accidental dropping of beverages, liquid, etc.

- The organizational policies do not check the consumption of food, tobacco products near computer equipment resulting in food particles leftover in computer facilities that attract rodents, insects which can damage cabling, hard disks.
- Chemical or liquid spills from a nearby unit may seep into the IPF (Information Processing Facility) thereby damaging equipment.
- Sudden surges in power or other voltage fluctuations can irreversibly damage computer equipment.
- Fungi formation on tapes can leads to tapes and disks being not readable.
- EMI (Electromagnetic Interference) from generators can damage integrity of contents on magnetic media.
- Water leakages can induce shocks and short circuits.

Other form of power degradations includes:

- a. **Blackout:** It is a complete loss of commercial power.
- b. **Sag/dip:** It is a short period of low voltage. The duration is usually for a few seconds. Most voltage sags originate from within the facility; they can be caused by starting an electrical motor that requires a large amount of power, loose or defective wiring, or faults or short circuits. They can also originate from the power company by faults on distant circuits or voltage regulator failures.
- c. **Surge:** Surge is a sudden rise in voltage in the power supply. A strong power surge can easily harm unprotected computers and other microprocessor circuits. It also puts a stress on anything else powered by the electric supply, from air conditioning motors to light bulbs.
- d. **Transient:** It is line noise or disturbance superimposed on the supply circuit and can cause fluctuations in electrical power.

4.3.3 Techniques of Environmental Controls

The IS supporting infrastructure and facilities not only provide the conducive environment for the effective and efficient functioning of the information processing facility (IPF) but should also protect the contents of such facilities from undesirable variations in the environment. Based on the risk profile, computing equipment, supporting equipment, supplies, documentation and facilities should be appropriately situated, protected to reduce risks from environmental threats and hazards or exposures. Following are list of controls which are to be implemented.

i. Choosing and designing a safe site

The considerations during choosing a location for the facility are (as discussed in the section on Physical Access Controls):

- **Natural disasters.** Probability of natural disasters as compared to other locations? Natural disasters can include weather-related problems (wind, snow, flooding, and so forth) and earthquake faults.

- **Transportation.** Does the site have a problem due to excessive air, highway, or road traffic?
- **External services.** Relative proximity of the local emergency services, such as police, fire, and hospitals or medical facilities are to be factored while choosing a site.

Considerations during designing a site are as follows:

- **Walls:** Entire walls, from the floor to the ceiling, must have an acceptable fire rating. Closets or rooms that store media must have a high fire rating.
- **Ceilings:** Issues of concern regarding ceilings are the weight-bearing rating and the fire rating.
- **Floors:** If the floor is a concrete slab, the concerns are the physical weight it can bear and its fire rating. If it is a raised flooring the fire rating, its electrical conductivity (grounding against static build-up), and that it employs a non-conducting surface material are major concerns. Electrical cables must be enclosed in metal conduit, and data cables must be enclosed in raceways, with all abandoned cable removed. Openings in the raised floor must be smooth and nonabrasive, and they should be protected to minimize the entrance of debris or other combustibles. Ideally, an IPF should be located between floors and not at or near the ground floor, nor should it be located at or near the top floor.
- **Windows:** Windows are normally not acceptable in the data centre. If they do exist, however, they must be translucent and shatterproof.
- **Doors:** Doors in the computer centre must resist forcible entry and have a fire rating equal to the walls. Emergency exits must be clearly marked and monitored or alarmed. Electric door locks on emergency exits should revert to a disabled state if power outages occur to enable safe evacuation. While this may be considered a security issue, personnel safety always takes precedence, and these doors should be manned in an emergency.
- **Media Protection:** Location of media libraries, fire proof cabinets, kind of media used (fungi resistant, heat resistant).
- **Sprinkler system and fire resistance:** The fire-resistance rating of construction material is a major factor in determining the fire safety of a computer operations room. Generally, the computer room must be separated from other occupancy areas by construction with a fire-resistant rating of not less than two hours.
- **Water or gas lines:** Water drains should be "positive;" that is, they should flow outward, away from the building, so they do not carry contaminants into the facility.
- **Air conditioning:** AC units should have dedicated power circuits. Similar to water drains, the AC system should provide outward, positive air pressure and have protected intake vents to prevent air carried toxins from entering the facility.
- **Electrical requirements:** The facility should have established backup and alternate power sources.

ii. Facilities Planning

As part of facilities planning, the security policy should provide for specific procedures for analysis and approval of facilities building and refurbishment plan. Depending on the size and nature of computing facilities, a separate function should exist for facilities planning and management. The following aspects need to be considered in this context:

- As part of environmental security clearance, procedures should be prescribed to ensure that all aspects relating to facilities planning are adequately considered.
- Approved list of materials to be used for construction of facilities, based on the class of computing facilities, the specification of equipment to be housed in such facilities should need consideration.
- The organization chart should provide for designated personnel assigned with the responsibility of risk assessment procedures as a dynamic function.
- The risk profile of the organization should take into consideration newer environmental threats. A few examples of threats to be considered are given below:
- Installation of a generator by a neighbour.
- Sudden changes in climate leading to extreme changes in humidity levels.
- Building construction in the vicinity of IPF leading to increase in suspended dust particles in the environment.
- Raising of foundation and flooring by a neighbour causing change in the flow of rainwater.
- Installation of high power consumption equipment adversely affecting the quality of power.

iii. Documentation

The documentation of physical and geographical location and arrangement of computing facilities and environmental security procedures should be modified promptly for any changes thereto. Access to such documentation should be strictly controlled. For example, knowledge of location and scheme of ventilation ducts can be used by a perpetrator to gain unauthorized entry to sensitive facilities which otherwise may be secured by physical and logical controls.

iv. People Responsibility and Training

Responsibility and accountability for environmental controls planning and management should be fixed and should be expressly communicated as part of job description. Awareness and training initiatives should encompass educating employees and stakeholders on environmental exposures and controls and their responsibilities thereof. New employee induction programs should include informing and educating employees on environmental control procedures, prohibited activities (eating, smoking, drinking inside IPF), and maintaining secrecy and confidentiality. Care should also be taken to ensure that sharing such information should not result in risks, where unauthorized persons could gain knowledge of sensitive environmental control vulnerabilities.

v. Emergency Plan

Disasters result in increased environmental threats e.g. smoke from a fire in the neighbourhood or in some other facility of the organization would require appropriate control action, evacuation plan should be in place and evacuation paths should be prominently displayed at strategic places in the organization.

- *Reporting procedures* should be in place to enable and support reporting of any environmental threats to a specified controlling authority.
- *Periodic inspection, testing and supervision* of environmental controls should form a part of the administrative procedures. The tests of such inspection, tests and drills should be escalated to appropriate levels in the organization.
- *Documented and tested emergency evacuation plans* should consider the physical outlay of the premises and orderly evacuation of people, shut down of power and computer equipment, activation of fire suppression systems.
- *Administrative procedures* should also provide for Incident Handling procedures and protocols due to environmental exposures.

vi. Vendors/Suppliers (Third Party)

In most cases installation and maintenance of environmental controls involves the services of third parties such as air conditioning, fire safety equipment, civil contractors, and carpenters. By virtue of their scope of work, knowledge of and access to sensitive computing facilities and environmental control vulnerabilities are available to such agencies. Procedures should include detailed analysis of considerations such as, whether to outsource, choice of such agency, background verification, security bonding, controlled access of maintenance staff and performance appraisal.

vii. Maintenance Plans

A comprehensive maintenance and inspection plan is critical to the success of environmental security and controls. Preventive maintenance plan and management procedures should be in place. This is a critical aspect of environmental control procedures, negligence in respect of which can lead to exposing the IPF to risks, e.g. prolonged ineffectiveness/failure of air conditioning facility can lead to risks of damage to servers and thereby loss of organizational data; a fire extinguisher not working at time of disaster due to negligence in refilling and maintenance. Maintenance plans should also include evaluation of effectiveness and efficiency of environmental facilities such as electric power distribution, heating plants, water, sewage, and other utilities required for system operation or staff comfort. Environmental controls should be documented and a suitable preventive maintenance should be put in place administered through schedules and logs.

viii. MTBF and MTTR

Failure modes of each utility, risks of utility failure, should be identified, parameterized and documented. This includes estimating the MTBF (Mean Time between Failures) and MTTR (Mean

Time to Repair/recover/respond/ restore). Planning for Environmental controls would need to evaluate alternatives with low MTBF or installing redundant units. Stocking spare parts on site and training maintenance personnel can reduce MTTR. Each of these strategies can be evaluated by comparing the reduction in risk with the cost to achieve it.

ix. Fire-resistant walls, Floors and Ceilings

The construction of IPF should use fire-resistant materials for walls, floors and ceilings. Depending on application and investment, manufacturers offer materials with varied fire ratings. Fire rating resistance of at least 2 hours is generally recommended.

x. Concealed Protective Wiring

Power and Communication cables should be laid in separate fire resistant panels and ducts. The quality rating of power cables should match the load and manufacturers specifications.

xi. Ventilation and Air Conditioning

The temperature in the IPF should be controlled depending on the type of equipment and processing. Improper maintenance of temperature leads to overheating of internal components. It should be examined if uninterruptible powers supply systems should supply power HVAC equipment that supports critical IPF units.

xii. Power Supplies

Computing equipment can be subject to risks of power failure and other power anomalies. Power supply should conform to computing equipment manufacturer specifications. Many elements can threaten power systems, the most common being noise and voltage fluctuations. Noise in power systems refers to the presence of electrical radiation in the system that is unintentional and interferes with the transmission of clean power. There are several types of noise, the most common being electromagnetic interference (EMI) and radio frequency interference (RFI). Voltage fluctuations are classified as Sag (momentary low voltage), Brownout (prolonged low voltage), and Spike (momentary high voltage), Surge (prolonged high voltage) and Blackouts (complete loss of power).

Some of the controls to ensure uninterrupted delivery of clean power are:

- a. **Uninterruptible Power Supply (UPS)/ Generator:** UPS usually consist of battery backup or kerosene powered generator that interfaces with the external power supplied to the equipment. On interruption in external power supply, the control is immediately switched to the battery back-up. Depending on the application, UPS are available with battery backup of a few minutes to a number of days. UPS can be on-line or off-line. UPS generally is a good solution in case of applications enabling their proper closure of processing and systems. In respect of continuous process equipment, UPS may fail to meet the purpose if regular power supply is not available for a prolonged period of time. Diesel or kerosene generators could also be used, but they

require some time to be switched on and the power from generators has to be cleansed before delivery to computer systems.

- b. **Electrical Surge Protectors/Line Conditioners:** Power supply from external sources such as grid and generators are subject to many quality problems such as spikes, surges, sag and brown outs, noise, etc. Surge protectors, spike busters and line conditioners are equipment which cleanses the incoming power supply of such quality problems and delivery clean power for the equipment.
- c. **Power leads from two sub-stations:** Failure of continued power supply to some high consumption continuous processing could even result in concerns regarding public safety such as refineries, nuclear reactors and hospitals. Electric power lines may be exposed to many environmental and physical threats such as floods, fire, lightning, careless digging, etc. To protect against such exposures, redundant power lines from a different grid supply should be provided for. Interruption of one power supply should result in the system immediately switching over to the stand-by line.

xiii. Smoke Detectors and Fire Detectors

Smoke and fire detectors activate audible alarms or fire suppression systems on sensing a particular degree of smoke or fire. Such detectors should be placed at appropriate places, above and below the false ceiling, in ventilation and cabling ducts. In case of critical facilities, such devices must be linked to a monitoring station (such as fire station). Smoke detector should supplement and not replace fire suppression systems.

xiv. Fire Alarms

Manually activated fire alarms switches should be located at appropriate locations prominently visible and easily accessible in case of fire (but should not be easily capable of misuse during other times). By manual operation of switch or levers, these devices activate an audible alarm and may be linked to monitoring stations both within and/or outside the organization.

xv. Emergency Power Off

When necessity of immediate power shutdown arises during situations such as computer facility fire or emergency evacuation, emergency power-off switches should be provided. There should be one within the computer facility and another just outside the computer facility. Such switches should be easily accessible should be shielded to prevent accidental use.

xvi. Water detectors

Risks to IPF equipment from flooding and water logging can be controlled by use of water detectors placed under false flooring or near drain hole. Water detectors should be placed on all unattended or unmanned facilities. Water detectors on detecting water activate an audible alarm.

Centralized Disaster monitoring and control Systems: Such systems provide for an organization-wide network control wherein all detection devices, alarms and corrective/suppression devices are controlled from a central monitoring command and control. It is necessary that such systems are powered by a more secure and reliable/uninterrupted power supply. Such systems should be failure tolerant and involve low maintenance

xvii. **Fire Suppression Systems**

Combustibles are rated as either Class A, B, or C based upon their material composition, thus determining which type of extinguishing system or agent is used. Fires caused by common combustibles (like wood, cloth, paper, rubber, most plastics) are classed as Class A and are suppressed by water or soda acid (or sodium bicarbonate). Fires caused by flammable liquids and gases are classed as Class B and are suppressed by Carbon Dioxide (CO), soda acid, or FM200. Electrical fires are classified as Class C fires and are suppressed by Carbon Dioxide (CO), or FM200. Fire caused by flammable chemicals and metals (such as magnesium and sodium) are classed as Class D and are suppressed by Dry Powder (a special smothering and coating agent). Class D fires usually occur only places like chemical laboratories and rarely in office environments. Note that using the wrong type of extinguisher while suppressing a fire can be life-threatening. Broadly, Fire Suppression systems for facilities are classed into

- a. Water based systems and
- b. Gas based systems

a. **Water Based Systems**

- **Wet Pipe Sprinklers:** In this case, sprinklers are provided for at various places in the ceiling or on the walls and water is charged in the pipes. As generally implemented a fusible link in the nozzle melts in the event of a heat rise, causing a valve to open and allowing water to flow. These are considered the most reliable but however they suffer from the disadvantage of leakage, breakage of pipes exposing the IPF to the risks of dampness and equipment suffering water damage.
- **Dry-Pipe Sprinklers:** These are similar to the wet pipe sprinklers except that in this the water is not kept charged in pipes but pipes remain dry and upon detection of heat rise by a sensor, water is pumped into the pipes. This overcomes the disadvantage with wet pipe systems of water leakages etc.
- **Pre-action:** At the present time, this is the most recommended water-based fire suppression system for a computer room. It combines both the dry and wet pipe systems by first releasing the water into the pipes when heat is detected (dry pipe) and then releasing the water flow when the link in the nozzle melts (wet pipe). This feature enables manual intervention before a full discharge of water on the equipment occurs.

b. Gas Based Systems

- **Carbon-dioxide:** Such systems discharge CO thus effectively cutting of oxygen supply from the air, which is a critical component for combustion. However, CO being potentially lethal for human life, such systems are recommended only in unmanned computer facilities or in portable or hand-held fire extinguishers. Portable fire extinguishers commonly contain CO or soda acid and should be commonly located at exits, clearly marked with their fire types Checked regularly by licensed personnel.
- **FM200:** Halon was once considered the most suitable agent for fire suppression. FM200 is an inert gas, does not damage equipment as water systems do and does not leave any liquid or solid residues, however it is not safe for humans as it reduces the levels of oxygen. Halon is not considered safe for environment as it is an ozone-depleting agent. Under an international agreement, the Montreal Protocol, the production of Halon has been suspended from 1994 and FM 200 replaced the Halon.

4.3.3 Integration and fine-tuning of environmental controls

As part of environmental risk assessment, facilities planning and facilities management, it is critical to consider the overall effectiveness, efficiency of controls. Planning for environmental controls should consider interdependencies of IS assets being secured, vulnerabilities of such assets and related nature of other controls such as logical and physical access controls. The security policy should orchestrate the overall design; effectiveness and efficiency of controls to ensure that investment in environmental controls are optimum without compromise on security.

4.3.4 Audit and evaluation of Environmental Controls

As part of audit procedures, the audit of environmental controls requires the IS auditor to conduct physical inspections and observe practices, which may include the following activities:

- Inspect the IPF and examine the construction with regard to the type of materials used for construction by referring to the appropriate documentation.
- Visually examine the presence of water and smoke detectors, examine power supply arrangements to such devices, testing logs, etc.
- Examine location of fire extinguishers, fire-fighting equipment and refilling date of fire extinguishers and ensure their adequate and appropriate.
- Examine emergency procedures, evacuation plan and marking of fire exits. If considered necessary, the IS Auditor can also require a mock drill to test the preparedness with respect to disaster.
- Examine documents for compliance with legal and regulatory requirements as regards fire safety equipment, external inspection certificate, shortcomings pointed out by other inspectors/auditors.

- Examine power sources and conduct tests to assure quality of power, effectiveness of power conditioning equipment, generators, simulate power supply interruptions to test effectiveness of back-up power.
- Examine environmental control equipment such as air-conditioning, dehumidifiers, heaters, ionizers etc.
- Examine complaint logs and maintenance logs to assess if MTBF and MTTR are within acceptable levels.
- Observe activities in the IPF for any undesired activities such as smoking, consumption of eatables etc.

Documentation of findings

As part of the audit procedures, the IS auditor should document all findings as part of working papers. The working papers could include audit assessment, audit plan, audit procedure, questionnaires, and interview sheets, inspection charts, etc.

Examples of environmental controls and their Audit procedures

Control Activities	Control Techniques	Audit Procedures
Safeguards against the risks of heating, ventilation and air-conditioning systems.	Identify systems that provide constant temperature and humidity levels within the organization.	Review a heating, ventilation and air-conditioning design to verify proper functioning within an organization.
Control of radio emissions effect on computer systems.	Evaluate electronic shielding to control radio emissions that affect the computer systems.	Review any shielding strategies against interference or unauthorized access through emissions.
Establish adequate interior security based on risk	Critical systems have emergency power supplies for alarm systems; monitoring devices, exit lighting, communication systems.	Verify critical systems (alarm systems, monitoring devices, and entry control systems) have emergency power supplies. Identify back -up systems and procedures and determine the frequency of testing. Review testing results.
Adequately protect against emerging threats, based on risk.	Appropriate plans and controls such as shelter in place or for a potential CBR attack(chemical, biological and radioactive attack)	Interview officials, review planning documents and related test results. Observe and document the controls in place to mitigate emerging threats.

Control Activities	Control Techniques	Audit Procedures
	Restricting public access and protect critical entry points-air intake vents, protective grills and roofs.	Observe location of these devices and identify security measures implemented. Verify the controls existence and intrusion detection sensors.
Adequate environmental controls have been implemented	Fire detection and suppression devices are installed and working.(smoke detectors, fire extinguishers and sprinkle systems) Controls are implemented to mitigate disasters, such as floods, earthquakes. Redundancy exists in critical systems like, uninterrupted power supply, air cooling system, and backup generators Humidity, temperature, and voltage control are maintained and acceptable levels Emergency lighting, power outages and evacuation routes are appropriately located.	Interview managers and scrutinize that operations staff are aware of the locations of fire alarms, extinguishers, shut-off power switches, air - ventilation apparatus and other emergency devices. Determine that humidity, temperature and voltage are controlled within the accepted levels. Check cabling, plumbing, room ceiling smoke detectors, water detectors on the floor are installed and in proper working order.
Staff have been trained to react to emergencies	Operational and support personnel are trained and understand emergency procedures. Emergency procedures are documented and periodically tested- incident plan, inspection plan and maintenance plan.	Interview security personnel to ensure their awareness and responsibilities. Review training records and documentation. Determine the scope and adequacy of training. Review test policies, documentation and know-how of operational staff. Review incident handling procedures and maintenance and inspection plan.

4.4 Summary

This chapter deals with the physical and environmental threats and their control and audit procedures on information system assets. The first step in providing a secured physical environment for the information system assets is listing the various assets in the computing environment. These assets could range from hardware, software, facilities and people that form the computing environment. The next step is to identify the various threats and exposures the assets are exposed to. These threats could include unauthorized access to the resources, vandalism, public disclosure of confidential information and the like, the main source of threats is from outside people and the employees of the organization. However, the information assets are exposed to various other sources of threats like natural damage due environmental factors like flood, earthquake, fire and rain etc.

4.5 Questions

1. Which of the following is first action when a fire detection system raises the alarm?
 - A. Turn off the air conditioning.
 - B. Determine type of fire.
 - C. Evacuate the facility.
 - D. Turn off power supply
2. Which of the following is most important controls for unmanned data center?
 - A. Access control for entry and exit for all doors.
 - B. The humidity levels need not be maintained.
 - C. The temperature must be at sub-zero level.
 - D. Halon gas based fire suppression system.
3. Primary purpose of access controlled deadman door, turnstile, mantrap is to:
 - A. Prevent unauthorised entry
 - B. Detect perpetrators
 - C. Meet compliance requirement
 - D. Reduce cost of guard
4. Which of the following is main reason for appointing human guards at main entrance of facilities?
 - A. Address visitors' requirements to visit.
 - B. Issue the access cards to visitors.
 - C. Cost of automation exceeds security budget.
 - D. Deter the unauthorized persons.

Module 4

5. Which of the following is major concern associated with biometric physical access control?
 - A. High acceptability.
 - B. High false positives.
 - C. High false negatives.
 - D. High cost.
6. Which of the following evidence is best to provide assurance on automated environmental controls?
 - A. Annual maintenance contract with vendor.
 - B. Simulation testing of devices during audit.
 - C. Device implementation report by vendor
 - D. Documented results of periodic testing.
7. What are the problems that may be caused by humidity in an area with electrical devices?
 - A. High humidity causes excess electricity, and low humidity causes corrosion.
 - B. High humidity causes power fluctuations, and low humidity causes static electricity.
 - C. High humidity causes corrosion, and low humidity causes static electricity.
 - D. High humidity causes corrosion, and low humidity causes power fluctuations.
8. Automated access controls opens doors based on access cards, pins, and/or biometric devices and are powered by electricity. Which of the following best policy in case of power failure?
 - A. Keep the door in locked state
 - B. Open door and appoint guard
 - C. Find root cause of power failure
 - D. Arrange for battery backup
9. While selecting site for a data center which of the site is best to be selected?
 - A. On topmost floor to delay the unauthorised visitor to reach.
 - B. In the basement not easily accessible to perpetrator.
 - C. On ground floor do that users can access is easily.
 - D. On middle floor to strike the balance for above concerns.
10. Which of the following is main reason for not allowing mobile devices into data center?
 - A. Unauthorized changes and access in configuration.
 - B. Prevent photography of data center layout.
 - C. User can provide information to attacker on phone.
 - D. Mobile devices generate wireless communication.

4.6 Answers and Explanations

1. **C.** Life safety takes precedence. Although other answers are important steps human life always is a priority.
2. **B.** Unmanned data center requires strong physical access controls and environmental access controls too. However most essential are strong access controls. B, C and D are inappropriate controls. Halon is environmentally hazardous gas.
3. **A.** Primary purpose of all types of physical access control is to prevent unauthorized entry. Other objectives are secondary.
4. **A.** Human guard make decisions and can address visitor's requirement and direct them appropriately. Others are supplementary functions.
5. **B.** False positive is a concern in biometric access security as it results in unauthorized access. Other option does not result in unauthorized access.
6. **D.** Automated environmental controls must be tested periodically by expert and provide report on effective performance of equipment. Simulated tests may not be possible for all controls. AMC is a contract, periodic testing is performance of contract.
7. **C.** High humidity can cause corrosion, and low humidity can cause excessive static electricity. Static electricity can short out devices or cause loss of information.
8. **B.** Best policy is to keep door open and appoint guard temporarily for monitoring accesses. Keeping doors locked shall be a problem in evacuation in case of emergency. Finding root cause can be done independently. Arranging Battery backup after power failure is not right policy.
9. **D.** Top floor and basement has risk of seepage and flooding. Ground floor has risk of easy attack.
10. **A.** Mobile devices can be connected to servers and resulting in unauthorized changes. Other concerns are secondary.

CHAPTER 5: LOGICAL ACCESS CONTROLS

5.1 Introduction

Virtually every day another news story highlights the importance of network security - corporate networks are breached, databases are accessed by unauthorized individuals, and identities are stolen and used to conduct fraudulent transactions. As a result, both businesses and governments are evaluating or implementing new identity management systems to provide more secure logical access. Today IT systems store and process a wide variety of data centrally in one system and provide access to the same to a large number of users. Keeping data stored centrally on a system contributes to cost effective and efficient information sharing and processing. In such an environment it is not unusual that there is a requirement that:

- Some information must be accessible to all users,
- Some is needed by several groups or departments,
- And some accessible by only a few individuals

Information that is residing on a system and accessed by many users has an associated risk of unauthorized access. Logical access controls are a means of addressing concerns associated with unauthorized accesses. Logical access controls are protection mechanisms that limit users' access to data and restrict their access on the system based on "need to know and need to do" basis. These access controls need to be part of assets that are designed to store and process information, i.e. application systems, database management systems, operating systems, middleware. However to minimize complexity organizations may choose to implement external access control systems like single sign-on, Citrix farm, LDAP and active directory etc. In this chapter, we will understand various ways that data can be accessed and how logical access controls can help to ensure that only the right persons access the right data.

5.2 Objectives of Logical Access Controls

The purpose of logical access controls is to prevent and detect unauthorized access to information assets / resources while ensuring that authorized users can access the information resources as per their role and responsibilities. This is achieved by providing access on "need to know and need to do" basis using principle of least privileges. It means that the access should not be so restrictive that it makes the performance of business functions difficult or it should not be so liberal that it can be misused i.e. it should be just sufficient for one to perform one's duty without any problem or restraint. Logical access controls is all about protection of information assets in all three states, namely: stored, in transit and being processed

5.3 Paths of Logical Access

An auditor has to identify the possible access paths permitting access to information resources. Auditor must document the logical paths and prescribe appropriate audit procedures to evaluate every component in the information systems infrastructure to enable identification of logical access paths. This is often a challenging and complex task when it comes to auditing in networking computing environments. Identification and documentation of access paths involves testing security at various layers:

- **Hardware:** This includes computer workstations, terminal devices, communication devices, peripherals etc., constituting the physical interface with the users. Here the auditor should consider vulnerabilities of different communication channels and devices (e.g. modems, network interface cards) connected to computers.
- **Systems software:** The command and control of hardware rests in the proper implementation of operating systems and other systems software. Hardware works in tandem with, and its operation is synchronized by, systems software which forms the foundation for effective systems security. From a logical perspective, a wrong setting of systems level parameters can compromise the security of the application and other systems software, which talk to the systems software. Auditor should ensure that logical accesses to system software are controlled to prevent and/or detect changes in system configuration.
- **Database Management System:** In environments involving voluminous data handling, a Database Management System (DBMS) manages the organisation of data in the databases. The auditor is required to evaluate the access security enforced by the DBMS, which could include schema definitions, access to data dictionary, directory services and scripts to restrict access implemented by the DBMS.
- **Application software:** Application software represents the business logic, which **interfaces with the user** and business process requirement, from the user perspective. The auditor focuses on the effectiveness of boundary controls and other input, processing and output controls, discussed elsewhere in this module.
- **Access control software:** The auditor may also encounter situations in networked environments with users having access to various applications. In such cases user and program access to applications and IS resources are controlled by an access control software. The auditor should evaluate the access permissions configured in the software and ascertain their appropriateness to the organisation's functional requirements.
- In the above cases, the assessment of state of access controls can be quite technical, presenting complexities for the IS auditor. Therefore, in cases, where the controls involve technical sophistication, the auditor has to rely on the services of a technical expert, who possesses special skills, knowledge and experience in the particular field. Where the auditor relies on the work of an expert, he should evaluate the work and the extent of reliance on the work of the expert. The auditor's report should explicitly state this fact of IS auditor's reliance on work of other experts.

Each of these routes has to be subjected to appropriate means of security in order to secure it from the possible logical access exposures.

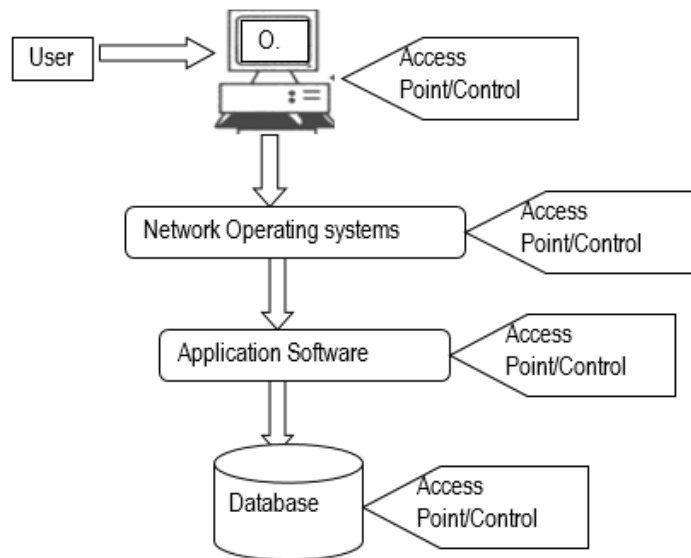


Figure 5.1: Logical Access Paths in an Enterprise Information System

5.4 Logical Access attacks

Improper logical access can result in loss or damage to information and resources leading to undesirable consequences for an organization. It can also result in violation of the confidentiality or integrity or availability of information. There are various types of exposures related to access controls where unauthorized persons tried to get information useful for breaking into organization system. These attacks can be grouped based on the object of attack i.e. Technology and/or user. Some of the technical attacks are discussed below:

Masquerading: It means disguising or impersonation. The attacker pretends to be an authorized user of a system in order to gain access to or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. The attempt may come from within an organization, for example, from an employee; or from an outside user through some connection to the public network. Weak authentication provides one of the easiest points of entry for a masquerade. Once the attacker has been authorized for entry, they may have full access to the organization's critical data, and (depending on the privilege level they pretend to have) may be able to modify and delete software and data or make changes.

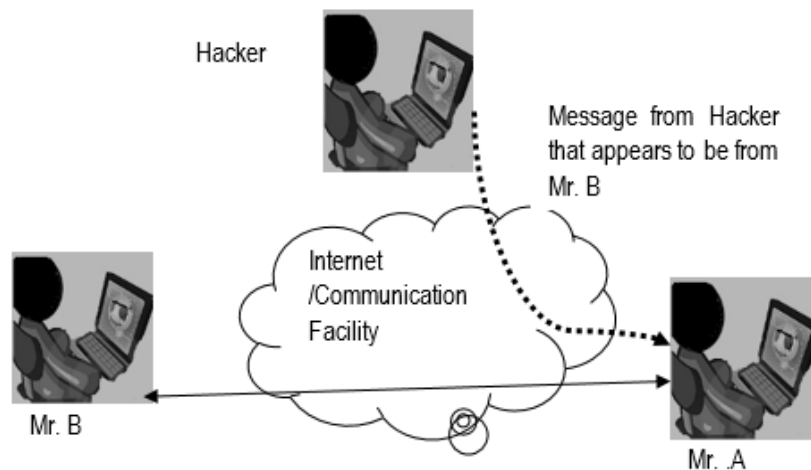


Figure 5.2: Masquerade or impersonating

Piggybacking: Unauthorized access to information by using a terminal that is already logged on with an authorized ID (identification) and left unattended.

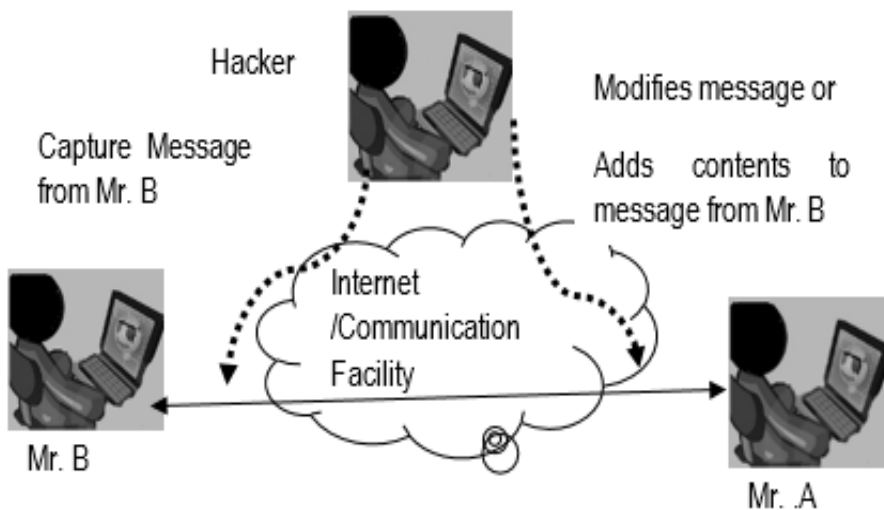


Figure 5.3: Piggybacking i.e. following authorized user

Wiretapping: Tapping a communication cable to collect information being transmitted.

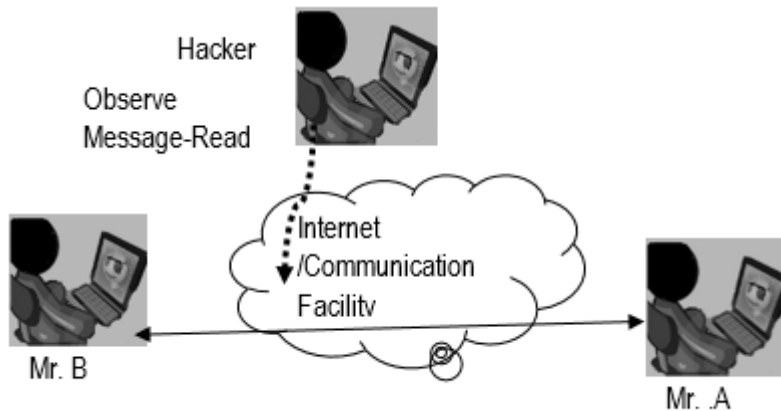


Figure 5.4: Wiretapping a passive attack to collect information

Denial of Service: The perpetrator attempts to flood memory buffers and communication ports to prevent delivery of normal services. (Covered in next chapter)

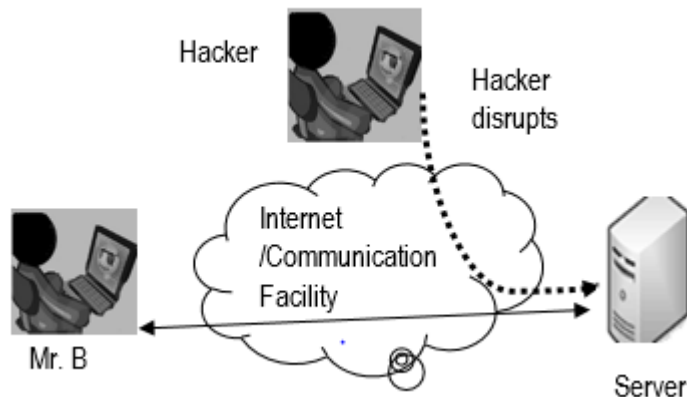


Figure 5.5: Denial of Service by disrupting traffic

Social Engineering

This is an attack on the weakest link i.e. human. The perpetrators uses different means including spoofing and masquerading resulting in person reveals confidential information like user ID, Password, PIN and any such information required for login as authorized user.

Examples of some of these attacks are:

- **Phishing:** User receives a mail requesting to provide authentication information by clicking on link provided. The mail and link appears to be actual originator e.g. Bank. Unaware users click on link and provide confidential information. The most popular attacks on banking systems in the recent times, they target gullible victims, using a combination of social engineering, e-mail and fake websites to con the victim to click on a link embedded in an apparent authentic mail from a reputed bank. The link takes the victim (generally a customer of the bank) to a look-alike Bank website that gets the personal details of the victim including details such as PIN and internet banking password, which is then exploited by the hacker.
- **Impersonating:** Uses the similar technique over telephone.
- **Key logger:** Perpetrator installs software that captures the key sequence used by user including login information. Key logger can be sent thru mail or infected pen drive like virus or other malware. There are hardware key loggers available that are connected to system where key board is attached.
- **Malware:** Specially designed programs that captures and transmits the information from compromised system.
- Malicious code (also called "Malware") is the name used for any program that adds to, deletes or modifies legitimate software for the purpose of intentionally causing disruption and harm or to circumvent or subvert the existing system's function. Examples of malicious code include viruses, worms, Trojan Horses, and logic bombs. Newer malicious code is based on Active X and Java applets.

Viruses:	• Are malicious code that attaches to a host program and propagates when an infected program is executed? The perpetrator's objective is to multiply and spread the code. However they are dependent on another program or human action to replicate or to activate their payload. They are not capable of self-actuating.
Worms:	• Are malicious programs that attack a network by moving from device to device and create undesirable traffic. • They differ from viruses in that for replication or activation of code, they do not depend on any program or human action but are self-actuating and self-sustaining and spread much more rapidly than viruses.
Trojan Horses:	• These are malicious code which hides inside a host program that does something useful. Once these programs are executed, the hidden malicious code is released to attack the workstation, server, or network or to allow unauthorized access to those devices. Some Trojans are programmed to open specific ports to allow access for exploitation. Then the open Trojan port could be scanned and located, enabling an attacker to compromise the system. These are also used as tools to create backdoors into the network for later exploitation by crackers.

Logic Bombs:	• These are legitimate programs, to which malicious code has been added. Their destructive action is programmed to “blow up” on occurrence of a logical event such as time or a logical event as number of users, memory/disk space usage, etc. • Every time the infected program is run, the logic bomb checks external environment to see whether the condition to trigger the bomb has been met. If not, control is passed back to the main application and the logic bomb waits. If the condition is satisfied, the rest of the logic bomb’s code is executed, and it attacks the system. • Logic bombs are very difficult to detect since they reside in the system and its destructive instruction set is known only after it blows up.
Macro Viruses:	• A macro is an instruction that carries out program commands automatically. Many common applications (e.g. word processing, spreadsheet, and slide presentation applications) make use of macros. • A macro virus is a computer virus that “infects” a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or an event trigger. If a user accesses a document containing a viral macro and unwittingly executes this macro virus, it can then copy itself into that application’s start-up files. • The computer is now infected and a copy of the macro virus resides on the machine. Any document on the machine that uses the same application can become infected. If the infected computer is on a network, the infection is likely to spread rapidly to other machines on the network. Because these types of files are commonly used and sent through e-mail, a computer network can be quickly infected by these viruses. • Macro viruses tend to be surprising but relatively harmless.
Polymorphic Viruses	• Polymorphic viruses are difficult to detect because they hide themselves from antivirus software by altering their appearance after each infection. Some polymorphic viruses can assume over two billion different identities.
Stealth Viruses	• Stealth viruses attempt to hide their presence from both the operating system and the antivirus software by encrypting themselves. They are similar to polymorphic viruses and are very hard to detect.

Adware and Spyware	• They are often software that tracks the Internet activities of the user usually for the purpose of sending targeted advertisements. • Besides the loss of privacy and waste of bandwidth (loss of availability), they do not pose other security related risks, as yet. However, it is quite likely that Trojans could be embedded in such software. • Adware and Spyware often come with some commercial software, both packaged as well as shareware software. There is often a reference to the Adware and Spyware software in the license agreement.

5.5 Logical Access Controls policy and procedures

Access control policy is part of overall information Security policy. It states a set of rules, principles, and practices that determine how access controls are to be implemented. Access control policy typically covers the following:

- User management
- User responsibilities
- Network access controls
- Application access controls
- Database access controls
- Operating system access controls

5.5.1 User management

It is a process to manage access privileges for identified and authorized users. The steps involved are:

- User registration
- Privilege management
- Password management
- Review and monitoring accesses;
- Revocation of access privilege.

User registration

It refers to identifying a user who needs to access information asset. This is generally done based on the job responsibilities and confirmed by User manager. This must be approved by information owner. User registration process must answer:

- Why the user is granted the access?
- Has the data owner approved the access?
- Has the user accepted the responsibility?

Privilege management

Access privileges are to be aligned with job requirements and responsibilities. These are defined and approved by the information asset owner. For example, an operator at the order counter shall have direct access to order processing activity of the application system or an assistant in Bank may have access to enter transaction and a manager can only approve but cannot enter the transaction. Changes in privileges are common activity based on changes in roles of users. Sometimes some users are provided additional privileges for temporary period or during emergencies. Revoking them need to be part of process. Many times application or database privilege management does not provide for automatic revocation of such accesses. In these cases manual monitoring and periodic reviews are compensating controls to correct the situation.

Password management

Password management is controlled based on the password policy. Passwords are used to authenticate user for access to systems. Password management functions include:

- Allocations of password which is generally done by system administrators
- Secure communication of password to appropriate user
- Force change on first login by the user so as to prevent possible misuse by system administrators
- Storage of password is generally should not be done in plain text. Most system stores password as hash of actual password.
- Authentication process is verifying password and user ID provided by user. Passwords are verified by generating hash and then hash is compared with stored hash.
- Password expiry must be managed as per policy. Users must change passwords periodically and system should be configured to expire the password after predefined period. Password may also be expired after predefined limit of unsuccessful logins.
- Reissue of password after confirming the identity of users in case of expired password or if users have forgotten the passwords. This process is typically same as allocation of password.
- Educating users is a critical component about passwords, and making them responsible for their password.

Review of user access rights

Periodic review of user's access rights is essential process to detect possible excess rights due to changes in responsibilities, emergencies, and other changes. These reviews must be conducted by information owner and administrators facilitates by providing available accesses recorded in system.

Default Users

Applications, operating systems and databases purchased from vendor have provision for default users with administrative privileges required for implementation and/or maintenance of application,

OS or database. The user ID and Passwords for these users are published by the vendor required for implementing. It is expected that these password must be changed immediately as soon as system is implemented. While reviewing these access controls IS auditor must ensure that these user ID are either disabled, or passwords have been changed and suitably controlled by the organization.

5.5.2 User responsibilities User responsibilities primarily include:

- User awareness about responsibility associated with access privileges granted
- Password change and use, particularly ensuring they are not shared intentionally or accidentally
Mandatory use of strong passwords to maintain confidentiality.
- Users should ensure that none of the equipment under their responsibility is ever left unprotected.
- Users should also secure their PCs with a password, and should not leave it accessible to others.

5.5.3 Network access control

Network access controls refers to the process of managing access for use of network based services like shared resources, access to cloud based services, remote login, network and internet access. There are various tools and techniques used to manage these accesses. Network based tools and techniques like protocol control, service monitoring are discussed in network security chapter.

Policy on use of network services

An enterprise wide applicable internet service requirements aligned with the business need policy based on business needs for using the Internet services is the first step. Selection of appropriate services and approval to access them will be part of this policy. The policy also specify the use on internet and internet based services while access internet using organization's devices.

Segregation of networks

Based on the sensitive information handling function; say a VPN connection between a branch office and the head-office this network is to be isolated from the internet usage service availability for employees.

Network connection and routing control

The traffic between networks should be restricted, based on identification of source and authentication access policies implemented across the enterprise network facility. The techniques of authentication and authorization as per access policy have been implemented across the organization's network.

Enforced path

Based on risk assessment, it is necessary to specify the exact path or route connecting the networks; say for example internet access by employees will be routed through a firewall. And to maintain a hierarchical access levels for both internal and external user logging. An Internet connection exposes an organization to the entire world. This brings up the issue of benefits the organization should derive along with the precaution against harmful elements.

Clock synchronization

Clock synchronization is useful control to ensure that event and audit logs maintained across an enterprise are in synch and can be correlated. This helps in auditing and tracking of transactions along with date and time that is uniform across organization. In modern networks this function is centralized and automated.

5.5.4 Application and monitoring system access control

Applications are most common assets that accesses information. Users invoke the programs/modules of application to access, process and communicate information. Hence it is necessary to control the accesses to application. Most modern applications provide independent user and access privilege management mechanism for example ERP, Core Banking applications. However, legally or old application may rely in database management system or operating system used to host these applications. In case of legacy applications IS auditors may have to review accesses at all layers i.e. application, database and/or operating systems. Ideally database administrators and system administrators are only roles that need to have access to database and operating system respectively.

The access to information is prevented by application specific menu interfaces, which limit access to system function. A user is allowed to access only to those items he is authorized to access. Controls are implemented on the access rights of users, For example, read, write, delete, and execute. And ensure that sensitive output is sent only to authorized terminals and locations.

Sensitive system isolation

Based on the critical constitution of a system in an enterprise it may even be necessary to run the system in an isolated environment. Monitoring system access and use is a detective control, to check if preventive controls discussed so far are working. If not, this control will detect and report any unauthorized activities.

Event logging

In Computer systems it is easy and viable to maintain extensive logs for all types of events. It is necessary to review if logging is enabled and the logs are archived properly.

Monitor system use

Based on the risk assessment a constant monitoring of some critical systems is essential. Define

the details of types of accesses, operations, events and alerts that will be monitored. The extent of detail and the frequency of the review would be based on criticality of operation and risk factors. The log files are to be reviewed periodically and attention should be given to any gaps in these logs.

5.5.5 Database access controls

Database management systems like oracle provide user management mechanism. DBA can build profile with settings defined by security policies. These profiles are then assigned to roles defines to performs functions on database like view, update, delete, commit. These roles are then assigned to users created on database. Generally these are stored in user table. Databases also provide storing of password hash for each user thus DBA can access but may not find out the password of users. Application developed to use this database can use database login mechanism for providing access to users. (More information on DB access control is provided in section 5.16.

5.5.6 Operating system access control

Operating system provides the platform for an application to use various IS resources and perform the specific business function. If an intruder is able to bypass the network perimeter security controls, the operating system is the last barrier to be conquered for unlimited access to all the resources. Hence, protecting operating system access is extremely crucial. Some of the key controls of operating system are outlined here.

- **Automated terminal identification:** This will help to ensure that a particular session could only be initiated from a particular location or computer terminal.
- **Terminal log-on procedures:** The log-on procedure does not provide unnecessary help or information, which could be misused by an intruder.
- **User identification and authentication:** The users must be identified and authenticated in a fool proof manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means like Digital Certificates should be employed.
- **Password management system:** An operating system could enforce selection of good passwords. Internal storage of password should use one-way encryption algorithms and the password file should not be accessible to users.
- **Use of system utilities:** System utilities are the programs that help to manage critical functions of the operating system—for example, addition or deletion of users. Obviously, this utility should not be accessible to a general user. Use and access to these utilities should be strictly controlled and logged.
- **Duress alarm to safeguard users:** If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities. An example could be forcing a person to withdraw money from the ATM. Many banks provide a secret code to alert the bank about such transactions.

- **Terminal/Session time out:** Log out the user if the terminal is inactive for a defined period. This will prevent misuse in absence of the legitimate user.
- **Limitation of connection time:** Define the available time slot. Do not allow any transaction beyond this time period. For example, no computer access after 8.00 p.m. and before 8.00 a.m.—or on a Saturday or Sunday. This is useful in preventing unauthorized accesses by authorized users.

5.6 Audit Trail

Primary objective of access controls is fix the accountability to individual user for the activities performed by them. This can be done only by generating and reviewing activity logs. However many times IT persons are reluctant to generate log since logs are resource consuming. It requires additional storage, separate access controls, and programming efforts. The issue can be resolved by defining priorities based on risk assessment results and logs for select critical activities like system administration, changes in configuration, access to sensitive information, business transactions, may be enabled.

Logs are also called 'audit trail'. It is a record of system activities that enables the reconstruction and examination of the sequence of events of a transaction, from its inception to output of final results. Violation reports present significant, security-oriented events that may indicate either actual or attempted policy transgressions reflected in the audit trail. Violation reports should be frequently and regularly reviewed by information owner to identify any unauthorized change or access.

Audit information comprises a history of transactions, including who processed the transaction, the date and time of the transition, where the transaction occurred, and related activities. An audit associated with information system security searches for the following:

- Internal and external attempts to gain unauthorized access to a system
- Patterns and history of accesses
- Unauthorized privileges granted to users
- Occurrences of intrusions and their resulting consequences

Depending upon requirements logs are generated at various levels. At application level logs of business transaction with time stamp are generated. These are used by auditors to perform audit. Administrator activity logs at application level, data base level, network device level and operating system level are critical to ensure security. Because of their importance, audit logs should be protected at the highest level of security in the information system.

5.7 Access controls and mobile computing

In today's organizations computing facility is not restricted to a particular data centre alone. Ease of access on the move provides efficiency and results in additional responsibility on users and the need to maintain information security on the management. Theft of data carried on the disk drives of

portable computers is a high risk factor. Both physical and logical access to these systems is critical. Information is to be encrypted and access identifications like fingerprint, eye-iris, and smart cards are necessary security features.

5.8 Access control Mechanism

Identification and Authentication The primary function of access control is to allow authorized access and prevent unauthorized access. Access control mechanism is actually a three step process as depicted in the figure below:

- (a) **Identification:** Identification is a process by which a user provides a claimed identity to the system such as an account number.
- (b) **Authentication:** Authentication is a mechanism through which the user's claim is verified.
- (c) **Authorization:** The authenticated user is allowed to perform a pre-determined set of actions on eligible resources.

The primary function of access control is to allow authorized access and prevent unauthorized access to information resources in an organization, therefore, it may become necessary to apply access control at each security architectural layer of an organization's information system architecture to control and monitor access in and around the controlled area. This includes operating system, network, database and application systems. In each of these layers attributes may include some form of identification; authentication and authorization and logging and reporting of user activities. Interfaces exist between operating system access control software and other system software access control programs such as those of routers, firewalls etc. that manage and control access from outside or within organization networks. On the other side operating system access control software may interface with databases and / or application system access controls to application data. **Please see details in figure 5.6 in next page.**

5.8.1 Identification Techniques

Of the above, implementing the right authentication is the most challenging. Authentication is the process of verifying that the identity claimed by the user is actually true. Users are authenticated using one of three personal authentication factors or techniques. The three categories of authentication factors are **Please see details in figure 5.7 in following page**

- Something the user knows (e.g., a password),
- Something the user has (e.g., a token or smart card), and
- Something the user is (a physical / biometric comparison).

Single-factor authentication uses any one of these authentication factors. Two-factor or dual factor authentication uses two factors and the three-factor authentication uses all the three factors. Individual authentication assurance increases when multiple authentication technologies and

techniques are combined and used. Authorized access to an information resource requires identification and authentication of the person requesting access.

Once the user is authenticated, the system must be configured to validate that the user is authorized (has a valid need-to-know) for the resource being protected and can be held accountable for any actions taken. Authorized access to logical assets can be implemented as a combination of manual, automated, and/or administrative methods. A deny-by-default policy, where access to the information resource is denied unless explicitly permitted should be mandated. The decision to grant or deny access to an information resource is the responsibility of the resource owner.

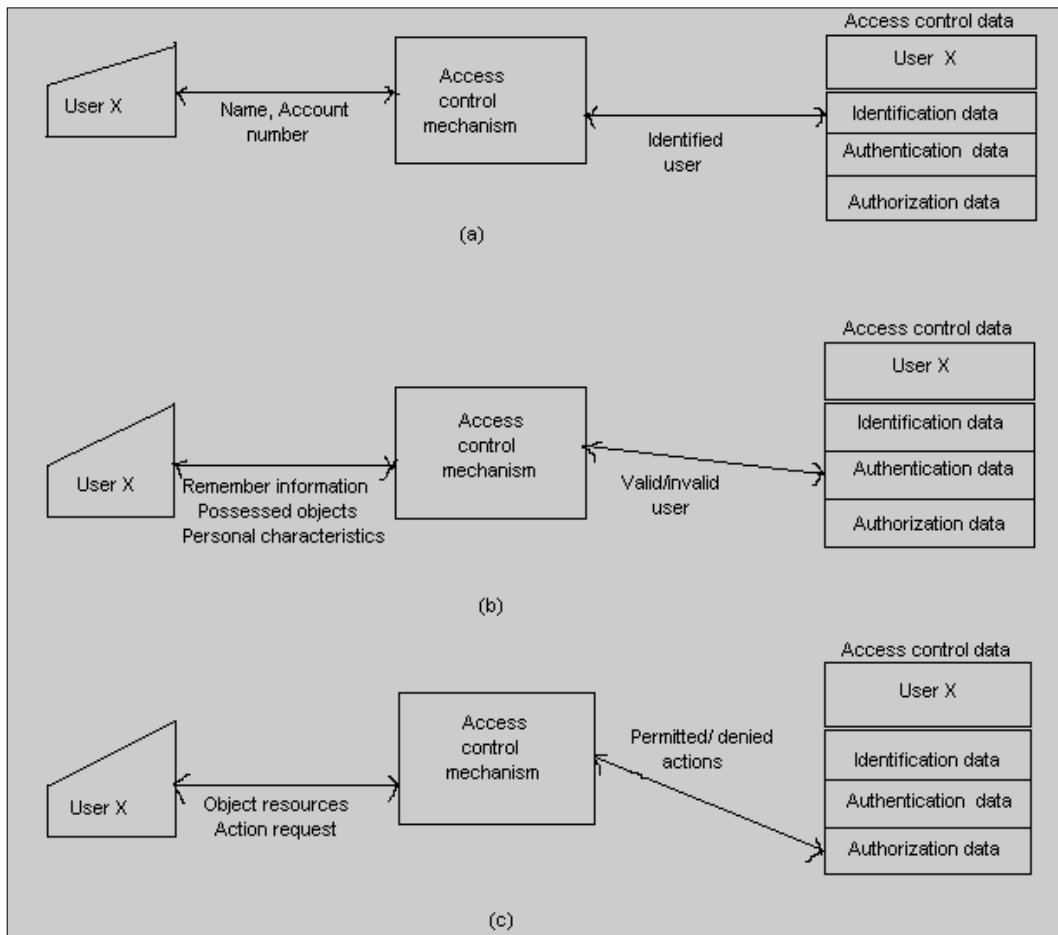


Figure 5.6: Identification, Authentication and Authorization

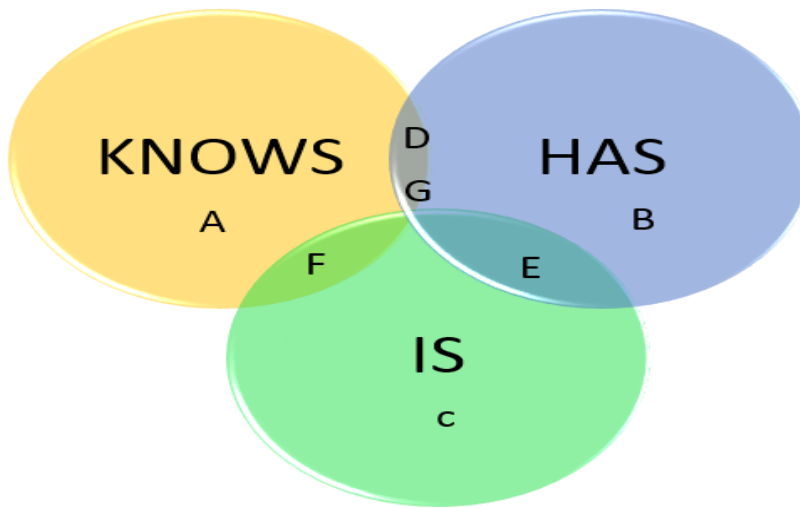


Figure 5.7: Multi-factor authentication.

- A. Password
- B. Identified Badge
- C. Fingerprint
- D. Bank Card and PIN
- E. Smart Card with Biometric template
- F. Fingerprint Detectors with PIN entry
- G. Identifying Badge with Photograph and associated Password.

5.8.2 Authentication Techniques

As stated above, authentication may be through remembered information, possessed tokens, or physical characteristics. We shall examine each class of authentication techniques below.



Figure 5.8: What you have (Token), what you know (password/PIN) and who you are (Biometric)

- **Passwords:** This is the most common authentication technique that depends on remembered information. The user, initially, identifies him using his login-id to the system and then provides the password information. Once the system is able to locate the match and is successful for both fields, the system authenticates the user and enables access to resources based on the authorization matrix. However if a match is not successful, the system returns a message (such as “Invalid User or password”) thus preventing access to resources.
- **Personal Identification Numbers (PINs):** Is a type of password, usually a 4-digit numeric value that is used in certain systems to gain access, and authenticate. The PIN should be such that a person or a computer cannot guess it in sufficient time by using a guess and check method, i.e. where it guesses the PIN, and checks for correctness by testing it on the system that the person is attempting to gain access to and the process is repeated with a different guess till access is obtained. PINs are commonly used for gaining access to Automatic Teller Machines (ATMs).

One-Time Passwords

One-time passwords solve the problems of user-derived passwords. With one-time passwords, each time the user tries to log on he is given a new password. Even if an attacker intercepts the password, he will not be able to use it to gain access because it is good for only one session and predetermined limited time period. For example one time password for online card transaction is provided by bank to user on registered mobile is valid for 10 minutes only. One-time passwords typically use a small hardware device or software that generates a new password every time. The server also has the same software running, so when a user types in his password, the server can confirm whether it is the correct password. Each time the user logs on he has a new password, so it is much more secure.

Challenge Response

An alternative to one-time passwords is challenge response schemes. Instead of having the device just blindly generate a password, a user identifies himself to the server, usually by presenting his user ID. The server then responds with a challenge, which is usually a short phrase of letters and numbers. The user types the challenge into the device and, based on the challenge, the device responds with an output. The user then types that output in as his password to the server. This scheme is slightly more complicated, but it allows the password to be based on changing input rather than just time.

5.8.3 Weaknesses of Logon mechanism

Logon/password access security is based on information to be remembered by the user (what the user knows). This results in the following weaknesses:

- Passwords are easily shared.

- Users often advertently or inadvertently reveal passwords leading to security being compromised.
- Repeated use of the same password could lead to being easily guessed by others.
- If a password is too short or too easy, the chances of it being guessed are quite high.
- If a password is too long or too complex, the user may forget or may write it down.
- If many applications are to be accessed by one user, many passwords have to be remembered.
- Passwords can be shared, guessed, spoofed or captured.

Recommended practices for strong passwords

- The user should not share the authentication information viz. password.
- The password should be easy for the user to remember but hard for the perpetrator to guess.
- On creation of a new user, the first password is allotted by the security administrator and a change of password is forced on the first login.
- Users should be encouraged or forced to change passwords periodically e.g. once in 60 days.
- Concurrent logins by same user should not be permitted.
- Passwords should not be too short and should not use name of user, pet-names, common words found in dictionary or such other attributes.
- Password combination should be random and use alphabetic, numeric and special characters (such as “!”, “#”, “^”, etc.).
- Passwords should be changed periodically.
- Number of wrong login tries should be restricted to three, after which the system should lockout the user. Further access can be granted only through the intervention of the security administrator.
- The logon ids active in the system should not exceed the number of users actually authorised to access systems resources.
- Passwords should be stored in an encrypted form using one-way encryption.
- In case the user remains inactive at a terminal, for a length of time (say 20 minutes), the terminal should lock out the user and require the user to login again.

5.8.4 Attacks on logon/password systems

Due to their inherent weaknesses, logon-id/password access control technique is vulnerable to various kinds of malicious attacks. Some of the common attacks on such systems are discussed below:

- **Brute force:** In this crude form of attack, the attacker tries out every possible combination to hit on the successful match. The attacker may also use various password cracking software that assist in this effort.

- **Dictionary attack:** On the similar lines as brute force, this type of attack is based on the assumption that users tend to use common words as passwords, which can be found in a dictionary, hence the name. The “dictionary” simply consists of a list of words, including proper names (Raju, Ramesh, Ibrahim, etc.) and also that of mythological or religious names (Krishna, Jesus, Osiris, Buddha, etc.).
- **Trojan:** A malicious software, which the attacker can use to steal access control lists, passwords or other information.
- **Spoofing attacks:** In this technique, the attacker plants a Trojan program, which masquerades as the system’s logon screen, gets the logon and password information and returns control to the genuine access control mechanism. Once the information is obtained, the attacker uses the information to gain access to the system resources.
- **Piggybacking:** As stated earlier, an unauthorized user may wait for an authorised user to log in and leave a terminal unattended. The logical techniques that are used to secure against this attack are to automatically log out the session after a pre-determined period of inactivity or by using password-protected screen savers.

Token Based Authentication

Objects that a user is required to possess for identification and authentication are known as tokens.

(i) **Plastic Cards:** Plastic cards contain information about the user and primarily provide a means of identification of the user and can enable authentication. Plastic cards can further be of the following types:



Figure 5.9 Tokens

• **Memory tokens:** In its most common form, the cards contain visible information such as name, identification number, photograph and such other information about the user and also a magnetic strip. This magnetic strip stores static information about the user. In order to gain access to a system, the user in possession of a memory token may be required to swipe his card through a card reader, which reads the information on the magnetic strip and

passes onto the computer for verification with stored information to enable access. E.g. Employee badges with encoded magnetic strips. Where two-factor authentication is adopted, the user is not only required to have his card read by a card reading device but also required to key in remembered information (passwords, PIN) to gain access to the system resources. E.g. Bank ATM Card.

- **Smart Tokens:** In this case, the card or device contains a small processor chip which enables storing dynamic information on the card. Besides static information about the user, the smart tokens can store dynamic information such as bank balance, credit limits etc., however the loss of such smart cards can have more serious implications.

(ii) Proximity Readers: In this case when a person in possession of the card reaches the restricted access area, the card data is read by the proximity readers (or sensors) which transmits information to the authentication computer, which enable access to the restricted area or system. The advantages are that the user is not required to insert the card into the device hence access time is faster. Proximity tokens can be either static or processor based. In static tokens, the card contains a bar code, which has to be brought in proximity of the reader device. In case of processor based tokens, the token device, once in the range of the reader, senses the reader and transmits a series of codes to the reader. Other token based systems include challenge response systems and one time passwords.

(iii) Single Sign-on: In many organisational situations, one user, by virtue of his job responsibilities is often required to log into more than one application. This raises the complex issue of multiple logon and passwords, for the user to remember. This is often solved by a single sign-on, which enables user access to various applications entitled for access. It is a session/user authentication process that permits a user to enter one name and password in order to access multiple applications. The single sign-on, which is requested at the initiation of the session, authenticates the user to access all the applications they have been given the rights to on the server, and eliminates future authentication prompts when the user switches applications during that particular session. This often requires transferring all login control to an access control system, careful configuration of authorities, strong passwords and adequate security of password information since compromise of a single login giving access to multiple applications can lead to many systems being compromised. The concern in a decentralized processing or database environment is that the passwords travel over communication lines. Also if the single username and password used for single sign on is compromised, unauthorized access to all related application is possible.

5.8.5 Biometric Security

Biometrics offers a very high level of authentication based on “what the user is”, as compared to logon and token based authentication. Biometrics as the name suggests is based on certain physical characteristics or behavioural patterns identified with the individual, which are measurable. The International Biometric Group defines biometrics as automated mechanism which uses physiological and behavioural characteristics to determine or verify identity and further explains that the physiological biometrics are based on measurements and data derived from direct measurement of a part of the human body. Behavioural biometrics are based on measurements and data derived from an action and indirectly measure characteristics of the human body Based on some feature

unique to every user, biometrics seek to minimize the weaknesses in other mechanisms of authentication. Some of the biometric characteristics which are used are:

- Fingerprint
- Facial Scan
- Hand Geometry
- Signature
- Voice
- Keystroke Dynamics
- Iris Scanners
- Retina Scanners

Implementation of biometric authentication is often expensive and involves the following phases:

- Identification of IS assets which require biometric security
- Based on the above, identification of appropriate biometric application
- Acquisition and Testing of appropriate hardware, calibration of error rates for effectiveness and efficiency of enrolment and readability
- Implementation of administrative procedures for exception reporting and adjustment for false positives
- Enrolment of Users
- Implementation of related physical and logical controls

Identification and authentication is based on a match with items in the database containing data captured during the user enrolment. Registration or enrolment of the individuals' physical or behavioural characteristics involves capture of information, digitizing and storage of the biometric data. Based on the data read by the sensor, the image or digitized data is compared to the stored data to obtain a match. If the match succeeds, authentication is successful. However due to the complexity of data, biometrics suffer from two types of error viz. False Rejection Rate (FRR) which is wrongfully rejecting a rightful user and False Acceptance Rate (FAR) which involves an unauthorized user being wrongfully authenticated as a right user. Ideally a system should have a low false rejection and low false acceptance rate. Most biometric systems have sensitivity levels which can be tuned. The more sensitive a system becomes, FAR drops while FRR increases. Thus, FRR and FAR tends to inversely related. An overall metric used is the Crossover Error Rate (CER) which is the point at which FRR equals FAR.

Due to their high cost of implementation, biometric access controls were initially implemented only for high value critical information resources such as defence, banking etc. However with the rapid decrease in the cost of biometric hardware biometric controls are being increasingly preferred for commercial applications. Finger print based biometric controls are quite popular and widely deployed in data centres.

5.8.6 Authorization Techniques: Operating Systems

Operating systems are fundamental to provide security to computing systems. The operating system supports the execution of applications and any security constraints defined at that level must be enforced by the operating system. The operating system must also protect itself because compromise would give access to all the user accounts and all the data in their files. A weak operating system would allow attackers access not only to data in the operating system files but data in database systems, if any, that use the services of the operating system. The operating system isolates processes from each other, protects the permanent data stored in its files, and provides controlled access to shared resources. Most operating systems use the access matrix as security model. An access matrix defines which processes have what types of access to specific resources.

General operating systems access control functions include:

- Authentication of the user
- User Management
- Restrict Logon IDs to specific workstations and / or specific times
- Manage account policies
 - Password Policy
 - Account Lockout Policy
- Manage audit policy
- Log events and report capabilities

5.8.7 Pluggable authentication modules

The pluggable authentication module (PAM) framework provides system administrators with the ability to incorporate multiple authentication mechanisms into an existing system through the use of pluggable modules. Applications enabled to make use of PAM can be plugged-in to new technologies without modifying the existing applications. This flexibility allows administrators to do the following:

Select any authentication service on the system for an application

- Use multiple authentication mechanisms for a given service
- Add new authentication service modules without modifying existing applications
- Use a previously entered password for authentication with multiple modules
- A general Authentication scheme independent of the authentication mechanism may be used.

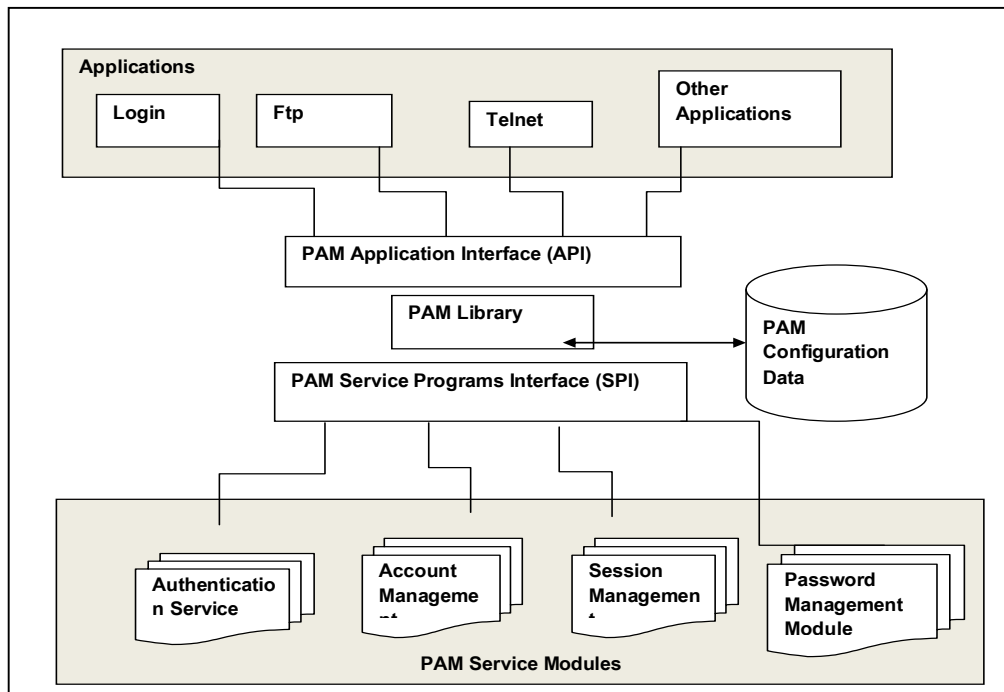


Figure 5.10: PAM Framework

5.8.8 File permissions

In most operating systems, every file is owned by a user and can be accessed by its owner, group or public, depending upon access permissions. When a user creates a file or directory, that user becomes the default owner of that file or directory. A user may be member of one group or many groups. Further, a user owner of a file may not be part of the group that also may have access to the file. Again, most operating systems have at least three types of file permissions; read, write and execute. The users have to be given at least read access to many of the system files.

5.9 Access Control Lists (ACL)

An access control list is a table that tells the computer operating system which access rights each user has to a particular system object, such as a directory/folder or an individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with his access privileges. The most common privileges include the ability to read a file (or all the files in a directory), to write to the file or files, and to execute the file (if it is an executable file, or program). The access control list is implemented differently by each operating system and is the foundation of any security functionality. Access control enables one to protect a system or part of the system (directories, files, file types, etc.). When the system receives a request, it determines access by consulting a hierarchy of rules in the ACL. ACL has one or more access control entries (ACEs),

each consisting of the name of a user or a group of users. The user can also be a role name, such as programmer or tester. For each of these users, groups, or roles, the access privileges are stated in a string of bits called an access mask. Generally, the system, administrator or the object owner creates the access control list for an object.

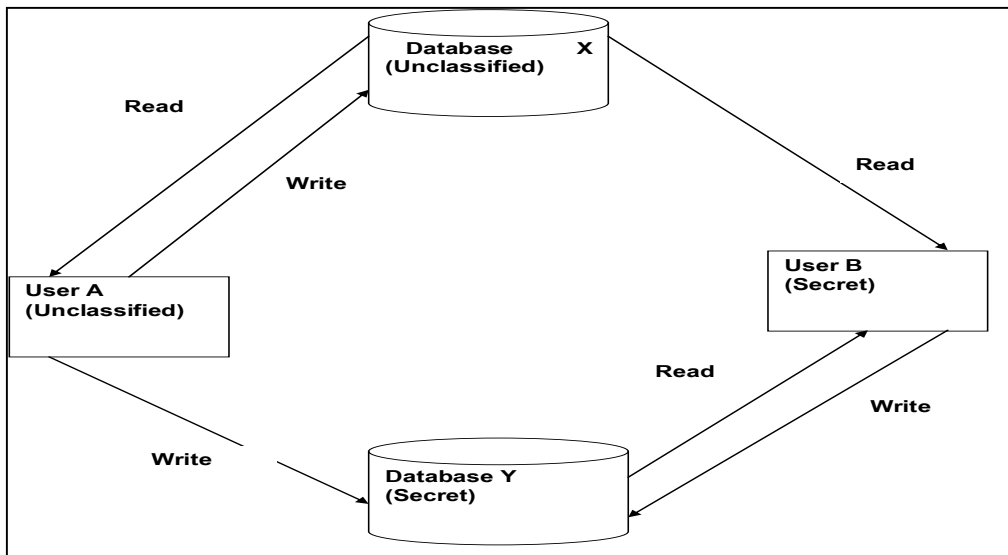


Figure 5.11: Read and Write Access Policy

Discretionary access privileges to user's poses problems within the organization therefore the need arise to have a mandatory and well documented access control policies. Access control policies use attributes to determine which user can access which resource. An example access policy implementation here allows both the user A and User B can read from the unclassified database, but the secret database can be read only by the secret user B. Suppose if both the user A and user B can write to the unclassified and secret database then the unclassified user can read the secret information written by the secret user B and hence the user B has been responsible in downgrading the information.

User	Resource	Database X	Database Y
User A		Read & Write	Write
User B		Read	Read & Write

5.10 Identity Management and Access Controls

Identity Management, also called **IDAM**, is the task of controlling the User Access Provisioning Lifecycle on Information Systems. It includes the task of maintaining the identity of a user, actions they are authorized to perform. It also includes the management of descriptive information about the user and how and by whom that information can be accessed and modified.

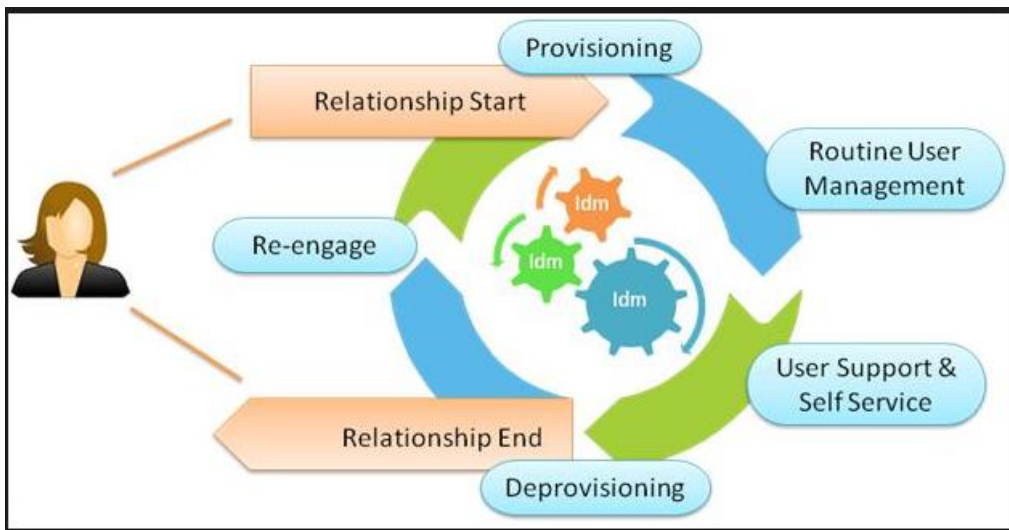


Figure 5.12: Components of identity management

The core objective of an IdM system in a corporate setting is: *one identity per individual*. And once that digital ID has been established, it has to be maintained, modified and monitored throughout what is called the "User access lifecycle." So IdM systems provide administrators with the tools and technologies to change a user's role, to track user activities and to enforce policies on an ongoing basis. These systems are designed to provide a means of administering user access across an entire enterprise and to ensure compliance with corporate policies and regulatory requirements like Sarbanes Oxley.

5.11 Privileged logons

Privileged user is a user who has been allocated powers within the computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator(s) and Network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users.

Privileged access should be assigned based upon function and job necessity and are subject to approval by the information owner. All Users that have access to privileged accounts should be assigned their own user ID for normal business use. Privileged Users must use their personal user IDs for conducting non-privileged activities. Wherever possible the User must login to a system using their personal user ID prior to invoking a privileged account. Privileged Users should be required to create strong passwords comprising of letters, numbers, and special characters. The user account that has privileged access should have a unique password that is different from all other accounts accessed by the User.

5.12 Bypass Security Procedures

Bypass, in general, means either to go around something by an external route rather than going through it, or the means of accomplishing that feat. In network security, a bypass is a flaw in a security system that allows an attacker to circumvent security mechanisms to get system or network access. The actual point of entry is through a mechanism (either a hardware device or program, even just a piece of code) that enables the user to access the system without going through the security clearance procedures (such as authentication) that were set up by the system administrator. A bypass may be a mechanism put in place by an attacker, a flaw in the design, or an alternate access route left in place by developers. A bypass that is purposefully put in place as a means of access for authorized users is called a **back door** or a **trap door**. A crypto bypass is a flaw that allows data to circumvent the encryption process and escape, unencrypted, as plaintext.

5.13 The Access control Matrix

The access matrix provides access rights to *subjects* for *objects*. Access rights are of the type read, write, and execute. A *subject* is an active entity that is seeking rights to a resource or object. A subject can be a person, a program, or a process. An *object* is a passive entity, such as a file or a storage resource. A typical access control matrix is shown in Table 5.1 here.

Table 5.1: Example of an access matrix

	Object		
Subject	Customer Master File	Salaries File	Print Server
Ajay	Read	Read/Write	Write
Deepak	Read/Write	Read	Write
Ram	Read	Read	None

The columns of the access matrix are called **Access Control Lists (ACLs)**, and the rows are called **capability lists**. The access matrix model supports discretionary access control because the entries in the matrix are at the discretion of the individual(s) who have the authorization authority over the table.

User of Generic / Group IDs:

Many time to maintain continuity group users IDs are created and password is shared among select users. This generally happens in case of administrator group. The main concern in using group id is the fixing accountability of actions to individual. However organization may implement manual controls to achieve this. IS auditor must review the effectiveness of such controls. However use of generic accounts like temp or guest should not be allowed, unless specifically approved by Information Security Officer, assigned to an individual and documented. It should have an owner accountable for all actions performed using that ID. These days, many ERP vendors (including SAP)

don't permit creation and use of generic/group accounts and is clearly documented in the licensing agreement. Besides, users should not be allowed to share their user IDs with others.

5.14 Single Sign-On (SSO)

Single Sign-On addresses the practical challenge of logging on multiple times to access different resources. A user must remember numerous passwords and IDs and might take shortcuts in creating passwords that might be open to attack. In SSO, a user provides one ID and password per work session and is automatically logged on to all the required applications. For SSO security, the passwords should not be stored or transmitted in the clear. SSO can be implemented by using scripts that replay the users' multiple logins or by using authentication servers to verify a user's identity and encrypted authentication tickets to permit access to system services.

The advantages of SSO include having the ability to use stronger passwords, easier administration of changing or deleting the passwords, and requiring less time to access resources. The major disadvantage of many SSO implementations is that once a user obtains access to the system through the initial logon, the user can freely roam the network resources without any restrictions. There are multiple methods used by organizations to implement single sign-on. Most popular being LDAP (Open Source) and Active directory (AD) (Microsoft directory service based on LDAP) where user groups and roles are defined for every user and accesses are granted based on access control matrix. There are some applications like Kerberos are also available

Active Directory (AD)

AD is a directory service implemented by Microsoft for Windows domain networks. It is included in most Windows Server operating systems. An AD domain controller authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user. Active Directory makes use of Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos, and DNS.

The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.[1] Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network. As examples, directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate email directory. Similarly, a telephone directory is a list of subscribers with an address and a phone number. A common usage of LDAP is to provide a "single sign on" where one password for a user is shared between many services, such as applying a company login code to web pages (so that staff log in only once to company computers, and then are automatically logged into the company intranet)

Kerberos

Kerberos may be one of the best-tested authentication mechanism available today. Kerberos was intended to have three elements to guard a network's entrance: **authentication**, **accounting**, and **auditing**.

Kerberos is effective in open, distributed environments where network connections to other heterogeneous machines are supported and the user must prove identity for each application and service. Kerberos assumes a distributed architecture and employs one or more Kerberos servers to provide an authentication service. This redundancy can avoid a potential single point of failure issue. The primary use of Kerberos is to verify that users are who they claim to be and the network components they use are contained within their permission profile. To accomplish this, a trusted Kerberos server issues "tickets" to users. These tickets have a limited life span and are stored in the user's credential cache.

Weakness of Single sign-on

SSO has a number of weaknesses that can make it vulnerable to attack. Some of these are:

- It is a single point of failure. One password is compromised, and attacker can have access to all privileges of users whose password is compromised.
- Vulnerable to password guessing.
- Does not protect network traffic.
- When a user changes password, SSO database needs to be updated with a new corresponding password.
- It is difficult to implement when organization has legacy applications or applications that cannot be plugged in with SSO.
- Maintaining SSO is tedious and prone to human errors.

Authorization

SSO system knows who user is (authentication) and must now decide if user can carry out the requested actions. This is where authorization comes into play. Authorization determines what the user is allowed to do. Once a user's identity and authentication are established, authorization levels determine the extent of system rights that a user can hold.

Access criteria types can be broken up into:

- Roles
- Groups
- Physical or logical (network) location
- Time of day
- Transaction type

All access criteria should default to “no access” and authorizations should be granted on need to know basis. Just because a subject has been identified and authenticated does not automatically mean they have been authorized. It is possible for a subject to be logged onto a network (i.e., identified and authenticated) but be blocked from accessing a file or printing to a printer (i.e., by not being authorized to perform that activity). Most users are authorized to perform only a limited number of activities on a specific collection of resources. Identification and authentication are all-or-nothing aspects of access control. Authorization has a wide range of variations between all or nothing for each individual object within the environment. A user may be able to read a file but not delete it, print a document but not alter the print queue, or log onto a system but not access any resources.

5.15 Access Controls in Operating Systems

This topic covers how authorization mechanism is applied to subjects and objects. **Subject** of operating systems are (active) entities that communicate with the system and use its resources. The best example for a subject is the user or a process. **Objects** on the other hand are entities of the operating system that are accessed (requested) by the subject. The access control mechanism should ensure that subjects gain access to objects only if they are authorized to. Depending on areas of usage, there are three types of access control used:

- **Mandatory Access Control**- It is a multi-level secure access control mechanism. It defines a hierarchy of levels of security. A security policy defines rules by which the access is controlled.
- **Discretionary Access Control**- In this type of access control, every object has an owner. The owner (subject) grants access to his resources (objects) for other users and/or groups. The matrix defines the whole state of the system concerning the rights of individual users. There are two ways how to implement the matrix. Either the system assigns the rights to the objects or to the subjects. In other words, either the object stores the column of the matrix, or the subject stores the row of the matrix. Access control lists are used to store the rights with object. On the other hand capability matrixes are used to store rights together with subjects. In the case of capability matrixes we would have to deal with biometrics, so in common operating systems access control lists are used to implement discretionary access control.
- **Role Based Access Control**- In some environments, it is problematical to determine who the owner of resources is. In role based systems, users get assigned roles based on their functions in that system. These systems are centrally administered, they are nondiscretionary. An example is a hospital.

5.16 Database Controls

One of the important objectives of access controls is to prevent any threats to the integrity and unauthorized access to the database resources. Relational Database works on the principles of tables and relations and allows rules of integrity and access to be specified. The principle of least privileges to data items can be enforced using views as against reads. Such rules can be restricted

by a range of parameters such as permissible values or limits, operations up to the granularity of a data field etc. The access to data base can be **Discretionary** based on the approved by data owner (usually business process owner who is accountable for data stored in database), and **Mandatory**. DBA may use various methods to implement access controls in database like depending upon role of user, access control matrix, classification of data item(for example credit card and password stored in database must be encrypted) mapped with roles and so on. Access to SQL and schema level are generally restricted to DBA or implemented through application controls.

5.16.1 Database Roles and Permissions

Access to database cab controlled through the permission settings. This can be useful when it is needed to:

- Share confidential information with other managers, but not the entire company.
- Allow all team members to enter and update issues in an issue tracking database.
- Post a widely referenced database such as a job postings database, but allow only a few people to edit.

Each database has its own customizable permissions system. The permission system is based on *access levels*. Each user of a database has an access level that controls what that user is allowed to do. For example, a user with Read access is only allowed to view information in the database, not change any of it. A user with Edit access can view and change information.

Table 5.2: Database access level

Access Level	Rights
No Access	Users can neither see nor use the database.
Read	Users can view any existing information and can use export to save that information to a file. They cannot add new information to the database, nor can they use import to create new information. They also cannot edit or delete existing information in the database. Users cannot edit the design of the database.
Read & Add	Users can view any existing information and can use export to save that information to a file. They can add information to the database either manually or by importing information from a file. Users with Read & Add access can only edit or delete information they added. They cannot change any information added by other users. Users cannot edit the design of the database.

Read & Add (Own Records Only)	Users can add information to the database either manually or by importing information from a file. Users can only view information they added. They can also edit, delete or export the information they added. They cannot view, edit, delete or export information added by other users. Users cannot change any details of the database design.
Edit	Users can view any existing information and can use export to save that information to a file. They can add information to the database either manually or by importing information from a file. Users can edit and delete any information in the database. They cannot change any details of the database design.
Manage	Users can view, edit, add, and delete any information in the database and any aspect of the database design. They can also export any information to a file, and import information from a file. A member who has Manage access is called a <i>Database Manager</i> . This is a powerful permission level, so use it carefully.

When a database is created, the Database application automatically gives the owner Manage access and everyone else No Access. DBA the use **database roles** to more easily manage privileges for groups of users. Database roles simplify the process of managing privileges because DBA can grant privileges to a role, and then grant the role to users. When owner wants to revoke privileges for a user, he/she can simply revoke role authorization from the user, rather than revoking each individual privilege. He/she can create and drop a role by using the same process that he would to make any database object change. Generally, there are two types of database-level roles: **fixed database roles** that are predefined in the database and **flexible database roles** that an owner can create.

5.16.2 Application Software Controls in a Database

Access to database and fields can be controlled through application thus eliminating need to create users at data base level or these users are mapped with application level users. Accesses are then granted within application and user can access data only through application. For example if a user role requires access to a report, a view can be created and assigned to application module/menu. User then provided access to the menu. Integrity of a DBMS system depends in part on the controls implemented in the application programs that provide the interface to the user to perform a job process activity with a sequence of commands and update parameters that are passed with respect to certain considerations or actions.

Direct access to database level (also sometimes referred as backend access) are then restricted only to data base administrators (DBA) to perform maintenance work. It is possible to restrict DBA to access data.

5.17 Audit of Access Controls

Some factors critical to the successful achievement of audit objectives with regard to evaluating logical access are:

- The *understanding of an organisation's information security framework*, security policy linkage of IT objectives to its business objectives and assessment of risk and controls. This often forms the foundation for risk management and criteria for determining the amount of investment and philosophy of access controls.
- *Selection and implementation of appropriate access controls* should be consistent with the organisation's structure, management controls and organisational culture.
- *Top management's commitment*, support and control must be communicated to all levels in the organisation and concerned stakeholders. Management support would be evident from the emphasis and investment on training and education of users, the importance given to access controls and the enforcement of access control discipline.
- *Management controls* should be evaluated to determine if adequate systems are in place. This also helps to detect report and take corrective action on access security violation.
- Access to all Systems should be granted in a controlled manner driven by business requirements. Users should be explicitly granted access to information or systems. There is no implicit right of access. Access is denied unless explicitly permitted.
- User access rights should be reviewed / audited periodically by the information owners and user access should be revoked based upon their request. This should include audit/review of privileged / super user access rights.
- User accounts that have not been accessed for a predetermined number of days should be disabled in accordance with company's records retention guidelines.

The auditor's opinion depends on his understanding of general and IS controls and audit procedures. These are used to test the effectiveness and efficiency of access to organizational information, in respect of which the auditor should exercise due care and diligence.

The objective and scope of audit would determine the audit procedures and IS resources to be covered. Often evaluation of logical access controls forms a part of a generic IS audit covering various other controls. However, the auditor may be required to evaluate the logical access security of a system, sub- system, application, operating software, database management software.

5.17.1 Audit Test Procedures

IS auditors should evaluate whether logical access policies and procedures are effectively implemented. For this the auditor has to test if:

- Necessary access control framework in the form of logical access security policies and standards are in place and effectively communicated. The auditor does this by studying the various policies, the system of communication of policy initiatives and the system of education and training users with respect to logical security of information resources. The auditor would need to interview data owners, users and custodians to evaluate their knowledge and skills on implementation of access controls.
- Procedures and mechanisms for logical access are implemented to ensure protection of organizational information. The IS auditor should evaluate the various logical security techniques and mechanisms for their effective implementation, operation and administration.
- The auditor must check if the controls are functioning effectively and efficiently. This requires the auditor to conduct various compliance and substantive tests to determine if the logical security of information resources is actually effective. The auditor can determine the level of effectiveness of logical security by determining compliance with procedure manuals such as administrator manuals and user manuals, interviewing users and administrators and testing the various logical security mechanisms to determine any weaknesses or incompatibilities.

Some audit considerations in this regard are outlined in next section.

5.17.2 Logical access: Audit considerations

Following considerations must be considered while reviewing logical accesses.

1. System Configuration
2. Logical access mechanism
3. Bypass security procedures

5.17.3 Systems Configuration

Test the appropriateness of system configuration and parameter settings. Appropriate configurations of access security parameter systems at the time of installing/ upgrading hardware, system software such as operating systems, DBMS and application software are critical in building a strong foundation for access security. In this respect the auditor would have to evaluate whether:

- The system configuration complies with the organisational security standards, security policy requirements, manufacturer specifications and best practices for security.
- There is a process to ensure that configuration of access security settings and parameters and changes thereto are authorised, documented and tested.
- Privileged and special purpose logons are controlled and documented.

- There is a procedure for control over purchase, custody and management of system utilities. Many systems utilities are powerful and can break through the various levels of access security.

5.17.4 Logical Access mechanisms

For testing of various logical access mechanisms such as token based authentication systems and biometric access control systems the auditor can conduct tests that determine:

- The control of authorisation, operation and termination over use of tokens such as memory and smart cards.
- Control over special terminals and devices. For instance, a hub may be exposed physically but with proper levels of encryption, logical security of information can be ensured.
- Security practices relating to unattended terminals, security of data in transit and control over production resources.
- Whether logging of transactions and events is appropriately enabled.

User account management and password management

Logon and passwords are the most commonly used mechanisms to secure logical access to information resources. The auditor should:

- Evaluate mechanisms such as access control features and software to identify weaknesses if any.
- Evaluate the effectiveness of user management procedures through audit of access control lists to assess if access is permitted based on the principle of least privileges and “need to know-need to do” basis, scan audit logs to determine the effectiveness of access control and interview users, and identify all entries in ACL with the authorized list of employees permitted to access systems.
- Test user profiles and group profiles to determine the access privileges and controls thereon.

Privileged logons and special user accounts

Privileged logons and special user accounts provide higher level of access to systems resources. Hence, they require a higher level of access security and management. The auditor should evaluate:

- The strength of controls on such privileged access. He should follow appropriate audit procedures to identify all individuals having access to such privileged logon facility and special user accounts. The auditor should critically evaluate the need for such access
- Review audit trails, access violation reports in respect of all privileged logons and special user accounts
- The strength and adequacy of monitoring and incident handling procedures

Access to file directories and application logic and system instruction sets

The auditor should evaluate the protection of:

- Systems files and directories containing critical hardware and systems software configuration and parameter files such as driver information, etc.
- Application files and directories containing application programs, support files, program libraries, parameter files, initialisation files, etc.
- Production data and directories containing production files and production resources.

5.17.5 Bypass Security Procedures

There may be various situations in the routine course of operations where security features are bypassed for operational and functional convenience during certain controlled operations. For instance, privileged logons may be provided to systems engineers to meet emergency situations, bypass label processing may be provided to meet certain bulk processing requirements or systems exits may be enabled during software implementation and maintenance phases. The auditor should identify all such provisions and critically audit the events.

5.18 Summary

When deciding on a logical access control strategy, it is important to review compliance and internal security requirements necessary to protect access to information assets. This can best be achieved by conducting a risk analysis that identifies the typical threats. In addition inputs from global standards are also useful. Most important consideration is identifying users, type of access, and type of asset. It best to adopt a least privilege policy on “need to know, need to do” basis. After answering these questions, it is possible to plan for a combination of access controls necessary to meet the security goals.

Auditor should know that access control defines how users should be identified, authenticated, and authorized. This is generally addressed in Security policies and procedures, hence the starting point of audit of logical access controls should be to understand the policies and procedures and ensure these are implemented uniformly and continuously.

5.19 Questions

1. Which of the following pair of authentication can be considered as two factor?
 - A. Password and passphrase
 - B. Passphrase and PIN
 - C. Token and access card
 - D. Access card and PIN

Module 4

2. Which of the following is primary requirement of granting user access to information asset?

- A. Identification
- B. Authorization
- C. Authentication
- D. Need to know

3. Mandatory access controls are those controls that are:

- A. Based on global standards
- B. Defined by security policy
- C. Part of compliance requirements
- D. Granted by asset owner

4. Which of the following is a major concern associated with Single-Sign-on?

- A. Multiple passwords are noted
- B. User may select easy password
- C. It is a single point of failure
- D. High maintenance cost

5. Which of the following non-compliance with security policy is most difficult to detect or get evidence for?

- A. Use of removable media
- B. Password sharing by user
- C. Access to banned web sites
- D. Passing information over phone

6. Which of following processes in user access management is most essential to detect errors and omissions resulting in unauthorised or excess accesses to users?

- A. Identification
- B. Authentication
- C. Authorization
- D. Review

7. While auditing compliance with password policy, IS auditor observed that configuration of password parameters in system is as per policy. Which of the following the auditor should verify?

- A. Review enforcement for sample users.
- B. Verify all assets have same configuration.

- C. Review log for password configuration.
 - D. Interview users on policy enforcement.
8. One time password is considered strong because they are:
- A. active for short period.
 - B. communicated on mobile.
 - C. unique for each user
 - D. unique for session
9. Which of the following has been attack to break the user password is difficult to control?
- A. Brute Force
 - B. Dictionary attack
 - C. Spoofing
 - D. Social engineering
10. Which of the following is a primary objective of implementing logical access controls?
- A. Identify users on the system
 - B. Fixing accountability of actions
 - C. Authorize users based on role
 - D. Compliance with policy

5.20 Answers and Explanations

1. **D.** The three factors are what a user knows (PIN, Password, Passphrase), what user possesses (Access card, Token) and what unique characteristics of user (Biometric) are. Use of any two factors for authentication is called two factor. Option A, B and C though strong use only one factor.
2. **A.** Identification of user is first and primary requirement of granting access. Next will be authentication method to be established and finally finding authorization levels based on role that also addresses need to know.
3. **B.** Mandatory accesses are those controls that are to be applied uniformly across organization and are defined by security policy. D is discretionary access controls. B and C generally do not specify such requirements.
4. **C.** Single point of failure is a major concern. One password if compromised, all accesses for that user are available to perpetrator.
5. **B.** Password sharing by user is most difficult to get evidence for or detect. Others can be monitored or enforced using technology.

6. **D.** Periodic user access review helps in ensuring that all users have appropriate level of accesses. This happens due to changes in internal environment like role changes, emergency situation, resignation and retiring of employees. In such situations sometimes revocation of accesses is missed out, and can be corrected during review.
7. **C.** Generally automated configuration need not be reviewed for samples except for sample assets. However it most important to review the password configuration changes for ongoing enforcement of policy.
8. **A.** Strength of one-time password is that they are active for short time, if user does not login during that time the password expires. Password is unique for each session and user, however it is not a strength. It can be communicated by suitable means.
9. **D.** Social engineering attacks weakest link that is human. Attacker uses techniques to compel users to reveal passwords and other confidential information. For example Phishing. Other options are technology based attacks and can be detected or controlled.
10. **B.** Primary objective of implementing access controls is to fix accountability on user for their actions. Others are means to implement access controls not objectives.

CHAPTER 6: NETWORK SECURITY CONTROLS

6.1 Introduction

We have seen the use of networks for business communication and application hosting in Module 1, in this section, we will review the risks and controls that are specific to networked computers. It is rare these days to find a standalone computer in any commercial environment, as networks offer tremendous advantages that far outweigh the cost of creating them. Although it is true that when we are implementing security controls it is necessary to focus on enterprise architecture as a whole for designing and implementing controls, network related controls are important since it is the first layer of architecture that is generally the focus of attacker. Therefore networks are also far more vulnerable to external and internal threats than are standalone systems.

Organization level general controls like physical security (cables, intruders trying to connect to network), environmental security (ensuring segregation between electrical and data cables, protecting cables from rodents), access controls, security policies (acceptable usage of internet) are applicable to network security. In addition one needs to look at network specific controls to ensure that organization's security objectives are achieved.

6.2 Network Characteristics

Advantages of enterprise wide network characteristics are described as the following:

- **Anonymity:** A network removes personal interaction i.e. most of the clues, such as appearance, voice, or context, by which we recognize acquaintances.
- **Automation:** In some networks, one or both endpoints, as well as all intermediate points, involved in a given communication may be machines with only minimal human supervision.
- **Distance:** Many networks connect endpoints that are physically far apart. Although not all network connections involve distance, the speed of communication is fast enough that humans usually cannot tell whether a remote site is near or far. Though it makes it easier to establish communication among geographically dispersed users/machines, it also introduces risks like impersonation, intrusion, tapping.
- **Opaqueness:** Because the dimension of distance is hidden, users cannot tell whether a remote host is in the room next door or in a different country. In the same way, users cannot distinguish whether they are connected to a node in an office, school, home, or warehouse, or whether the node's computing system is large or small, modest or powerful. In fact, users cannot tell if the current communication involves the same machine with which they communicated the last time.
- **Routing diversity:** To maintain or improve reliability and performance, routings between two endpoints are usually dynamic. That is, the same interaction may follow one path through the

network the first time and a very different path the second time. In fact, a query may take a different path from the response that follows a few seconds later.

6.3 Threats and Vulnerabilities

This section describes the various kinds of vulnerabilities and threats associated with networks that aim to compromise the confidentiality, integrity, or availability of data, software and hardware by accidents, non-malicious humans, and malicious attackers. The threats and vulnerabilities are listed under the following heads:

- Information Gathering
- Communication Subsystem Vulnerabilities
- Protocol Flaws
- Impersonation
- Message Confidentiality Threats
- Message Integrity Threats
- Web Site Defacement
- Denial of Service

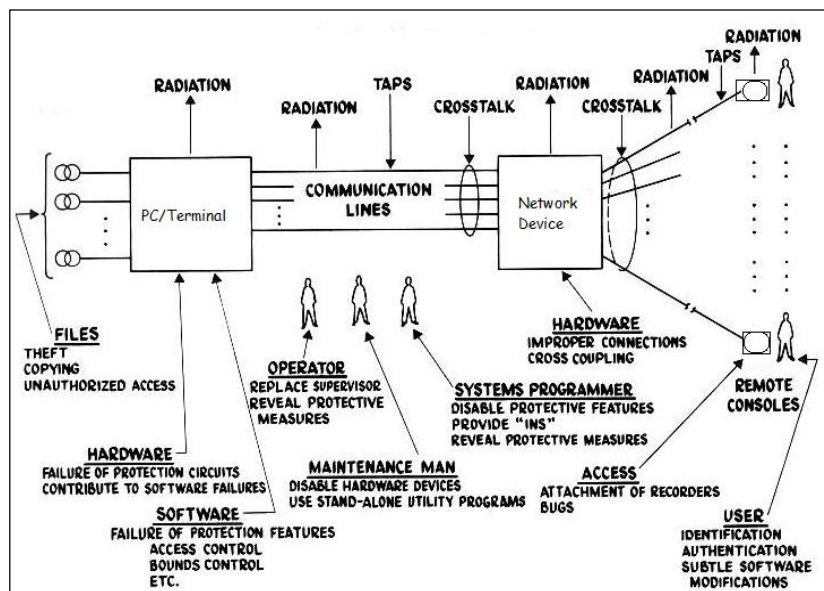


Figure 6.1. Network Vulnerabilities

However it needs to be understood that most of these threats operate in tandem and it is difficult to associate them with network security alone. Figure 6.1 illustrates the various threats in and their

source or initiator. This will help auditors in understanding types of threat that might materialize in which part of IT installation and verify controls for those threats, based on risk assessment results.

6.3.1 Information Gathering

A serious attacker will spend a lot of time obtaining as much information as s/he can about the target before launching an attack. The techniques to gather information about the networks are examined below:

- **Port Scan:** An easy way to gather network information is to use a port scanner, a program that, for a particular IP address, reports which ports respond to messages and which of several known vulnerabilities seem to be present.
- **Social Engineering:** Social engineering involves using social skills and personal interaction to get someone to reveal security-relevant information and perhaps even to do something that permits an attack. The point of social engineering is to persuade the victim to be helpful. The attacker often impersonates someone occupying a senior position inside the organization and is in some difficulty. The victim provides the necessary assistance without verifying the identity of the caller, thus compromising security.
- **Reconnaissance:** Reconnaissance is the general term for collecting information. In security, it often refers to gathering discrete bits of information from various sources and then putting them together to make a coherent picture. One commonly used reconnaissance technique is “dumpster diving.” It involves looking through items that have been discarded in garbage bins or waste paper baskets. One might find network diagrams, printouts of security device configurations, system designs and source code, telephone and employee lists, and more. Even outdated printouts may be useful. Reconnaissance may also involve eavesdropping. The attacker or his accomplice may follow employees to lunch and listen in from nearby tables as co-workers discuss security matters.
- **Operating System and Application Fingerprinting:** Here the attacker wants to know which commercial server application is running, what version, and what the underlying operating system and version are. While the network protocols are standard and vendor independent, each vendor has implemented the standard independently, so there may be minor variations in interpretation and behaviour. The variations do not make the software noncompliant with the standard, but they are different enough to make each version distinctive. How a system responds to a prompt (for instance, by acknowledging it, requesting retransmission, or ignoring it) can also reveal the system and version. New features also offer a clue, for example a new version will implement a new feature but an old version will reject the request. All these peculiarities, sometimes called the operating system or application fingerprint, can mark the manufacturer and version.
- **Bulletin Boards and Chats:** Underground bulletin boards and chat rooms support exchange of information among the hackers. Attackers can post their latest exploits and techniques, read what others have done, and search for additional information on systems, applications, or sites.

- **Documentation:** The vendors themselves sometimes distribute information that is useful to an attacker. For example, resource kits distributed by application vendors to other developers can also give attackers tools to use in investigating a product that can subsequently be the target of an attack.
- **Malware:** Attacker may use malware like virus or worms to scavenge the system and keep sending information to attacker over network without the knowledge of system user.

6.3.2 Exploiting communication subsystem vulnerabilities

- **Eavesdropping and Wiretapping:** An attacker can pick off the content of a communication passing in unencrypted form. The term eavesdrop implies overhearing without expending any extra effort. For example, an attacker (or a system administrator) is eavesdropping by monitoring all traffic passing through a node. (The administrator might have a legitimate purpose, such as watching for inappropriate use of resources.) A more hostile term is wiretap, which means intercepting communications through some effort. Passive wiretapping is just “listening,” just like eavesdropping. But active wiretapping means injecting something into the communication stream. A wiretap can be done in such a manner that neither the sender nor the receiver of a communication will know that the contents have been intercepted.
- **Microwave signal tapping:** Microwave signals are broadcast through the air, making them more accessible to outsiders. An attacker can intercept a microwave transmission by interfering with the line of sight between sender and receiver. It is also possible to pick up the signal from an antenna located close to the legitimate antenna.
- **Satellite Signal Interception:** In satellite communication, the potential for interception is even greater than with microwave signals. However, because satellite communications are heavily multiplexed, the cost of extracting a single communication is rather high.
- **Wireless:** Wireless networking is becoming very popular, but threats arise in the ability of intruders to intercept and spoof a connection. A wireless signal is strong for approximately 30 to 60 meters. A strong signal can be picked up easily. Wireless also has a second problem, the possibility of unauthorized use of a network connection, or a theft of service.
- **Optical Fiber:** It is not possible to tap an optical system without detection. Further optical fiber carries light energy, not electricity, which does not emanate a magnetic field as electricity does. Therefore, an inductive tap is impossible on an optical fiber cable. However, the repeaters, splices, and taps along a cable are places at which data may be intercepted more easily than in the fiber cable itself.
- **Zombies and BOTnet:** BOTnets is a term (robotic network) used for virtual network of zombies. BOTnet operator launches malware/virus on system that once activated remains on system and can be activated remotely. This malware helps the BOTnet operator use the compromised system (Zombie) remotely with to launch attack or collect information. For example Zombies have been used extensively to send e-mail spam. This allows spammers to avoid detection and presumably reduces their bandwidth costs, since the owners of zombies pay for their own bandwidth.

6.3.3 Protocol Flaws

Internet protocols are publicly posted for scrutiny. Many problems with protocols have been identified by reviewers and corrected before the protocol was established as a standard. Despite this process of peer review, flaws exist in many of the commonly used protocols. These flaws can be exploited by an attacker. For example FTP is known to transmit communication including user id and password in plain text.

6.3.4 Impersonation

In many instances, an easy way to obtain information about a network is to impersonate another person or process. An impersonator may foil authentication by any of the following means:

- **Authentication foiled by guessing:** Guess the identity and authentication details of the target, by using common passwords, the words in a dictionary, variations of the user name, default passwords, etc.
- **Authentication foiled by eavesdropping or wiretapping:** When the account and authentication details are passed on the network without encryption, they are exposed to anyone observing the communication on the network. These authentication details can be reused by an impersonator until they are changed.
- **Authentication Foiled by Avoidance:** A flawed operating system may be such that the buffer for typed characters in a password is of fixed size, counting all characters typed, including backspaces for correction. If a user types more characters than the buffer would hold, the overflow causes the operating system to by-pass password comparison and act as if a correct authentication has been supplied. Such flaws or weaknesses can be exploited by anyone seeking unauthorized access.
- **Non-existent Authentication:** Here the attacker circumvents or disables the authentication mechanism at the target computer. If two computers trusts each other's authentication an attacker may obtain access to one system through an authentication weakness (such as a guest password) and then transfer to another system that accepts the authenticity of a user who comes from a system on its trusted list. The attacker may also use a system that has some identities requiring no authentication. For example, some systems have "guest" or "anonymous" accounts to allow outsiders to access things the systems want to release to the public. These accounts allow access to unauthenticated users.
- **Well-Known Authentication:** Most vendors often sell computers with one system administration account installed, having a default password. Or the systems come with a demonstration or test account, with no required password. Some administrators fail to change the passwords or delete these accounts, creating vulnerability.
- **Spoofing and Masquerading:** Both of them are impersonation. Refer to chapter on logical access controls for details.

- **Session Hijacking:** Session hijacking is intercepting and carrying on a session begun by another entity. In this case the attacker intercepts the session of one of the two entities that have entered into a session and carry it over in the name of that entity. For example, in an e-commerce transaction, just before a user places his order and gives his address, credit number etc. the session could be hijacked by an attacker.
- **Man-in-the-Middle Attack:** A man-in-the-middle attack is a similar to session hijacking, in which one entity intrudes between two others. The difference between man-in-the-middle and hijacking is that a man-in-the-middle usually participates from the start of the session, whereas a session hijacking occurs after a session has been established. The difference is largely semantic and not particularly significant.

6.3.5 Message Confidentiality Threats

An attacker can easily violate message confidentiality (and perhaps integrity) because of the public nature of networks. Eavesdropping and impersonation attacks can lead to a confidentiality or integrity failure. Here we consider several other vulnerabilities that can affect confidentiality.

- **Mis-delivery:** Message mis-delivery happens mainly due to congestion at network elements which causes buffers to overflow and packets dropped. Sometimes messages are mis-delivered because of some flaw in the network hardware or software. Most frequently, messages are lost entirely, which is an integrity or availability issue. Occasionally, however, a destination address will be modified or some router or protocol will malfunction, causing a message to be delivered to someone other than the intended recipient. All of these “random” events are quite uncommon. More frequent than network flaws are human errors, caused by mistyping an address.
- **Exposure:** The content of a message may be exposed in temporary buffers, at switches, routers, gateways, and intermediate hosts throughout the network; and in the workspaces of processes that build, format, and present the message. A malicious attacker can use any of these exposures as part of a general or focused attack on message confidentiality.
- **Traffic Analysis (or Traffic Flow Analysis):** Sometimes not only is the message itself sensitive but the fact that a message exists is also sensitive. For example, if a wartime enemy sees a large amount of network traffic between headquarters and a particular unit, the enemy may be able to infer that significant action is being planned involving that unit. In a commercial setting, messages sent from the president of one company to the president of a competitor could lead to speculation about a takeover or conspiracy to fix prices.

6.3.6 Message Integrity Threats

In most cases, the integrity or correctness of a communication is more important than its confidentiality. Some of the threats which could compromise integrity are by:

- Changing some or all of the content of a message

- Replacing a message entirely, including the date, time, and sender/ receiver identification
- Reusing (replaying) an old message
- Combining pieces of different messages into one false message
- Changing the apparent source of a message
- Redirecting a message
- Destroying or deleting a message

These attacks can be perpetrated in the ways already stated, including:

- Active wiretap
- Trojan horse
- Impersonation
- Compromised host or workstation

6.3.7 Web Site Defacement

Web site defacement is common not only because of its visibility but also because of the ease with which one can be done. Web sites are designed so that their code is downloaded and executed in the client (browser). This enables an attacker to obtain the full hypertext document and all programs and references programs embedded in the browser. This essentially gives the attacker the information necessary to attack the web site. Most websites have quite a few common and well known vulnerabilities that an attacker can exploit.

6.3.8 Denial of Service

Denial of Service (DoS) attacks lead to loss of network availability. The electronic threats are more serious and less obvious. Some of them are described below:

- **Connection Flooding:** This is the oldest type of attack where an attacker sends more data than what a communication system can handle, thereby preventing the system from receiving any other legitimate data. Even if an occasional legitimate packet reaches the system, communication will be seriously degraded.
- **Ping of death:** It is possible to crash, reboot or otherwise kill a large number of systems by sending a ping of a certain size from a remote machine. This is a serious problem, mainly because this can be reproduced very easily, and from a remote machine. Ping is an ICMP protocol which requests a destination to return a reply, intended to show that the destination system is reachable and functioning. Since ping requires the recipient to respond to the ping request, all the attacker needs to do is send a flood of pings to the intended victim.
- **Traffic Redirection:** A router is a device that forwards traffic on its way through intermediate networks between a source host's network and a destination's. So if an attacker can corrupt the routing, traffic can disappear.

- **DNS Attacks:** DNS attacks are actually a class of attacks based on the concept of domain name server. A domain name server (DNS) is a table that converts domain names like www.icaai.org into network addresses like 202.54.74.130, a process called resolving the domain name or name resolution. By corrupting a name server or causing it to cache spurious entries, an attacker can redirect the routing of any traffic, or ensure that packets intended for a particular host never reach their destination.

6.3.9 Distributed Denial of Service

In distributed denial of service (DDoS) attack more than one machine are used by the attacker to attack the target. These multiple machines are called zombies that act on the direction of the attacker and they don't belong to the attacker. These machines have some vulnerability that can be exploited to use it to attack another machine. The attacker exploits vulnerabilities in multiple machines and uses them to attack the target simultaneously. In addition to their tremendous multiplying effect, distributed denial-of-service attacks are a serious problem because they are easily launched by using scripts.

6.3.10 Threats from Cookies, Scripts and Active or Mobile Code

Some of the vulnerabilities relating to data or programs that are downloaded from the server and used by the client are as follows:

- **Cookies:** Cookies are NOT executable. They are data files created by the server that can be stored on the client machine and fetched by a remote server usually containing information about the user on the client machine. Anyone intercepting or retrieving a cookie can impersonate the cookie's legitimate owner.
- **Scripts:** Clients can invoke services by executing scripts on servers. A malicious user can monitor the communication between a browser and a server to see how changing a web page entry affects what the browser sends and then how the server reacts. With this knowledge, the malicious user can manipulate the server's actions. The common scripting languages for web servers, CGI (Common Gateway Interface), and Microsoft's active server pages (ASP) have vulnerabilities that can be exploited by an attacker.
- **Active Code:** Active code or mobile code is a general name for code that is downloaded from the server by the client and executed on the client machine. The popular types of active code languages are Java, JavaScript, VBScript and ActiveX controls. Such executable code is also called applet. A hostile applet is downloadable code that can cause harm on the client's system. Because an applet is not screened for safety when it is downloaded and because it typically runs with the privileges of its invoking user, a hostile applet can cause serious damage.

6.3.11 Malicious Code

Malicious code is the name used for any program that adds to, deletes or modifies legitimate software for the purpose of intentionally causing disruption and harm or to circumvent or subvert the existing system's function. Examples of malicious code include viruses, worms, Trojan Horses, and logic bombs. Newer malicious code is based on mobile Active X and Java applets.

Viruses

A computer virus is a type of malware (program) that attaches itself to a file and gets transmitted. When executed, it damages the infected system and also replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected".

Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes. However, not all viruses carry a destructive payload or attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without the user's consent.

Motives for creating viruses can include seeking profit; desire to send a political message, personal amusement, to demonstrate that vulnerability exists in software, for sabotage and denial of service.

Viruses often are classified based on the type of damage they do when infected. The major types are:

- a. **Master Boot Record (MBR) Viruses:** Affects the boot sector of storage device and further infects when the storage is accessed.
- b. **Stealth Viruses:** Stealth viruses hide themselves by tampering the operating system to fool antivirus software into thinking that everything is functioning normally.
- c. **Polymorphic Viruses:** Polymorphic viruses are difficult to detect because they can modify themselves and change their identity thus able to hide themselves from antivirus software
- d. **Macro Viruses:** Macro viruses are the most prevalent computer viruses and can easily infect many types of applications, such as Microsoft Excel and Word.
- e. **Worms:** Worms are stand-alone viruses that are they are transmitted independently and executes themselves.
- f. **Trojan horse:** Malicious code hidden under legitimate program, such as a game or simple utility. Trojans are primarily used by attackers to infect the system and then get control remotely to make that system work for them.

Logic Bomb/Time Bomb

Logic bombs are malicious code added to an existing application to be executed at a later date. These can be intentional or unintentional. For example Year2000 problem was an unintentional logic bomb. Every time the infected application is run, the logic bomb checks the date to see whether it is time to run the bomb. If not, control is passed back to the main application and the logic bomb waits. If the date condition is correct, the rest of the logic bomb's code is executed and the result can be anything from a harmless message to a system crash.

6.3.12 Virus / Malicious Code protection mechanisms:

Various countermeasures that can be deployed to protect against virus are:

- a) **Anti-Virus:** Antivirus is most common protection from virus and is installed on most of laptops and desktops. Most of the antivirus software utilizes a method known as signature detection to identify potential virus infections on a system. Essentially, they maintain an extremely large database that contains the known characteristics (signatures) of all viruses. Depending upon the antivirus package and configuration settings, it can scan storage media periodically, check for any files that contain data matching those criteria. Antivirus tools have three types of controls –
 - Active monitor: Monitors traffic and activity to check the viruses. Although most tools use signatures, few have developed heuristic scan abilities to look for possible malicious codes
 - Repair or quarantine: These tools tries to remove the virus from file/mail or quarantines and reports.
 - Scheduled scan: Users are prompted for scanning the storages to detect virus already present, that were not detected by active monitors. This happen when the new virus enters the system. (Zero day attack)It is essential to ensure following controls:
 - Virus signatures are updated
 - Alerts from antivirus are reviewed for root cause
 - Schedules scans are performed regularly
- b) **Incident handling:** Incident Handling is an action plan for dealing with virus attack, intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is comprised of a six step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. In case of virus incidents it is most essential to find out root cause to ensure that the incident does not recur.
- c) **Training and Awareness programs:** It is said that human beings are the weakest link in information security. Periodic training and awareness programs need to be organized to ensure that employees and other 3rd party users are made aware of the risks arising out of improper use of organisation's information systems. These cover:

- Enforcing policy on use of removable devices
- Handling of mail attachments particularly from unknown senders
- Accessing internet
- Ensuring antivirus is updated and scheduled scan are performed (generally it is automated and centralized)

6.4 Current Trends in attacks

Most attacks and threats discussed above are being in use for a considerable time. Organizations being aware of their existence mostly ensure that controls are in place to prevent, detect and/or recover from these attacks. However attackers are always a step ahead. Attackers are now using other means to attack some of these are discussed below.

6.4.1 Exploiting application vulnerabilities

With use of internet based technologies and clouds organizations have hosted applications that can be accessed from internet and/or intranet. These applications might contain vulnerabilities if exploited can compromise the security of information. Attackers tried to exploit these vulnerabilities to launch the attacks like SQL Injection, Cross site scripting. OWASP (Open web application Security project) identifies top ten security threats every years. Threats identified in 2013 are listed below. (Source: www.owasp.org)

- **Injection (SQL Injection):** Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
- **Broken Authentication and Session Management:** Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
- **Cross-Site Scripting (XSS):** XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
- **Insecure Direct Object References:** A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
- **Security Misconfiguration:** Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and

platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

- **Sensitive Data Exposure:** Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
- **Missing Function Level Access Control:** Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.
- **Cross-Site Request Forgery (CSRF):** A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
- **Using Components with Known Vulnerabilities:** Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defences and enable a range of possible attacks and impacts.
- **Invalidated Redirects and Forwards:** Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

6.4.2 Advanced persistent threat (APT)

A sustained targeted attack on identified subject. Attacker tried to introduce malware to compromise the system. For this attacker uses possible social engineering methods. Once the system is compromised the malware resides in system. Since malware is specifically written antivirus may not be able to detect it. This malware is designed to send small bits of information from system to attacker without getting detected by network based controls like anomaly detection, traffic analysis etc. The attack continues for a longer duration till all required confidential information about organization is received by the attacker.

6.5 Network Security Controls

This section examines controls available to ensure network security from the various threat identified listed earlier. The controls are listed under the following broad heads.

- Architecture
- Cryptography/Encryption
- Content Integrity
- Strong Authentication
- Remote Access Security
- Firewalls
- Intrusion Detection Systems
- Monitoring (Security Incident and Event Management (SIEM))

6.5.1 Architecture

The architecture or design of a network can have a significant effect on its security. Some of the major considerations are:

- **Segmentation / Zoning:** Segmentation / Zoning can limit the potential for harm in a network in two important ways. Segmentation reduces the number of threats, and it limits the amount of damage a single vulnerability can allow. A web server, authentication server, applications and database are residing on a single server or segment for facilitating electronic commerce transactions are a very insecure configuration. A more secure design will use multiple segments. Since the web server has to be exposed to the public, that server should not have other more sensitive functions on it or residing on the same segment such as user authentication or access to the database. Separate segments and servers reduce the potential harm should any subsystem be compromised. (Please see figure 6.2 in next page).
- **Redundancy:** Another key architectural control is redundancy, allowing a function to be performed on more than one node. Instead of having a single web server; a better design would have two servers, using a “failover mode”. If one server is used and that server is down for some reason the whole application is not available. In failover mode, the servers communicate with each other periodically, each determining if the other is still active. If one fails, the other takes over processing for both of them. Although performance is cut approximately in half when a failure occurs, some minimum processing is being done which can be used to maintain critical functions.
- **Eliminate Single Points of Failure:** Good network architecture provides for its availability by eliminating single points of failure. This is true for all critical components including servers, network devices and communication channels in a network that will compromise its availability, if it fails.

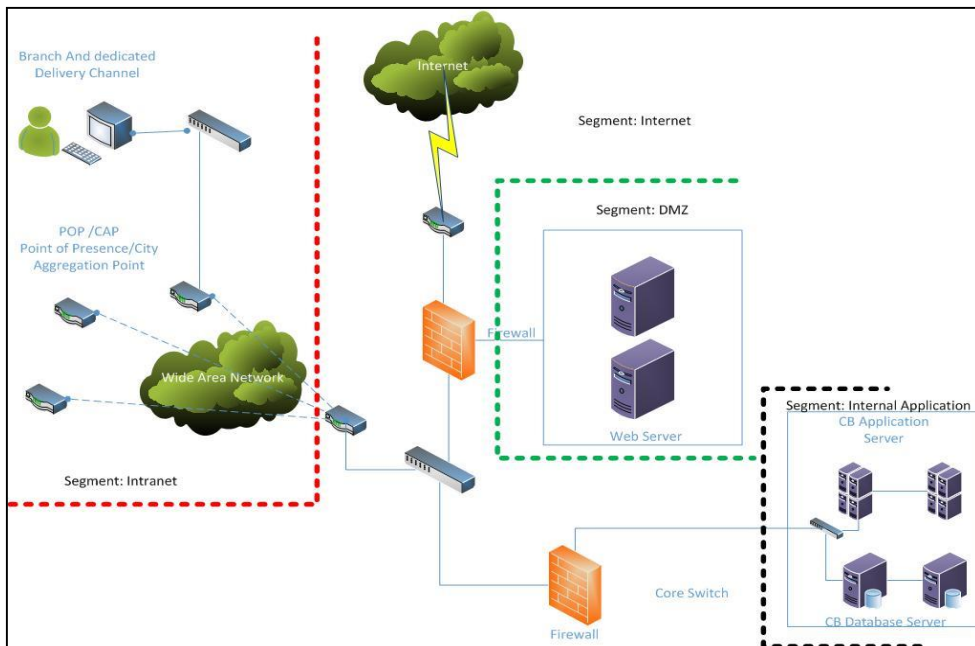


Figure 6.2: Segmented Architecture

6.5.2 Cryptography/Encryption

The technical details of cryptography have been dealt with in an earlier module. Only certain applications of cryptography that are relevant to Network security are discussed here.

Link Encryption

In link encryption, data are encrypted just before the system places them on the physical communications link, that is, encryption occurs at the Data Link layer in the OSI model. Correspondingly, decryption occurs at the Data Link layer of the receiving host. Link encryption protects the message in transit between two computers, but the message is in plaintext inside the hosts (above the data link layer). Headers added by the network layer (which includes addresses, routing information and protocol) and above are encrypted, along with the message/data. The message is, however, exposed at the Network layer and thus all intermediate nodes through which the message passes can read the message. This is because all routing and addressing is done at the Network layer. Link encryption is invisible to user and appropriate when the transmission line is the point of greatest vulnerability. Link encryption provides protection against traffic analysis.

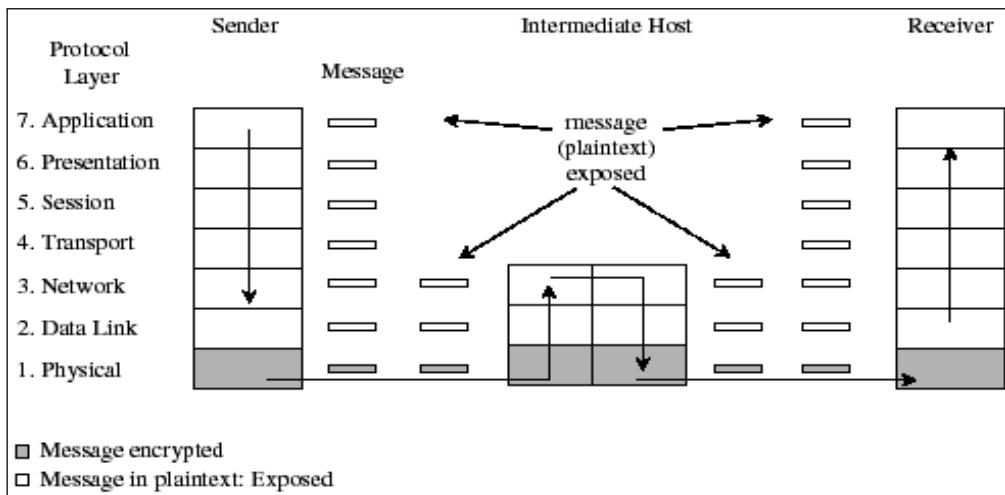


Figure 6.3: Link Encryption

End-to-End Encryption

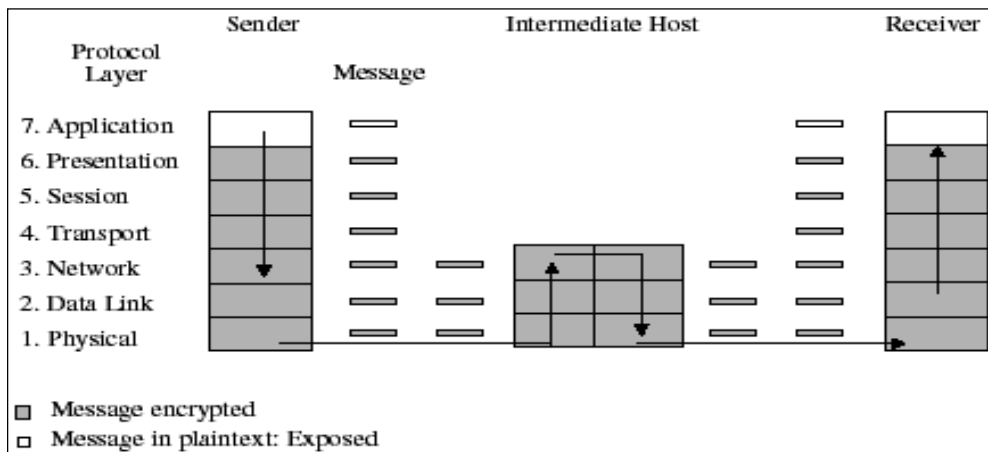


Figure 6.4: End-to-End Encryption

End-to-end encryption provides security from one end of a transmission to the other. The encryption can be applied by a hardware device between the user and the host or the encryption can be done by software running on the host computer. In either case, the encryption is performed at the higher layers, usually application or presentation layer. When end-to-end encryption is used, messages, even when sent through several insecure intermediate hosts, are protected. This is because the data content remains encrypted at all the intermediate layers. However, since the headers below the transport is not encrypted (networks, data link, etc.) end-to-end does not provide protection against

traffic analysis. Note that it is possible use both Link and End-to-end encryption at the same time. One does not preclude the other.

Table 6.1: Comparison of Link and End-to-End Encryption

Link Encryption	End-to-End Encryption
Security within hosts	
Data exposed in sending host	Data encrypted in sending host
Data exposed in intermediate nodes	Data encrypted in intermediate nodes
Role of user	
Applied by sending host	Applied by sending process
Invisible to user	User applies encryption
Host maintains encryption	User must find algorithm
One facility for all users	User selects encryption
Typically done in hardware	Either software or hardware implementation
All or no data encrypted	User chooses to encrypt or not, for each data item
Implementation concerns	
Requires one key per host pair	Requires one key per user pair
Provides node authentication	Provides user authentication

PKI and Certificates

A public key infrastructure (PKI) is a process created to enable users to implement public key (asymmetric) cryptography, usually in a large and distributed setting. PKI offers each user a set of services, related to identification and access control, as follows:

- Create certificates associating a user's identity with a (public) cryptographic key
- Issue certificates from its database
- Sign certificates, adding its credibility to the authenticity of the certificate
- Confirm (or deny) the validity of a certificate
- Revoke certificates for users who no longer are allowed access or whose private key has been exposed

PKI is a set of policies, procedures and products and not a standard. The policies define the rules under which the cryptographic systems should operate. In particular, the policies specify how to handle keys and valuable information and how to match level of control to level of risk. The procedures dictate how the keys should be generated, managed, and used. Finally, the products actually implement the policies, and they generate, store, and manage the keys. Entities, called certificate authorities, implement the PKI policy on certificates. The functions of a certificate authority can be done in-house or by a commercial service or a trusted third party. PKI may also involve a registration authority that acts as an interface between a user and a certificate authority. The

registration authority captures and authenticates the identity of a user and then submits a certificate request to the appropriate certificate authority.

SSL Encryption

The SSL (Secure Sockets Layer) protocol was originally designed by Netscape to protect communication between a web browser and server. It is also known now as TLS, for transport layer security. SSL interfaces between applications (such as browsers) and the TCP/IP protocols to provide server authentication, optional client authentication, and an encrypted communications channel between client and server.

To create a SSL connection, the client requests an SSL session. The server responds with its public key certificate so that the client can determine the authenticity of the server. The client returns symmetric session key encrypted under the server's public key. The server decrypts the session key and then they switch to encrypted communication, using the shared session key.

IPSec

IETF (Internet Engineering Task Force) adopted IPSec, or the IP Security Protocol Suite. Designed to address spoofing, eavesdropping, and session hijacking, the IPSec protocol defines a standard means for handling encrypted data. IPSec is implemented at the IP layer, so it affects all layers above it, in particular TCP and UDP.

IPSec is similar to SSL, in that it supports authentication and confidentiality in a way that does not necessitate significant change either above it (in applications) or below it (in the TCP protocols). Like SSL, it was designed to be independent of specific cryptographic protocols and to allow the two communicating parties to agree on a mutually supported set of protocols.

Physical Header	IP Header	TCP Header	Data	Physical Trailer

Figure 6.5: Traditional Packets

Physical Header	IP Header	ESP Header (TCP Header + Data)	Physical Trailer

Figure 6.6: IPSec Packet

Signed Code

As already noted, it is possible for someone to place malicious active code on a web site to be downloaded by unsuspecting users. A partial solution to reduce this risk is to use signed code. A trustworthy third party appends a digital signature to a piece of code (or macro), supposedly connoting more trustworthy code. A signature structure in a PKI helps to validate the signature. A well-known manufacturer would be recognizable as a code signer.

Encrypted E-Mail

An electronic mail message generally has no privacy at all. The service provider and any intermediate host can read not just the address but also everything in the message field. To protect the privacy of the message and routing information, we need encryption to protect the confidentiality and integrity of the message. The two popular approaches to key management are using a hierarchical, certificate based PKI solution for key exchange and using a flat, individual-to-individual exchange method. The hierarchical method is called S/MIME (Secure Multi-Purpose Mail Extensions) and is employed by many commercial mail programs, such as Microsoft Exchange. The individual method is called PGP (Pretty Good Privacy) and is a commercial add-on.

6.5.3 Content Integrity

Content integrity is automatically implied when cryptographic systems are used. Most kinds of malicious threats are addressed by cryptographic systems very effectively. For non-malicious threats to integrity, the controls are Error Correcting codes and Message Digests (Cryptographic Checksums)

Error Correcting Codes

Error detection codes detect when an error has occurred, and error correction codes can actually correct errors without requiring retransmission of the original message. The error code is transmitted along with the original data, so the recipient can re-compute the error code and check whether the received result matches the expected value.

- **Parity Check:** The simplest error detection code is a parity check. An extra bit (the parity bit) is added to an existing group of data bits depending on their sum. With even parity the extra bit is 0 if the sum of the data bits is even and 1 if the sum is odd; that is, the parity bit is set so that the sum of all data bits plus the parity bit is even. Odd parity is the same except the sum is odd. Parity bits are useful only when the error is in a single bit (called single bit error).
- **Checksum and CRCs:** A checksum is a form of redundancy check that at its simplest, works by adding up the basic components of a message, usually the bits or bytes, and storing the resulting value. Later, anyone who has the authentic checksum can verify that the message was not corrupted by doing the same operation on the data, and checking the sum. A more

sophisticated type of redundancy check is the cyclic redundancy checks (CRC) which considers not only the value of each bit/byte but also the order of the values. A cyclic redundancy check (CRC) uses a hash function used to produce a checksum which is a small integer from a large block of data, such as network traffic or computer files, in order to detect errors in transmission or duplication. CRCs are calculated before and after transmission or duplication, and compared to confirm that they are the same.

- **Other Codes:** Other kinds of error detection codes, such as hash codes and Hamming codes are used to detect burst errors (several errors occurring contiguously) and multiple bit errors (multiple errors among non-adjacent bits). Some of the more complex codes (like Hamming codes) can detect multiple-bit errors and may be able to pinpoint which bits have been changed, thus allowing the data to be corrected.

Message Digests (Cryptographic Checksums)

Checksums and CRCs are useful in detecting accidental modification such as corruption to stored data or errors in a communication channel. However, they provide no security against malicious agents, as their simple mathematical structure makes them trivial to circumvent. To protect against malicious changes cryptographic checksum are used. A cryptographic checksum is created by performing a complicated series of mathematical operations (the cryptographic algorithm) that translates the data in the file into a fixed string of digits called a hash value, which is then used as a checksum. Without knowing which cryptographic algorithm was used to create the hash value, it is highly unlikely that an unauthorized person would be able to change data without inadvertently changing the corresponding checksum.

A cryptographic hash function must ensure that the following is computationally infeasible:

- Determining the content of a message from its Cryptographic Checksums
- Finding “collisions”, wherein two different messages have the same Cryptographic Checksums.

Cryptographic checksums are also known as message digests, message authentication codes, integrity check-values, modification detection codes, or message integrity codes.

6.5.4 Strong Authentication

A security policy specifies who—which individuals, groups, subjects can access which resources and objects. Crucial to that policy is authentication: knowing and being assured of the accuracy of identities. Organization must adopt strong authentication methods appropriate for use in networks like one-time passwords, Challenge Response systems and Kerberos, discussed in previous chapter.

6.5.5 Remote Access Security

Remote access technologies can be defined as those data networking technologies that are focused on providing the remote user with access into a network, while striving to maintain the principal tenets of Confidentiality, Availability, and Integrity. There are many obvious advantages to employing secure remote network access, such as the following:

- Reducing networking costs by using the Internet to replace expensive dedicated network lines
- Providing employees with flexible work styles such as telecommuting
- Building more efficient ties with customers, suppliers, and employees

Virtual Private Networking (VPN)

A virtual private network (VPN) is created by building a secure communications link between two nodes by emulating the properties of a point-to-point private link. A VPN can be used to facilitate secure remote access into a network, securely connect two networks together, or create a secure data tunnel within a network. Encryption coupled with access controls (including firewalls) can provide users with the same level of privacy that can be provided on a private network, even when the communication traverses a part of the public network. For more details, refer the previous module.

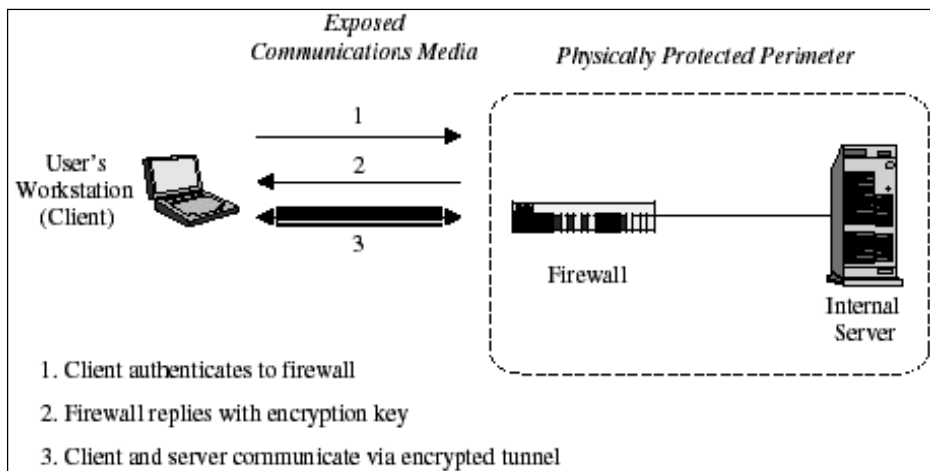


Figure 6.7: Secure VPN

Dial back procedures

In a networked computing environment, user may often require access to the systems resources from remote locations. Dial-back systems are a control to ensure that access is made only from

authorised lines or locations. When a user dials into the server and identifies itself, the server hangs up and calls the user at a pre-determined telephone number and then enables the user to access the resources based on password authentication. A weakness in this procedure is call-forwarding. An unauthorized person could enable calls to a pre-determined number to be forwarded to the number designated by him, thus enabling him to gain unauthorized access to the resources.

Other controls

To minimize the risk of unauthorized dial-in access, remote users should never store their passwords in plain text login scripts on notebooks and laptops.

Authentication Servers

In widely spread out networked systems, the problem of user management and enabling authorised access is crucial since users are spread over a wide geographical areas including telecommuting. In such cases all access control is transferred to a centralized or decentralized access authentication mechanism. Two of the popular applications of remote authentication mechanisms depending on centralized/decentralized access authentication implementations are TACACS (Terminal Access Controller Access Control System) and RADIUS (Remote Authentication Dial in User Service). Some of the features of such systems are:

- Enable secure remote access
- Facilitates centralized user management
- Facilitates centralized access monitoring and control
- Changes to user access rights made easy
- Provides event logging and extended audit trails

6.5.6 Firewalls

The technical details of firewalls, their types and configurations have been dealt with in the first module. Only certain specialised applications of firewalls for network security are dealt with here.

Intranet

An intranet is a network that employs the same types of services, applications, and protocols present in an Internet implementation, without involving external connectivity. For example, an enterprise network employing the TCP/IP protocol suite, along with HTTP for information dissemination would be considered an Intranet. Most organizations currently employ some type of intranet, although they may not refer to the network as such. Within the internal network (intranet), many smaller intranets can be created by the use of internal firewalls. As an example, an organization may protect its personnel network with an internal firewall, and the resultant protected network may be referred to as the personnel intranet. Since intranets utilize the same protocols and application services present on the Internet, many of the security issues inherent in Internet implementations are also present in

intranet implementations. Therefore, intranets are typically implemented behind firewall environments.

Extranets

An extranet is usually a business-to-business intranet; that is, two intranets are joined via the Internet. The extranet allows limited, controlled access to remote users via some form of authentication and encryption such as provided by a VPN. Extranets share nearly all of the characteristics of intranets, except that extranets are designed to exist outside a firewall environment. By definition, the purpose of an extranet is to provide access to potentially sensitive information to specific remote users or organizations, but at the same time denying access to general external users and systems. Extranets employ TCP/IP protocols, along with the same standard applications and services. Many organizations and agencies currently employ extranets to communicate with clients and customers. Within an extranet, options are available to enforce varying degrees of authentication, logging, and encryption.

Securing a Firewall

Firewall platforms should be implemented on systems containing operating system builds that have been stripped down and hardened for security applications. Firewalls should never be placed on systems built with all possible installation options. Firewall operating system builds should be based upon minimal feature sets. All unnecessary operating system features should be removed from the build prior to firewall implementation. All appropriate operating system patches should be applied before any installation of firewall components.

The operating system build should not rely strictly on modifications made by the firewall installation process. Firewall installation programs rely on a lowest common denominator approach; extraneous software packages or modules might not be removed or disabled during the installation process.

The hardening procedure used during installation should be tailored to the specific operating system undergoing hardening. Some often-overlooked issues include the following:

- Any unused networking protocols should be removed from the firewall operating system build. Unused networking protocols can potentially be used to bypass or damage the firewall environment. Finally, disabling unused protocols ensures that attacks on the firewall utilizing protocol encapsulation techniques will not be effective.
- Any unused network services or applications should be removed or disabled. Unused applications are often used to attack firewalls because many administrators neglect to implement default-restrictive firewall access controls. In addition, unused network services and applications are likely to run using default configurations, which are usually much less secure than production-ready application or service configurations.

- Any unused user or system accounts should be removed or disabled. This particular issue is operating system specific, since all operating systems vary in terms of which accounts are present by default as well as how accounts can be removed or disabled.
- Applying all relevant operating system patches is also critical. Since patches and hot fixes are normally released to address security-related issues, they should be integrated into the firewall build process. Patches should always be tested on a non-production system prior to rollout to any production systems.
- Unused physical network interfaces should be disabled or removed from the server chassis.

6.5.7 Intrusion Detection Systems

After the perimeter controls, firewall, and authentication and access controls block certain actions, some users are admitted to use a computing system. Most of these controls are preventive, that is, they prevent known undesirable things from happening. Many studies, however, have shown that most computer security incidents are caused by insiders, people who would not be blocked by a firewall. And insiders require access with significant privileges to do their daily jobs.

Intrusion detection systems complement these preventive controls as the next line of defence. An intrusion detection system (IDS) is a device, usually another separate computer, which monitors activity to identify malicious or suspicious events. An IDS is a sensor that raises an alarm if specific things occur. The alarm can range from writing an entry in an audit log, to something significant, such as paging the system security administrator. An IDS receives inputs from sensors. It saves those inputs, analyses them, and takes some controlling action.

The functions performed by IDS are:

- Monitoring users and system activity
- Auditing system configuration for vulnerabilities and mis-configurations
- Assessing the integrity of critical system and data files
- Recognizing known attack patterns in system activity
- Identifying abnormal activity through statistical analysis
- Managing audit trails and highlighting user violation of policy or normal activity
- Correcting system configuration errors
- Installing and operating traps to record information about intruders
- Special considerations in audit of remote access and network security

Many intrusion detection systems are also capable of interacting with firewalls in order to bring a reactive element to the provision of network security services. Firewalls that interact with intrusion detection systems are capable of responding to perceived remote threats automatically, without the delays associated with a human response. For example, if an intrusion detection system detects a denial of service attack in progress, it can instruct certain firewalls to automatically block the source of the attack (although, false positives responses can occur).

The two general types of intrusion detection systems are signature based and heuristic. Signature-based intrusion detection systems perform simple pattern-matching and report situations that match a pattern corresponding to a known attack type. Heuristic intrusion detection systems, also known as anomaly based, build a model of acceptable behaviour and flag exceptions to that model; for the future, the administrator can mark a flagged behaviour as acceptable so that the heuristic IDS will now treat that previously unclassified behaviour as acceptable.

Intrusion detection devices can be network based or host based. A network-based IDS is a stand-alone device attached to the network to monitor traffic throughout that network; a host-based IDS runs on a single workstation or client or host, to protect that one host. For more details, please see the previous module.

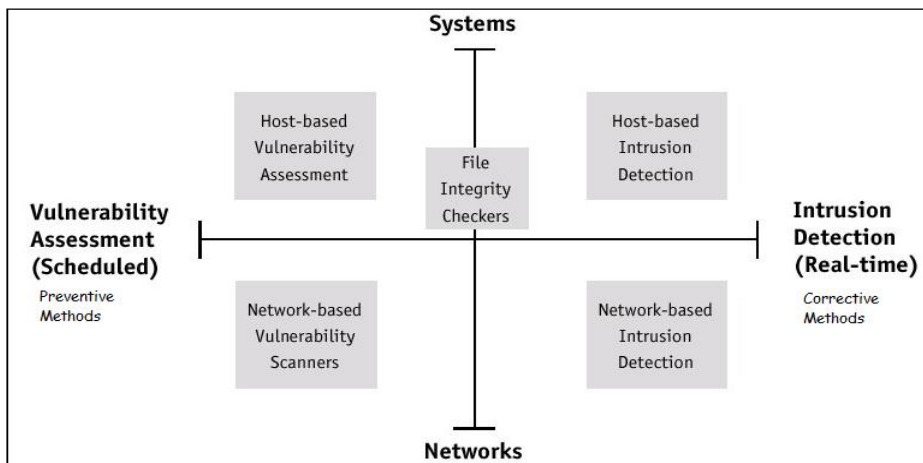


Figure 6.8: Intrusion Detection System

6.6 Monitoring Controls

Most controls implemented for network generates lot of logs related to activities as per rule set. Monitoring and reviewing these logs is a mammoth task and need lot of efforts and resources. There are various tools available in market that helps organizations in collecting these logs, co-relating them based on possible use cases and generate alerts for important logs. This way the efforts can be minimized but cannot be eliminated. Also resources required to manage these tools are specially trained and skilled. These tools are known as Security Incident and event management (SIEM) tools. Organizations use these tools and establish a security operations center (SOC) to monitor these logs, analyse alerts and record incidents and events to be responded. Broad Objectives of SOC are:

- Detect attacks and malware
- Enhance incident response capability
- Detect Advanced persistent threats
- Compliance requirements

A typical SOC is connected with other systems as shown in figure 6.9 given here.

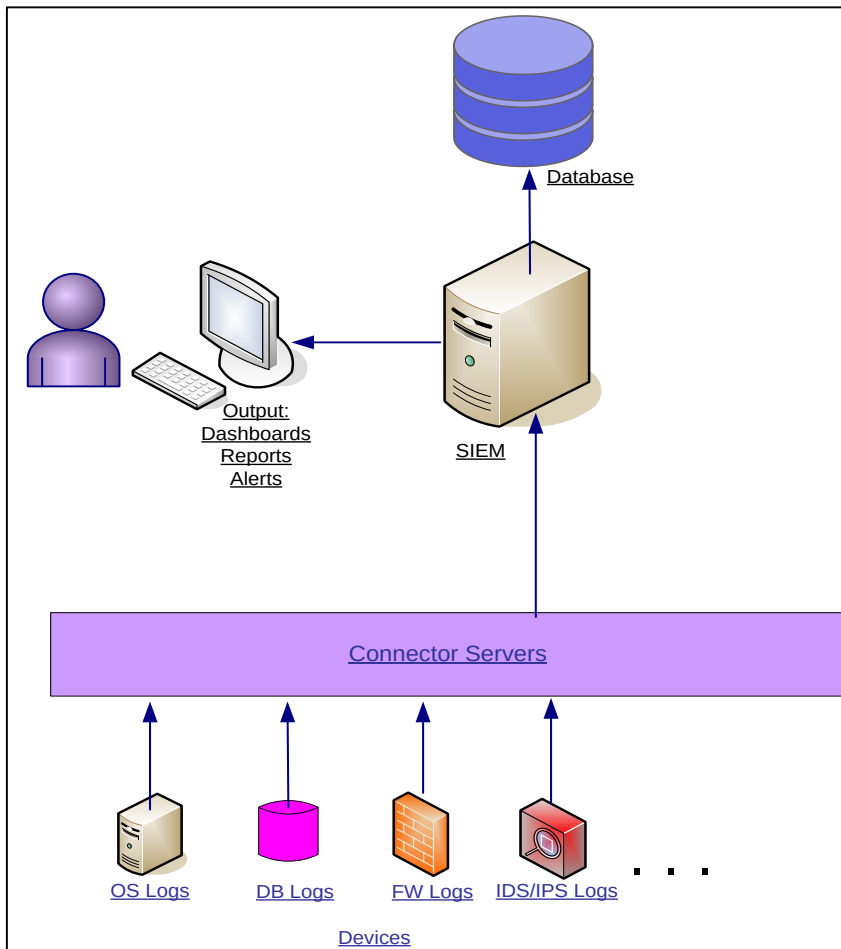


Figure 6.9: Security operations Center

Establishing SOC requires huge cost and resources and small organizations may prefer to outsource such services to vendor.

6.7 End-point security

In network security, endpoint security refers to a methodology of protecting the corporate network when accessed via remote devices such as laptops or other wireless and mobile devices. Each device with a remote connection to the network creates a potential entry point for security threats. Endpoint security is designed to secure each such access from the endpoint (device) to the network resources.

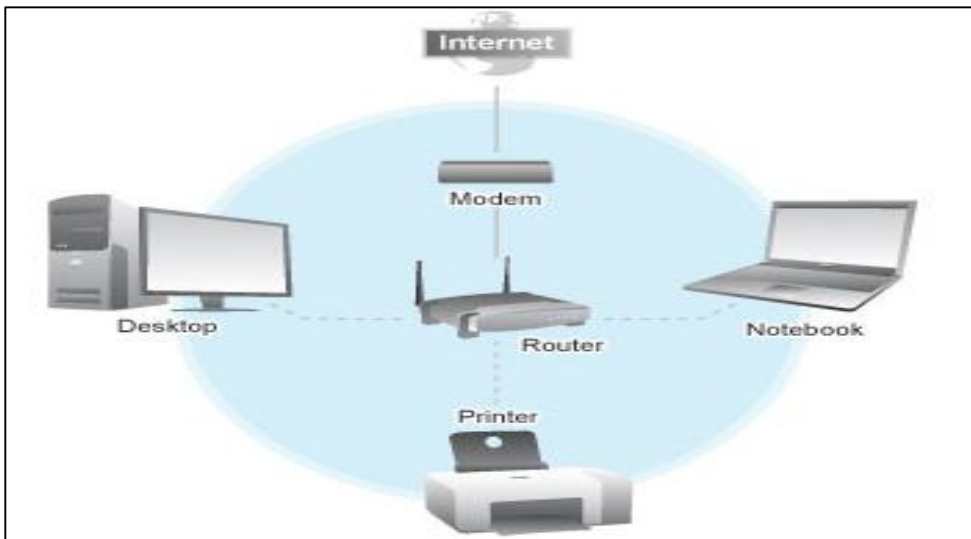


Figure 6.10: Typical wireless network

Usually, endpoint security is a security system that consists of security software, located on a centrally managed and accessible server or gateway within the network, in addition to client software being installed on each of the endpoints (or devices). The server authenticates logins from the endpoints and also updates the device software when needed. As an end-point wants to make an access to the network, the server software authenticates the device (i.e. the end pint) and checks whether it conforms to the security policy of the organization before allowing the access. While endpoint security software differs by vendor, you can expect most software offerings to provide antivirus, antispyware, personal firewall and also a host intrusion prevention system.

Endpoint security is becoming a more common IT security function and concern as more employees bring consumer mobile devices to work and companies allow its mobile workforce to use these devices on the corporate network.

6.8 Wireless Security threats and Risk Mitigation

A wireless network is a type of computer network that uses wireless data connections for connecting network nodes. It is a method by which enterprise (office), homes, etc. avoid the costly process of introducing cables into a building, or as a connection between various equipment locations.

Wireless networking presents many advantages like network configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also creates new threats and alters the existing information security risk profile. For example, because communication takes place "through the air" using radio frequencies, the risk of interception is greater than with wired networks.

If the message is not encrypted, or encrypted with a weak algorithm, the attacker can intercept and read it, thereby compromising confidentiality.

Wireless network has numerous vulnerabilities such as:

- **Ad-hoc networks:** Ad-hoc networks can pose a security threat. Ad-hoc networks are defined as peer-to peer networks between wireless computers that do not have an access point in between them.
- **Non-traditional networks:** Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a security risk. Even barcode readers, handheld PDAs, and wireless printers and copiers should be secured. These non-traditional networks are commonly overlooked by IT personnel who have narrowly focused on laptops and access points.
- **MAC spoofing:** MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address is hard-coded on a network interface card (NIC) and cannot be changed. However, there are tools which can make an operating system believe that the NIC has a MAC address different than its real MAC address.
- **Man-in-the-middle attacks:** A man-in-the-middle attack is an attack in which an attacker secretly intercepts the electronic messages going between the sender and the receiver and then capture, insert and modify messages during message transmission.
- **Accidental association:** Unauthorized access to organisation's wireless and wired networks can come from a number of different methods and intents. One of these methods is referred to as "accidental association". When a user turns on a computer and it latches on to a wireless access point from a neighbouring organisation's overlapping network, the user may not even know that this has occurred. However, it is a security breach in that proprietary organisation information is exposed and now there could exist a link from one organisation to the other. This is especially true if the laptop is also hooked to a wired network.
- **Denial of service:** It is an attempt to make a machine not available to its intended user.

Wireless network provides numerous opportunities to increase productivity and manage costs. Although it is impossible to totally eliminate all risks associated with wireless networking, it is possible to achieve a reasonable level of security by adopting a systematic approach to assessing and managing risk. Most common controls which are implemented in wireless environment are:

- **Encryption:** The best method for protecting the confidentiality of information transmitted over wireless networks is to encrypt all wireless traffic.
- **Signal-Hiding Techniques:** In order to intercept wireless transmissions, attackers first need to identify and locate wireless networks. There are, however, a number of steps that an organization can take to make it more difficult to locate their wireless access points. The easiest options include: Turning off the service set identifier (SSID) broadcasting by wireless access points and reducing signal strength to the lowest level that still provides requisite

coverage. More effective, but also more costly methods for reducing or hiding signals include: using directional antennas to constrain signal emanations within desired areas of coverage or using signal emanation-shielding techniques, also referred to as TEMPEST to block emanation of wireless signals.

- **Anti-virus and anti-spyware software:** Computers on a wireless network need the same protections as any computer connected to the Internet. Install anti-virus and anti-spyware software, and keep them up-to-date. If your firewall was shipped in the “off” mode, turn it on.
- **Default passwords:** Wireless routers generally come with standard default password that allows you to set up and operate the router. These default passwords are also available on the web. So change the router password immediately after its installation.
- **MAC address:** Every computer that is able to communicate with a network is assigned its own unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses access to the network.

6.9 Voice-over IP

Voice over Internet Protocol (VoIP) is a methodology for delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are IP telephony, Internet telephony, voice over broadband (VoBB) and broadband telephony.

The term Internet telephony specifically refers to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public Internet, rather than via the public switched telephone network (PSTN). The steps and principals involved in originating VoIP telephone calls are similar to traditional digital telephony, and involve signalling, channel setup, digitization of the analog voice signals, and encoding. Instead of being transmitted over a circuit-switched network, however, the digital information is packetized and transmission occurs as Internet Protocol (IP) packets over a packet-switched network. VoIP is available on many smartphones, personal computers, and on Internet access devices. Calls and SMS text messages may be sent over 3G or Wi-Fi.

6.9.1 Security Threats to VOIP

VoIP systems rely on a data network, which means security weaknesses and the types of attacks associated with any data network are possible. For example, in a conventional telephone system, physical access to the telephone lines or a compromise of the office private branch exchange (PBX) is required for in order to conduct activities such as wire-tapping. But for VoIP, voice is converted into IP packets that may travel through many network access points. Therefore the data is exposed to many more possible points of attack that could be used for interception by intruders. In fact, all the security risks associated with IP, such as computer viruses, Denial of Service and man in the middle attacks, are also dangerous to VoIP systems. Most of the VoIP traffic over the Internet is not

encrypted, so this traffic is exposed to the hackers. Hackers can intercept the communication or shut down the voice services by flooding servers (supporting VoIP) with bogus traffic.

6.9.2 VOIP Security

Encryption: Encryption is a means of preserving the confidentiality of transmitted signals.

- a. **Physical security:** Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to perform traffic analysis and derive call information from encrypted messages. Therefore, adequate physical security should be in place to restrict access to key VoIP network components.
- b. **Anti-virus and firewalls:** Computers which use software for VoIP connections should be protected with a personal firewall, along with anti-virus and anti-malicious code software that are up to date with the latest virus signature and/or malicious code definitions. This provides basic protection against attacks on the data segment that could be transferred to the voice segment.
- c. **Segregation of Voice and Data segments:** IP-based telephony provides a platform for telephone calls over an existing IP data network. However, in order to maintain quality of service (QoS), scalability, manageability, and security, voice and data should be separated using different logical networks as far as possible. Segmenting IP voice from a traditional IP data network greatly enhances the mitigation of VoIP attacks.

6.10 Penetration Testing

Penetration Testing is used by organizations to evaluate the effectiveness of information security implementation. As its name implies, penetration testing is a series of activities undertaken to identify and exploit security vulnerabilities. The idea is to find out how easy or difficult it might be for someone to “penetrate” an organization’s security controls or to gain unauthorized access to its information and information systems.

A penetration test is performed by team of experts. This team simulates attack using similar tools and techniques used by hackers. Penetration test cannot be expected to identify all possible security vulnerabilities because Penetration testing is conducted at a point in time. New technology, new hacker tools and changes to an organization’s information system can create exposures not anticipated during the penetration testing. Hence organizations perform these tests periodically.

Penetration Testing Scope

The scope of a penetration testing is to determine whether an organization’s security vulnerabilities can be exploited and its systems compromised. Conducting such a test involves gathering information about an organization’s information systems and information security and then using this information to attempt to identify and exploit known or potential security vulnerabilities. Evidence to support the penetration testing team’s ability to exploit security vulnerabilities can vary from gathering

“computer screen shots” or copying sensitive information or files to being able to create new user accounts on the system or being able to create and/or delete particular files on the organization's servers. Penetration testing can have a number of secondary objectives, including testing the security incident identification and response capability of the organization, testing employee security awareness or testing users' compliance with security policies.

Penetration Testing Strategies

Various strategies for penetration testing, based on specific objectives to be achieved, include:

- **External vs. internal testing.** External testing refers to attacks on the organization's network perimeter using procedures performed from outside the organization's systems as they are visible to hacker. This can be a **Blind test** where testing expert has been provided with limited information.
- **Internal testing** is performed from within the organization's technology environment. The focus is to understand what could happen if the network perimeter were successfully penetrated or what an authorized user could do to penetrate specific information resources within the organization's network.
- **Targeted testing:** (often referred to as the “lights-turned-on” approach) involves both the organization's IT team and the penetration testing team being aware of the testing activities and being provided information concerning the target and the network design. A targeted testing approach may be more efficient and cost-effective when the objective of the test is focused more on the technical setting, or on the design of the network, than on the organization's incident response and other operational procedures. A targeted test typically takes less time and effort to complete than blind testing, but may not provide as complete a picture security vulnerabilities and response capabilities of the organization.

6.10.1 Types of Penetration Testing

In addition to the penetration testing strategies to be used, consideration should be given to the types of testing the testing team is to carry out. These could include:

- **Application security testing:** Many organizations offer access to core business functionality through web-based applications. This type of access introduces new security vulnerabilities, because even with a firewall and other monitoring systems, security can be compromised, since traffic must be allowed to pass through the firewall. The objective of application security testing is to evaluate the controls over the application and its process flow. Areas of evaluation may include the application's usage of encryption to protect the confidentiality and integrity of information, how users are authenticated, integrity of the Internet user's session with the host application, and use of cookies – a block of data stored on a customer's computer that is used by the web server application.
- **Denial of Service (DoS) testing:** The goal of DoS testing is to evaluate the system's susceptibility to attacks that will render it inoperable so that it will “deny service,” that is, drop

or deny legitimate access attempts. Decisions regarding the extent of Denial of Service testing to be incorporated into a penetration testing exercise will depend on the relative importance of ongoing, continued availability of the information systems and related processing activities.

- **War Dialling:** War dialling is a technique for systematically calling a range of telephone numbers in an attempt to identify modems, remote access devices and maintenance connections of computers that may exist on an organization's network. Well-meaning users can inadvertently expose the organization to significant vulnerability by connecting a modem to the organization's information systems. Once a modem or other access device has been identified, analysis and exploitation techniques are performed to assess whether this connection can be used to penetrate the organization's information systems network.
- **Wireless network penetration testing:** The introduction of wireless networks, whether through formal, approved network configuration management or the inadvertent actions of well-meaning users, introduce additional security exposures. Sometimes referred to as "war-driving," hackers have become proficient in identifying wireless networks simply by "driving" or walking around office buildings with their wireless network equipment. The goal of wireless network testing is to identify security gaps or flaws in the design, implementation or operation of the organization's wireless network.
- **Social Engineering:** Often used in conjunction with blind and double blind testing, this refers to techniques using social interaction, typically with the organization's employees, suppliers and contractors, to gather information and penetrate the organization's systems. Such techniques could include:
 - Posing as a representative of the IT department's help desk and asking users to divulge their user account and password information;
 - Posing as an employee and gaining physical access to restricted areas that may house sensitive information;
 - Intercepting mail, courier packages or even trash to search for sensitive information on printed materials.

Social engineering activities can test a less technical, but equally important, security component: the ability of the organization's people to contribute to, or prevent, unauthorized access to information and information systems.

6.10.2 Risks associated with Penetration Testing

While management sponsors the testing activities, those activities do, in themselves, represent some level of risk. Some of the key risks include the following:

- The penetration test team may fail to identify significant vulnerabilities;
- Misunderstandings and miscommunications may result in the test objectives not being achieved;
- Testing activities may inadvertently trigger events or responses that may not have been anticipated or planned for (such as notifying law enforcement authorities);

- Sensitive security information may be disclosed, increasing the risk of the organization being vulnerable to external attacks.

Generally penetration testing is performed by external experts, hence it is necessary to enforce non-disclosure agreement and also define content of report, since it will contain the vulnerabilities within the system.

Table 6.2: Network Vulnerabilities and Controls

Target	Vulnerability	Control
Precursors to attack	Port scan	Firewall Intrusion detection system Running as few services as possible Services that reply with only what is necessary
	Social engineering	Education, user awareness Policies and procedures Systems in which two people must agree to perform certain security-critical functions
	Reconnaissance	Firewall Hardened"(self-defensive) operating system and applications Intrusion detection system
	OS and application fingerprinting	Firewall "Hardened" (self-defensive) applications Programs that reply with only what is necessary Intrusion detection system
Authentication failures	Impersonation	Strong, one-time authentication
	Guessing	Strong, one-time authentication Education, user awareness
	Eavesdropping	Strong, one-time authentication Encrypted authentication channel
	Spoofing	Strong, one-time authentication
	Session hijacking	Strong, one-time authentication Encrypted authentication channel Virtual private network
	Man-in-the-middle attack	Strong, one-time authentication Virtual private network Protocol analysis

Programming flaws	Buffer overflow	Programming controls Intrusion detection system Controlled execution environment Personal firewall
	Addressing errors	Programming controls Intrusion detection system Controlled execution environment Personal firewall Two-way authentication
	Parameter modification, time-of-check to time-of-use errors	Programming controls Intrusion detection system Controlled execution environment Personal firewall Two-way authentication
	Server-side include	Programming controls Personal firewall Controlled execution environment Intrusion detection system
	Cookie	Firewall Intrusion detection system Controlled execution environment Personal firewall
	Malicious active code: JavaScript, ActiveX	Intrusion detection system Controlled execution environment Signed code
	Malicious code: virus, worm, Trojan horse	Intrusion detection system Signed code Controlled execution environment Intrusion detection system
	Malicious typed code	Signed code Intrusion detection system Controlled execution environment
Confidentiality	Protocol flaw	Programming controls Controlled execution environment
	Eavesdropping	Encryption
	Passive wiretap	Encryption
	Mis-delivery	Encryption
	Exposure within the network	End-to-end encryption
	Traffic flow analysis	Encryption Traffic padding

		Onion routing
	Cookie	Firewall Intrusion detection system Controlled execution environment
Integrity	Protocol flaw	Firewall Controlled execution environment Intrusion detection system Protocol analysis Audit
	Active wiretap	Encryption Error detection code Audit
	Impersonation	Firewall Strong, one-time authentication Encryption Error detection code Audit
	Falsification of message	Firewall Encryption Strong authentication Error detection code Audit
	Noise	Error detection code
	Web site defacement	Error detection code Intrusion detection system Controlled execution environment Hardened host Honey pot Audit
	DNS attack	Firewall Intrusion detection system Strong authentication for DNS changes Audit
Availability	Protocol flaw	Firewall Redundant architecture
	Transmission or component failure	Architecture
	Connection flooding, e.g., echo-charge, ping of death, smurf, syn flood	Firewall Intrusion detection system ACL on border router Honey pot
	DNS attack	Firewall

		Intrusion detection system ACL on border router Honey pot
	Traffic redirection	Encryption Audit
	Distributed denial of service	Firewall Intrusion detection system ACL on border router Honey pot

The layers of security controls on the network are depicted in the following table.

Table 6.3: Layers of security controls on network

Security Level	Applicable Security/Control measures
Perimeter	Firewall Network-based anti-virus VPN encryption
Network	Intrusion detection /prevention system (IDS/IPS) Vulnerability management system Network access control Access control /user authentication
Host	Host IDS and Host vulnerability assessment (VA) Network access control Anti-virus Access control/user authentication
Application	Application shield Access control/user authentication Input validation
Data	Encryption Access control/user authentication

6.11 Auditing Network Security

Auditing networked computing environments presents significant complexities. Networking enables several virtual machines to operate together using a limited set of systems resources, irrespective of the barriers of geographic location of the user and systems infrastructure. For example, a customer can now access his bank account from anywhere in the world. This means that logical paths open up enabling access through insecure networks and diverse computing infrastructures. Audit of network security requires the auditor to take special considerations into account and plan accordingly to achieve his audit objectives. The considerations while auditing network security are:

- Locating logical access paths by reviewing network diagrams
- Identifying network topologies, virtual paths spanning across LANs, WANs and the open networks such as shared networks and the Internet.
- Recognizing logical access threats, risks and exposures in the networked environment.
- Identifying and controlling over access paths used for distributed processing and distributed databases.
- Evaluating network management and change control in respect of technical components such as modems, switches, routers, firewalls, VPNs, network management and access control software, encryption, protocols, middleware controls and Internet security.
- Identifying information resource owners can be quite complex since in a distributed computing environment, an application process can span several systems and networks, including those outside the organisation's control.
- Evaluating logical network security policies and practices.
- Evaluating effectiveness of logical access security with respect to network security components such as:
 - Firewalls and filtering routers - architecture, configuration setting as per firewall security policy, port services, anti-virus configuration, reporting and management controls
 - Intrusion detection systems - architecture, configuration, interface with other security applications, reporting and management controls
 - Virtual private networks - architecture, devices, protocol, encryption process integration with firewall security, change management
 - Security protocols - selection of appropriate protocol, seamless security integration of protocols between devices running different protocols
 - Encryption - selection of appropriate encryption methods to various application processes
 - Middleware controls - middleware design and access control with respect to identification, authentication and authorisation, management of components and middleware change management.
- Network event logging and monitoring

Type of System	Intrusion Detection				Vulnerability		
System Control Features	Monitoring				Assessment		
Controls D- Detective P-Preventive C- Corrective S-Support	Application Based	Host Based	Target Based	Network Based	Host Based	Network Based	Password Assessment

Confidentiality	Unauthorized access to files and system resources		D			P	P	P
	Modification to files		D	D		P	P	P
	Violation of enterprise system access policies	D	D			P	P	
	Violation of security policies	D	D	D	D	P	P	
	Weak or non-existent passwords	D	D			D		D
Integrity	Placement of Trojan horse or malicious software		D	D		P	P	
	Presence of Trojan horse or malicious software			D				
	Attack Against network services				D		P	
	Script based attacks	D			D	P		
Availability	Denial of Services Attacks				D		P	
	Failure or Mis-configuration of firewalls	D			D	P	P	
	Attacks Happening Over Encrypted Links	D	D					
	Unusual activity or variation from normal data pattern		D		D			
Other	Errors in Network configuration		D			DPC	DPC	
	Liability Exposure associated with attacker using own resources to attack others	P	P	P	P	P	P	P
	Post incident damage assessment	S	S	S	S	S	S	S

6.12 Summary

Networks are veins of market place. Organizations cannot imagine implementing IT without networks. Networks have added most important attribute to business performance that is efficiency. However it is not without risks. This has helps organizations in expanding their business empire and attackers in remaining unanimous. Most security breaches today are due to availability of networks. And therefore it is most essential for organizations to protect their networks in order ensure reasonable security has been implemented. IS auditor also must focus on the network security. Although sometimes it may not be in scope, but considering the architecture auditors cannot perform any IS audit without evaluating network controls. For example if the scope of audit is application control audit, auditor have consider network since the application is accessed by users over networks and sometimes using internet.

As technology is updating its capabilities, so are attackers and they are trying to use more and more innovative methods to attack organizations. IS auditors must be aware of trends in new technology as well as current threat scenarios.

6.13 Questions

1. Which of the following is a method used to gather information about the communication network?
 - A. Reconnaissance
 - B. Brute force
 - C. Eavesdropping
 - D. Wiretapping

2. Message digest helps organization in getting assurance on:
 - A. Communication delivery
 - B. Data availability
 - C. Data integrity
 - D. Data confidentiality

3. While auditing organization's network which of the following control IS auditor must verify first?
 - A. Encrypted communication.
 - B. Network zoning.
 - C. Firewall configuration.
 - D. Penetration test report.

4. Cryptographic checksum is a network control that:

- A. Adds a parity bit after adding the data bits.
 - B. Translates data in a file into a hash value.
 - C. Transmits the data after encryption.
 - D. Translates the data into a parity checksum combination.
5. Primary function of Security operations center (SOC) is to:
- A. Define baseline
 - B. Configure firewall
 - C. Monitor logs
 - D. Implement Antivirus
6. The intrusion detection monitoring on a host for data integrity attack by malicious software is a:
- A. Technical control
 - B. Corrective control
 - C. Detective Control
 - D. Preventive Control
7. Which of the following is most important while performing penetration testing?
- A. Maintain secrecy about testing.
 - B. Get consent from affected stakeholders.
 - C. Report to be provided to all users.
 - D. Perform test after office hours.
8. Most web based application attacks can be prevented by:
- A. Input validation
 - B. Encryption
 - C. Penetration test
 - D. Access controls
9. Social engineering attacks can best be prevented by:
- A. Intrusion detection system
 - B. Strong access controls
 - C. Two factor authentication
 - D. Awareness training
10. Which of the following is a type of malware that can be unintentional?

- A. Virus
- B. Logic bomb
- C. Trojan
- D. Worm

6.14 Answers and Explanations

1. **A.** Other methods are active attacks on network after getting information about networks.
2. **C.** Message digest is a hash function that helps in confirming integrity of data communicated over network.
3. **B.** Network segmentation or zoning is first control to implement network security. Other controls depends upon segmentation.
4. **B.** Checksum is a type of hash that is used to check integrity of data after communication. It is different that parity bit that adds an extra bit for each byte and word.
5. **C.** Primary function of SOC is to collect and monitor logs based on identified rules. It also defines correlation between various logs and identifies possible incidents which are communicated to respective asset owners. A is role of security manager, B and D are role of network team.
6. **C.** Intrusion detection detects the possible intrusion attempt. It does not prevent or corrects it. It is a control implemented using technology.
7. **B.** It is most essential to get consent from affected asset owners for before performing test, so that they can ensure that operations are not affected. Maintaining secrecy shall depend upon type of test. Report must be kept confidential and accessed only by select few. Test generally is performed when it will have least impact, but is not most important.
8. **A.** Most web application attacks like SQL injection can be prevented by validating input which can reject the attackers input that can exploit vulnerability. Encryption may or may not prevent an attack. Penetration test shall provide input on vulnerability that must be closed. Access controls may prevent some attacks.
9. **D.** Social engineering attack is attack on human and hence no technology can prevent it. It is best prevented by awareness training.
10. **B.** Logic bomb can be unintentional due to mistakes of developers going unnoticed.

6.15 References

a. Publication:

Security in Computing, 3rd Edition, By Charles P. Pfleeger, Shari Lawrence Pfleeger Published Dec 2, 2002 by Prentice Hall.

b. Websites:

- 1) <http://compnetworking.about.com/>
- 2) <http://theirm.org/>
- 3) <http://www.cert.org/>
- 4) <http://www.isaca.org/>
- 5) <http://www.iso.org/iso/home/standards/iso31000.htm>
- 6) <http://www.webopedia.com>
- 7) <https://na.theiia.org/Pages/IIAHome.aspx>
- 8) <https://www.dataprotection.ie/>
- 9) www.ehow.com
- 10) www.en.wikipedia.org
- 11) www.firesafetyinstitute.org
- 12) www.resources.infosecinstitute.com/access-control-models-and-methods
- 13) www.technet.microsoft.com/en-us
- 14) www.owasp.org

SECTION 3: APPENDIX

This section contains few checklist that might be useful for IS auditors while performing audit of different areas discussed in this module. Please note that contents of this section are for information and may not be complete in all respects. Auditors must pick and choose the different sections from these checklist while conducting audit and modify suitably as per the requirements and scope of audit.

1. Audit Checklist: Risk Management Process

Below are some of the suggested criteria and procedures for conducting an audit of risk management. The auditor's primary role is to ascertain whether the methods and procedures used were appropriate and conform to the policies and guidelines which make up the organization's approach to risk management. The auditor's secondary role is to ensure that any identified deficiencies are dealt with and that follow-ups are made.

Sl. No.	Section	Control Objective	Audit Procedure
1	Risk Management framework	Organization must have a risk management policy and framework that guides users in risk identification and assessment	Review Risk policies for common terminology, Risk response options and definition of risk and control owners Understand risk management process and framework. Interview managers that they understand the terminology, process and framework. Review risk register and its updating process. Interview senior management to understand risk appetite and risk tolerance levels.
2	Risk Identification	Management understands the risk identification concept and has identified key risks.	Check whether all managers are aware of the key risks to the organization and / or their function Assess the depth of the manager's understanding of the risk identification process based on his or her awareness.

			Verify that managers have assessed the key risks to the organization. Assess the completeness and accuracy of the risk assessment.
3	Risk Mitigation	Management has performed valid risk assessments.	Verify that management has documented risk assessments for each of the significant risks identified.
		Management has selected and implemented cost-effective risk control measures.	Verify that management has developed a series of risk-minimization, cost-effective options.
		As a result of implementing control measures, the overall risk to the organization has declined.	Assess whether the control measures introduced have managed the threat from the threats, as intended.
4	Risk Monitoring	Investigate incidents, changes, acquisitions, Projects and verify that the management has reviewed risk associated with root cause and risk register is updated.	Review the root cause of incident and ensure updating of risk register Review changes and acquisitions and their linkage to risk registers during assessment of impact due to change. Review project risk management process.
5	Risk register	Review risk register to contain risk identification, Risk response risk owner, controls implemented.	Verify that there is a clear and comprehensive procedure for recording, filing, maintaining and reporting on data sources, risk register Determine whether procedures associated with risk management activities are carried out Assess whether all occurrences of risk-related incidents have been reported.
6	Risk review	Ensure risk review process is in place and risk review happens periodically for	Review risk register for updating after risk review.

		reassessment of identified risks and assessment of new risks	Interview risk owners to confirm they have followed the review process.
7	Control identification	Controls should be identified based on the risk assessment. The cost benefit analysis for selected controls must be performed.	Check controls selected and implemented are against identified risk. Review the cost-benefit analysis (qualitative or quantitative) for implemented controls against total impact/exposure of risk

2. Audit of Security management

Sl. No.	Audit Area	Test Procedures
1	Security Management framework	Interview senior management on their commitment for information security Check minutes of board meeting, Security reports submitted, reporting frequency of security reports to management Check action and follow up by senior management on security initiatives Verify adequacy of security budget
2	Information security policies	Check whether Information Security Policies have been created, approved by management, and communicated to concerned users. Whether the policy states management commitment and sets out the organizational approach to managing information security. Ensure that security policies have link with risk assessment and suitable policies for organization's need are appropriately developed.
3	Review of Informational Security Policies	Check whether the Information Security Policies are reviewed at planned intervals, or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness. Check whether the results of the management review are taken into account. Check whether management approval is obtained for the revised policy.
4	Confidentiality And Non-	Check whether the organization's need for Confidentiality or Non-Disclosure Agreement (NDA) for protection of information is clearly defined and regularly reviewed.

	Disclosure Agreements	
5	Independent review of information security	Check whether the organization's approach to managing information security, and its implementation, is reviewed independently and periodically or when substantial changes to security policies occur.
6	Identification of risks related to 3 rd parties	Check whether risks to the organization's information and information systems, from 3 rd party access, are identified and appropriate control measures implemented before granting access.
7	Exception process	Check if the exception process is defined and implemented Verify if exception is against compensating controls and is for limited period of time and management has a plan to close the exceptions Ensure exceptions are reviewed periodically Interview approver for exceptions that they are aware of associated risks.
8	Procedures, standards	Check the internal standards for system configuration, documentation standard, segmentation and security baseline are defined and implemented Review the documented operating procedures for security controls and ensure these are reviewed and updated.

3. Audit of information and asset classification

Sl. No.	Audit Area	Test Procedures
1	Information security policies	Check whether Information Security Policies address the Information and asset classification standards Verify the data/asset classification schema defined by organization and it is based on the risk assessment Ensure that policy established accountability for asset owners and custodians Interview asset owners and custodians to confirm that they understand their accountabilities. Ensure that policy specifies protection levels for each class of asset.
2	Asset classification process	Review the asset classification process Review the asset inventory including information assets Select sample to review the appropriateness of classification Interview users involved in classification

3	Review of classification	Ensure that asset owners have classified the assets and suitably labelled Check the controls implemented to protect the assets

4. Audit checklist for physical and environmental security

To ensure IS assets are maintained in a secured manner within a controlled environment.

No.	Checkpoints
Secured Physical Access	
1.	Whether Physical Access Control Policy is documented and approved?
2.	Whether the policy on the following is appropriate and covers: Lay out of facilities Physical Security of the assets Access to the assets Maintenance of the assets Signage on the facilities Labels for assets Visitors' authorization and recording Entrance and exit procedures Legal & regulatory requirements
3.	Whether critical IS facilities (like data center) are located appropriately? (Verify the location for the following as:- Protection against natural disasters like earthquakes, flooding, extreme weather etc. Not in congested places Not being on ground or top floor Not being below ground level to avoid water leakage etc. Not having a showcase window Not having a direct access from the outside or through a public hallway Place which is not obvious externally).
4.	Whether the access to IS facilities is controlled through a secured mechanism? (Verify the access control mechanism - e.g. access card, lock and key or manned reception).
5.	Whether the access to the IS facilities is limited to approved persons only? (Approved persons may include employees, vendors and customers).
6.	Whether the physical access control procedures are adequate and appropriate for approved persons? (Access should be provided on need to do and need to know basis).
7.	Whether the visitor to critical IS facilities are escorted by employees? (Records for visitors' access should be maintained).
8.	Whether a periodical review of access rights is carried out?
9.	Whether the physical security is continually addressed?
10.	Whether all access routes are identified and controls are in place?

11.	Whether the security awareness is created not only in IS function but also across the organization?
12.	Whether the physical security is ensured at suppliers' facilities also in cases where organization's assets (either physical or data) are processed at supplier's facilities?
13.	Whether the usage of any equipment outside the business premises for information processing is authorized by the management?
14.	Is the security provided to equipment used outside business premises similar to / same as that offered to equipment used inside the business premises?
15.	Whether adequate monitoring equipment are present to monitor the movements of the personnel inside the facility?
16.	In case of outsourced software, whether all maintenance work is carried out only in the presence of/ with the knowledge of appropriate IS staff?
17.	Whether appropriate access controls like password, swipe card, bio-metric devices etc. are in place and adequate controls exist for storing the data/ information on them? Are there controls to ensure that the issue and re-collection of such access devices are authorized and recorded?
18.	Whether access violations are recorded, escalated to higher authorities and appropriate action taken?
19.	Whether employees are required to keep the critical / sensitive documents in secured places?
20.	Check if facility IS related risks with respect to lighting, building orientation, signage and neighbourhood characteristics are identified?
21.	Do the network, operating system and application monitoring procedures provide ample information to identify associated risks?
22.	Verify that surveillance systems are designed and operating properly?
23.	Ensure that physical access control procedures are comprehensive and being followed by security staff.
24.	Verify if the security controls in place are appropriate to prevent intrusion into sensitive IS facilities –data centre, communication hubs, emergency power services facilities?
25.	Review facility monitoring measures to ensure that alarm conditions are addressed promptly.
Environmental Controls	
1.	Whether the Environmental Control policy is documented and approved?
2.	Whether IS facilities are situated in a place that is fire resistant? (Verify for wall, floor, false ceiling, furniture and cabling being non-combustible / fire resistant / fire retardant).
3.	Whether smoking restrictions in IS facilities are in place?
4.	Whether adequate smoke / temperature detectors are installed, connected to the fire alarm system and tested?
5.	Whether fire instructions are clearly posted and fire alarm buttons clearly visible?

6.	Whether emergency power-off procedures are laid down and evacuation plan with clear responsibilities in place?
7.	Whether fire prevention and control measures implemented are adequate and tested periodically?
8.	Whether fire drill and training are conducted periodically?
9.	Whether air-conditioning, ventilation and humidity control procedures are in place, tested periodically and monitored on an ongoing basis?
10.	Whether an adequate alternate power arrangement is available? If so, is it covered under maintenance?
11.	Whether alternative water, fuel, air-conditioning and humidity control resources are available?
12.	Check if heating, ventilation, and air-conditioning systems maintain constant temperatures within a data center and other IS facilities?
13.	Evaluate the data centre's use of electronic shielding to verify that radio emissions do not affect computer systems or that system emissions cannot be used to gain unauthorized access to sensitive information.
14.	Verify if there are sufficient battery backup systems providing continuous power during momentary black-outs and brown-outs along with generators that protect against prolonged power loss and are in good working.
15.	Ensure that a fire alarm is protecting a critical IS facility like data center from the risk of fire, a water system is configured to detect water in high-risk areas of the data center and a humidity alarm is configured to notify data center personnel of either high or low-humidity conditions.
16.	Check logs and reports on the alarm monitoring console(s) and alarm systems which are to be monitored continually by data center/IS facility personnel.
17.	Verify that fire extinguishers are placed every 50ft within data center isles and are maintained properly with fire suppression systems are protecting the data center from fire.
18.	Whether there are emergency plans that address various disaster scenarios for example backup data promptly from off-site storage facilities?
19.	Ensure if there exists a comprehensive disaster recovery plan that key employees are aware of their roles in the event of a disaster and are updated and tested regularly.
20.	Ensure that detail part inventories and vendor agreements are accurate and current and maintained as critical assets.

Some key tips

1. Physical security is usually the first line of defence against natural/environmental risks and unpredictable human behaviour.

2. Automated environmental controls help minimize the resulting damage and speeds up the recovery process. Manual controls, on the other hand, can be time consuming and error prone.
3. If any physical security controls conflicts with life safety then this issue needs to be addressed; human life is always more important than protecting a facility or the information assets it contains.
4. HVAC should maintain appropriate temperature and humidity levels; provide closed-loop recirculating air conditioning, and positive pressurization and ventilation.
5. High humidity can cause corrosion, and low humidity can cause static electricity.
6. Emergency procedure documentation (including Disaster Recovery Plan) should be readily available and periodically reviewed and updated.
7. Interior partitions may not go all the way up to the ceiling; as, an intruder can remove a ceiling tile and climb over the partition into a critical portion of the facility.
8. CCTV enables one person to monitor a large area, but should be coupled with alerting functions to ensure proper response.
9. Company property should be marked clearly, and security guards should be trained how to identify when these items leave the facility in an improper manner.
10. Piggybacking, when unauthorized access is achieved to a facility via another individual's legitimate access, is a common concern with physical security.
11. There can be two power source- Primary and Alternate. The primary power source is what is used in day-to-day operations, and the alternate power source is a backup in case the primary source fails.
12. Brownouts may also be the result of power companies facing excessive power demand.
13. Power noise is a disturbance of power and can be caused by electromagnetic interference (EMI) or radio frequency interference (RFI).
14. Power regulators helps condition the line to keep voltage steady and clean.
15. Shielded lines protect from electrical and magnetic induction, which causes interference to the power voltage.
16. Fire detectors should be located below raised floors, on and above suspended ceilings, and in air ducts to provide maximum fire detection.
17. The HVAC should be turned off before activation of a fire suppressant to ensure that it stays in the affected area and smoke is not spread to other areas.
18. Dry pipe systems reduce the accidental discharge of water because the water does not enter the pipes until an automatic fire sensor indicates that there is an actual fire. In locations with freezing temperatures where broken pipes cause problems, dry pipes are preferred.
19. Gases, like halon, FM-200, and other halon substitutes, interfere with the chemical reaction of a fire. Halon is no longer available because it depletes the ozone. FM-200 or other similar substances are used instead of halon.

5. Audit Checklist on Logical Access Controls

The following is an illustrative questionnaire that could be used to review Logical Access Controls within operating systems and databases

No	Checkpoints
	User Access Management Policy and Procedure
1.	Whether the user access management policy and procedure are documented?
2.	Whether the user access management policy and procedure are approved by the management?
3.	Whether the user access management policy and procedure document includes: Scope and objective. Procedure for user ID creation, approval, review, suspension, and deletion. Granting access to third parties. Password management. User access rights assignment & modifications. Emergency access Granting. Monitoring access violations. - Review and update of document.
	User Access Management
1.	Whether User ID & access rights are granted with an approval from appropriate level of IS and functional head? (Verify the user ID creation, granting of access right and approval process)
2.	Whether the organization follows the principle of segregation of duties adequately in granting access rights? (Verify Access rights should be given on need to know and need to do basis – without unchecked concentration of power.)
3.	Whether User IDS are in a unique format? (Verify the naming conventions for the user IDs)
4.	Whether invalid log in attempts are monitored and User IDs are suspended on specific attempt? (Verify the parameters set for unsuccessful log in attempt)
5.	Whether the organisation follows complex composition for password parameters? (Complex composition of password parameter should be used as to make it difficult for guess and prevent unauthorised users from access e.g. special character and numbers should be part of password, Restrict use of organisation's name, 123, xyz or other generic terms as password).
6.	Whether granting access to the third parties is according to the User Access Management policy and procedure? (The organization should specify and implement a process for granting access to third parties like contractors, suppliers, auditors, consultants etc.)

7.	Whether users are forced to change password on first log-on and at periodic intervals? (Verify password parameters for first log on and password aging).
8.	Whether the organisation implemented clear screen and clear desk policies? (Terminals should be automatically logged off if remaining idle for specific time.)
9.	Whether the organisation restricted concurrent log- on? (One user ID should not be allowed to be logged-in for two different terminals at the same time)
10.	Whether users' IDs are shared? (Verify whether users' IDs are shared among the employees/ users or not?)
11.	Whether multiple user IDs are allocated to a single individual?
12.	Are user access policy and procedure documents communicated / available to the respective users?
13.	Whether User IDs and Password are communicated to the user in a secured manner? (Verify the procedure for communicating user ID and password for the first time and after suspension).
14.	Whether the organisation reviews user IDs and access rights at periodic intervals?
15.	Whether the organisation monitors logs for the user access?
16.	Whether policy and procedure documents reviewed and updated at regular intervals?
17.	Whether the access to scheduled job is restricted to the authorised?
18.	Whether an emergency user creation is according to the policy and procedure for User Access Management? (Verify the emergency access granting procedure, including approvals and monitoring).
19.	Whether periodic review process ensures user accounts align with business needs and removal on termination/transfer? (Review and evaluate procedures for creating user accounts and ensure that accounts are created only when there's a legitimate business need and that accounts are removed or disabled in a timely fashion in the event of termination or job change.)
20.	Whether passwords are shadowed and use strong hash functions? (Ensure the strength of passwords and access permission to password files. Review and evaluate the strength of system passwords and the use of password controls such as aging.)
21.	Review the process for setting initial passwords for new users and communicating those passwords and evaluate the tracking of each account to a specific employee.
22.	Whether the use of groups and access levels set for a specific group determines the restrictiveness of their use? (Evaluate the use of passwords, access rights at the group level)
23.	Ensure that the facility to logon as super/root user is restricted to system console for security reasons.
24.	Check whether the parameters to control the maximum number of invalid logon attempts has been specified properly in the system according to the security policy.

25.	Check whether password history maintenance has been enabled in the system to disallow same passwords from being used again and again on rotation basis.
26.	Verify the parameters in the system to control automatic log-on from a remote system, concurrent connections a user can have, users logged on to the system at odd times (midnight, holidays, etc.) and ensure whether they have been properly set according to security policy.
Maintenance of sensitive user accounts	
1.	Ascertain as to who is the custodian of sensitive passwords such as super/root user and verify if that person is maintaining secrecy of the password, whether the password has been preserved in a sealed envelope with movement records for usage in case of emergency.
2.	From the log file, identify the instances of use of sensitive passwords such as super user and verify if records have been maintained with reason for the same. Ensure that such instances have been approved/ authorized by the management.
3.	From the log file, identify the instances of unsuccessful logon attempts to super user account and check the terminal ID / IP address from which it is happening. Check if appropriate reporting and escalation procedures are in place for such violations

6. Audit Checklist for Network Administration and Security Auditing

The following is a general checklist for the audit of Network Administration and Security.

Sl.no	Checklist
Process	
1.	Is there an Information Security guidelines document, which defines the minimum configuration for any device/link on the organisation's network, including levels of encryption?
2.	Are all platforms/links/devices in compliance with the guidelines? If not, has an appropriate level of management reviewed the non-compliant parts of the network to ensure that the risk levels are acceptable?
3.	For all items supported by external vendors, does the vendor or the manufacturer verify that all cryptographic functions in use by the product/service, such as encryption, message authentication or digital signatures, use approved cryptographic algorithms and key lengths.
4.	Wherever applicable, whether background and reference checks for both internal and outsourced vendor staff who perform security-related functions for the product/service under review are carried out.

5.	This includes job applicants who have accepted a job offer, temporaries, consultants, full time staff as well as the outsourced vendor who is involved in product/service management and operations.
Authentication	
1.	Does the product/service authenticate (verify) the identity of users (or remote systems) prior to initiating a session or transaction? Have these authentication mechanisms been approved by then organization's IT Department? (These include Passwords, Personal Identification Numbers (PINs), (static and dynamic), public keys and biometrics.)
2.	Does the organization verify that the initial authentication has used a mechanism that is acceptable for the application? Has the approach been approved by IT Department and required compensating controls have been implemented?
3.	Does the organisation have a comprehensive password construction, implementation and management policy?
4.	Do the Products/Services utilizing biometrics authentication only use biometrics for local authentication?
Public Key Infrastructure (PKI)	
1.	Do the Products/services using Public key (or asymmetric) cryptography for authentication either on a session basis (peer authentication) or on a per-message/transaction basis (digital signatures) use approved security protocols to comply with the public key technology standard?
2.	For products/services that use PKI, private keys which are stored in hardware or software must be protected via an approved mechanism. The protection mechanism includes user authentication to enable access to the private key. Are these protections mechanisms adequate?
3.	For products/services that use PKI, an approved process for verifying the binding of a user identity to the public key (e.g., digital certificate) is required for any server relying on public key authentication. Is such a processes in place?
Access Control	
1.	Is the access to highly privileged IDs (e.g., system administration access) strictly controlled, audited and limited in its use?
2.	Does the product/service support the need to perform a periodic entitlement review? A periodic entitlement review process should validate access privileges.
3.	Does the product/service support the requirement to limit individual user sessions to a maximum of X minutes of inactivity using either session time out or a password protected screen saver?
4.	Is there a process in place to ensure that access rights reflect changes in employee or job status within X hours of the change? This includes physical access tokens and dial-in capabilities as well as any systems or applications.

5.	For any products/services, which has been outsourced, is there a process in place to ensure that all platforms, services and applications are configured to meet organisation's Information Security Standards?
6.	Does the product/service display the (a) date and time of last successful login and (b) the number of unsuccessful login attempts since the last successful login?
7.	Does the product/service support a periodic process to ensure that all user IDs for employees, consultants, agents, auditors, or vendors are disabled after X days and deleted after Y days from the day they were not used unless explicitly approved by the concerned business manager.
Cryptography	
1.	Is there a cryptography/encryption policy for various types of classified information that travels/gets stored within and outside the organisation's network(s)?
Network Information Security	
1.	Is the approved Legal Affairs banner being displayed at all entry point where an internal user logs into the product/service? An automated pause or slow roll rate is in place to ensure that the banner is read. The Legal Affairs Banner usually carries the following kind of text: "You are authorized to use this system for approved business purposes only. Use for any other purposes is prohibited. All transactional records, reports, e-mail, software and other data generated or residing upon this system are the property of the Company and may be used by the Company for any purpose. Authorized and unauthorized activities may be monitored." NOTE: This is required for all mainframe, mid-range, workstation, personal computer, and network systems.
2.	Has dial-in connectivity been prohibited on network-connected machine (server and workstation) except where documented and explicitly approved in writing by Business Management and the IT Department. When explicitly approved, the modem must, as a minimum control, prohibit answer or pick up until after the 5th ring.
3.	Have the remote control products used in a dial-in environment been approved by the IT Department explicitly?
4.	Is it ensured that only software (applications /operating systems, etc.) supported by the vendors are used? (Unsupported software could be vulnerable to attacks since the vendors would not come up with the relevant patches.)
Information Security Administration	
1.	Is there an approved document clearly outlining the Security Administrator's (SA) responsibility?

2.	Are all the administrative actions (e.g., adding/deleting users, changes to entitlements/passwords) backed up by an independent review?
3.	Does the Security Administrator function review all security audit logs, incident reports, and on-line reports at least once per business day?
4.	In case of Wide Area Networks (WAN), are the router tables maintained securely in Routers?
5.	Are router login IDs and passwords treated as sensitive information and managed by authorised administrators? Are all changes to router table entries logged and reviewed independently?
6.	Are access violations taken note of, escalated to higher authority and acted upon in a timely manner?
7.	Is there a process to report all unusual or suspicious activity? (Reporting to IT Department, investigating immediately, and bringing the case to closure without delay)?
8.	Does the Security Administrator function assess compliance with their security procedures quarterly and reports their results to the IT Department?
9.	Have all the all security related administrative procedures under the control of the Security Administrator been documented and approved by management (annual exercise)? At minimum procedures should include: Information Ownership Data Classification User registration/Maintenance Audit Trail review Violation logging and reporting Sensitive activity reporting Semi-Annual Entitlement Reviews Password resets Escalation reporting
Microcomputer/PC Security	
1.	Do the LAN servers, mail servers, and microcomputers have IT department approved anti-virus products installed?
2.	Are all product/service specific microcomputers/PCs secured against removal and theft commensurate with the value of the computer and information it holds along with a process to report any thefts to the IT Department?
3.	Are microcomputers / PCs having sensitive information protected with power-on password to prevent unauthorized access?
4.	Are sensitive data in such microcomputers / PCs backed up and preserved properly to ensure recovery in case of failure?
Audit Trails	
1.	Does the audit trail associate with the product/service support the ability to log and review all actions performed by systems operators, systems managers,

	system engineers, system administrators, highly privileged accounts and emergency IDs?
2.	Does the financial transactions as well as additions, changes and deletions to customer's and vendor's data, get recorded in the product/ service audit trail?
3.	Does the audit trail for product/service record all identification and authentication processes? Also is there a retention period for the audit trails? Is it adequate?
4.	Does the audit trail associate with the product/service log all actions by the Security Administrator?
5.	Is there a process to log and review all actions performed by systems operators, systems managers, system engineers, system administrators, security administrators, and highly privileged IDs?
6.	Is there a process in place to log and review actions performed by emergency IDs associated with the product/service?
Violation Logging Management	
1.	Whether the product/service is capable of logging the minimum criteria specified to log and report specific security incidents and all attempted violations of system integrity
2.	Are the product/service owners aware of their responsibilities with respect to Security incident reporting?
Information Storage and Retrieval	
1.	Has all the media (File/Floppy/Disks/Tapes etc.) under the control of the product/service owner been marked with the classification and securely stored with access restricted to authorized personnel only?
2.	Is there a process in place to ensure that all media under the control of the product/service owner containing critical information is destroyed in a manner that renders the data unusable and unrecoverable?
3.	Is there a procedure in place that enforces and maintains a clean desk program, which secures all critical information from unauthorized access?
Penetration Testing	
1.	Is it ensured that products/services that use the Internet for connectivity or communications have undergone a successful penetration test prior to production implementation?
2.	Is there a penetration test process that ensures whether modifications to the product/service that uses the Internet for connectivity or communication have been reviewed to determine whether a subsequent penetration test is warranted?
3.	Is there an intrusion detection system in place for all the external IP connections?

7. Network Infrastructure Auditing Checklist

The following is a general illustrative checklist for the audit of Network infrastructure.

Network Server

- Obtain or prepare logical and physical diagrams of the network and attached local and wide area networks, including the systems' vendor and model description, physical location, and applications and data residing and processing on the servers and workstations.
- Using the information obtained in the prior steps, document the server and directory location of the significant application programs and data within the network; document the flow of transactions between systems and nodes in the network.
- Assess whether the trusted domains are under the same physical and administrative control and are logically located within the same sub-network.
- Determine that router filtering is being used to prevent external network nodes from spoofing the IP address of a trusted domain.
- Determine that the Administrator/SuperUser and Guest accounts have passwords assigned to them (by attempting to log on without providing a password). Also ascertain that the Administrator account password is well controlled and used/known by only the system administrator and one backup person.
- Review the account properties settings active in each user's individual profile, which may override the global account policy.
- List out the security permissions for all system directories and significant application programs and directories and ensure that they are consistent with security policy
- Review and assess permissions assigned to groups and individual accounts, noting that Full Control (all permissions) and Change (Read, Write, Execute, and Delete) permissions are restricted to authorized users.
- Review the audit log for suspicious events and follow up on these events with the security administrator.

Router

- Determine the types of accounts that were used to access the routers.
- Determine what users had access to these accounts.
- Were access attempts to the routers logged?
- Determine if all accounts had passwords and determine the strength of the passwords.
- Was simple network management protocol (SNMP) used to configure the network?
- Determine the version of SNMP employed by the Company. (Version one stores passwords in clear-text format. Version two adds encryption of passwords.)
- Determine if open shortest path first (OSPF) was defined on the router. Determine the authentication mechanism that was employed in the Company's implementation of OSPF.

- Determine whether directed broadcast functionality was enabled on the router. This setting, if enabled, could allow a denial-of-service (DoS) attack of the network (Smurf attack).
- Obtain population of routers with modems and obtain the telephone numbers of the routers.
- Determine if users were properly authenticated when remotely accessing the routers.
- Determine how changes to the router environment were made.
- Were there procedures for changing router configurations? If so, were these procedures well-documented and consistent with security policy?
- Determine if changes to the router configuration were documented.
- Was there a separation of duties within the change control of the router environment?

Firewalls

- Obtain background information about the firewall(s), in place, e.g., segment diagrams, software, hardware, routers, version levels, host names, IP addresses, connections, any specific policies for an overview of the firewall security
- Determine that the firewall components, both logical and physical, agree with the firewall strategy.
- Determine whether the firewall components are the latest possible version and security patches are current.
- Determine that the root cannot telnet to the system.
- Determine the telnet OS banner and other banners such as FTP banner, etc. has been eliminated.
- Ensure that there are no compilers/interpreters on the firewall.
- Ensure that a lockdown rule has been placed at the beginning of the rule base. The lockdown rule protects the firewall, ensuring that whatever other rules are put in later, it will not inadvertently compromise the firewall.
- Obtain and review the connections table for time out limits and number of connections
- Attempt to test the rule base by scanning secured network segments from other network segments
- Identify accessible resources behind the firewall that are to be encrypted and determine the connections are encrypted
- Determine if there is a change control process in place for the rule base
- Determine the use of the firewall's automatic notification/alerting features and archiving the detail intruder information to a database for future analysis.

Module-5

Systems Development: Acquisition, Maintenance and Implementation

TABLE OF CONTENTS

MODULE 5: SYSTEMS DEVELOPMENT: ACQUISITION, MAINTENANCE AND IMPLEMENTATION.....	205
SECTION 1: OVERVIEW	205
Learning Objectives.....	205
Task Statements.....	205
Knowledge Statements	206
Relationship between Task and knowledge statements	207
Knowledge Statement Reference Guide	210
SECTION 2: CONTENTS.....	213
Chapter 1: System Development Life Cycle (SDLC) introduction and Concepts	213
Learning objectives	213
1.1 Introduction	213
1.1.1 Objectives of SDLC approach	214
1.1.2 Steps of Systems development.....	214
1.1.3 Organisation of chapters.....	215
1.2 Concepts of SDLC	216
1.2.1 When is SDLC initiated?	216
1.2.2 What is SDLC?	217
1.2.3 Business Application System	218
1.3 Typical phases of SDLC	218
Phase 1: Feasibility Study.....	219
Role of IS Auditor in project initiation and feasibility study phase:.....	219
Phase 2: Requirements Definition	220
Role of IS Auditor in requirements definition phase:.....	220
Phase 3: System Analysis.....	220
Role of IS Auditor in system analysis phase:	220
Phase 4: Design	221
Role of IS Auditor in detailed design phase:	221
Phase 5: Development.....	222

Some key aspects of development:	222
Role of IS Auditor in development phase:	223
Phase 6: Testing	223
Role of IS Auditor in testing phase:	223
Phase 7: User acceptance testing (UAT) or final testing	224
Phase 8: Implementation	225
Role of IS Auditor in implementation phase:	225
Phase 9: Support and operations	225
Role of IS Auditor in maintenance and post implementation phase:	226
1.4 Changes in SDLC phases	226
Introduction of a decision on Make or Buy	227
Phase 3B: Outsource the application development	227
Phase 3C: Select and Purchase software available in market	227
Phase 4B: Requirement finalization	228
Phase 4C: Request for Proposal (RFP)	228
Phase 5B: Contract and SLA	228
Phase 5C: Purchase	230
Phase 6B: Vendor development and monitoring	230
Phase 6C: Configuration (purchased systems)	230
Changes in Phase 7: UAT	230
1.5 Secure SDLC	231
1.6 Risk associated with SDLC and mitigation planning	232
1.7 Roles and responsibilities of SDLC	234
1.8 Summary	235
1.9 Questions	236
1.10 Answers and Explanations	237
Chapter 2: Initiating SDLC	239
Learning Objectives	239
2.1 Introduction	239
2.1.1 Drivers, pain points and triggers	239

Pain points.....	239
Triggers.....	240
2.2 Feasibility study.....	240
2.2.1 Technical Feasibility.....	240
2.2.2 Economic Feasibility	242
2.2.3 Schedule or Time Feasibility	242
2.2.4 Resources Feasibility	242
2.2.5 Operational Feasibility	243
2.2.6 Social Feasibility.....	243
2.2.7 Compliance Feasibility	243
2.2.8 Internal Controls	244
2.3 Organisational methods for benefit realization	244
Benefits Realization Techniques.....	244
2.4 Business case development	245
2.5 Business Requirements Identification	246
2.5.1 Techniques for requirements gathering	246
1. Understanding Requirements	246
2. Study of History, Structure and Culture	247
3. Study of Information Flows.....	247
2.5.2 Types of requirements	247
Functional requirements	248
Non-functional requirements	248
Requirements Engineering (RE) Process	248
2.6 Summary	249
2.7 Questions	250
2.8 Answers and Explanations	251
Chapter 3: Project Management for SDLC	253
Learning Objectives.....	253
3.1 Introduction	253
3.2 Project management frameworks	253

3.3 Key concepts of project management	254
3.4 Program and project management and organisation	256
3.4.1 Portfolio/Program Management	256
3.4.2 Program/Project management Organisation forms	257
3.5 Project Initiation	258
3.5.1 Project management methodology	259
3.5.2 Project Context and Environment	259
3.5.3 Project Communication and Culture	260
3.5.4 Project Objectives	260
3.5.5 Project Management Practices	261
3.6 Project Planning	261
3.7 Project Controlling	262
3.7.1 Management of Scope	263
3.7.2 Resource management	263
3.7.3 Project risk management standards and methods	264
Risk in project management	264
Risk management process	265
3.8 Project Closing	265
3.9 Roles and responsibilities	266
3.9.1 Steering committee	266
Role of project steering committee	266
3.9.2 Project Sponsor	267
3.9.3 Project Manager	267
3.9.4 Senior management	267
3.9.5 Business management	267
3.9.6 Systems development project team	268
3.9.7 Business function representatives/domain specialists	268
3.9.8 Security Officer	268
3.9.9 IS Auditor	268
Role of IS Auditor in SDLC	269

3.9.10 Quality assurance (QA)	269
3.9.11 Technology Specialist.....	270
3.9.12 Systems Analyst.....	270
3.9.13 Programmers/Developers.....	270
3.9.14 Testers	270
3.9.15 Documentation Specialist	270
3.9.16 Database Administrator (DBA)	271
3.10 SDLC Project management techniques and tools	271
1. Computer Aided Software engineering (CASE) tools	271
Code Generators.....	271
Development environments and non-procedural languages.....	272
2. Software Size Estimation	272
Source lines of Code (SLOC).....	272
Function Point Analysis (FPA)	273
FPA Feature Points.....	273
Cost Budgets	274
3. Project Controlling tools and techniques.....	274
A. Program Evaluation Review Technique (PERT).....	274
B. Critical Path Methodology	276
C. Gantt Charts	277
3.11 Summary.....	278
3.12 Questions	278
3.13 Answers and Explanations	279
Chapter 4: Different models and methods for SDLC.....	281
Learning objectives	281
4.1 Introduction	281
4.2 SDLC Models	282
4.2.1 Waterfall model	282
Strengths:.....	283
Weaknesses:	283

Verification and validation - a variant of waterfall model	284
4.2.2 Prototyping methodology	285
Generic phases of model.....	285
Strengths:.....	286
Weaknesses:	287
4.2.3 Spiral Model.....	287
Key characteristics.....	288
Strengths:.....	288
Weaknesses:	288
4.2.4 The Incremental Model	289
Strengths:.....	290
Weaknesses:	291
4.3 SDLC Methodologies	291
4.3.1 Rapid Application Development (RAD).....	291
Strengths:.....	292
Weaknesses:	292
4.3.2 Agile software development methodology	293
Key Characteristics of Agile processes	294
Key features of agile methodologies.....	295
Strengths:.....	295
Weaknesses:	295
4.3.3 Software reengineering and reverse engineering	296
Software reengineering	296
What is software reengineering?	296
When to reengineer?.....	296
Software Reengineering Activities.....	296
Reverse Engineering	297
4.3.4 Object oriented software development (OOSD).....	298
Advantages of OOSD:	299
4.3.5 Component Based development.....	299

Advantages of component-based development are:	300
Disadvantages:	300
4.3.6 Web-based application development.....	300
4.4 Summary	301
4.5 Questions	302
4.6 Answers and Explanations	303
Chapter 5: System acquisition framework.....	305
Learning objectives	305
5.1 Introduction	305
5.2 Requirements Analysis.....	307
5.3 Product selection.....	308
5.4 Request for proposal	309
5.5 Vendor selection criteria/process	311
5.5.1 Service Level Agreements (SLAs)	311
5.5.2 Vendor monitoring	312
5.6 Summary	313
5.7 Questions	313
5.8 Answers and Explanations	314
Chapter 6: Implementation and Maintenance.....	317
Learning objectives	317
6.1 Introduction	317
6.2 Testing	318
6.2.1 Unit Testing	318
Methods of Unit Testing	319
6.2.2 Integration Testing	321
6.2.3 Regression Testing	322
6.2.4 System Testing.....	322
6.2.5 Final Testing	322
6.2.6 Other types of Testing.....	324

6.3 Implementation.....	325
6.3.1 Implementation Strategies	326
6.3.2 Preparing for implementation	328
6.3.3 Training	329
6.3.4 Conversion.....	329
6.4 Change management process	331
6.4.1 Emergency Changes	332
6.4.2 Implementing Changes into Production	333
6.4.3 Segregation of Duties	333
6.4.4 Configuration Management	334
6.5 Summary	335
6.6 Questions	335
6.7 Answers and Explanations	336
Chapter 7: Trends in technology impacting SDLC.....	339
Learning objective	339
7.1 Introduction	339
7.2 Technology Trends.....	339
7.2.1 Virtualization	339
Characteristics of virtualizations affecting SDLC	339
7.2.2 Cloud computing and sourcing options.....	340
Auditing Cloud services	341
7.2.3 Mobile Computing	342
Mobile devices and applications development.....	342
7.2.4 Bring your own device (BYOD)	343
Benefits of BYOD	343
Risks of BYOD	343
7.2.5 Big data and Data analytics	344
Big Data	344
Risks.....	344
Risk mitigation	345

Audit questions	345
Data analytics	345
Benefits of data analytics	346
Risks.....	346
7.3 Summary	347
7.4 Questions	347
7.5 Answers and Explanations	348
Chapter 8: SDLC Reviews and Audit	351
Learning objectives	351
8.1 Introduction	351
8.2 Role of IS Auditor in SDLC	351
8.2.1 IS Auditor as Team member.....	351
8.2.2 Mid-project reviews	352
8.2.3 Post implementation review.....	353
8.3 Summary	354
Key factors to be considered by IS Auditor in SDLC process.....	355
8.4 Questions	355
8.5 Answers and Explanations	356
SECTION 3: APPENDIX	357

MODULE 5: SYSTEMS DEVELOPMENT: ACQUISITION, MAINTENANCE AND IMPLEMENTATION

SECTION 1: OVERVIEW

Learning Objectives

Most IT departments or software development companies, irrespective of their size, have a formal set of procedures for initiating and developing new business information systems. This is often termed as System Development Life Cycle (SDLC) or the System Development Methodology (SDM). SDLC is an essential process of developing software solutions within organisations. This module covers all aspects of SDLC such as development or acquisition of application software as well as implementing IT using project management practices. This module covers the following topics:

1. Phases in SDLC and changes in these phases due to changes in environment and security requirements.
2. Initial phases of SLDC covering feasibility study, requirement definition, expected benefits to organisation and developing business case for SDLC project.
3. Project management practices for executing SDLC project.
4. Various models and methods that can be adopted based on requirements for development of application software.
5. Process for acquisition and/or outsourcing development, in case an organisation has decided to acquire software or outsourced development.
6. Implementation methods for application acquired/developed.
7. Impact on SDLC due to changes in technology.
8. Guidelines for auditing SDLC project.

Task Statements

The task statements are what the ISA candidate is expected to know “how to perform”. The knowledge statements delineate the areas in which ISA candidate must have a good understanding in order to perform the tasks.

- 5.1 Review SDLC objectives and organisation objectives, practices, requirement analysis and initiating SDLC.
- 5.2 Review need for SDLC projects, project management practices, milestones and framework are appropriate to meet organisation requirements, governance mechanism including benefits

realization practices, (e.g., steering committee, business cases, total cost of ownership [TCO], ROI).

- 5.3 Review Systems Development Life Cycle (SDLC) methods and associated tools and techniques and alternate SDLC models used are appropriately deployed.
- 5.4 Review software and other acquisition processes, vendor selection process, SLA, etc. are in line with organisation objectives.
- 5.5 Assess risks associated with project are addressed in system design specification based on organisation and security requirements.
- 5.6 Assess systems implementation processes and techniques: system implementation plan, acceptance testing approach, data conversion approach, project benefits, resources used (financial and people), adequacy of acquisition, development and deployment, and the opportunities for improvement.
- 5.7 Assess controls for information systems during the requirements, acquisition or design, development and testing phases for compliance with the organisation's policies, standards, procedures and external requirements.
- 5.8 Review required software quality attributes, testing process against predefined performance metrics and use of software benchmarks as appropriate.
- 5.9 Review relevant use of industry trends when developing a solution strategy.
- 5.10 Perform post-implementation review of systems to determine whether project deliverables, controls and organisation requirements are met.

Knowledge Statements

- 5.1 Systems Development Life Cycle (SDLC) concepts, importance, and phases.
- 5.2 Roles and responsibilities in SDLC, implementation and functional segregation of duties within SDLC.
- 5.3 Need for initiating SDLC, triggers and pain points, defining business requirements including security requirements, business case development and benefits from output of SDLC (i.e. new application system) including risk management and definition of controls.
- 5.4 Project governance mechanisms (steering committee, project oversight board, organisational standards for program and project management practices, program and project management office, benefits realization practices, (e.g., feasibility studies, business cases, total cost of ownership [TCO], Return on Investment (ROI) and resource management.
- 5.5 Software development methods such as: Waterfall, Spiral, Rapid Application Development, Agile Development, Prototypes, Object Oriented Analysis, baseline procedures in SDLC.
- 5.6 Use of CASE and other tools, software Re- engineering/Reverse Engineering, development effort estimates and software sizing techniques (e.g. LOC, FPA, etc.)
- 5.7 Project resource management, coding and testing practices, QAT and UAT, quality attributes and performance measurements of quality, testing methodologies and practices related to information systems development and software accreditation.

- 5.8 Systems implementation processes and techniques: system implementation plan, acceptance testing approach, data conversion approach, communication and training, hardware/software facilities, installation, cut-over plan, configuration and release management relating to the development of information systems.
- 5.9 Software support and maintenance practices, change management framework and practices, emergency changes, help desk, communication and training.
- 5.10 Sourcing and contracting strategies, policies and management practices, hardware/software acquisition and support policies.
- 5.11 Requirements mapping, software selection and evaluation practices and process.
- 5.12 Industry trends – cloud computing, mobile computing, BYOD, Big data and data analytics.
- 5.13 Post-implementation reviews of application systems.
- 5.14 Auditing SDLC processes.

Relationship between Task and knowledge statements

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
5.1 Review SDLC Objectives and organisation objectives, practices, requirement analysis and initiating SDLC. .	5.1 SDLC concepts, importance, and phases. 5.3 Need for initiating SDLC, triggers and pain points, defining business requirements including security requirements, business case development and benefits from output of SDLC (i.e. new application system) including risk management and definition of controls.
5.2 Review need for SDLC Projects, project management practices, milestones and framework are appropriate to meet organisation requirements, governance mechanism including benefits realization practices, (e.g., steering committee, business cases, total cost of ownership [TCO], ROI).	5.3 Need for initiating SDLC, triggers and pain points, defining business requirements including security requirements, business case development and benefits from output of SDLC (i.e. new application system) including risk management and definition of controls. 5.4 Project governance mechanisms (steering committee, project oversight board, organisational standards for program and project management practices, program and project management office, benefits realization

	practices, (e.g., feasibility studies, business cases, total cost of ownership [TCO], Return on Investment (ROI) and resource management.
5.3 Need for initiating SDLC, triggers and pain points, defining business requirements including security requirements, business case development and benefits from output of SDLC (i.e. new application system) including risk management and definition of controls.	5.1 SDLC concepts, importance, and phases. 5.5 Software development methods such as: Waterfall, Spiral, Rapid Application Development, Agile Development, Prototypes, Object Oriented analysis, baseline procedures in SDLC.
5.4 Review software and other acquisition processes, vendor selection process, SLA, etc. are in line with organisation objectives.	5.3 Need for initiating SDLC, triggers and pain points, defining business requirements including security requirements, business case development and benefits from output of SDLC (i.e. new application system) including risk management and definition of controls. 5.7 Project resource management, coding and testing practices, QAT and UAT, quality attributes and performance measurements of quality, testing methodologies and practices related to information systems development and software accreditation 5.10 Sourcing and contracting strategies, policies and management practices, hardware/software acquisition and support policies. 5.11 Requirements mapping, software selection and evaluation practices and process 5.12 Industry trends: cloud computing, mobile computing, BYOD, Big data and data analytics.
5.5 Assess risks associated with project are addressed in system design specification based on business and security requirements.	5.3 Need for initiating SDLC, triggers and pain points, defining business requirements including security requirements, business case development and benefits from output of SDLC (i.e. new application system) including risk management and definition of controls.

5.6 Assess Systems implementation processes and techniques: system implementation plan, acceptance testing approach, data conversion approach, project benefits, resources used (financial and people), adequacy of acquisition, development and deployment, and opportunities for improvement	5.8 Systems implementation processes and techniques: system implementation plan, acceptance testing approach, data conversion approach, communication and training, hardware/software facilities, installation, cut-over plan, configuration and release management relating to the development
5.7 Assess controls for information systems during the requirements, acquisition or design, development and testing phases for compliance with the organisation's policies, standards, procedures and external requirements.	5.2 Roles and responsibilities in SDLC, implementation and functional segregation of duties within SDLC. 5.3 Need for initiating SDLC, triggers and pain points, defining business requirements including security requirements, business case development and benefits from output of SDLC (i.e. new application system) including risk management and definition of controls. 5.9 Software support and maintenance practices, change management framework and practices, emergency changes, help desk, communication and training.
5.8 Review required software quality attributes, testing process against predefined performance metrics and use of software benchmarks as appropriate.	5.7 Project resource management, coding and testing practices, QAT and UAT, quality attributes and performance measurements of quality, testing methodologies and practices related to information systems development, software accreditation 5.11 Requirements mapping, software selection and evaluation practices and process.
5.9 Review relevant use of industry trends when developing a solution strategy.	5.12 Industry trends: cloud computing, mobile computing, BYOD, Big data and data analytics.
5.10 Perform post-implementation review of systems to determine whether project deliverables, controls and organisation requirements are met.	5.1 SDLC concepts, importance, and phases 5.13 Post-implementation reviews of application systems. Auditing SDLC processes.

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 chapters.

5.1 Systems development life cycle (SDLC) concepts, importance, and phases.

Knowledge area	Reference
Systems development life cycle (SDLC) introduction, importance, and SDLC phases	1.1 to 1.6

5.2 Roles and Responsibilities in SDLC and implementation, functional segregation of duties within SDLC

Knowledge area	Reference
SDLC roles and responsibilities, Segregation and other requirements	1.8, 3.6, 6.3

5.3 Need for initiating SDLC, triggers and pain points, defining business requirements including security requirements, business case development and benefits from output of SDLC (i.e. new application system) including risk management and definition of controls.

Knowledge area	Reference
Initiation, triggers and pain points, requirements and business case development, risk management and controls	2.1 to 2.5, 1.7, 7.1 to 7.6

5.4 Project governance mechanisms (steering committee, project oversight board, organisational standards for program and project management practices, program and project management office, benefits realization practices, (e.g., feasibility studies, business cases, total cost of ownership [TCO], Return on Investment (ROI) and resource management.

Knowledge area	Reference
Project management and governance processes	3.1 to 3.5

5.5 Software development methods such as: Waterfall, Spiral, Rapid, Application Development, Agile Development, Prototypes, Object Oriented Analysis, baseline procedures in SDLC.

Knowledge area	Reference
Software development methods	4.1 to .4.13

5.6 Use of CASE and other Tools, software Re- engineering/Reverse Engineering, development effort estimates and software sizing techniques (e.g. LOC, FPA etc.)

Knowledge area	Reference
CASE and other Tools, software sizing techniques	3.7

5.7 Project resource management, Coding and testing practices, QAT and UAT, Quality attributes and Performance measurements of quality, Testing methodologies and practices related to information systems development, Software accreditation

Knowledge area	Reference
Testing and QAT and UAT, Resource management	6.4 and 6.5

5.8 Systems implementation processes and techniques: system implementation plan, acceptance testing approach, data conversion approach, communication and training, hardware/software facilities, installation, cut-over plan, configuration and release management relating to the development of information systems.

Knowledge area	Reference
Implementation methods, plan, conversion, fall back, support and training	6.1 to.6.3 and 6.5

5.9 Software support and maintenance practices, change management framework and practices, emergency changes, help desk, communication and training.

Knowledge area	Reference
Software support and maintenance	.6.5, 3.3. 3.5

Module 5

5.10 Sourcing and contracting strategies, policies and management practices, hardware/software acquisition and support policies

Knowledge area	Reference
Sourcing strategies for software, hardware and support.	5.1 to 5.7

5.11 Requirements mapping, software selection and evaluation practices and process.

Knowledge area	Reference
Software selection, evaluation, functional mapping	5.1 to 5.7

5.12 Industry trends – cloud computing, mobile computing, BYOD, Big data and data analytics.

Knowledge area	Reference
Current trends: cloud, mobile, Big data and data analytics	7.1 to 7.7

5.13 Post-implementation reviews of application systems

Knowledge area	Reference
Post implementation review	8.3

5.14 Auditing SDLC processes

Knowledge area	Reference
Auditing software development process	8.1 to 8.6

SECTION 2: CONTENTS

CHAPTER 1: SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) INTRODUCTION AND CONCEPTS

Learning objectives

After completion of this chapter you should have conceptual clarity on the basic concepts of System Development Life Cycle (SDLC), how SDLC has changed over a period of time due to changes in technology and environment and how this has led to inclusion of additional phases in SDLC. This chapter covers:

- Traditional SDLC phases and overview of the main activities;
- Additional phases due to availability of outsourcing and generic customizable software; and
- Steps added in different phases due to security requirements (Secure SDLC or SSDLC).

1.1 Introduction

In the present era, the critical need for Information Technology (IT) can be understood from the need to plan and develop safe, secure, and reliable system solutions using information systems which form the backbone for developing innovative product offerings and services. Information systems also play a key role in performing short and long term management functions and activities. There is also greater need to ensure appropriate level of security when developing information systems so as to establish appropriate privacy and protection practices and to develop acceptable implementation strategies for these practices. The SDLC methodology is designed to satisfy these needs by establishing procedures, and practices governing the initiation, definition, design, development, deployment, operation, maintenance, enhancement, and retirement of automated information systems.

If information is the currency of the current century then information systems provide the edifice for designing and deploying information technology for implementing organisation processes which improve efficiency and effectiveness of business functions. Organisations use Information systems to perform various business functions such as processing of business transactions, providing information for decision-making, resolve recurring issues, assisting senior management in designing strategy, linking information with corporate data. Applications systems represent the synergy of human, IT hardware and software. IT has been continuously developing at a rapid pace but the most important aspect for use of IT is human know-how and the use of ideas to harness IT to perform the organisation processes, tasks and activities. The process of developing application software to achieve functional objectives is called 'system development'. Due to dynamic changes in requirements, these systems may require regular update and maintenance to address these

changes and finally at a point in time, these must be replaced, i.e. retired with new system. Hence, it is said to follow a life cycle.

1.1.1 Objectives of SDLC approach

- Deliver quality systems which meet or exceed customer expectations and within cost estimates.
- Develop quality systems using an identifiable, measurable, and repeatable process.
- Establish an organisational and project management structure with appropriate levels of authority to ensure that each system development project is effectively managed throughout its life cycle.
- Identify and assign the roles and responsibilities of all affected parties including functional and technical managers throughout SDLC.
- Ensure that system development requirements are well defined and subsequently satisfied.
- Provide visibility to the functional and technical managers for major system development resource requirements and expenditure.
- Establish appropriate levels of management authority to provide timely direction, coordination, control, review, and approval of the system development project.
- Ensure accountability structure and mechanism for project management.
- Ensure that projects are developed within current and planned IT infrastructure.
- Identify project risks early and manage them before they become problems.

1.1.2 Steps of Systems development

An information system undergoes following steps of development: (Figure 1.1)

- Conceptualization
- Feasibility
- Design and development
- Testing
- Implementation
- Use
- Retirement(replacement)

The stages from conception to retirement of an information system are said to undergo a life cycle. With availability of readymade products and availability of outsourcing options, the design, development and testing phases have undergone changes.

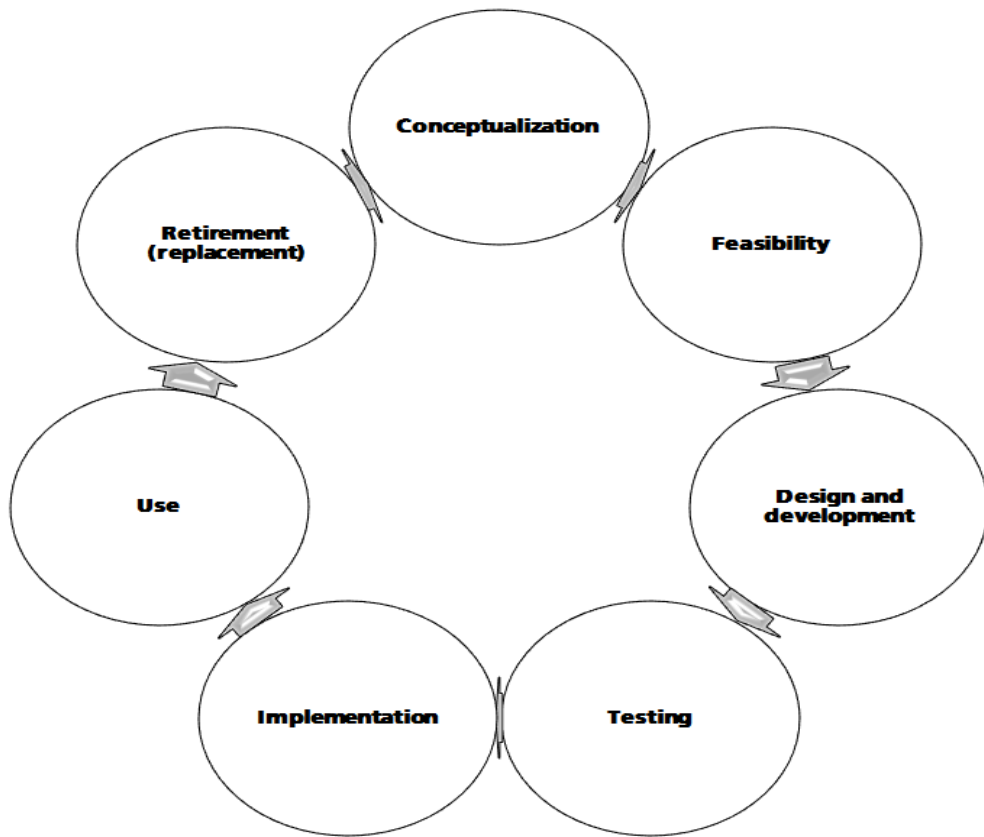


Figure 1.1: Application life cycle

Current trends and threats scenarios have impacted System Development leading to consideration of security in the various phases of SDLC. This is referred to as Secure SDLC and involves additional step in each phase of SDLC requiring consideration of security aspects in each of the phases. This chapter covers key activities of each phase and provides overview of each of the steps. The detailed explanation of the phases and steps are covered in ensuing chapters.

1.1.3 Organisation of chapters

The chapters (1 to 6) in Section 2 of this module are organized as per the logical sequence in which an SDLC project is typically executed in an organisation.

Chapter 1 provides the basic information about SDLC that is required for IS auditor and project manager involved in SDLC activities. The chapter tries to answer why it is called life cycle? What are typical activities or phases through which development happens? These activities have undergone changes over a period of time and hence knowledge about these changes and security requirements in SDLC are covered.

Chapter 2 focuses on actions organisations need to take relating to when to initiating SDLC project. This covers initial phases of SDLC including feasibility study, requirement definition, expected benefits to organisation and developing business case for SDLC project. Decision about execution of next phases is based on business case and hence it necessary to understand these activities. Phase 1 feasibility study and Phase 2 requirement definition of typical SDLC phases (discussed in chapter 1) are covered in this chapter (2).

Chapter 3 provides the basic knowledge on project management with focus on SDLC. Once the organisation has decided to initiate project for automated solution using SDLC, IS auditor may be involved in reviewing this. Hence, IS auditor needs to have knowledge about SDLC project management activities. The details of Phase 3 and 4 of a typical SDLC which were discussed in chapter 1 are explained. This chapter does not cover general project management concepts but focuses on project management practices required for executing SDLC project.

Chapter 4 introduces models and methods used for system design and development that go together. To ensure that final system meets business requirements, project manager and system analyst has to choose the right development method for new application. IS auditor has to know key characteristics, strength and weaknesses of these methods. All these methods have the common objective of application development with many steps being similar.

Chapter 5 discusses software acquisition and outsourcing of development. In case organisation has decided to purchase the software then phases 3, 4 and 5 of typical SDLC are not applicable for the organisation. However, the accountability of actions cannot be outsourced. Hence, the organisation has to provide necessary inputs on controls to be implemented in the application.

Chapter 6 provides information on testing, UAT, implementation and support and operation activities which are covered in phases 6 to 9. Once the application is ready to be implemented whether it is developed or acquired, it must be implemented across the organisation using steps outlined in phases 6 to 9 to derive the benefits.

Chapter 7 discusses what IS auditor has to know about new trends in IT deployment and its impact on SDLC.

Chapter 8 provide basic and high-level information on auditing of SDLC project.

1.2 Concepts of SDLC

1.2.1 When is SDLC initiated?

The need for business development or acquisition of new applications may arise due to following situations:

- New service delivery opportunity that relates to a new or existing business process (e.g. e-commerce);

- Issues and problems with an existing systems/business process (complaints from customers/users);
- Change in strategic focus leading to an opportunity that will provide benefits to the organisation (Mergers and acquisitions, or new service delivery channels like ATM for banks);
- New opportunity due to advancement of existing technology or availability of new technology (e.g. use of mobile technology for banking services); and
- Use of automation by competitors to enhance quality of services.

All of these situations directly affect the business drivers. Business drivers can be defined as the attributes of a business function (service delivery) that arise out of strategic objectives to enhance targets and goals of business function to achieve the strategic business goals. In other words business objectives defined by strategy gets translated into drivers for business operations which require new application software or upgrading of existing application software. This results in initiating an SDLC project.

Business application system/software is designed to support a specific organisational service, function or process, such as inventory management, payroll, market analysis or e-commerce. The goal of an application system is to turn data into information. System development involves developing or acquiring and maintaining application systems which are used for various day-to-day business activities. These business activities are called as Business Processes and they process data of relevant business processes.

1.2.2 What is SDLC?

SDLC refers to the process of examining a business situation with the intent of improving it through better procedures and methods. This is required when there is need to change business processes due to requirements arising out of customers/stakeholders expectations and business strategy. These changes are generally attributed to need to automate the service delivery using information and related technology. System development involves developing or acquiring and maintaining application systems that are used for various day-to-day business process activities. Generally these system processes data of business transactions.

A standard set of steps used for developing systems is called a SDLC. SDLC generally uses various methods depending upon the type and nature of application. For example a batch processing application that processes historical data to generate reports for management's information may use a model where activities are performed one after another (waterfall model), where as if there is no clear understanding of what functions can be automated, an iterative (spiral) model may be used. *(These models are discussed in detail in chapter 4)*. Similarly, depending upon the availability of skilled resources, the development team may adopt different methodology for developing software.

1.2.3 Business Application System

Business application system, also called application software, is designed to support a specific organisational function or process, such as inventory management, payroll, or market analysis. The goal of application system is to turn data into information. For example, software developed for the inventory department at a bookstore may keep track of the number of books in stock for the latest bestseller. Application system for the payroll department may keep track of the changing pay scales of the employees.

System development involves developing or acquiring and maintaining application systems which are used for various day-to-day business activities. These business activities are called as business processes and they process data. The effective management and control of this system development is critical as the business systems process and control information assets of the organisation. The use of a standard set of steps to develop and support business applications is called Systems Development Methodology. **It is important to remember that the terms SDLC and SDM are often used interchangeably.**

1.3 Typical phases of SDLC

Typically a SDLC consists of phases as shown in figure 1.2. Although these phases are common for any SDLC model, the way these are executed vary for each model. Although figure 1.2 is titled as 'SDLC'; this does not cover the last two phases shown in figure 1.1 i.e. using the application and retirement or replacement of application. System Development life cycle is a sequence of activities performed by group of users and IT development experts. These set of activities are grouped together to form phases and generally each phase has predetermined set of deliverables and/or a milestone to be reached.

The number of phases might vary for each SDLC project depending upon milestones and/or deliverables. For example: if an organisation is developing a software using internal development team, it may not lay much emphasis on user acceptance testing(UAT) and may club this activity with testing phase, whereas in case of outsourced development or acquired software, user acceptance testing (UAT) is a major milestone and has predefined deliverables that are signed off. In the diagram below, considering the criticality of outsourced applications, UAT has been shown as a separate phase.

The concept or idea is starting point where automation of business function using information system is considered from business benefit perspective. For example a bank may decide to launch a new service delivery channel like internet banking, or a store may provide on-line shopping service through internet or an airline may implement a system via information kiosk for user enabled check-in and web check-in for reducing manual process. Once the idea is considered it passes through SDLC phases till it is materialized. Sometimes the concept requires further

investigation (preliminary investigation) before SDLC project is initiated. Preliminary investigation is not considered part of typical SDLC phases but some organisations may include it in SDLC.

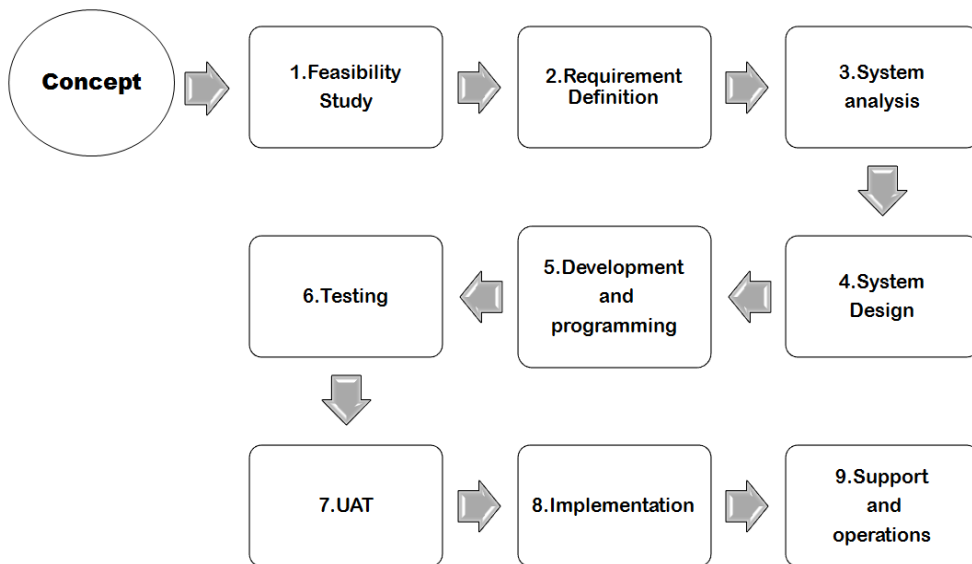


Figure1.2: Typical phases of SDLC process

Phase 1: Feasibility Study

The feasibility study is based on technical, economical and social aspects and this helps in determining strategic benefits of using system. These benefits can be either in productivity gains or in future cost avoidance. The study has to also identify and quantify the cost savings and estimate the probable return on investment. This information is used to building a business case covering both tangible as well as intangible factors such as readiness of the business users and maturity of the business processes. The business case provides justification for proceeding to the next phase and is also used for reviewing progress or evaluating success of SDLC project.

Detailed steps of feasibility study are discussed in chapter 2. The feasibility study shall be different for different application depending upon the expected benefits for the organisation. For example if an organisation intends to implement an application that is already implemented by various organisation of similar type, it may use a generic feasibility study and focus only on the benefits to the organisation, such as providing internet banking services or mobile banking services.

Role of IS Auditor in project initiation and feasibility study phase:

- Review the documentation for the reasonableness.

- Review cost justification/benefits with schedule of when the anticipated benefits will be realized.
- Identify if the business needs used to justify the system actually exist.
- Justification for going for a development or acquisition.
- Review the alternate solutions for reasonableness.
- Review the reasonableness of the chosen solution.

Phase 2: Requirements Definition

This phase involves preparing the statement of intent explaining the problem or the need for new application to provide functional, service and quality requirements of the solution system. The user needs to be actively involved in requirements definition. This involves:

- Studying needs of the users
- Obtaining inputs from employees and managers on their expectations
- Determining information requirements of the users

Several fact-finding techniques and tools such as questionnaires, interviews, observing decision-maker behaviour and their office environment etc. are used for understanding the requirements.

Role of IS Auditor in requirements definition phase:

- Identify the affected users and the key team members on the project to verify that they are having an appropriate representation.
- Review detailed requirements definition document and verify its accuracy and completeness through interviews with the affected and requested user departments.
- Review existing data flow diagrams and other related specifications like forms, data descriptions, output formats, etc., to ensure that they cover the user requirements.

Phase 3: System Analysis

This refers to the process of gathering and interpreting facts, diagnosing problems, and using the information to recommend improvements to the system. Before arriving at new design, one must thoroughly understand existing process/system and map them against new requirements to understand changes and rationale for changes. Analysis is also important to decide upon system design approach. Traditional system development generally adopt a data oriented approach since it had been focused on processing and presenting of business data., However, due to extensive use of technology in modern organisations, the focus now is more on service oriented approach where the objective of the system is to provide services using data models.

Role of IS Auditor in system analysis phase:

- Verify that management has approved the initiation of the project and the cost.

- In case of acquisition, determine that an appropriate number of vendors have been given proposals to cover the true scope of the project and requirements of the users.
- Determine whether the application is appropriate for the user of an embedded audit routine and if so request may be made to incorporate the routine in conceptual design of the system.

Phase 4: Design

This phase takes primary inputs from *phase 1 requirement definition*. Based on the requirements identified, the team may need to finalize requirements by multiple user interactions and establishes a specifications baseline for development of system and subsystem.

These specifications describe:

- Parts of the system
- How they interface
- How the system need to be implemented
- Type of hardware, operating system and other software
- Network facilities
- Program and database specifications
- Security considerations

Additionally, a formal change control process is established to prevent uncontrolled entry of new requirements during development process.

Role of IS Auditor in detailed design phase:

- Review system flowcharts for adherence to the general design
- Review input, processing and output controls have been appropriately included in the system.
- Assess adequacy of the audit trails which provide traceability and accountability.
- Verify key calculations and processes for correctness and completeness.
- Interview users to ascertain their level understanding of the system design, input to the system, screen formats and output reports.
- Verify that system can identify erroneous data correctly and can handle invalid transactions.
- Review conceptual design to ensure the existence of appropriate controls.
- Review quality assurance and quality control results of programs are developed.
- Verify the design for its completeness and correctness and it meets the defined requirements.
- Verify that functional data created during requirement phase is complete and test plans are developed.

Phase 5: Development

Use the design specifications to begin programming and formalizing supporting operational processes of the system. After the system design details are resolved, the resources needs such as specific type of hardware, software, and other services are determined. The choices depend on many factors such as time, cost and availability of skilled resources programmers and testers. The analyst works closely with the programmers. During this phase, the analyst also works with users to develop required documentation for software, including various procedure manuals. In the development phase, the design specifications are converted into a functional system that will work in planned system environment. Application programs are written, tested and documented. Finally this results in development of a fully functional and documented system. A very well coded application program should have the following characteristics:

- **Reliability:** It refers to the consistency with which a program operates over a period of time. However, poor setting of parameters and hard coding of some data subsequently could result in the failure of a program after some time.
- **Robustness:** It refers to the applications' strength to perform operations in adverse situations by taking into account all possible inputs and outputs of a program considering even the least likely situations.
- **Accuracy:** It refers not only to 'what program is supposed to do', but also the ability to take care of 'what it should not do'. The second part is of great interest for quality control personnel and auditors.
- **Efficiency:** It refers to the performance per unit cost with respect to relevant parameters and it should not be unduly affected with the increase in input values.
- **Usability:** It refers to a user-friendly interface and easy-to-understand internal/external documentation.
- **Readability:** It refers to the ease of maintenance of program even in the absence of the program developer.

Some key aspects of development:

1. **Program Coding Standards:** The logic of the program outlined in the flowcharts is converted into program statements or instructions. For each language, there are specific rules concerning format and syntax. Syntax means vocabulary, punctuation and grammatical rules available in the language manuals that the programmer has to follow strictly and pedantically. Different programmers may write a program using different sets of instructions but each giving the same results. This might create a problem for changes to be done to the program which has been written by another programmer. Therefore, the coding standards are to be defined so as to serve as a method of communication between teams, amongst the team members and users resulting in better controls. Coding standards minimize the system development

issues due to programmer turnover. These standards provide simplicity, interoperability, compatibility, efficient utilization of resources and reduce processing time.

2. **Programming Language:** Depending upon the development approach, the analyst decides the programming language to be used. Application programs are coded in the form of statements or instructions and the same is converted by the compiler to object code for the computer to understand and execute. The programming languages commonly used are:
 - High level general purpose programming languages such as COBOL and C;
 - Object oriented languages such as C++, JAVA etc.;
 - Scripting language such as JavaScript, VBScript; and
 - Decision Support or Logic Programming languages such as LISP and PROLOG.

The choice of a programming language may depend on various pertinent parameters. In general, language selection may be made on the basis of application area; algorithmic complexity; environment in which software has to be executed; performance consideration; data structure complexity; knowledge of System Development staff; and capability of in-house staff for maintenance.

Role of IS Auditor in development phase:

- Ensure that documentation is complete.
- Review QA report on adopting coding standards by developers.
- Review the testing and bugs found are reported and sent for rework to developers.

Phase 6: Testing

Before the information system can be used, it must be tested. Systems testing are done at various stages during development till implementation. There are primarily two types of testing:

1. Quality assurance testing includes unit testing, interface testing, integration testing and peer reviews.
2. User acceptance testing (UAT) also known as final acceptance testing (next phase).

Testing primarily focuses on ensuring that the software does not fail i.e. it will run according to its specifications and in the way users expect. Special test data are input for processing and the results are examined against predetermined output. If it is found satisfactory, it is eventually tested with actual data from the current system. (*Testing is discussed in more detail in chapter 6*)

Role of IS Auditor in testing phase:

- Review the test plan for completeness and correctness.
- Review whether relevant users have participated during testing phase.
- Review error reports for their precision in recognizing erroneous data and for resolution of errors.

- Verify cyclical processes for correctness(example: year-end process, quarter-end process)
- Interview end-users of the system for their understanding of new methods, procedures and operating instructions.
- Review the system and end-user documentation to determine its completeness and correctness.
- Review whether reconciliation of control totals and converted data has been performed to verify the integrity of the data after conversion.
- Review all parallel testing results.
- Test the system randomly for correctness.
- Review unit test plans and system test plans to determine that tests for internal control are addressed.
- Verify that the system security is functioning as designed by developing and executing access tests.
- Ensure test plans and test results are maintained for reference and audit

Phase 7: User acceptance testing (UAT) or final testing

Establishes the actual operation of the new information system, with the final iteration of user acceptance testing and user sign-off. Organisation may consider going for a certification and accreditation process to assess the effectiveness of the business application. This provides assurance to the management about:

1. Mitigating risks to an appropriate level.
2. Providing accountability over the effectiveness of the system in meeting objectives.
3. Establishing an appropriate level of internal control.

UAT supports the process of ensuring that the system is production-ready and satisfies all documented requirements. The methods include:

- Definition of test strategies and procedures.
- Design of test cases and scenarios.
- Execution of the tests.
- Utilization of the results to verify system readiness.

Acceptance criteria are defined so that a deliverable satisfies the predefined needs of the user. A UAT plan must be documented for the final test of the completed system. The tests are written from a user perspective and should test the system in a manner as close to production as possible. For example, tests may be based around typical pre-defined, business process scenarios. If new business processes have been developed to accommodate the new or modified system they should also be tested at this point. A key aspect of testing should also include testers seeking to verify that supporting processes integrate into the application in an acceptable manner. Successful completion would generally enable a project team to hand over a complete integrated package of application and supporting procedures.

Ideally, UAT should be performed in a secure testing or staging environment. A secure testing environment where both source and executable code are protected helps to ensure that unauthorized or last-minute changes are not made to the system without going through the standard system maintenance process. The nature and extent of the tests will depend on the magnitude and complexity of the system change.

Test plan, data and results are to be maintained for subsequent audits.

Phase 8: Implementation

This involves roll out of the application which has been developed or acquired for the business function based on the current state. The approach for implementation will be decided based on this state. One of the following approaches may be adopted: (This is *discussed in more detail in chapter 6*)

1. **Cut-off:** Where old system/process is discontinued and new application is made live (operational).
2. **Phased implementation:** Where new application is started in logical phases for different functions.
3. **Pilot:** Where a part function is implemented using new application and based on result either phased or cut-off approach is followed.
4. **Parallel:** Where both the old and new system run simultaneously and based on problem resolution and reliability of processing by the new system, the old system is discontinued.

Role of IS Auditor in implementation phase:

- Ensure test plans, test data and test results are maintained for reference and audit.
- Determine that the formal acceptance has been signed by the project development team, user management, quality assurance, security professional or auditor.
- Verify that the system has been installed according to the organisation's change control procedures.
- Review programmed procedure used for scheduling and running the system along with the system parameters are used in executing the production schedule.
- Review all system documentation to ensure its completeness and verify whether all recent updates from the testing phase have been incorporated.
- Verify that data conversion is correct and complete and is confirmed by the respective user departments before the system is implemented and final user sign-off is obtained.

Phase 9: Support and operations

This is the post-implementation stage following the successful implementation of a new or extensively modified system. This requires, implementation of a formal process that:

1. Provides support and assistance to users in smooth operations and end-user management.
2. There is a mechanism to record, review and implement deficiencies and future changes required.
3. Assess adequacy of the system and projected ROI measurements as per business case.
4. Update project management process based on lessons learned and recommendations for future projects regarding system development.

Role of IS Auditor in maintenance and post implementation phase:

Sufficient time should be allowed before post implementation review for the system to stabilize in the live environment. Then only there may be significant problems would have been surfaced.

- Determine that the systems objective requirements were achieved
- Determine if the cost benefits identified in the feasibility study are being measured.
- Review the required controls have built into the system to ensure that they are operating as designed.
- Review error logs to determine if there is any resource or operating problems inherent with the system. Logs may indicate the inappropriate planning or testing of the system prior to implementation.
- Review input and output control balances and reports to verify that system is processing data correctly and completely.
- Evaluate adequacy of procedures for authorizing, prioritizing and tracking system changes.
- Identify system changes and verify that appropriate authorization was given to make the change in accordance with organisational standards.
- Review permanent program documentation to ensure that evidence (audit trail) is retained regarding program changes.
- Evaluate adequacy of the security access restrictions over production source and executable modules.
- Evaluate adequacy of the organisation's procedures for dealing "emergency" program changes.
- Evaluate the adequacy of the security access restrictions over the use of the "emergency" logon-ids.
- Verify existence and adequacy of the records for system changes.
- Evaluate adequacy of the access protection of the maintenance records.

1.4 Changes in SDLC phases

With changing technology and outsourcing practices, the concept of in-house development is slowly phasing out. Organisations prefer outsourcing to get benefit of skills and experience and this also helps management in focusing on core business. These changes in environment require introduction of additional phases to traditional typical SDLC phases.

Introduction of a decision on Make or Buy

Organisations may choose either to develop the software in-house or may opt for buying an available product from market. This is based on analysis performed during first 2 phases, which takes into consideration 'what is being done in industry? Based on this information, organisation may choose one of the following three options:

1. Develop software using in-house resources.
2. Hire a third party vendor to develop the software (i.e. outsource software development)
3. Purchase customizable software that is available in market.

Depending upon the decision, organisation follows different path for phases 3 to 6. Figure 1.3 shows these phases for all three decisions. *(Some aspects of phase 3B and 3C are discussed in more details in chapter 5)*

If an organization is purchasing or outsourcing the software development, they still need to follow SDLC. Although SDLC refers to Software development, the phases 1, 2, 7, 8 and 9 remains the responsibility of organization. In case organizations miss out any of the steps, impact will be higher. For example, if organization misses out identifying key requirements, the purchased or outsourced software may not provide required functionality. Further, making changes after implementation is always costly and time consuming. Similarly if testing is not performed meticulously, software implemented may have bugs.

Phase 3B: Outsource the application development

Organisation may hire a third party firm having necessary skills and experience to develop software specifically for organisation's use. The third party typically follows the phases 3 to 6 for actual development of software. However, the organisation that hires the firm follows phases 3B to 6B. In this situation hiring organisation focuses on requirements for automating the functional processes rather than development model and methodology, but may indicate or stipulate fully or partially preferences. Organisation may follow standard process for selection of third party based on requirements and risk assessment.

Phase 3C: Select and Purchase software available in market

The organisation may select and purchase standard software available in the market (For example, SAP or Core Banking solution or standard accounting software) and configure it as per organisation's requirements. In this case the purchaser does not have control on phases 3 to 6 and must follow entirely different steps to ensure that objectives are achieved.

These phases are described as 3C to 6C. Organisations generally map the available products against the requirements and identify the gaps based on the following criteria:

- If required functionality is not available, can this be configured?
- If required functionality cannot be configured, is it possible to implement a work around?
- Is additional functionality available which was not considered in the requirements?

Based on gap analysis and subsequent availability of maintenance and support (Phase 9) organisation selects the software to be purchased.

Phase 4B: Requirement finalization

Based on vendor risk assessment, an RFP is forwarded to select vendors along with functional, operational, hardware, software, support and maintenance requirements. Once a vendor is selected, vendor may want to finalize and baseline the requirements so as to ensure that the efforts and associated commercials are appropriate. This is very important since there is always a possibility of changing the requirements during development. Many times these changes may require rework and efforts might go waste, affecting commercials and project timelines. Hence it is better for both to agree upon the scope and method to deal with changes required when the project is in development stage itself. The organisation floating the RFP is responsible for deciding requirements.

Phase 4C: Request for Proposal (RFP)

Based on the gap analysis results, RFP is forwarded to the suppliers of system to be purchased. In addition to the functionality requirements, it also includes operational, support and technical requirements, and these, together with considerations of the suppliers' financial viability and provision for escrow, will be used to select the system that best meets the organisation's total requirements.

Phase 5B: Contract and SLA

Based on agreed upon requirements a contract containing service levels is drafted and executed by organisation and vendor. This contract generally covers project timelines, deliverables, monitoring development progress, change management (method to handle scope creep), vendor's responsibility for support and maintenance, ownership of software design, data and source code and method for arbitration in case of disputes.

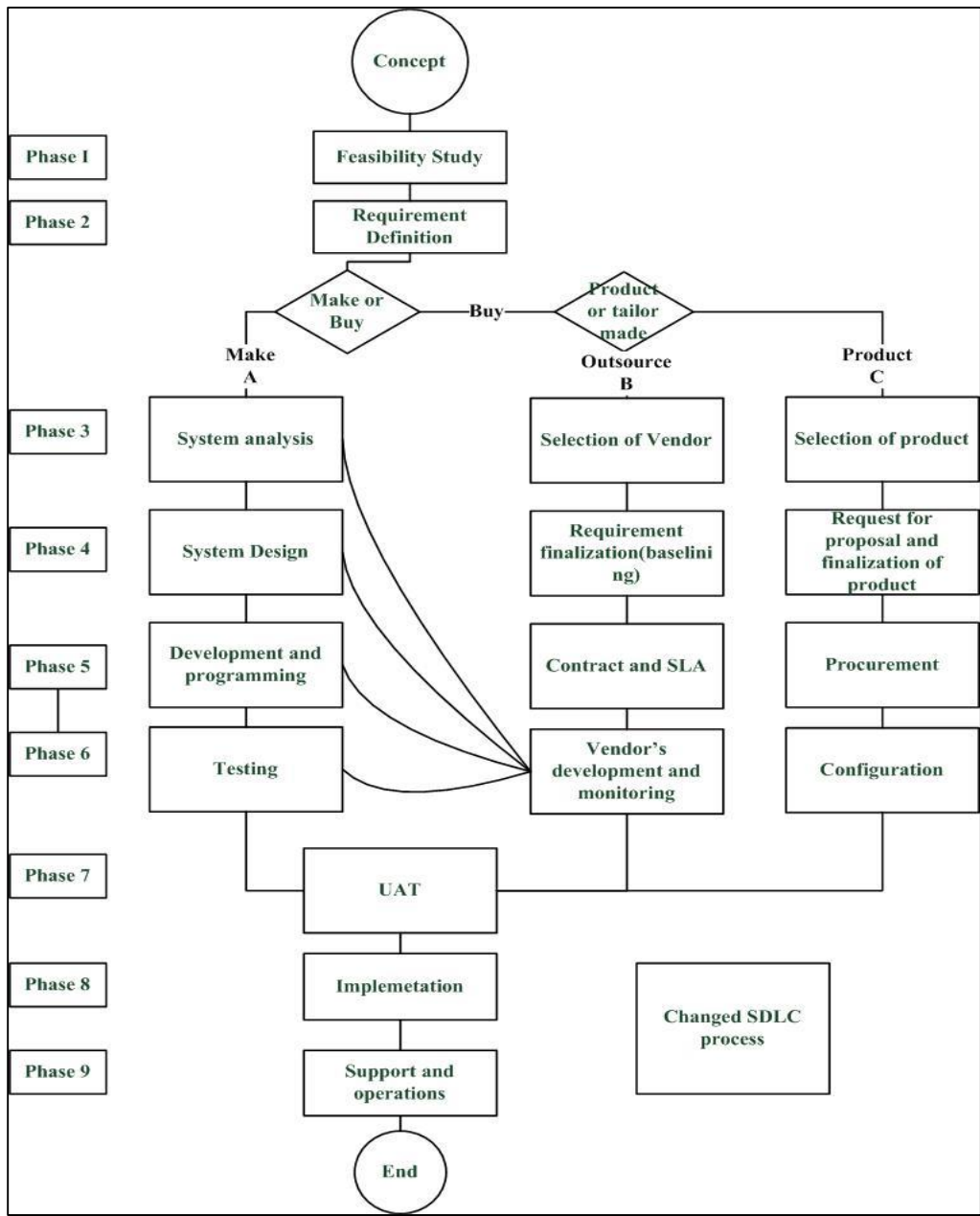


Figure 1.3: Changed SDLC phases

Phase 5C: Purchase

A formal contract for purchase of software is executed which may include cost of software, usage of licenses, implementation support, configuration support, user training, helpdesk and maintenance levels to be provided by the vendor.

Phase 6B: Vendor development and monitoring

During this phase vendor executes development phases described in 3A, 4A, 5A and 6A. Organisation should implement a mechanism to monitor development progress to ensure that project is on time. This includes appointing a single point of contact and reporting mechanism by vendor.

Phase 6C: Configuration (purchased systems)

This involves configuring the system (if it is a packaged system) to tailor it to the organisation's requirements. This is best done through the configuration of system control parameters, rather than changing program code. Modern software packages are extremely flexible, making it possible for one package to suit many organisations simply by switching functionality on or off and setting parameters in tables. There may be a need to build interface programs that will connect the acquired system with existing programs and databases.

Note: Outsourcing development or purchasing and configuring software might reduce the software development efforts, but introduces vendor management and monitoring efforts and also managing risks associated with outsourcing.

Changes in Phase 7: UAT

Although packaged systems are tested by the vendor prior to distribution, these systems and any subsequent changes should be tested thoroughly by the end user and the system maintenance staff. These supplemental tests will help ensure that programs function as designed by the vendor and the changes do not interact adversely with existing systems. In the case of acquired software, after attending to the changes during testing by the vendor, the accepted version should be controlled and used for implementation. In the absence of controls, the risk of introducing malicious patches/Trojan horse programs is very high.

Changes in Phase 9: Support and operations from vendor need to be part of contract executed with vendor.

1.5 Secure SDLC

Earlier security was an afterthought for SDLC; normally developers used to check the security related aspects through penetration testing, which requires a lot of rework. For example, if a security related vulnerability, bug or flaw is detected after development then correction of the same will require re-examining all the aspects starting from requirements till coding. This entire exercise will increase the cost and efforts of the project, which sometimes may create a typical situation both for the client and development company. To overcome this issue, latest research studies suggest that the security should be incorporated right from the beginning in the SDLC. Information security trends indicate that embedding security within application development helps in addressing various issues may arise subsequently. For example, when multiple users are expected to access application hosted at central location from different nodes, the application should be able to provide access depending upon the function the specific users has to perform. This requires developers have to design role definition and providing functionality for assigning these roles to different users as defined.

Another example can be in case the application is developed using web based technologies and users are expected to access it using different browsers (like internet explorer, Google chrome etc.), application may not depend upon users to secure their browsers, but embed security within application. In case application is hosted on internet, it is subject to various application level attacks that need to be closed by adopting secure development and coding practices.

The following table describes the additional steps that need to be added to the traditional SDLC phases to make it Secure SDLC.

Table 1.1: Security steps in various phases of SDLC

SDLC Phase	Security Steps
Requirement Definition	To identify security requirements including compliance for privacy and data loss. To determine risks associated with security and prepare mitigation plan. To train users on identification and fixing of security bugs.
Design Phase	To ensure security requirements are considered during design phase e.g. access controls for privacy sensitive data. To identify possible attacks and design controls e.g. implementing least privilege principle for sensitive data, and apply layered principle for modules.
Development Phase	To develop and implement security coding practices such as input data validation and avoiding complex coding. To train developers on security coding practices.

Testing Phase	To review code for compliance of secure coding practices. To develop test cases for security requirement testing. To ensure security requirements are tested during testing. To test application for identified attacks.
Implementation Phase	To analyze all functions and interfaces are secured. To perform security scan of application after implementation.
Maintenance Phase	To monitor for vulnerabilities on a continuous basis, To issue the patches for fixing the reported vulnerabilities, accordingly, To evaluate the effectiveness of countermeasures periodically.

1.6 Risk associated with SDLC and mitigation planning

Organisation requiring new software or changing the software initiate a project. The risks of SDLC are:

1. Risks associated with project management (discussed in chapter-3: project management)
2. Risks associated with SDLC: It is necessary to know these risks prior to undertaking SDLC projects. The objectives are to:
 - Identify risks based on business requirements
 - Discovering methods to respond to risks (accept, avoid, mitigate, transfer)
 - Accepting residual risk and going ahead with the project

Some of the SDLC risks (apart from project risks, which are discussed separately) are:

- Inaccurate requirements definition.
- Inappropriate selection of platform (hardware, operating system, database).
- Compromise on quality and testing resulting in bugs after implementation
- Missing or inadequate or incomplete documentation.
- Absence of skilled resources.
- Scope creep (changing requirements).
- Poor coding techniques.
- Inadequate QA and QC (including testing inadequacies)
- Lack of proper change control and controls over promotion into production
- Inappropriate processes for development.
- Technical vulnerabilities and how these could materialize and are to be controlled or addressed.

In order to mitigate risks on time, it is best to perform risk assessment during each phase of SDLC. In case of outsourcing and/or purchased software the risk associated with outsourcing and vendor management have to be managed by the organisation.

Mitigation of risks identified need to be planned during project planning and implemented during each phase of SDLC. Possible mitigation plans for risks listed above are given in table 1.2 below.

Table 1.2: SDLC Risk and Mitigation plan

Risk	Mitigation plan
Inaccurate requirements definition	Select prototyping model to finalize the requirements. Meet various stake holders to confirm identified requirements.
Inappropriate selection of platform (hardware, operating system, database etc.)	Understand technical and performance requirements (e.g. user response time, number of transactions per second etc.) and determine technical specification of proposed platform. In case platform specifications are available (existing hardware); ensure that application development can address requirements. Understand organisation baseline for infrastructure and incorporate in design.
Compromise on quality and testing resulting in bugs after implementation	Ensure standard coding practices are adopted. Provide enough time for building test cases to cover all function, performance and security requirements. Build test cases along with design.
Missing or Inadequate or incomplete documentation	Ensure completion of documentation along with design and development. Standardization of coding practice helps in this process Ensure documentation experts and technical writers are part of team.
Absence of skilled resources	Consider outsourcing or hiring skilled resources on contract.
Scope creep (changing requirements)	Perform scope base lining. Introduce change management process to evaluate and adopt changes in requirements.
Poor coding techniques or inadequate documentation	Develop and implement standard coding practices.
Inadequate QA and QC(including testing inadequacies)	Plan QA process along with project and development plan. Implement standard coding practices. Implement performance monitoring process.
Lack of proper change control and controls over promotion into production	Perform scope base lining. Introduce change management process to evaluate and adopt changes in requirements

Inappropriate processes for development	Understand requirements and select appropriate development method suitable for identified requirements.
Technical vulnerabilities	Ensure integration and system testing is performed on target platforms.

1.7 Roles and responsibilities of SDLC

There are certain standard functions (not designations) performed by individual resources during the SDLC process. These roles may be combined, especially for small organisations and some roles may be performed by one individual. Under such cases, IS Auditor has to evaluate conflicts between the roles (segregation of duties). The roles are listed here in brief: (Table 1.3)

Table 1.3: SDLC Roles and Responsibilities

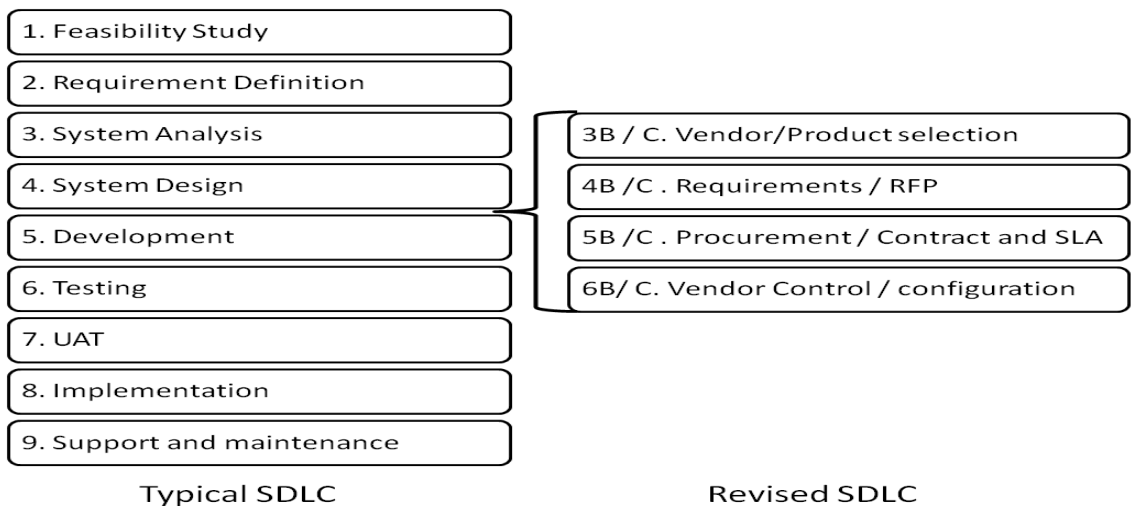
Role	Function
Steering Committee	A steering committee is set up to approve, supervise and direct IT projects, including SDLC. This committee provides overall direction and monitors progress of all IT projects including SDLC projects.
Program Manager	Responsible for all projects that are associated with large IT related program. E.g. Implementation of ERP across many locations of an organisation. A program consists of multiple projects.
Project Manager	A project manager is normally responsible for more than one project and liaisons with the client or the affected functions. This is a middle management function. The Project manager is responsible for delivery of the project within the time and budget.
Systems Analyst	The system analyst also has a responsibility to understand existing problem/system/data flow and new requirements. System analysts convert the user's requirements in the system requirements to design new system.
Module Leader/Team Leader	A project is divided into several manageable modules and the development responsibility for each module is assigned to module leaders.
Programmers	Programmers convert design into programs by coding using programming language. They are also referred to as coders or developers.
Database Administrator (DBA)	The data in a database environment has to be maintained by a specialist in database administration so as to support the application program. The database administrator handles multiple projects; and ensures the integrity and security of information stored in the database.

Role	Function
Quality Assurance Team	This team checks compliance with the SDLC related standards (Documentation, Coding standards, Security requirements etc.) set by the organisation, by project teams on a periodic basis.
Testers	Testers are junior level quality assurance personnel attached to a project. They test programs and subprograms as per the plan given by the module / project leaders and prepare test reports.
Domain Specialist	Whenever a project team has to develop an application in a field that's new to them, they take the help of a domain specialist, who understands the business requirements and helps system analyst, designer and programmer in understanding the requirements.
Technology Specialist	IT is developing so rapidly that even IT professionals find it difficult to keep track of all developments, let alone develop expertise. This has resulted in experts in specific technology areas, such as Microsoft technology, Web-enablement and the like.
Documentation Specialist	These professionals are responsible for the creation of user manuals and other documentation.
IS Auditor	As a member of the team, IS auditor can ensure that controls required for process for which application is being developed are included in requirements. IS auditor would be involved in design stage to ensure that the required controls have been included at the design stage.

1.8 Summary

SDLC is an essential aspect of automating business processes using information technology. It has been evolving with changing technology and global proliferation of computers. Today's business heavily depends on IT and any problem faced has multi-fold repercussions. Controlling SDLC process helps organisations in mitigating risks associated with implementation and use of IT. An IS auditor must be aware of phases and key steps of each of the SDLC phases. Although there are various models and methods (Discussed in detail in chapter 4) the basic process discussed in this chapter are common for any model or method used. An IS auditor while auditing SDLC process is not expected to be an expert in all technologies but should always focus on associated risks, assessment of these risks and assess whether the implemented solutions are as per the business objectives.

SDLC phases discussed above are represented as below for easy reference.



1.9 Questions

1. System development life cycle (SDLC) primarily refers to the process of:
 - A. Developing IT based solution to improve business service delivery.
 - B. Acquiring upgraded version of hardware for existing applications.
 - C. Redesigning network infrastructure as per service provider's needs.
 - D. Understanding expectations of business managers from technology.
2. Organizations should adopt programming/coding standards mainly because, it:
 - A. Is a requirement for programming using high level languages.
 - B. Helps in maintaining and updating system documentation.
 - C. Is required for security and quality assurance function of SDLC.
 - D. Has been globally accepted practice by large organizations.
3. Which of the following is main reason to perform User acceptance testing (UAT)?
 - A. To train and educate users on features of new solution.
 - B. To confirm form users that solution meets requirements.
 - C. To complete formality of sign-off to mark end of project.
 - D. To finalize the implementation plan for new IT solution.
4. An organization decided to purchase a configurable application product instead of developing in-house. Outcome of which of the following SDLC phase helped organization in this decision?
 - A. Requirement definition
 - B. Feasibility Study
 - C. System analysis
 - D. Development phase

5. In which of the following phases of SDLC, controls for security must be considered FIRST?
- A. Requirement definition
 - B. Feasibility study
 - C. System design
 - D. Implementation
6. IS auditor has been part of SDLC project team. Which of the following situation does not prevent IS auditor from performing post implementation review? The IS Auditor has:
- A. designed the security controls.
 - B. implemented security controls.
 - C. selected security controls.
 - D. developed integrated test facility.

1.10 Answers and Explanations

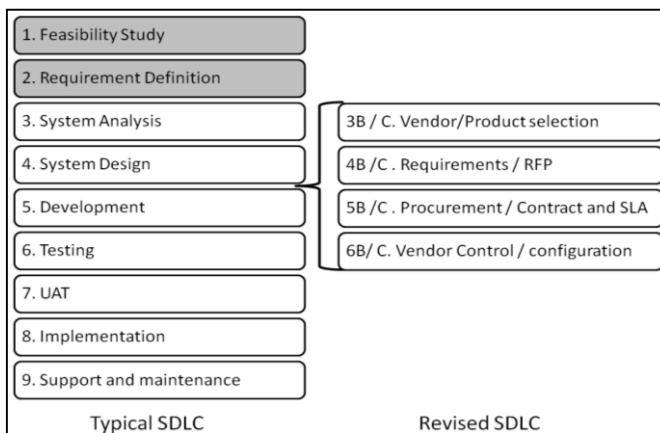
1. A. SDLC primarily focuses on identifying IT based solution to improve business processes delivering services to customers. Other activities may be part of SDLC however, these are IT projects not SDLC projects.
2. C. Adopting coding standards helps organization in ensuring quality of coding and in minimizing the errors. It also helps in reducing obvious errors which may lead to vulnerabilities in application. A is not true since it is required for all languages, B is partially true but is not main reason. D is not main reason.
3. B. UAT is mainly conducted to confirm from the users and application owners that application meets their requirements. Sign-off is a formality to be completed only if requirements are met. Training and implementation planning are different activities which are not dependent on UAT.
4. B. Make or buy decision is the outcome of feasibility study where technical, economical and social feasibilities are considered.
5. A. Security requirements must be considered during requirement definition. However, the nature of controls to be implemented for security must be considered first during design phase. This will ensure that necessary security controls are built while developing application. Security controls are implemented and not designed during implementation phase.
6. D. Active role of IS auditor in design and development of controls affects the independence. Hence, IS auditor cannot perform review or audit of the application system. However, developing integrated test facility within application is not a control, but a facility to be used by auditors in future. Hence, this does not impact independence of IS auditor.

CHAPTER 2: INITIATING SDLC

Learning Objectives

This chapter outlines the steps an organisation follows while initiating a SDLC project. These steps involve understanding of pain points and triggers, conducting feasibility study, analysing benefit realization, preparing business case for management approval and finalizing requirements. These steps help organisations in deciding whether to develop or acquire the software solution.

2.1 Introduction



This chapter primarily provides information on phase 1 Feasibility study and Phase 2 requirement definition, of typical SDLC (shadowed area). It also discusses the relevant information required to execute these phases within organisation.

Feasibility study focuses on analyzing the economic,

technical and social aspects of new IT based solution based on requirement definitions and the benefits to be derived from such implementation.

2.1.1 Drivers, pain points and triggers

Use of information technology has prompted organisations for automating data intensive service delivery processes. Initiatives for automation are considered based on business priorities and requirements. These priorities that prompt for selection of automation initiatives are called drivers for initiating SDLC. When there are multiple requests for initiating SDLC projects, organisations may need to prioritize based on the pain points, triggers and the expected benefit realization.

Pain points

Given below are some of the pain points an organisation may be facing which lead to initiating SDLC process:

- Increasing customer complaints related to service delivery.

- Decreasing level of user satisfaction.
- Loss of business opportunities.
- Problems with existing technology.
- Major changes required in current application.
- Obsolescence of technology affecting service delivery.

Triggers

Pain points and triggers prompt organisations to initiate a SDLC process. Examples of such triggers are:

- Competitors using technology for providing better products or services.
- Increasing market demands.
- Strategic policy changes targeting business growth.
- Availability of technology facilitating new service delivery channels.
- Acquisitions and mergers requiring integration of technology.

2.2 Feasibility study

Feasibility Study refers to evaluating the proposed solution for automating the business process using information technology. It is a process to arrive at a decision, whether the proposed IT solution will deliver business value to the organisation through the IT enabled investments. A feasibility study is generally carried out using various parameters such as technology, direct and indirect investments, expected value materialization period, social acceptability, compliance requirements etc. The feasibility study of a system considers following dimensions:

- **Technical:** Availability of technology for automation.
- **Economic:** Required investments against expected benefits and time required for return on investments.
- **Schedule/Time:** The time required to implement solutions or to go to market.
- **Resources:** Availability of resources like skilled personnel, technology, power and if not available, can they be made available and at what cost?
- **Operational:** The expected improvement in efficiency of service delivery to customers and stakeholders after implementing solution.
- **Social:** Perceived impact on work-life balance on employees.
- **Compliance:** Evaluation benefits of adverse impact on compliance requirements due to proposed solution.

2.2.1 Technical Feasibility

This refers to review of availability of technology and impact of expected obsolescence in future. For example, an organisation which currently deutes its employees to various training courses

now proposes to automate training solutions and provide them via intranet portal hosted in-house. The technical feasibility includes evaluation of the following factors:

- Can the solution work on existing infrastructure or does organisation need to acquire new hardware or software? If currently the organisation is not using an automated solution, they may have to invest in acquiring technology and solution.
- Will the proposed system provide adequate responses to inquiries, regardless of the number or location of users? Currently there are many organisations that have deployed such solutions and hence we can conclude that the technical solutions can be made available to meet the response requirements.
- Is system scalable and can it handle the expected business and data growth? There are multiple training courses and those can be deployed using scalable infrastructure.
- Does the technology offer adequate security? Those requirements need to be considered while developing or acquiring solution. However since many organisations have already implemented similar solution, the required security can be embedded.

Some of the technical issues which are to be considered are given in the Table 2.1 below.

Table 2.1: Technical Issues

Design Considerations	Design Alternatives
Communications Channel configuration	Point to point, line sharing, store and forward (multi-drop)
Communications Channel	Telephone lines, coaxial cable, fibre optics, microwave, or satellite
Communications network	Centralized, decentralized, distributed, or local area
Computer programs	Independent vendor or in-house
Data storage medium	Tape, hard disk, or hard copy
Data storage structure	Files or database
File organisation and access	Direct access or sequential files
Input medium	Keying, OCR, MICR, POS, EDI, or voice recognition
Operations	In-house or outsourcing
Output frequency	Instantaneous, hourly, daily, weekly, or monthly
Output medium	CRT, hard copy, voice, or turn-around document
Output scheduling	Pre-determined times or on demand
Printed output	Pre-printed forms or system-generated forms
Processor	Micro, mini, or mainframe
Transaction processing	Batch or online
Update frequency	Instantaneous, hourly, daily, weekly, or monthly

2.2.2 Economic Feasibility

Use of IT requires financial investments. Economic or financial feasibility refers to evaluation of investments and operating costs as against expected return on investment (qualitative or quantitative). Qualitative benefits refer to better service levels, improved efficiency, increased customer satisfaction etc. Quantitative feasibility refers to direct financial returns like increase in customer base resulting in increased revenue, growth in business, new opportunities etc. Considering the case of previous example the organisation may not be able to depute all employees for training, however the new solution offers following benefits:

1. 100% of employees can be trained (Improved Compliance) (Qualitative)
2. Employee need not to be deputed for external training (quantitative)
3. Employees can undergo training as per their convenience (improved productivity) (Partially quantitative)
4. Improved skills and motivation of employees (qualitative)

These benefits can be weighed against the investments for:

1. Infrastructure (Direct quantitative)
2. Outsourced development (quantitative)
3. Content development by employees (Partially quantitative)

By comparing both the benefits, cost benefits analysis can be done and then ROI can be calculated.

In short economic feasibility provides answers to the following:

- The cost of conducting a full systems development/acquisition, implementation and operation.
- The cost of hardware and software for the class of applications being considered.
- The benefits derived from new application such as improved efficiency, reduced costs, business growth, and customer and user satisfaction.
- Opportunity cost, i.e. if nothing changes (i.e. the proposed system is not developed/acquired).

2.2.3 Schedule or Time Feasibility

This refers to the expected time required for the new system to become operational. For example, in the above example, if the contents design and development can be run in parallel, it might take say 6 months, the system design might require one month and the testing and deployment may need another 2 months i.e. totally, the organisation have to wait for 9 months to make the solution operational and start deriving benefits.

2.2.4 Resources Feasibility

This focuses on availability of technical and skilled human resources required for developing/acquiring and implementing the required solutions. It may also focus on sourcing options and costs thereof. In the example since development shall be outsourced, organisation need to consider the availability of content developers and ensure that they are available when

required. In case of non-availability of content developers the project might be delayed. The project shall also be impacted if outsourced vendor fails to provide adequate resources to develop required application in time.

2.2.5 Operational Feasibility

This refers to establishing a process while implementing new solution that will provide ease of operation and also improve efficiency of operations. Some of the questions, which help in testing the operational feasibility are:

- Is there improvement in service efficiency? For example: customers are getting services more efficiently than earlier.
- Is there mechanism that ensures support to users and provides solutions for new system?
- Have the users been involved in planning and development of the project to provide inputs on operations?
- Will the proposed system cause harm? Will it produce poorer results in any respect or area? Will loss of control result in any areas? Will accessibility of information be lost?
- Will individual performance improve after implementation than before?

In the above example, the existing training involves identification of employees, deputing them, providing alternate resource during their absence, cost for training material and trainer. The new process shall not require these operations, however there will be new operations of communicating employees about training, maintaining contents, monitoring that employees attend training on portal, train users on using new system.

2.2.6 Social Feasibility

It is a concern associated with the views of stakeholders like management, workers, employees, customers and suppliers about the use of new solution and acceptance by them. Non-acceptance by majority stakeholders might result in not achieving desired results. In order to ensure acceptance an appropriate change management process involving stakeholders might help. For example the new training system in above example may not be acceptable by employees since it is depriving them a kind of paid holiday from daily routine for attending training. Management may consider offering another incentive to make new solution acceptable.

2.2.7 Compliance Feasibility

Any change in process must not affect the compliance level of the organisations. Any organisation may have to comply with legal, regulatory, contractual and internal compliances. Compliance feasibility is concerned with whether there will be any conflict between a newly proposed system and the organisation's compliance obligations. For example, a revised training system should comply with all applicable statutes about financial and statutory reporting requirements, as well as the company's contractual obligations.

2.2.8 Internal Controls

Automation might require changes in existing internal control environment. These aspects must be considered while considering the feasibility aspects as the assurance on internal controls is accountability of management. It is necessary to inform management about the changes in internal controls along with compliance requirements and associated risks.

2.3 Organisational methods for benefit realization

After completing feasibility study, the next step is preparing business case and presenting it to management for approval. Assessment of the benefits realization is a key component of business case. This is extended aspect of economic feasibility where the granular analysis of qualitative and quantitative benefits is considered. This section discusses about the various aspects of benefit realization.

Benefits realization of projects considers major factors such as cost, quality, development/delivery time, reliability and dependability. Project sponsor perform a comprehensive study and evaluate which factors are qualifying and then compare those factors with strengths, weaknesses opportunities, associated risks and competencies of services available to develop/acquire, implement and maintain systems.

Benefits Realization Techniques

Business benefits from SDLC projects are determined based on the changes in strategy, business objectives, changes in technology etc. The realization of benefits has become a more complex task due to evolution of IT applications, automation of work using embedded technology, business transformation through information management. Benefits do not just happen when the new technology is delivered; they occur throughout the business cycle. A planned approach to benefits realization with long term cycles that consider the total benefits and total costs throughout the life of the new system. Although it is possible that benefits may not come exactly as planned, organisations have to keep checking and adjusting the strategies.

Benefits realization is a continuous process that must be managed just like any business process and this requires organisations to:

- Describe benefits realization, for example customer growth, revenue growth due to technology.
- Assign measure and target for each aspect i.e. percentage and number to be achieved/expected.
- Establish a tracking/measuring process for expected benefits i.e. have we achieved expected numbers? If not what needs to be done? Were the assumptions correct?
- Document the assumptions against which the benefits are assessed.

- Define responsibilities for realization i.e. which organisational resources can be diverted due to automation to achieve benefit realization.
- Validate benefits predicted against current data, past achievement, industry experience and so on.
- Plan the benefits to be realized. For example automation is expected to achieve growth, but customers are not aware of changes in service process/levels.

Organisation wide benefits realization studies should be aggregated and lessons learned should be used to fine-tune the organisation benefit realization process.

Benefits realization often includes a post implementation review within 6-18 months after the implementation of systems. Time must be allowed for initial technical problems to be resolved and for the project benefits to accrue as users become familiar with the new processes and procedures.

Benefits realization must be part of management practice of projects. There must be business sponsorship of projects. Project governance structures should involve the project and the functional line organisation. All governance decisions about the project should be driven through the business case, and there must be periodic review of benefits.

IS auditor should understand how the business defines and monitors return on investment (ROI) for SDLC projects. Not achieving expected benefits or failure to monitor and take corrective actions in meeting ROI objectives, may point to weakness in benefit realization process and related project management practices

2.4 Business case development

A business case is normally derived from the benefit realization plan and feasibility study. A business case provides the information required for an organisation to decide whether the SDLC project should be undertaken and if approved, becomes the basis for a project execution and assessment. An IT project can have different scope and objectives. A project may be initiated for development of a new application system (SDLC) or for an investment in new infrastructure (partially touch SDLC), or for major modification in existing application and technology (Full or partial SDLC). A business case identifies and recognizes the achievement of business benefits to be derived from project.

Depending on the size of IT investments, organisations may choose to prepare business case at high level for program and proceed further to develop business cases for underlying projects. The initial business case would normally be derived from a feasibility study. The feasibility study will normally scope the problem, identify and explore a number of solutions and make a recommendation on what action to take. Part of the work in identifying options requires outlining

and calculation of benefits. A business case contains a comparison of costs and business benefits for different options for proposed solutions.

The business case should contain sufficient details to describe the justification for the project along with the reasons and should provide justification for the question, “Why the project should be approved?” The business case is a key element of the decision making process throughout the life cycle of project. If at any stage the business case is thought to no longer be valid, through increased costs or through reduction in the anticipated benefits, the project sponsor or steering committee shall refer to business case to arrive at a decision on whether the project should be terminated or should continue. If the business case changes during the course of an IT project, the project should be reapproved through the departmental planning and approval process.

While performing audit of benefit realization IS auditor has to understand and validate the methods identified and adopted by the organization for determining benefit realization and also the process for monitoring the benefits through put project life cycle. **These reviews happen after achieving predefined milestones (i.e. mid-term project review) and post-implementation review is generally conducted after 6 (or more) months.**

2.5 Business Requirements Identification

Once the business case is approved, the project is initiated. The primary part of this process is to prepare detailed requirements analysis. This is particularly required in case of acquiring of the software or outsourcing of software development. In between approval for business case and initiating the project, organisation should consider undertaking the detailed requirement analysis.

If it is decided to outsource the development, the vendor selected may require detailed function requirement specifications in order to arrive at efforts required and hence the cost. If organisation does not perform this step, the vendor shall perform it, to arrive at appropriate project costing. This section describes the various aspects of such analysis.

2.5.1 Techniques for requirements gathering

1. Understanding Requirements

The following are major activities under this section:

- Identifying stakeholder expectations. Stakeholders generally are not aware about the type of information required and may end up in providing high-level requirements. For example, for a payroll system, stakeholders may expect employee appraisals to be part of system but may assume that it might be considered. However since employee appraisal requirements are generally classified under HR Management project manager may ignore them.
- Analyzing requirements by discussing with stakeholder to detect and correct gaps in understanding and trim down extended expectations and determine priorities.

- Verifying that requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable.
- Resolving conflicts between the requirements set and the resources that are available.
- Identifying how the system needs to interact with its environment. For example, in a financial accounting system, requirement may state that the system must scan the supporting bills / documents and attach it to the financial transaction. Or in a payroll system an interface with internet banking may be required to be built to generate data for direct credit to employee accounts.

2. Study of History, Structure and Culture

The study of the history of systems in an organisation gives an idea about the types of systems that have been extremely useful, issues that have not been addressed over a period and new issues that require attention. It is essential to understand organisational structure and culture as the solutions that are not consistent with the culture often fail.

3. Study of Information Flows

In designing a new system, it is necessary to study the existing system. This involves study of the business processes, underlying activities, actors that perform these activities and resources required. This provides information on the essential aspects and controls while designing the new system and also helps in identifying changes required in existing process, without affecting internal control/compliance mechanism. Sometimes it is possible to collect user's expectation and requirements; however sometimes it also provides insight on what else is required to be done (e.g. prototyping) during project design phase to ensure that user's requirements are collected properly. The information gathering is a series of activities such as:

- Meetings with users at various levels
- Observation of users at work
- Forms, documents, registers being handled in the system
- Verbal interactions done by users to collect and disseminate the information

2.5.2 Types of requirements

Software solution has two types of requirements viz. functional requirements and non-functional requirements. Many times functional requires are prepared and presented by users however non-functional requirements has to be derived based on the analysis of functional requirements. A non-functional requirement consists of technical requirements, performance requirements, operational requirements and security requirements.

Functional requirements

These are primarily requirements related to service to be provided by business to customers. For example if a tour operator intends to offer online booking service to its customers, the list of functions that can be offered online shall be described in functional requirements, say user interface requirements and may include feature that once user visits home page there need to be an options for information on tours available, booking options with calendar, availability of seats, payment options, collecting and storing information on booking, forwarding e-mails and SMS on confirmation. Operational requirements may include back end operations of ensuring and confirming booking, arranging travel and stay as required, building tie-ups with travel agents, hotel managements and establishing communication process. However the business users may not be able to comprehend the technical requirements or define performance requirements beyond 'within what time the customer must get confirmation and communication'.

Non-functional requirements

These requirements covers what technology to be used and why? What are performance expectations e.g. CPU usage, number users, expected number of hits, user experience in getting next screen after click, designing frames so that user need not have to click multiple times etc. These requirements are generally captured during interview and information gathering. For example in above example if the tour operator expects around 1000 bookings per day, there could be high number of hits, since all hits may not materialize in booking. The implemented technology must support (e.g. multiple servers with load balancing) expected high number of hits or else the application may fail to serve. Similarly user may expect response from tour operator for any query or booking within specific time and the application should be able to (if automated) respond within that time or should be able to schedule response or generate alert for manual response. The technical requirements may also include providing personal communication using telephone or VOIP. In such a scenario, the technical requirements need to be defined to meet requirements. Once the requirements are defined the organisation may be able to decide on the right option which could be: in house development or acquisition of solution or outsourcing the development.

Requirements Engineering (RE) Process

RE is one of the most important areas of System Development. During this stage, the customer and Requirement Engineers come to an agreement as to 'what constitutes the software to be developed'. This is a critical stage because anything that is (or is not) resolved at this time, will be carried down through the rest of the System Development lifecycle. Good RE process is therefore essential for successful system development. RE process have several phases, which facilitate to understand the customers' needs, define the system requirements and constraints, analyze them, evaluate their feasibility, determine customers' real need, validate requirements specification and manage the requirements. Basically, there are five major phases of RE, which are explained here:

1. **Elicitation:** The RE process is normally considered as the process of finding out 'what are the real needs of the customers as well as of the system'. It also includes activities to explore 'how the software can meet the stakeholders' goals' and 'what alternatives might exist'.
2. **Analysis and Negotiation:** This phase consists of a set of activities aimed to discover problems within the system requirements and achieve agreement on changes to satisfy all system stakeholders. If an analyst discovers some problems with the requirements during the analysis phase, such requirements are referred back to the elicitation phase. This process is related to the requirements that are incomplete, ambiguous and/or conflicting. Negotiation part is known as 'the process of discussing conflicts in requirements and finding some compromise which all of the stakeholders can live with'. The principle of this process should be objective, where the judgments and the compromise for the system requirements should be based on technical and organisational needs. All the conflict requirements identified during the analysis process should be negotiated and discussed individually with the stakeholders in order to resolve the conflicts.
3. **Documentation:** Once the requirements have been analyzed, it is important to record them in order to make them formal through proper specification mechanism. During this phase, the team organizes the requirements in such a way that ascertains their clarity, consistency, and traceability etc. This phase is extremely important because often 'the document produced during specification is what the rest of the development stages will be based upon'.
4. **Validation:** This phase ensures that models and documentation accurately express the stakeholders' needs along with checking the final draft of requirements document for conflicts, omissions and deviations from different standards.
5. **Management:** This phase of requirements lifecycle is similar to the maintenance of a software system. Some of the most important maintenance tasks during this phase include the updating of the requirements as well as the degree of evolution support that the approach provides.

2.6 Summary

Once the SDLC project is initiated it is critical to ensure that:

- Feasibility study is complete and based on realistic and plausible assumptions.
- Benefit realization covers both qualitative and quantitative analysis of expected benefits from the project.
- Benefit realization process is defined and contains measurable achievements. It also contains what needs to be measured during project execution.
- Business case is prepared and approved and covers sufficient details so as to form a project baseline document.

The next step is to execute the project. For this the organisation must have a uniform project management practices, methodology and process. The next chapter covers the various steps required for project execution.

2.7 Questions

1. An organization has implemented an IT based solutions to support business function. Which of the following situation shall indicate the need to initiate SDLC project?

- A. Vendor has launched a new hardware which is faster.
- B. Organizations has unused surplus budget for IT.
- C. Regulators have requested additional reports from business.
- D. Competitor has launched an efficient IT based service.

2. A “Go or No Go” decision for SDLC project is primarily based on:

- A. Feasibility Study
- B. Business case
- C. Budget provision
- D. Market situation

3. Which of the following is the primary reason for organization to outsource the SDLC project?

Non-availability of:

- A. Skilled resources
- B. Budgetary approvals
- C. Security processes
- D. Infrastructure

4. Which of the following is an example of addressing social feasibility issue in SDLC project?

- A. Organization decides to use existing infrastructure.
- B. Beta version of application is made available to users.
- C. Configuration of purchased software requires more cost.
- D. Allowing employees to access social media sites.

5. Which if the following is not an indicator to assess benefit realization for internal application software developed in-house?

- A. Increase in number of customers because of new application.
- B. Decrease in audit findings related to regulatory non-compliance.
- C. Reduced number of virus attacks after implementing new software.
- D. Increase in productivity of employees after implementation.

6. Which of the following requirements for an application to be developed for use by human resource department are non-functional requirements? The application should:

- A. Capture the employee data at the time of hiring.
- B. Provide option to all only to edit own information.

- C. Capture performance details required for appraisals.
- D. Use relational database as backend to store data.

2.8 Answers and Explanations

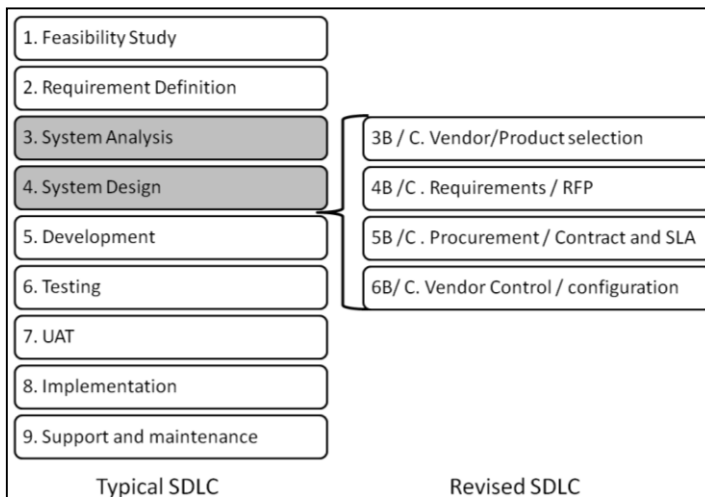
1. D. When a competitor launches new IT based efficient service, it becomes necessary for management to consider the impact in market place and in order to remain in competition should provide similar or better services. Option A and C may not require SDLC since it can be adopted with change management process. B may help in deciding for D, but is not the reason for initiating SDLC project.
2. C. Business case is a document that narrates all aspect including benefit realization, cost and effort estimates, outcome of feasibility study, available budget. That helps management in decision on the need of the SDLC project.
3. A. Non availability of skilled resources required for application development is primary reason for outsourcing the SDLC project. Other reasons can be addressed. i.e. (B) budget can be made available, (C) security processes can be established. (D) Infrastructure can be acquired, depending upon design of new application and hence it is not a reason.
4. B. In order to ensure the acceptability by users, beta version of solution is made available to users. Based on feedback changes are made so that the solution can be socialized. Option A addresses technical feasibility, Option C addresses economic feasibility. Option D addresses IT policy that has nothing to do with SDLC.
5. C. Since the application is for internal use and developed in house it has nothing to do with reduction in virus attacks. This can be benefit realization for anti-virus solution.
6. D. Specification of technology to be used are non-functional requirements.

CHAPTER 3: PROJECT MANAGEMENT FOR SDLC

Learning Objectives

This chapter focuses on providing insights on System Development project management. This includes initiation of program/project, establishing project management methodology, defining objective, project risk management, planning, resource management, monitoring and controlling project, managing changes, closing project and tools and techniques required for software project management.

3.1 Introduction



This chapter primarily provides information on phase-3: System Analysis and Phase-4: System Design of typical SDLC (shadowed area). However the detailed discussions on methods of system analysis and design are also discussed in chapter 4.

This chapter provides inputs on basic understanding of

project management as executing SDLC is a project till new solution is operational and organisation starts deriving benefits.

IS auditor primarily should be looking for control aspects in analysis and design hence the focus is on project management where the controls aspects are planned at the design stage.

3.2 Project management frameworks

Project is initiated once it is approved. In order to ensure that the project is successful, i.e. it meets its predefined objectives and delivers value, the organisation must adopt effective and efficient project management practices. Without project management practices, tools and control frameworks, it is not possible to manage all the relevant aspects like planning, scheduling, resource management, risk management, sizing and estimation of efforts, milestone achievements, quality,

deliverables and budget monitoring, of a large project. IS auditor must understand the need for a project management framework within the organisation, and associated elements required to establish a standard methodology. This chapter covers the various project management practices and how these are executed within the organisation.

There are many approaches for project management defined by various professional bodies. The most commonly used approaches are:

- Project Management Body of Knowledge (PMBOK®) version 5, i.e. IEEE standard 1490 from the Project Management Institute (PMI),
- Projects in a Controlled Environment (PRINCE2™) from the Office of Government Commerce (OGC) in the UK, and the International Project Management Association (IPMA).

Since there are significant differences in scope, content and wording in each of these standards, an auditor has to become familiar with the standard adopted by auditee organisation, prior to involvement in project. Although each project management approach has its own pros and cons, several elements are common across all project management methodologies. Some are focused on software development, others have a more general approach; some concentrate on a holistic and systemic view, others provide a very detailed workflow including templates for document creation

3.3 Key concepts of project management

Project is a temporary endeavour undertaken to generate defined outcome (like crating a service or product). Temporary need not be short, what it means is it has predefined beginning and end. For example a project can be initiated to build a housing complex, that is completed once tenants have occupied it, or it can be for building infrastructure, or designing a new product, e.g. Tata motors designing the Nano car. The project is closed once the expected outcome is delivered or results are achieved or if the project becomes technically or economically unviable. In short projects can be initiated for any reason. Developing Software and deploying it can be a project or depending upon size, it can be group of projects.

A project management refers to the practice of managing a project. Management may not want to initiate a project as it involves providing resources and waiting till the end to get deliverables. Management has to monitor the progress of project and intervene periodically to ensure that the project finally achieves the defined objectives.

Project management practice is a set of multiple processes grouped in five major process groups:

1. Project initiation
2. Project Planning
3. Project execution
4. Project controlling and monitoring
5. Project closing

Although these processes are grouped they are not executed in sequence, Process groups under project planning, project execution and controlling are executed in iteration. (Figure 3.1)

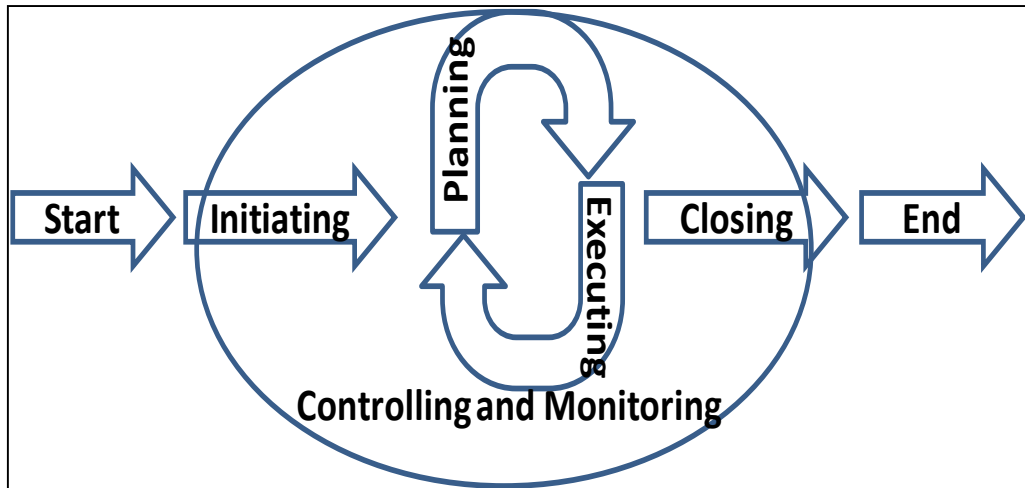


Figure 3.1: Project process groups

Each group consists of various processes, however all processes may not be applicable to all projects.

Project initiation group consists of mainly processes related to developing project charter based on scope of project. In SDLC project it is business case (discussed in previous chapter), Identifying beneficiaries and stakeholders of project.

Project planning consists of processes related to developing project execution plan, finalizing requirements, defining work breakdown structure and modules to be developed, estimating efforts and cost, resource planning, risk management, procurement planning and plan for communications with stakeholders.

Project execution consists of processes related to direct project teams, ensuring quality assurance and testing, managing requirements and changes in requirements, ensuring timely procurements and manage resources.

Project controlling and monitoring consists of processes related to monitoring risks, scope creeps, quality of deliverables, costs and budgets, performance reporting.

Project closing has processes for handing over deliverables or terminating project.

SDLC project management is further discussed in ensuing sections.

3.4 Program and project management and organisation

3.4.1 Portfolio/Program Management

A program is a group of projects and/or time-bound tasks that are linked together through common objectives. It may share a common budget and can have intertwined schedules. Like projects, programs have a limited time frame (start and end date), predetermined budget, defined deliverables/outcomes and sometimes organisational boundaries. A program is more complex than a project and many times consists of multiple projects. For example implementing ERP at all plants can be a program consisting of multiple projects for implementing ERP at each plant. (Figure 3.2 explains the relationship of portfolio, programs and projects)

A portfolio is group of all projects/programs (related or unrelated) being carried out in an organisation at a given point in time.

A project/program management office (popularly referred as PMO) controls and manages Portfolios, programs and projects. PMO also governs the processes of project management but not involved in management of project content.

The program management includes management of:

- Program scope
- Program financials (costs, resources, cash flow, etc.)
- Program schedules
- Program objectives and deliverables
- Program context and environment
- Program communication and culture
- Program organisation

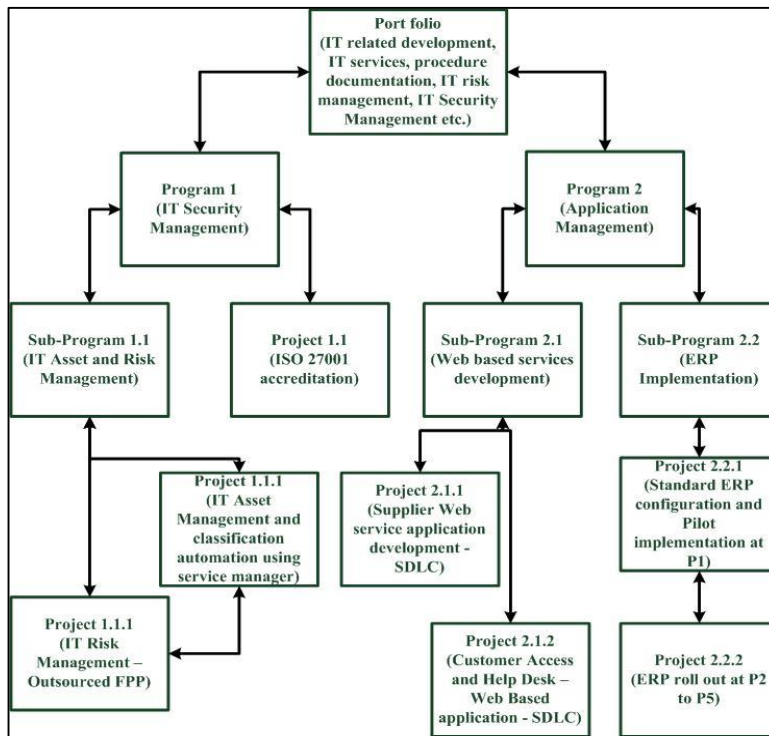


Fig 3.2: Portfolio, program and project

3.4.2 Program/Project management Organisation forms

A project may be considered as a group of complex tasks executed by a temporary organisation. However depending upon the nature of business, from a project management perspective, organisations can be categorized as follows:

- Functional organisation that is influenced by the projects:** These are business organisations that are involved in production of goods and services. Projects are undertaken to support the functional activities. For example, a manufacturing organisation may want to automate administrative processes (like finance, HR, pay roll etc.) using IT. In such organisations, project manager has only a staff function without formal management authority. The project manager is only allowed to advise peers and team members as to which activities should be completed. In such organisation project team consist of staff that report to functional manager, except for the purpose of project activities assigned, reports to project manager.
- Projectile organisation:** These are pure project organisations that execute projects. For example, an infrastructure development organisation or consulting organisations that executes projects. In such organisations project manager has formal authority over those taking part in

the project. Often, this is bolstered by providing a special working area for the project team that is separated from their normal office space.

- **Matrix project organisation:** The organisation that provides product and services and also executes projects. Most IT companies falls under such categories where these organisations undertake project to manage business functions for other organisations and also executes projects for customer organisation. In such organisation, management authority is shared between the project manager and the department heads.

IS auditor has to understand these organizational forms and their implications on controls in SDLC project management activities.

3.5 Project Initiation

Whenever a business entity decides (i.e. stakeholders in the business or senior management) to undertake computerization, a project will have to be initiated. Some examples of a formal project initiation are:

- A new business application is required to be developed to address a new or existing business process e.g. HR management system, billing system, order processing etc.
- Adoption of a new technology invented or available becomes advantageous to the business e.g. Internet based advertising for an advertising company.
- The application software to be developed, is expected to rectify the present problem related to existing business e.g. computerization of college admissions.
- The application software to be developed, is expected to rectify the present problem related to existing technology e.g. migrating from text-based computerized system to GUI based system as in case of old COBOL / XBASE based distributed banking to RDBMS based Core Banking system.

A project may be initiated from any part of the organisation, including the IS department. A project is time bound, with specific start and end dates, a specific objective and a set of predetermined deliverables. Once a project is initiated a project sponsor and project manager is appointed to execute the further activities including gathering the information required to gain approval for the project to be created. This will often be compiled into terms of reference or a project charter that states the objective of the project, the stakeholders in the system to be produced, and the project manager and sponsor. Approval of a project initiation or project request is authorization for a project to begin.

During project initiation, the project manager performs several activities that assess the size, scope, and complexity of the project, and establishes procedures to support subsequent activities. The major activities to be performed in the project initiation are:

- **Establishing the project initiation team:** This activity involves organizing an initial core of project team members to assist in accomplishing the project initiation activities.
- **Establishing a relationship with the customer:** A thorough understanding of the customer builds stronger partnerships and higher levels of trust.
- **Establishing the project initiation plan:** This step defines the activities required to organize the initiation team while it is working to define the scope of the project.
- **Establishing management procedures:** Successful projects require the development of effective management procedures.
- **Establishing the project management environment and project workbook:** The focus of this activity is to collect and organize the tools that will be used while managing the project and to construct the project workbook. For example, most diagrams, charts, and system descriptions provide much of the project workbook contents. Thus, the project workbook serves as a repository for all project correspondence, inputs, outputs, deliverables, procedures, and standards established by the project team.

Many organisations that follow standard process for project management prepare a formal Project Initiation Report that is presented to senior management or Board of Directors. Once accepted this becomes formal charter for the project and triggers next phases of SDLC.

3.5.1 Project management methodology

IT projects are divisible into pre-defined phases (*SDLC phases are described in chapter 1 and various methods and models are discussed in chapter 4*). The project management process begins with the project charter and ends with the closure of the project. Since the project management can be complex, like other business processes, it also requires a standardized approach. Organisations may adopt standard processes prescribed by globally accepted standards developed by organisations like PMI or can define a project management process within organisation based on such prescribed standards.

Organisations following a standard project management process have higher possibility of completing projects in time, within budget and deliverables meeting with expected quality. The following section explains general project management practices used by various organisations.

3.5.2 Project Context and Environment

Organisation may be running several projects at the same time. These projects need not be SDLC projects or IT projects. At organisation level the relationships between these projects have to be established to identify common objectives for the business, which is a function of a project portfolio management and/or a program management. This helps in consolidating common activities (e.g. identify and manage risks) and managing of common resource requirements. (Refer Figure 3.1)

A context of the project may be determined based on:

- Importance of the project deliverables to organisation's objectives

- Connection between the organisation's strategy and the project outcome
- Relationship with other projects
- Priority based on the business case

In addition while considering the time context of the project, following aspects must be considered:

- Start and end time of the project, particularly if it is expected that the outcome of project has linkages to other projects.

The objective is to determine whether all relevant environments for the project, which will have a significant influence on overall project planning and project success, have been considered.

3.5.3 Project Communication and Culture

Success of project depends upon timely communication with stakeholders and affected parties. This can be achieved by:

- One-on-one meetings
- Kick-off meetings
- Project start workshops
- Periodic reporting

Communication helps in obtaining cooperation from all team members and buy-in from stakeholders. One of the major activities for project manager during execution of project is to develop and execute communication plan so as to inform issues, concerns, if any and to report project progress.

3.5.4 Project Objectives

Primary objective of project is to deliver the defined outcome/deliverables/product in time, within budget and of desired quality. The measurement of success depends upon clearly defining results that are specific, measurable, attainable, realistic and timely (SMART). The main objectives of project are always directly coupled with business expectations. Additional objectives are objectives that are not directly related to the main results of the project but may contribute to project success (e.g., business unit reorganisation in a System Development project).

A commonly accepted approach to define project objectives is to start with a work breakdown structure (WBS) with each work module having its own objectives derived from main objectives. The WBS represents the project in terms of manageable and controllable units of work and forms the baseline for cost and resource planning. Detailed specifications regarding the WBS can be used to develop work packages (WP). Each WP must have a distinct owner and a list of main objectives, and may have a list of additional objectives. The WP specifications should include dependencies on other WPs and a definition of how to evaluate performance and goal achievement.

A task list is a list of actions to be carried to complete each work package and includes assigned responsibilities and deadlines. The task list aids the individual project team members in operational planning and scheduling, that when merged together forms a project schedule. Project schedules are work documents containing the start and finish dates, percentage completed, task dependencies, and resource names of individuals planned to work on tasks.

3.5.5 Project Management Practices

Every organisation uses project/program to implement new concepts, changes, business strategies etc. Collective knowledge of executing projects may be used to execute the projects; however it is a prudent for the organisation to adopt a standard project management practice, across entire organisation. Many organisations prefer to adopt the practices based on global standards/best practices e.g. PMBOK, Prince2 etc.

Project management is the application of knowledge, skills, tools and techniques to a broad range of activities to achieve organisational objectives. For example: meeting user requirements by developing/acquiring new software within budget and timelines. Project management practices consist of defined processes for initiating, planning, executing, controlling and closing a project.

A successful project planning is a risk-based management process that is iterative in nature. Project management practices for SDLC projects also provide standards for systematic quantitative and qualitative approaches to software size estimating, scheduling, allocating resources and measuring productivity. There are numerous project management tools available (e.g. MS project) that can be adapted to implement techniques to assist the project manager in controlling the time and resources utilized during execution of project.

3.6 Project Planning

To plan and control SDLC projects, project manager needs to determine:

- The various project tasks and management tasks that need to be performed to develop/acquire and implement business application system.
- The order in which these tasks should be performed.
- The estimated duration for each task.
- The priority of each task.
- The IT resources, available, transferred/loaned or to be acquired to perform these tasks.
- Budget or costing for each of these tasks. This can be notional for internal resources and monetary for outsourced projects.

In complex projects the planning is dynamic and has to be reviewed/adjusted at the beginning and end of each project phase. This is to ensure that resources are available, quality of work during earlier phase has been as expected (i.e. no rework is required, or if required adjusting the plan by considering the delay and so on.)

There are some techniques like program evaluation review technique (PERT), critical path method (CPM), Gantt chart etc., that are useful in creating and monitoring project plan. The major activities which are performed during project planning are:

- Measure the development efforts. (Different software sizing techniques are discussed in section 3.8.)
- Another activity is to identify resources (e.g., people with requisite skills, development tools, facilities) for software development.
- Budgeting is next activity. Although overall budget for the project has been allocated at high-level during business case development, project manager need to prepare granular budget for monitoring. This is done by considering the cost for each resource and their expected use. For example group of testing professionals might be required in the project, however they need not be available from the beginning of project and thus can be inducted (on boarded) at a later date thus optimizing the cost associated with their release from another project.
- Scheduling and establishing the time frame is another activity. While budgeting involves adding up the cost for human and machine resource usage involved in each task, scheduling involves establishing when these resources are required in the project. This is achieved by arranging tasks according to:
 - The logical sequential and parallel tasks relationship and determining earliest start date.
 - Based on estimated efforts (section 3.7) for each resource arriving at latest expected finish date.
 - Schedules are presented using PERT, CPM diagrams and Gantt Charts. (*Discussed in section 3.7.*)

3.7 Project Controlling

The controlling activities of a project include:

- Management of scope
- Monitoring of resource usage
- Risk management.

It is critical to ensure that new requirements for the project are documented and, if approved, appropriate resources are allocated. Control of changes during a project ensures that projects are completed meeting stakeholder requirements of: time, use of funds and quality objectives. Stakeholder satisfaction should be addressed with effective and accurate requirements capture, proper documentation, baselining and skilled steering committee activity.

During mid-term project review IS auditor should focus on project planning and controlling activities to ensure that these are not deviating from primary objectives of the project.

3.7.1 Management of Scope

Quite often, it is noticed that the majority of the SDLC projects suffer from “Scope creep”. This happens particularly when the requirement analysis is incomplete or the dynamic nature of business environment forces users to include these requirements and all these requirements cannot be put on hold. The scope creep affects the project planning seriously. This can be controlled by:

- Baseline the requirements before project planning.
- Establishing process for change management to decide which requirements must be included during development and how it is affecting the project time, cost, quality and outcome. Change management process must define who can request for change, how a formal change request be made, what it should contain and the reasons for the change. For complex deliverables, it is best to document the work breakdown structure.
- The project manager then assesses the impact of change request on project activities, schedule and budget.
- A change advisory board is appointed to evaluate change requests and decide on approving changes.
- If the change is accepted, the project manager should update the project plan.
- The updated project plan must be formally confirmed by the project sponsor—accepting or rejecting the recommendation of the change advisory board.

3.7.2 Resource management

Monitoring resource usage in project execution is the process to control budget and ensure that cost plan is on track. Budget and project plan assumes certain productivity of resources. For example, if a program development is expected and hence planned to take 16 person-hours, then it is supposed that the resource being deployed is capable of finishing that task in 16 person-hours with expected quality level. (Using coding standards might help in improving productivity). Whether this is actually happening can be verified using earned value analysis (EVA).

Earned Value Analysis consists of comparing expected budget till date, actual cost, estimated completion date and actual completion at regular intervals during the project. In above example the program development is expected to take two working days, with eight hours spent each day. At the end of first day cost is as per budget but EVA cannot be determined unless 50% or more work has been completed. Alternate is to get information on how much time is required to complete remaining program. If the answer is 8 hours the project is on track, if it is less resource might be idle and if it is more, the project might be delayed. In short at the end of first day resource spent is according to budget, but the “earned value” will be based on remaining time to complete the task. (Figure 3.3)

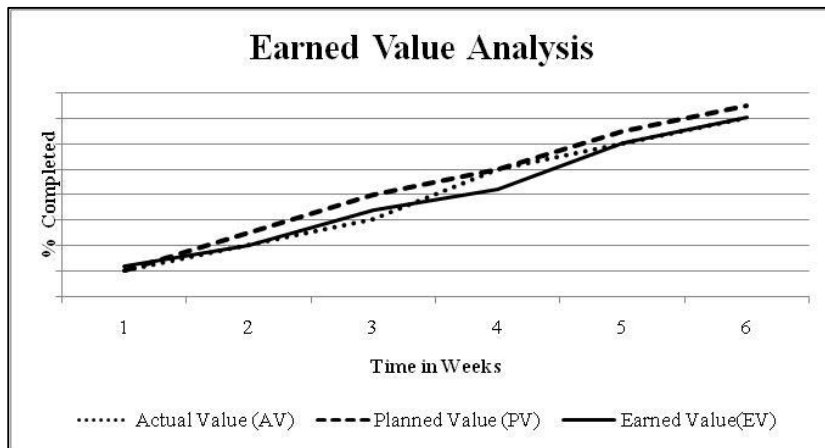


Figure 3.3: Earned Value Analysis

3.7.3 Project risk management standards and methods

Project management practices require the project manager must adopt the risk management frameworks. PMBOK of PMI specifies following activities for project manager:

Project Planning Phase

- Plan Risk
- Identify Risk,
- Qualitative analyses of risks
- Quantitative analysis of risk
- Plan risk response

Project monitoring phase

- Control risks

Risk in project management

Risk is defined as a possible negative event or condition that would disrupt relevant aspects of the project. There are two main categories of project risk: the category that impacts the business benefits (and therefore endangers the reasons for the project's very existence) and the category that impacts the project itself. The project *sponsor* is responsible for mitigating the first category of risk and the project *manager* is responsible for mitigating the second category. The risk management process consists of five steps that are repeatedly executed during a project. Phase-end milestones are a good anchor point in time at which to review and update the initial risk assessments and related mitigations.

Risk management process

- **Identify risk:** Perform a brainstorming session with your team and create an inventory of possible risk.
- **Assess and evaluate risk:** Quantify the likelihood (expressed as a percentage) and the impact of the risk (expressed as an amount of money). The “insurance policy” (total impact) that needs to be in the project budget is calculated as the likelihood multiplied by the impact.
- **Manage risk:** Create a risk management plan, describing the strategy adopted and measures to deal with the risk. Generally, the more important the risk, the more budget should be made available for countermeasures. Countermeasures could include prevention, detection and damage control/reconstruction activities. Any risk can be mitigated, avoided, transferred or accepted depending on its severity, likelihood and cost of countermeasures and the organisation’s policy.
- **Monitor risk:** Discover risk that materializes, and act accordingly.
- **Evaluate the risk management process:** Review and evaluate the effectiveness and costs of the risk management process.

IS auditor has to focus on the risk management process as it provides detailed insight on the effectiveness of project management.

3.8 Project Closing

Projects should be formally closed to provide accurate information on project results, improve future projects and allow an orderly release of project resources. The closure process should determine whether project objectives were met or excused, and should identify lessons learned to avoid mistakes and encourage repetition of good practices. Project closure is to be planned in two situations:

1. **Project deliverables are completed and are ready to be implemented:**
 - The project sponsor should be satisfied that the system produced is acceptable and ready for implementation/delivery.
 - Custody of contracts may need to be assigned, and documentation archived or passed on to those who will need it.
 - Survey the project team, development team, users and other stakeholders to identify any lessons learned that can be applied to future projects.
 - Achievement of objectives of project and performance fulfilment, adherence to the schedule, costs, and quality of the project.
 - Post project review in which lessons learned and an assessment of project management processes used are documented.
 - Release of project teams either to other projects or line functions.

2. Project is suffering from risk materialization and has to be terminated.

These are generally exceptional situations like changes in functional requirements, obsolescence of planned technology, availability of new technology, unforeseen budget constraints, strategy changes etc. In rare cases the project may have to be terminated due to non-performance of project teams. In such situations closure of project may have to be planned depending upon the status of project. For example, based on project planning, organisation may have placed order for required software and hardware or might have made some changes to its existing infrastructure. These need to be undone or planned so as to minimize the impact on organisation.

IS auditor conducting review after project closure has to consider the overall project execution on various parameters such as objectives achieved, time overrun, cost overrun, quality of deliverables? If the review is being done immediately after implementation, IS auditor may also review the challenges faced by the users and the resolution methods.

Achieving business objectives must be the focus of project review. Accordingly, the auditor may review and comment on budget and time overrun situations.

3.9 Roles and responsibilities

The various roles and responsibilities of groups/individuals that are associated with the project and program management for SDLC project are described below:

3.9.1 Steering committee

Project steering committee provides overall direction and monitors the project execution this is assured by representation of major stakeholders. The project steering committee is ultimately responsible for all deliverables, project costs and schedules.

This committee should be comprised of senior representatives having authority for decision from business areas likely to be impacted by the proposed system or change. Mostly project sponsor will chair the steering committee. The project manager is member of steering committee.

Role of project steering committee

Project steering committee performs the following functions:

- Reviews project progress periodically (fortnightly or monthly or as required)
- Serves as coordinator and advisor to project. Members of the committee should be available to make user-related decisions about system and program design.
- Takes corrective action based on reviews. The committee should evaluate progress and take action or make recommendations to resolve project issues related to budget, schedules, resources, and scope and project objectives.

- Assess risks and decide upon mitigation plan. Also resolve issues that are escalated and cannot be resolved at the project level.
- Take decision on and if required recommend the project be halted or discontinued.
- Works closely with the project manager to define project success factors and metrics in measurable and quantifiable terms.

3.9.2 Project Sponsor

Head of business function or senior management (generally who has highest stake in benefit realization from project) is designated as project sponsor who provides funding and assumes overall ownership and accountability of the project. Project sponsor is responsible for providing funding and budget for the project execution.

3.9.3 Project Manager

A project manager should be identified and appointed by the IS steering committee. The project manager, who need not be an IS staff member, should be given complete operational control over the project and be allocated the appropriate resources, including IS professionals and other staff from user departments, for the successful completion of the project. A project manager is appointed for execution of project. The project manager can be from the user department, or from IS department or hired separately to handle the project.

Primary functions of Project manager are:

- Provide day-to-day management and leadership.
- Ensure that project activities are in line with predetermined objectives.
- Involve affected departments.
- Follow organisation's project management standards.
- Ensure expected quality of deliverables.
- Resolve conflicts.
- Monitor and controls costs, schedules and associated risks.

3.9.4 Senior management

Demonstrates commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project. Generally senior management representative is appointed on steering committee.

3.9.5 Business management

Business management, most of the times, assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process

redesign, system requirements definition, test case development, acceptance testing and user training. Business management should review and approve system deliverables as they are defined and implemented.

Business management is concerned particularly with the following questions:

- Are the required functions available in the software?
- How reliable is the software?
- How efficient is the software?
- Is the software easy to use?
- How easy is it to transfer or adapt old data from pre-existing software to this environment?
- How easy is it to transfer the software to another environment?
- Is it possible to add new functions?
- Does it meet regulatory requirements?

3.9.6 Systems development project team

System development team consist of System analyst, Developers, testing professionals, control consultants (IS Auditor), hardware and network consultants, The teams members completes assigned tasks, communicates effectively with users by actively involving them in the development process, works according to local standards and advises the project manager of necessary project plan deviations.

3.9.7 Business function representatives/domain specialists

Consists of subject matter experts (SME) that provides inputs to developers and system analysts on requirements, business related controls, and sometime approves the low level design specifications.

3.9.8 Security Officer

Ensures that system controls and supporting processes provide an effective level of protection, based on the data classification set in accordance with corporate security policies and procedures; consults throughout the life cycle on appropriate security measures that should be incorporated into the system; reviews security test plans and reports prior to implementation; evaluates security-related documents developed in reporting the system's security effectiveness for accreditation; and periodically monitors the security system's effectiveness during its operational life.

3.9.9 IS Auditor

The IS auditor can be part of SDLC project team as consultant for internal controls or for the review of the project activities. They may also provide an independent, objective review to ensure appropriate level of commitment of the responsible parties. IS auditor has to understand the

systems development; acquisition and maintenance methodologies used by the organisation and identify potential vulnerabilities. If auditor observes control weakness either as a result of review due to organisational structure or the software methods used, or weakness in process execution, it is the IS auditor's role to advise the project team and senior management of the deficiencies in project management and provide recommendations for improvement.

Role of IS Auditor in SDLC

Throughout the project management process, IS Auditor should analyze the associated risks and exposures inherent in each phase of SDLC. He should assure that appropriate control mechanisms are in place to minimize the risks in a cost effective manner. While reviewing SDLC various phases as well as attend the project team meetings offering advice through Software Development process. He will also assess the project development team's ability to produce key deliverables by the promised dates. Adequate and complete documentation of all phases should be collected and reviewed by processes, IS Auditor is expected to obtain necessary and available documentation from the IS Auditor. The specific areas of review are:

- Understand standards adopted and followed by the organisation through the process of inquiry, observation and documentation review.
- To determine significant phases for the various size and type.
- To assess efficiency and effectiveness of each function to satisfy the users goals and organisation objectives.
- To test methodology adopted and determine compliance with the organisation standards by reviewing the documentation produced.
- To evaluate controls designed for compliance with internal control principles and standards.
- To determine compliance with common security, auditability and change control standards

If IS auditor is part of project team not for performing an audit, but is participating on the project in an advisory role then depending on the level of involvement, IS auditor may become ineligible to perform audits of the application when it becomes operational.

3.9.10 Quality assurance (QA)

Quality assurance function consists of following key activities:

1. Develop test plan and test the code.
2. Review and ensure that project documentation is complete.
3. Review deliverables of the project.

The objective is to ensure that the quality of the project by measuring the adherence by the project staff to the organisation's standard methodology of System Development life cycle (SDLC), advise

on deviations, and propose recommendations for process improvements or greater control points when deviations occur.

Specific objectives of the QA function include:

- Ensuring the active and coordinated participation by all relevant parties in the revision, evaluation and dissemination, and application of standards, management guidelines and procedures
- Ensuring compliance with the agreed on systems development methodology
- Reviewing and evaluating large system projects at development milestones, and making appropriate recommendations for improvement
- Establishing, enhancing and maintaining a stable, controlled environment for the implementation of changes within the production software environment
- Defining, establishing and maintaining a standard, consistent and well-defined testing methodology for applications
- Reporting to management on systems that are not performing as defined or designed

3.9.11 Technology Specialist

IT is developing so rapidly that even IT professionals find it difficult to keep track of all developments, let alone develop expertise. This has resulted in experts in specific technology areas, such as Microsoft technology, Web-enablement and the like.

3.9.12 Systems Analyst

The system analyst also has a responsibility to understand existing problem/system/data flow and new requirements. System analysts convert the user's requirements in the system requirements to design new system.

3.9.13 Programmers/Developers

Programmers convert design into programs by coding using programming language. They are also referred to as coders or developers.

3.9.14 Testers

Testers are junior level quality assurance personnel attached to a project. They test programs and subprograms as per the plan given by the module / project leaders and prepare test reports.

3.9.15 Documentation Specialist

These professionals are responsible for the creation of user manuals and other documentation.

3.9.16 Database Administrator (DBA)

The data in a database environment has to be maintained by a specialist in database administration so as to support the application program. The database administrator handles multiple projects; and ensures the integrity and security of information stored in the database.

3.10 SDLC Project management techniques and tools

System development process may be associated with various automated tools that help in improving productivity and maintaining record and documentation of application being developed. Tools that help in improving productivity include code generators, development environments (also referred to as developer's workbench) like visual studio and Computer-Aided Software Engineering (CASE) applications that help in documenting the SDLC process. In addition project managers may use project management tools like MS Project. This section provides information about these tools. This section covers following three areas:

1. CASE tools
2. Software size estimation covering various techniques used like LOC, FPA analysis etc.
3. Project controlling tools like PERT, CPM and Gantt Charts.

1. Computer Aided Software engineering (CASE) tools

SDLC requires collecting, organizing and presenting information required at application systems and program level. This involves building data flows, documenting design of application system, identifying modules/functions/program required to be developed and sometimes developing prototypes to capture requirements. These are essential but time consuming processes that are required for developing, using and maintaining computer applications.

Computer-aided software engineering (CASE) is automated tools that aid in the software development process. Their use may include tools for capturing and analysing requirements, software design, code generation, testing, document building and other software development activities.

Although IS auditor is not expected to have detailed knowledge of how to use CASE tools, they may have to learn how to use CASE tools for effective audit of SDLC project, as required.

Code Generators

Code generators are tools that are part of CASE tools or development environment like visual studio. These tools generate program source code based on parameters provided. These products significantly reduce the development (particularly coding) time; however maintaining or changing these programs might be painful and time consuming.

Development environments and non-procedural languages

Developer's workbench: Provides environment to developer for editing, simulating code, temporary storage, file management and sometime code generation. It may also provide Software facilities that include the ability to design or paint retrieval screen formats, develop computer-aided training routines or help screens, and produce graphical outputs. It is often referred to as an integrated development environment (IDE).

Non-procedural languages: These are event driven and make extensive use of object-oriented programming concepts such as objects, properties and methods. These languages cannot perform data intensive or online operations however are best suited to provide environment to end user for generating their own views and report required for data analysis and decision making. These languages provide environmental independence (portability) across computer architectures, operating systems and telecommunications monitors. These languages generally have simple language subsets that can be used by less-skilled users.

These languages are classified in the following ways:

- **Query and report generators:** These languages can extract and produce reports and sometimes can access database records, produce complex online outputs.
- **Embedded database languages** are more user-friendly but also may lead to applications that are not integrated well with other production applications.
- **Relational database languages** are usually an optional feature on a vendor's DBMS. These allow the applications developer to make better use of the DBMS product, but they often are not end-user-oriented.

2. Software Size Estimation

Once the work breakdown structure is completed and SDLC methodology (discussed in chapter 4) is finalized project manager must perform Software size estimation, i.e. determining the physical size of application (number of programs, modules, reusable function/modules etc.). This helps the project manager in deciding resource and skills requirements, to judge the time and cost required for development, and to compare the total effort required by the resources.

Source lines of Code (SLOC)

Traditionally, particularly when COBOL like languages was used, software sizing used to be performed using number of source lines of code (SLOC). However it does not work well for complex systems using different types of programs and automated tools like source code generators. This puts limitation on planning for cost, schedule and quality metrics.

With new technologies multi-point estimations techniques were developed that now uses diagrams, objects, spreadsheet cells, database queries and graphical user interface (GUI) widgets. These

technologies are more closely related to functionality that needs to be created rather than lines of code.

Function Point Analysis (FPA)

The function point analysis (FPA) technique has evolved over the years and is widely used for estimating complexity in developing large business applications. The results of FPA are a measure of the size of an information system based on the number and complexity of the inputs, outputs, files, interfaces and queries with which a user views and interacts with the data. This is an indirect measure of software size and the process of development. It is based on the number and complexity of inputs, outputs, files, interfaces and queries.

Function points (FPs) are computed by considering various parameters like number of users, number of inputs, number of outputs, expected user actions, data elements to be processed and external interfaces to determine whether a particular module/program is simple, average or complex. This information is used to compute function point using an algorithm that takes into account complexity adjustment values (i.e., rating factors) based on responses to questions related to reliability, criticality, complexity, reusability, changeability and portability.

Function points (FP) derived from this equation are then used as a measure for cost, schedule, productivity and quality metrics (e.g., productivity = FP/person-month, quality = defects/FP, and cost = monetary value/FP).

IS auditor should be familiar with the use of Function Point Analysis. However, IS Auditors are not expected to be experts in this technique.

FPA Feature Points

A slightly different approach for function point analysis for system software such as operating systems, telephone switching systems, etc. was developed. To differentiate from FPA it is called "Feature Points." It is used for software that has well-defined algorithms like systems software, embedded software, real time software, CAD, Artificial intelligence and some traditional MIS software.

In web-enabled applications, the development effort depends on the number of forms, number of images; type of images (static or animated), features to be enabled, interfaces and cross-referencing that is required. Thus, from the point of view of web applications, the effort would include all that is mentioned under function point estimation, plus the features that need to be enabled for different types of user groups. The measurement would involve identification or listing of features, access rules, links, storage, etc.

Cost Budgets

Cost estimates of a SDLC project are based on the amount of effort likely to be required to carry out each task. The estimates for each task contain one or more of the following elements:

- Person-hours for all type of resources e.g. system analyst, programmers, support staff, Testing teams etc. (Pl. refer section 3.9 roles and responsibilities)
- Infrastructure (Hardware, software, networks etc.), other specialized software, if any and communication equipment)
- Other costs such as third-party services, automation tools required for the project, consultant or contractor fees, training costs, etc.

Based on estimates following steps are used in arriving at cost budget:

- Prepare estimate of human and machine effort by for all tasks.
- Determine hourly rate for each type of person-hours and arrive total person cost.

3. Project Controlling tools and techniques

Project manager uses various tools and techniques to control the project. The graphical techniques used to represent schedule are:

- A. Project evaluation review technique(PERT)
- B. Critical path method(CPM)
- C. Gantt Chart

A. Program Evaluation Review Technique (PERT)

PERT is a technique to estimate the efforts and time required to complete the work/task described by work breakdown structure (WBS). Project manager lists out the major tasks and arrives at three different duration estimates of each activity. The three estimates are then used to derive single estimate applying a mathematical formula. PERT is often used in projects with uncertainty about the duration.

Table 3.1 illustrates one such formula for a hypothetical project where activities are named from A to L. The first is the most optimistic time (if everything went well) and the third is the pessimistic or worst-case scenario. The second is the most likely scenario.

This estimate is based on experience attained from projects that are similar in size and scope. To calculate the PERT time estimate for each given activity, the following calculation is applied:

$$[\text{Optimistic} + \text{Pessimistic} + 4(\text{most likely})]/6$$

Table 3.1: PERT table

Activity	Optimistic Estimate	Pessimistic Estimate	Most Likely Estimate	Final Estimate
A	2	6	4	4
B	4	10	7	7
C	4	14	9	9
D	7	19	10	11
E	2	6	4	4
F	1	5	3	3
G	2	8	5	5
H	3	9	6	6
I	2	6	4	4
J	1	5	3	3
K	2	6	4	4
L	1	3	2	2

Figure 3.4 illustrates use of the PERT network management technique. (Each circle represents milestones and the arrow represents activities. Number after activity shows the number of days required to complete the activity.)

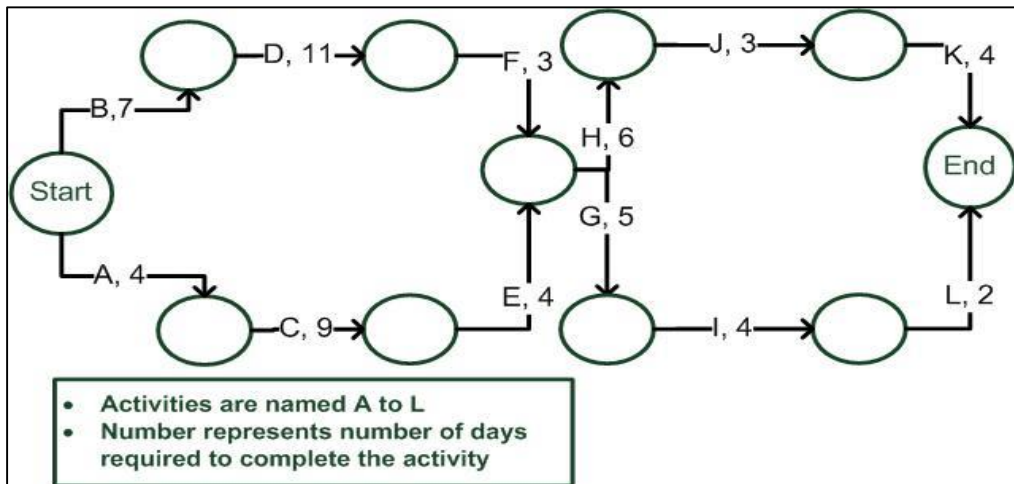


Figure 3.4: PERT Diagram

Some project managers show all estimates in the PERT diagram.

B. Critical Path Methodology

All project schedules have a critical path. Activities of a project are in sequence or independent or parallel, a project can be represented as a network of activities is shown in PERT diagram. (Some project managers refer to PERT diagram as PERT network).

A path through the network is any set of successive activities which go from the beginning to the end of the project. Associated with each activity in the network is a single number that represents estimates the amount of time that the activity will require to complete.

The critical path is the sequence of activities whose sum of activity time is highest than that for any other path through the network. Critical paths represents the shortest possible project completion time, if everything goes according to schedule. In other words, delay in completing any activity on critical path delays the overall project.

Activities which are not in the critical path have slack time, i.e. delay in performing these activities may not affect the overall project schedule. Activities on critical path have zero slack time.

The PERT diagram shown in figure 3.4 has following 4 paths:

1. A – C – E – G – I – L
2. A – C – E – H – J – K
3. B – D – F – H – J – K
4. B – D – F – G – I – L

Using the time estimates the total time require for each path is 28, 30, 34 and 32 days respectively. Third path hence is Critical Path. (Shown by thick arrows in figure 3.5

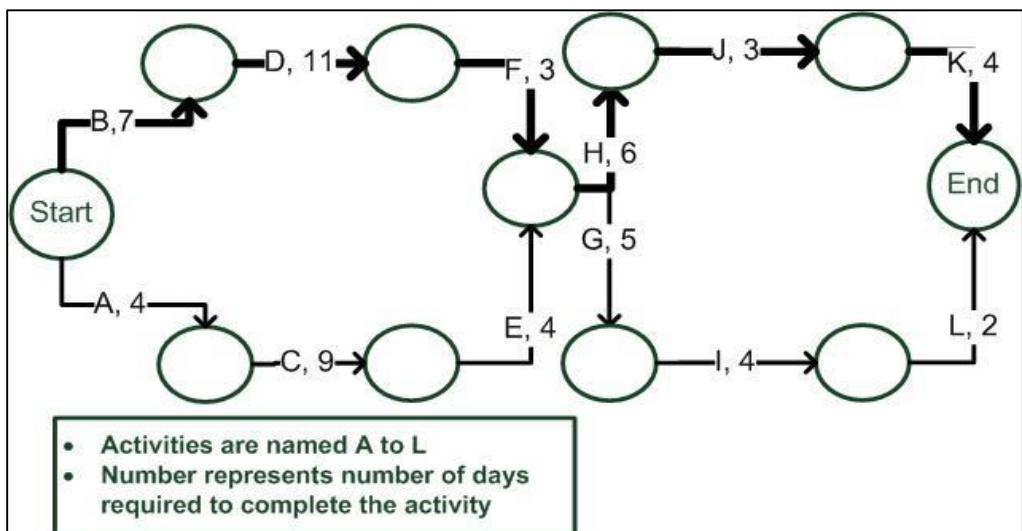


Figure 3.5: Critical Path Method (CPM)

Project manager can use the slack time on non-critical path for scheduling resources optimally, since slack time provides flexibility to start activity late than scheduled start date. The slack times for a project are computed by working forward through path, computing the earliest possible completion time for each activity, until the earliest possible completion time for the total project is found. Then by working backward through the network, the latest completion time for each activity is found, the slack time computed and the critical path identified.

Most CPM packages facilitate the analysis of resource utilization per time unit (e.g., day, week, etc.) and resource levelling, which is a way to level off resource peaks and valleys.

C. Gantt Charts

Gantt charts are aid for scheduling activities/tasks needed to complete a project. These charts show details related to activities calculated during PERT and CPM. The charts also show which activities are in progress concurrently and which activities must be completed sequentially. Gantt charts may reflect the resources assigned to each task and by what percent allocation. The charts aid in identifying activities that have been completed early or late. Progress of the entire project can be tracked from the Gantt chart. Gantt charts can also be used to track the milestones for the project.

Figure 3.6 Provides example of Gantt chart.

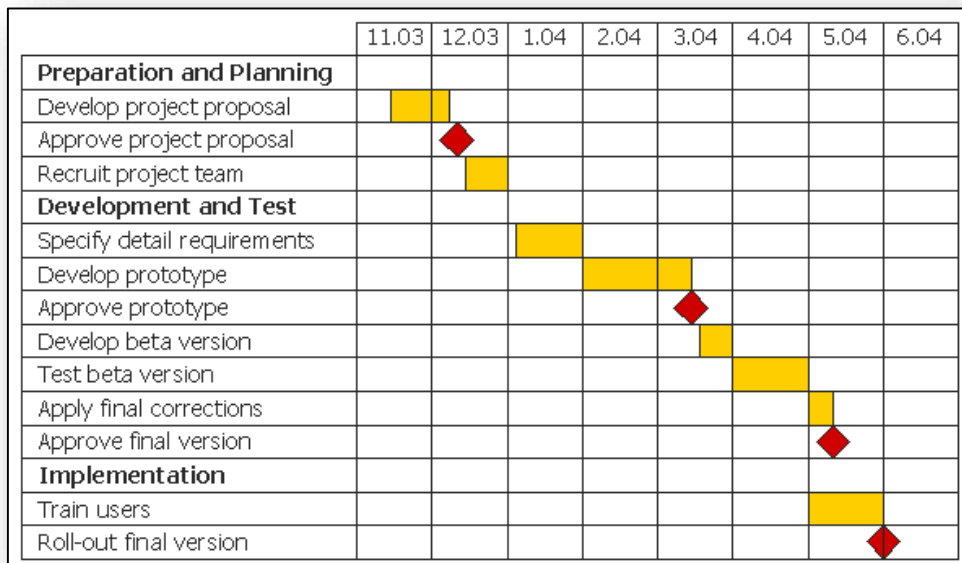


Figure 3.6: Gantt chart

3.11 Summary

Every project has unique success criteria based on the expectations of stakeholders. Generally success criteria are measurable and manageable such as cost, time and scope. However some criteria, such as meeting business needs, are subjective but essential. The project sponsor is a key stakeholder who defines such success criteria. The project team should capture project requirements and document them at the initial stage to complete the project successfully. Activity of capturing requirements is usually difficult because it involves subjective decisions and extensive interaction between users and developers. Requirements should be formally approved and then frozen (baselined) to prevent scope creep. Success criteria allow the project manager to focus on managing risks that can affect desirable outcome and successful completion of the project.

IS auditor should review adequacy of the following project management activities:

- **Levels of oversight by project committee/board**
- **Risk management methods within the project**
- **Issue management**
- **Cost management**
- **Processes for planning and dependency management**
- **Reporting processes to senior management**
- **Change control processes**
- **Stakeholder management involvement**
- **Sign-off process**
- **Adequate documentation of all phases of the SDLC process such as:**
 - **Availability of clearly defined objectives on what is to be accomplished during each phase.**
 - **Key deliverables of each phase with project personnel assigned direct responsibilities for these deliverables.**
 - **A project schedule with highlighted dates for the completion of key deliverables**
 - **An economic forecast for each phase, defining resources and the cost of the resources required to complete the phase.**

3.12 Questions

1. Who among the following is responsible for ongoing facilitation of a SDLC project?
 - A. Project sponsor
 - B. Project manager
 - C. Steering committee
 - D. Board of directors

2. A multi-national organization has decided to implement an ERP solution across all geographical locations. The organization shall initiate a:
- A. Project
 - B. Program
 - C. Portfolio
 - D. Feasibility study
3. Which of the following primarily helps project manager in mitigating the risk associated with change in scope of software development project?
- A. Change management process
 - B. Use of prototyping
 - C. Revising effort estimates
 - D. Baselining requirements
4. Monitoring which of the following aspect of SDLC project shall help organization in benefit realization over sustained period of time? The project adhering to:
- A. Quality
 - B. Budget
 - C. Schedule
 - D. Methodology
5. Which of the following tools and techniques primarily help in improving productivity of SDLC project team members?
- A. Use of standard methodology
 - B. Software sizing using FPA
 - C. Developers' workbench
 - D. Appropriate HR policies
6. While performing mid-term review of SDLC project, the IS auditor primarily focuses on:
- A. Project risk management process
 - B. Adherence to the schedule
 - C. Reviewing minutes of steering committee meeting
 - D. Cost management is as per budget

3.13 Answers and Explanations

1. A. Project sponsor is a stake holder having maximum interest / stake in the success of project and is primary responsibility is to coordinate with various stakeholders for project success. Project manager is responsible for executing the project activities. Steering committee monitors project progress but is not ongoing activity. Board of director provides direction.
2. B. Considering the spread of organization the organization shall initiate a program for implementing ERP, consisting of different project for each location. The program shall be part of IT

program portfolio of organization. Since the decision has been made, feasibility study either has been completed or shall be initiated as part of program.

3. D. Scope creep of continued changes in requirements during SDLC project is most common risk. If not properly handled the project may be delayed and benefit realization from the project shall be affected. The project manager therefore, must freeze the scope by base-lining requirements. Any change after base-lining shall follow change management process. Change management process without base-lining may not help. Project manager may or may not use prototyping for freezing the requirements. Revised effort estimate are applicable after change is approved.

4. A. Quality is most important aspect for SDLC project, since it minimizes errors that can impact operations.

5. C. Automated tools help team in improving productivity as these tools help in managing mundane and structure activities and developers can focus on core activities. Developers' workbench provides various functions that help in improving productivity. Use of standards help in following uniform methods and reducing rework. Software sizing is useful in monitoring productivity. HR policies may help in motivating team but it is secondary.

6. A. Auditor should primarily focus on risk management that will provide inputs on events that has impact on all aspects of project. Option B, C and D help in confirming the findings from review of risk management process.

CHAPTER 4: DIFFERENT MODELS AND METHODS FOR SDLC

Learning objectives

This chapter provide information on various software development models and methods. A project manager may adopt these models/methods depending upon functional and non-functional requirements to ensure the timely deliverables. The method selected is dependent on cost, time, quality and business requirements of the project.

4.1 Introduction

This chapter mainly covers basic understanding of system design and development methodologies being used while executing SDLC project. A Project manager and system analysis depending on requirements selects one or more software development methods and/or models for developing software. Execution of these models primarily focuses on converting requirements into a system design and to develop the solution. This chapter provides information of various models and methods that might be required for executing phases 4 and 5 of SDLC. IS auditor primarily should be looking for control aspects associated with development methodology.

Software development undergoes different phases as discussed in chapter 1. However the execution of these phases vary based on the requirements, particularly phase 3 to 6, i.e. analysis, design, development and testing. This chapter discusses the various models and methods used for software development. These models have been evolving due to changes in:

1. **Technology:** Few examples of impact of Technological advancement on SDLC process are:
 - a. Availability of faster processor and network has created a requirement of client server and web based application where application and data are segregated and hosted at one central location.
 - b. Separation of application from platform (OS, Hardware etc.). Organisations needed software that can run on any platform/OS, which has enabled development of platform independent systems using JAVA (or similar) development environments.
2. **Business requirements:** Spread and growth of business expects faster delivery of application/solutions from SDLC project. For example:
 - a. Dynamic changes in functional requirements due to customer focus and competition has reduced turnaround time in change management. This has been enabled by object oriented methodology which facilitates development of reusable and independent program modules.
 - b. Reduced time between conceptualization and go-to-market due to customer focused service approach. This has created the need for Rapid Application Development (RAD) and Agile Development Methodology.

3. **Availability of outsourcing for software development:** This has prompted changes in the SDLC methodology, for example:
 - a. **Requirement finalization:** Due to commercial aspects associated with outsourcing, requirement base lining using the prototype model has become the most popular model.
 - b. **Faster delivery of product:** This has enabled development teams to modify SDLC models e.g. waterfall model was changed to verification and validation model, spiral model and incremental model.

In this chapter, we will discuss salient features of various traditional SDLC models and methodologies such as:

1. Waterfall model
2. Spiral Model
3. Incremental model
4. Prototyping model

Further, we will also discuss some important methodologies that have evolved and are currently being used. The following six methodologies are explained here with strengths and weaknesses of each of them:

1. Rapid Application development (RAD)
2. Agile development
3. Re-engineering and reverse engineering
4. Object oriented development
5. Component based development
6. Web application development

4.2 SDLC Models

4.2.1 Waterfall model

The waterfall approach is a traditional development approach in which each phase is executed in sequence or in linear fashion. These phases include requirements analysis, specifications and design requirements, coding, final testing, and release. Fig. 4.1 shows representative model of this method. When the traditional approach is applied, an activity is undertaken only when the prior step is completed.

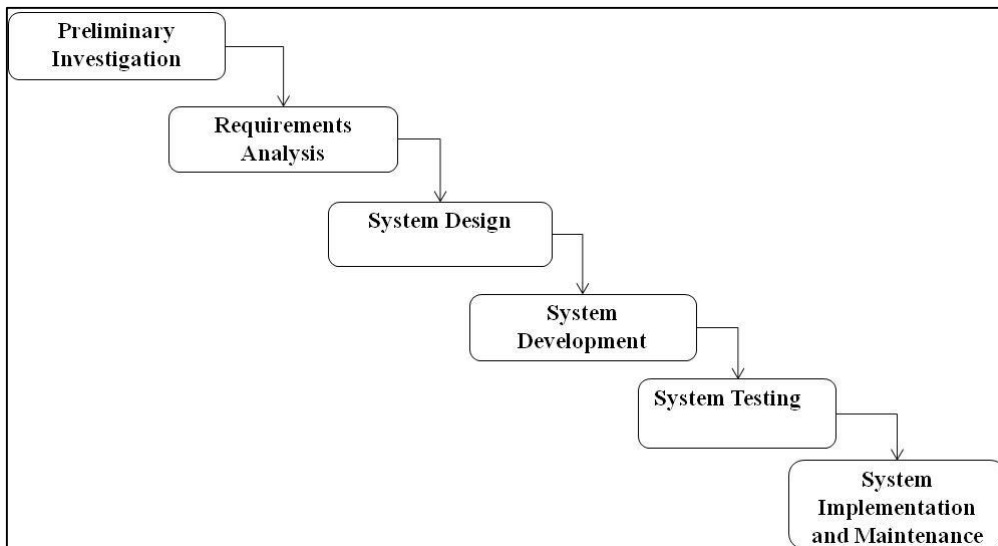


Fig. 4.1: Waterfall Approach

The characterizing features of this model have influenced the development community in big way. Some of the key characteristics are:

- Project is divided into sequential phases, with some overlap and splash back acceptable between phases.
- Emphasis is on planning, time schedules, target dates, budgets and implementation of an entire system at one time.
- Tight control is maintained over the life of the project through the use of extensive written documentation, as well as through formal reviews and approval/signoff by the user and information technology management occurring at the end of most phases before beginning the next phase.

Strengths:

- It is ideal for supporting less experienced project teams and project managers or project teams, whose composition fluctuates.
- The orderly sequence of development steps and design reviews help to ensure the quality, reliability, adequacy and maintainability of the developed software.
- Progress of system development can be tracked and monitored easily.
- It enables to conserve resources.

Weaknesses:

- It is criticized to be Inflexible, slow, costly, and cumbersome due to significant structure and tight controls.

- Project progresses forward, with only slight movement backward.
- There is a little to iterate, which may be essential in situations.
- It depends upon early identification and specification of requirements, even if the users may not be able to clearly define 'what they need early in the project'.
- Requirement inconsistencies, missing system components and unexpected development needs discovered during design and coding are most difficult to handle.
- Problems are often not discovered until system testing.
- System performance cannot be tested until the system is almost fully coded, and under capacity may be difficult to correct.
- It is difficult to respond to changes, which may occur later in the life cycle, and if undertaken it proves costly and are thus discouraged.
- Written specifications are often difficult for users to read and thoroughly appreciate.
- It promotes the gap between users and developers with clear vision of responsibility.

Verification and validation - a variant of waterfall model

In order to get benefits and reduce the inflexibility verification and validation variant was introduced. Figure 4.2 shows the changes made in the waterfall model. The model has introduced validation and verification at each stage (shown by dotted line). This model minimizes some weaknesses in waterfall model by retaining strengths.

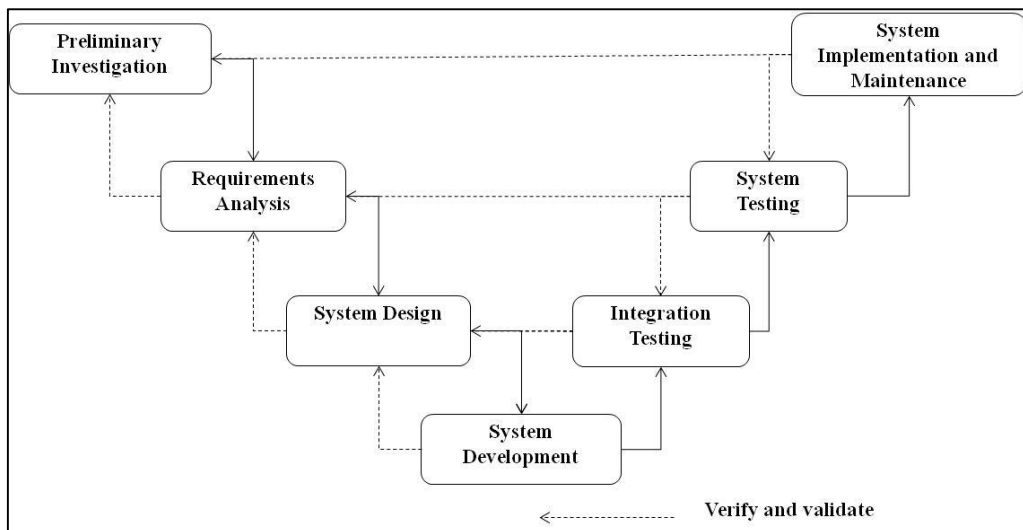


Figure 4.2: Variant of waterfall model

4.2.2 Prototyping methodology

The traditional approach sometimes may take long time to analyze, design and implement a system. More so, many a times we know a little about the system until and unless we go through its working phases, which are not available. In order to avoid such bottlenecks and overcome the issues, organisations are increasingly using prototyping techniques to develop smaller systems such as DSS, MIS and Expert systems. The goal of prototyping approach is to develop a small or pilot version called a prototype of part or all of a system. A prototype may be a usable system or system component that is built quickly and at a lesser cost, and with the intention of modifying/replicating/expanding or even replacing it by a full-scale and fully operational system. As users work with the prototype, they learn about the system criticalities and make suggestions about the ways to manage it. These suggestions are then incorporated to improve the prototype, which is also used and evaluated. Finally, when a prototype is developed that satisfies all user requirements, either it is refined and turned into the final system or it is scrapped. If it is scrapped, the knowledge gained from building the prototype is used to develop the real system.

Prototyping can be viewed as a series of four steps, symbolically depicted in Fig. 4.5 wherein implementation and maintenance phases followed by full-blown developments take place once the prototype model is tested and found to be meeting users' requirements.

Generic phases of model

- **Identify Information System Requirements:** In traditional approach, the system requirements are to be identified before the development process starts. However, under prototype approach, the design team needs only fundamental system requirements to build the initial prototype, the process of determining them can be less formal and time-consuming than when performing traditional systems analysis.
- **Develop the Initial Prototype:** The designers create an initial base model and give little or no consideration to internal controls, but instead emphasize system characteristics such as simplicity, flexibility, and ease of use. These characteristics enable users to interact with tentative versions of data entry display screens, menus, input prompts, and source documents. The users also need to be able to respond to system prompts, make inquiries of the information system, judge response times of the system, and issue commands.
- **Test and Revise:** After finishing the initial prototype, the designers first demonstrate the model to users and then give it to them to experiment and ask users to record their likes and dislikes about the system and recommend changes. Using this feedback, the design team modifies the prototype as necessary and then resubmits the revised model to system users for re-evaluation. Thus iterative process of modification and re-evaluation continues until the users are satisfied.
- **Obtain User Signoff of the Approved Prototype:** Users formally approve the final version of the prototype, which commits them to the current design and establishes a contractual obligation about what the system will, and will not, do or provide. Prototyping is not commonly used for developing traditional MIS and batch processing type of applications such as

accounts receivable, accounts payable, payroll, or inventory management, where the inputs, processing, and outputs are well known and clearly defined.

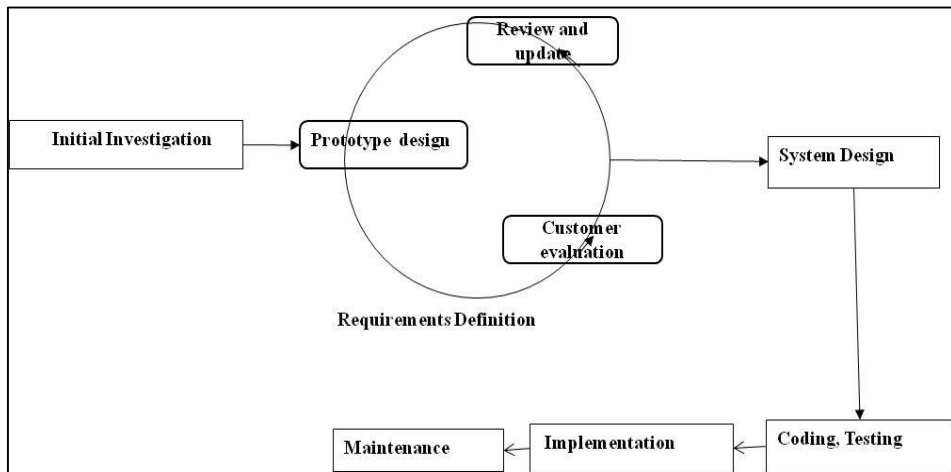


Fig. 4.3: Prototyping Model

Strengths:

- It improves both user participation in system development and communication among project stakeholders.
- It is especially useful for resolving unclear objectives and requirements; developing and validating user requirements; experimenting with or comparing various design solutions, or investigating both performance and the human computer interface.
- Potential exists for exploiting knowledge gained in an early iteration as later iterations are developed.
- It helps to easily identify, confusing or difficult functions and missing functionality.
- It enables to generate specifications for a production application.
- It encourages innovation and flexible designs.
- It provides for quick implementation of an incomplete, but functional, application.
- It typically results in a better definition of these users' needs and requirements than does the traditional systems development approach.
- A very short time period is normally required to develop and start experimenting with a prototype. This short time period allows system users to immediately evaluate proposed system changes.
- Since system users experiment with each version of the prototype through an interactive process, errors are hopefully detected and eliminated early in the developmental process. As a result, the information system ultimately implemented should be more reliable and less costly to develop than when the traditional systems development approach is employed.

Weaknesses:

- Approval process and control are not formal.
- Incomplete or inadequate problem analysis may occur whereby only the most obvious and superficial needs will be addressed, resulting in current inefficient practices being easily built into the new system.
- Requirements may frequently change significantly.
- Identification of non-functional elements is difficult to document.
- Designers may prototype too quickly, without sufficient upfront user needs analysis, resulting in an inflexible design with narrow focus that limits future system potential.
- Prototype may not have sufficient checks and balances incorporated.
- Prototyping can only be successful if the system users are willing to devote significant time in experimenting with the prototype and provide the system developers with change suggestions. The users may not be able or willing to spend the amount of time required under the prototyping approach.
- The interactive process of prototyping causes the prototype to be experimented with quite extensively. Because of this, the system developers are frequently tempted to minimize the testing and documentation process of the ultimately approved information system. Inadequate testing can make the approved system error-prone, and inadequate documentation makes this system difficult to maintain.
- Prototyping may cause behavioural problems with system users. These problems include dissatisfaction by users if system developers are unable to meet all user demands for improvements as well as dissatisfaction and impatience by users when they have to go through too many interactions of the prototype.

In spite of above listed weaknesses, to some extent, systems analysis and development has been greatly improved by the introduction of prototyping. Prototyping enables the user to take an active part in the systems design, with the analyst acting in an advisory role. Prototyping makes use of the expertise of both the user and the analyst, thus ensuring better analysis and design, and prototyping is a crucial tool in that process.

Prototype has one major drawback that many times users do not realize that prototype is not actual system or code but is just a model whereas users may think that the system is ready. Actual development starts only after the prototype is approved. Hence, the actual system may require time before it is ready for implementation and use. In the meantime, users may get restless and wonder why there is so much delay.

4.2.3 Spiral Model

The Spiral model is a repetitive software development process combining elements of both design and prototyping within each of the iterations. It combines the features of the prototyping model and

the waterfall model (given in Fig. 4.3). Initially spiral model was intended for large, expensive and complicated projects like Game development because of size and constantly shifting goals of large projects. Spiral model when defined was considered and best model and further models were developed using spiral models.

Key characteristics

- Spiral model is an iterative model where each iteration helps in optimizing the intended solution.
- The new system requirements are defined in as much detail as possible. This usually involves interviewing a number of users representing all the external or internal users and other aspects of the existing system.
- A preliminary design is created for the new system during initial iterations. This phase is the most important part of “Spiral Model” in which all possible alternatives that can help in developing a cost effective project are analysed and strategies are decided to use them. This phase has been added specially in order to identify and resolve all the possible risks in the project development. If risks indicate any kind of uncertainty in requirements, prototyping may be used to proceed with the available data and find out possible solution in order to deal with the potential changes in the requirements.
- A first prototype of the new system is constructed from the preliminary design during first iteration. This is usually a scaled-down system, and represents an approximation of the characteristics of the final product.
- A second prototype is evolved during next iteration by a fourfold procedure by evaluating the first prototype in terms of its strengths, weaknesses, and risks; defining the requirements of the second prototype; planning and designing the second prototype; and constructing and testing the second prototype.

Strengths:

- Enhances the risk avoidance.
- Useful in helping for optimal development of a given software iteration based on project risk.
- Incorporates Waterfall, Prototyping, and Incremental methodologies as special cases in the framework, and provide guidance as to which combination of these models best fits a given software iteration, based upon the type of project risk. For example, a project with low risk of not meeting user requirements but high risk of missing budget or schedule targets would essentially follow a linear Waterfall approach for a given software iteration. Conversely, if the risk factors were reversed, the Spiral methodology could yield an iterative prototyping approach.

Weaknesses:

- It is challenging to determine the exact composition of development methodologies to use for each of the iterations around the Spiral.

- A skilled and experienced project manager is required to determine how to apply it to any given project.
- Sometimes there are no firm deadlines, cycles continue till requirements are clearly identified. Hence has an inherent risk of not meeting budget or schedule.

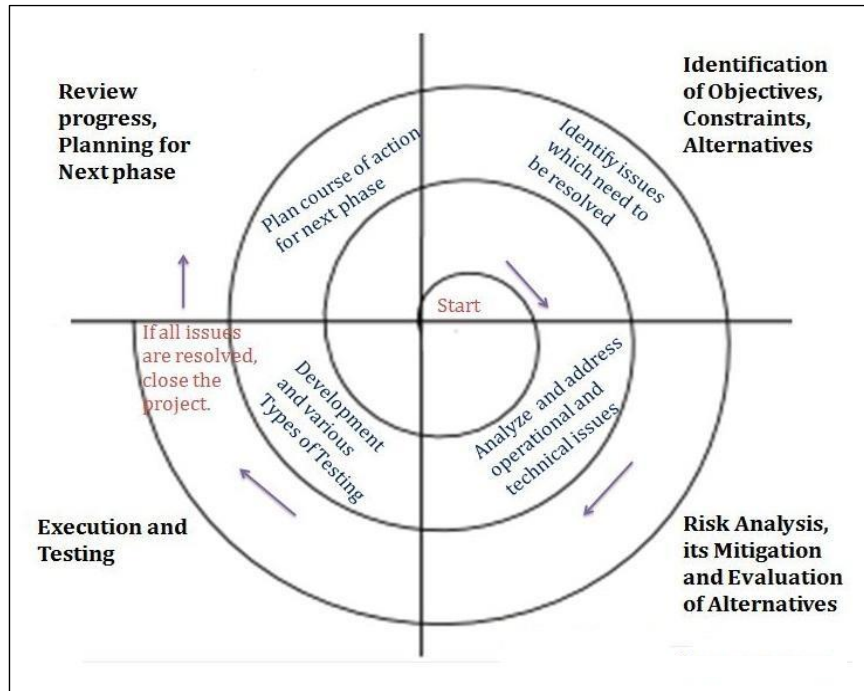


Fig. 4.4: Spiral Model

4.2.4 The Incremental Model

The Incremental model is a method of software development where the model is designed, implemented and tested incrementally (a little more is added each time) until the product is finished. The product is defined as finished when it satisfies all of its requirements. This model combines the elements of the waterfall model with the iterative philosophy of prototyping. It is pictorially depicted in Fig. 4.4.

The product is decomposed into a number of components, each of which are designed and built separately (termed as builds). Each component is delivered to the client when it is complete. This allows partial utilization of product and avoids a long development time. It also creates a large initial capital outlay with the subsequent long wait avoided. This model of development also helps to ease the traumatic effect of introducing completely new system all at once. A few pertinent features are listed as follows:

- A series of mini-waterfalls are performed, where all phases of the waterfall development model are completed for a small part of the system, before proceeding to the next increment.
- Overall requirements are defined before proceeding to evolutionary, mini – Waterfall development of individual increments of the system.
- The initial software concept, requirement analysis, and design of architecture and system core are defined using the Waterfall approach, followed by iterative Prototyping, which culminates in installation of the final prototype (i.e. working system).

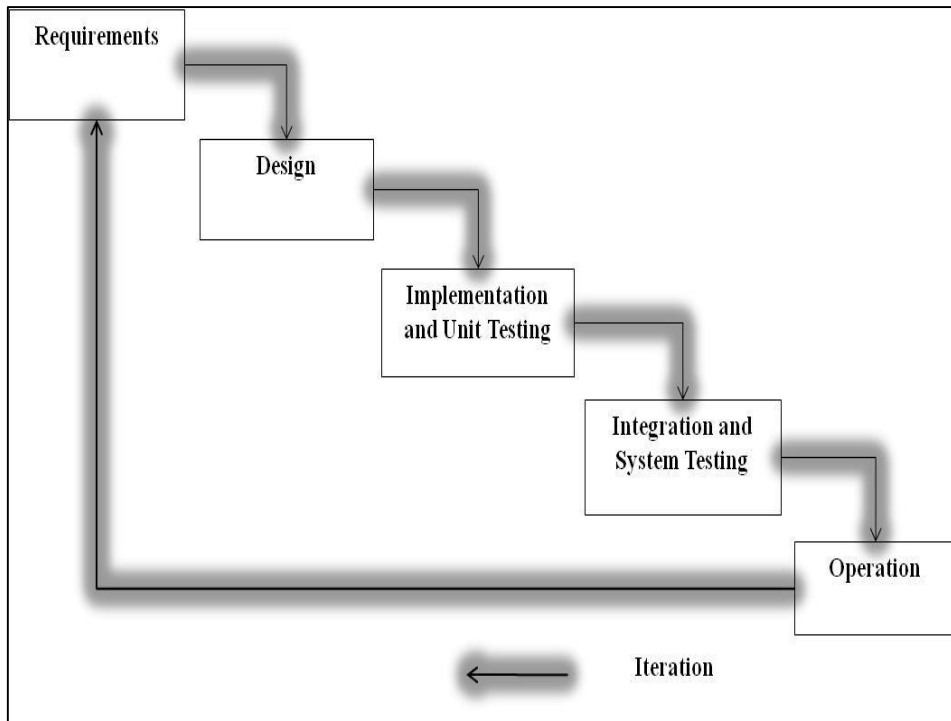


Fig. 4.5: Incremental Model

Strengths:

- Potential exists for exploiting knowledge gained in an early increment as later increments are developed.
- Moderate control is maintained over the life of the project through the use of written documentation and the formal review and approval/signoff by the user and information technology management at designated major milestones.
- Stakeholders can be given concrete evidence of project status throughout the life cycle.
- It is more flexible and less costly to change scope and requirements.
- It helps to mitigate integration and architectural risks earlier in the project.

- It allows the delivery of a series of implementations that are gradually more complete and can go into production more quickly as incremental releases.
- Gradual implementation provides the ability to monitor the effect of incremental changes, isolated issues and make adjustments before the organisation is negatively impacted.

Weaknesses:

- When utilizing a series of mini-waterfalls for a small part of the system before moving onto the next increment, there is usually a lack of overall consideration of the business problem and technical requirements for the overall system.
- Each phase of an iteration is rigid and do not overlap each other.
- Problems may arise pertaining to system architecture because not all requirements are gathered up front for the entire software life cycle.
- Since some modules will be completed much earlier than others, well-defined interfaces are required.
- It is difficult to demonstrate early success to management.

4.3 SDLC Methodologies

4.3.1 Rapid Application Development (RAD)

RAD refers to a type of software development methodology, which uses minimal planning in favour of rapid prototyping. (Figure 4.6) The planning of software developed using RAD is interleaved with writing the software itself. The lack of extensive pre-planning generally allows software to be written much faster, and makes it easier to change requirements. The key features are:

- Key objective is fast development and delivery of a high quality system at a relatively low investment cost,
- Attempts to reduce inherent project risk by breaking a project into smaller segments and providing more ease-of-change during the development process.
- Aims to produce high quality systems quickly, primarily through the use of iterative Prototyping (at any stage of development), active user involvement, and computerized development tools like Graphical User Interface (GUI) builders, Computer Aided Software Engineering (CASE) tools, Database Management Systems (DBMS), Fourth generation programming languages, Code generators and object-oriented techniques.
- Key emphasis is on fulfilling the business need while technological or engineering excellence is of lesser importance.
- Project control involves prioritizing development and defining delivery deadlines or “time boxes.” If the project starts to slip, emphasis is on reducing requirements to fit the time box, not in increasing the deadline.
- Generally includes Joint Application Development (JAD), where users are intensely involved in system design, either through consensus building in structured workshops, or through electronically facilitated interaction.

- Active user involvement is imperative.
- Iteratively produces production software, as opposed to a throwaway prototype.
- Produces documentation necessary to facilitate future development and maintenance.
- Standard systems analysis and design techniques can be fitted into this framework.

Strengths:

- The operational version of an application is available much earlier than with Waterfall, Incremental, or Spiral frameworks.
- Because RAD produces systems more quickly and to a business focus, this approach tends to produce systems at lower cost.
- Quick initial reviews are possible.
- Constant integration isolates problems and encourages customer feedback.
- It holds a great level of commitment from stakeholders, both business and technical, than Waterfall, Incremental, or spiral frameworks. Users are seen as gaining more of a sense of ownership of a system, while developer are seen as gaining more satisfaction from producing successful systems quickly.
- It concentrates on essential system elements from user viewpoint.
- It provides for the ability to rapidly change system design as demanded by users.
- It leads to a tighter fit between user requirements and system specifications.

Weaknesses:

- Fast speed and lower cost may affect adversely the system quality.
- The project may end up with more requirements than needed (gold-plating).
- Potential for feature creep where more and more features are added to the system during development.
- It may lead to inconsistent designs within and across systems.
- It may call for violation of programming standards related to inconsistent naming conventions and inconsistent documentation,
- It may call for lack of attention to later system administration needs built into system.
- Formal reviews and audits are more difficult to implement than for a complete system.
- Tendency for difficult problems to be pushed to the future to demonstrate early success to management.
- As some modules are completed much earlier than others, well-defined interfaces are required.

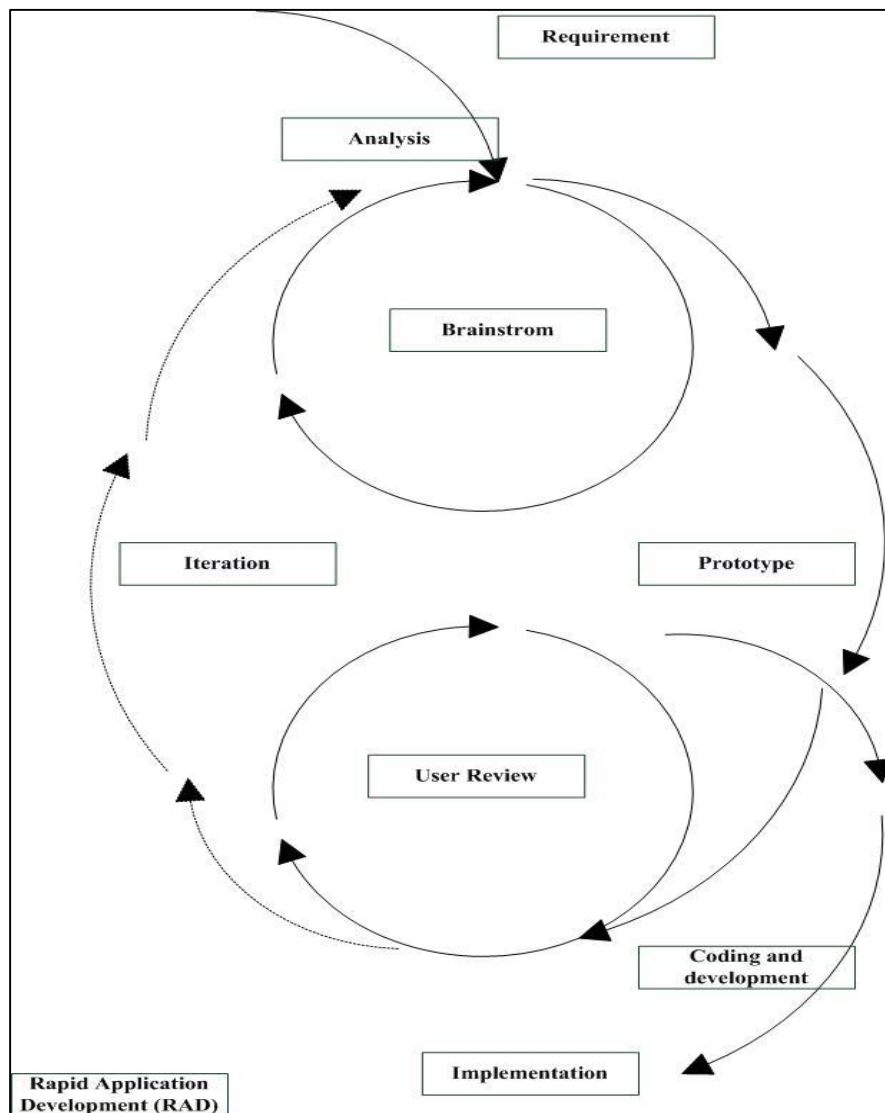


Figure 4.6: RAD

4.3.2 Agile software development methodology

The term “agile development” refers to a family of similar development processes that adopt a non-traditional way of developing complex systems. The term “agile” refers to characteristic of processes that are designed to flexibly handle changes to the system being developed. Scrum is the first project management approach that fits well with other agile techniques. Other agile processes that have since emerged such as Extreme Programming (XP), Crystal, Adaptive

Software Development, Feature Driven Development, and Dynamic Systems Development Method.

Key Characteristics of Agile processes

- Use of small, time-boxed subprojects or iterations where each iteration forms basis for planning next iteration.
- Re-planning the project at the end of each iteration (referred to as a “sprint” in Scrum), including reprioritizing requirements, identifying any new requirements and determining within which release delivered functionality should be implemented
- Relatively greater reliance, compared to traditional methods, on the knowledge in people’s heads(tacit knowledge), as opposed to external knowledge that is captured in project documentation
- A heavy influence on mechanisms to effectively disseminate tacit knowledge and promote teamwork. Therefore, teams are kept small in size, comprise both business and technical representatives, and are located physically together. Team meetings to verbally discuss progress and issues occur daily, but with strict time limits.
- At least some of the agile methods stipulate pair-wise programming (two persons code the same part of the system) as a means of sharing knowledge and as a quality check.
- A change in the role of the project manager, from one primarily concerned with planning the project, allocating tasks and monitoring progress to that of a facilitator and advocate. Responsibility for planning and control is delegated to the team members.

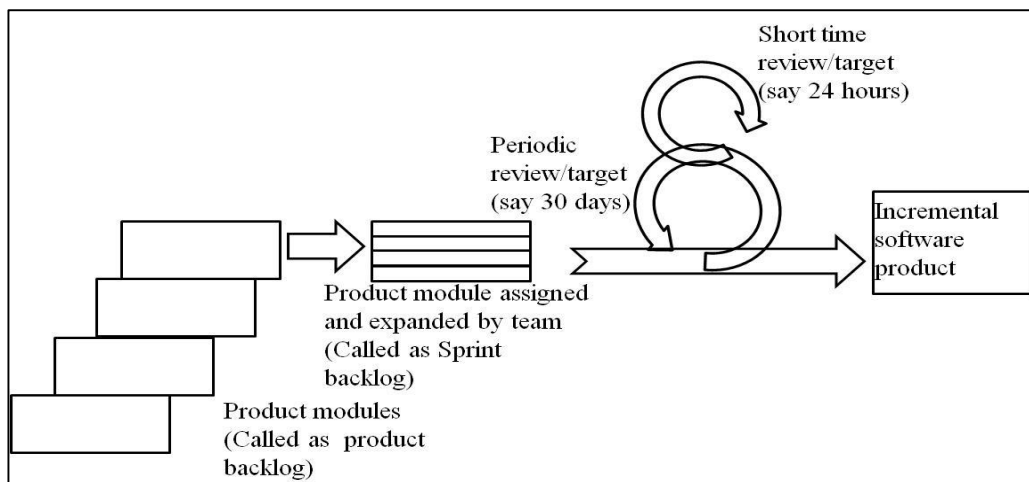


Figure 4.7: Agile (Sprint) review cycle

The agile methodology may be considered as *iterative and incremental* development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development and delivery; time boxed iterative

approach and encourages rapid and flexible response to change. It is a conceptual framework that promotes foreseen interactions throughout the development life cycle.

Key features of agile methodologies

- Customer satisfaction by rapid delivery of useful software;
- Welcome changing requirements, even late in development;
- Working software is delivered frequently (weeks rather than months);
- Working software is the principal measure of progress;
- Sustainable development, able to maintain a constant pace;
- Close, daily co-operation between business people and developers;
- Face-to-face conversation is the best form of communication (co-location);
- Projects are built around motivated individuals, who should be trusted;
- Continuous attention to technical excellence and good design;
- Simplicity; Self-organizing teams; and
- Regular adaptation to changing circumstances.

Strengths:

- Agile methodology has the concept of an adaptive team, which enables to respond to the changing requirements.
- The team does not have to invest time and efforts and finally find that by the time they delivered the product, the requirement of the customer has changed.
- Face to face communication and continuous inputs from customer representative leaves a little space for guesswork.
- The documentation is crisp and to the point to save time.
- The end result is generally the high quality software in least possible time duration and satisfied customer.

Weaknesses:

- In case of some software deliverables, especially the large ones, it is difficult to assess the efforts required at the beginning of the System Development life cycle.
- There is lack of emphasis on necessary designing and documentation due to time management and generally is left out or incomplete.
- Agile increases potential threats to business continuity and knowledge transfer due to verbal communication and weak documentation.
- Agile requires more re-work and due to the lack of long-term planning and the lightweight approach to architecture.
- The project can easily get taken off track if the customer representative is not clear about the requirements and final outcome.
- Agile lacks the attention to outside integration.

4.3.3 Software reengineering and reverse engineering

Software reengineering

Reengineering as name suggest is a process of updating an existing system by reusing design and program components. Although it updates existing software it is used in case of major changes in existing system, it differs from change management due to the extent of changes. These changes typically prompts for new software development project, however as interim solution a reengineering project is initiated. A number of tools are now available to support this process.

What is software reengineering?

- Restructuring or rewriting part or all of a system without changing its functionality
- Applicable when some (but not all) subsystems of a larger system require frequent maintenance
- Reengineering involves putting in the effort to make it easier to maintain
- The reengineered system may also be restructured and re-documented

When to reengineer?

- When system changes are confined to one subsystem, the subsystem needs to be reengineered
- When hardware or software support becomes obsolete
- When tools to support restructuring are readily available
- When some business processes or functions are reengineered

Software Reengineering Activities

- **Inventory analysis** – listing and identifying active software applications and components required by business. The attributes of applications can be criticality, longevity, current maintainability. This helps in identifying reengineering criteria.
- **Document restructuring** – Identify documentation for identified applications/modules. (Identifying poor or weak documentation for re-documentation sometimes considered as reengineering activity)
- **Design recovery** –Identify the design of the application module to be reengineered. (In case it is not available it may have to be built based on code or use reverse engineering method)
- **Reverse engineering** – process of design recovery - analyzing a program in an effort to create a representation of the program at some abstraction level higher than source code
- **Code restructuring** – source code is analysed and violations of structured programming practices are noted and repaired, the revised code also needs to be reviewed and tested
- **Data restructuring** – usually requires full reverse engineering, current data architecture is dissected and data models are defined, existing data structures are reviewed for quality
- **Forward engineering** – also called reclamation or renovation, recovers design information from existing source code and uses this information to reconstitute the existing system to

improve its overall quality and/or performance.

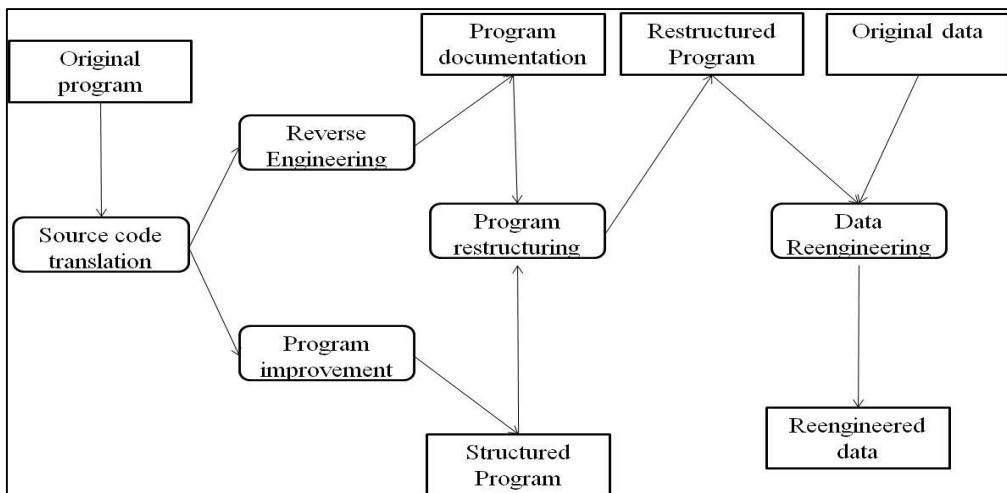


Figure 4.8: Reengineering and reverse Engineering

Reverse Engineering

Reverse engineering is the process of studying and analyzing an application, a software application or a product to see how it functions and to use that information to develop a similar system. This process can be carried out in several ways:

- Decompiling object or executable code into source code and using it to analyze the program
- Black box testing the application to be reverse-engineered to unveil its functionality

The major advantages of reverse engineering are:

- Faster development and reduced SDLC duration
- The possibility of introducing improvements by overcoming the reverse-engineered application drawbacks

The IS auditor should be aware of following risks:

- **Software license agreements often contain clauses prohibiting the licensee from reverse engineering the software so that any trade secrets or programming techniques are not compromised.**
- **Decompilers are relatively new tools with functions that depend on specific computers, operating systems and programming languages. Any change in one of these components may require developing or purchasing a new decompiler.**

4.3.4 Object oriented software development (OOSD)

OOSD differs from traditional SDLC approach which considers data separately from the procedures that act on them (e.g., program and database specifications). OOSD is the process of solution specification and modelling where data and procedures can be grouped into an entity known as an object. An object's data are referred to as its attributes and its functionality is referred to as its methods. Proponents of OOSD claim the combination of data and functionality is aligned with how humans conceptualize everyday objects.

Objects usually are created from a general template called a class. The template contains the characteristics of the class without containing the specific data that need to be inserted into the template to form the object.

Classes are the basis for most design work in objects. Classes are either super-classes (i.e., root or parent classes) with a set of basic attributes or methods, or subclasses which inherit the characteristics of the parent class and may add (or remove) functionality as required. In addition to inheritance, classes may interact through sharing data, referred to as aggregate or component grouping, or sharing objects.

Aggregate classes interact through messages, which are requests for services from one class (called a client), to another class (called a server). The ability of two or more objects to interpret a message differently at execution, depending on the superclass of the calling object, is termed polymorphism.

For example consider a car owned by you as an object. The object is complete in itself and all necessary data (components and specifications) are embedded into object. You can use this object for specific use it has been designed for. However there are different objects either having similar data (same model, same company) or different data (Different model, different companies etc.) These all objects belong to class cars. All object cars have common attributes (i.e. steering, gear, break, wheels etc.) that are inherited from class cars (or may be from superclass vehicles). One can modify car by keeping basic common attributes and add few more functions to it. (Polymorphism)

There are many programming languages that are used for developing object oriented systems. To realize the full benefits of using object-oriented programming, it is necessary to employ object-oriented analysis and design approaches. Dealing with objects should permit analysts, developers and programmers to consider larger logical chunks of a system and clarify the programming process. Although it is possible to do object-oriented development using a waterfall model in practice most object-oriented systems are developed with an iterative approach. As a result in object-oriented processes "analysis and design" are often considered at the same time. OOSD being programming method, a particular programming language, or use of a particular programming technique, does not imply or require use of a particular software development methodology.

Advantages of OOSD:

- The ability to manage an unrestricted variety of data types
- Provision of a means to model complex relationships
- The capacity to meet the demands of a changing environment

A significant development in OOSD has been the decision by some of the major players in object-oriented development to join forces and merge their individual approaches into a unified approach using the Unified Modelling Language (UML). UML is a general-purpose notational language for specifying and visualizing complex software for large object-oriented projects. This signals a maturation of the object-oriented development approach. While object-orientation is not yet pervasive, it can accurately be said to have entered the computing mainstream.

Applications that use object-oriented technology are:

- Web applications
- E-business applications
- CASE for software development
- Office automation for email and work orders
- Artificial intelligence
- Computer-aided manufacturing (CAM) for production and process control

4.3.5 Component Based development

Component-based development is an outgrowth of object-oriented development. Component-based development is in fact assembling packages of executable software that make their services available through defined interfaces. These packages also called as enabling pieces of programs are called objects. These objects are independent of programming languages or operating system. The basic types of components are:

- **In-process client components:** These components must run from within defined program (called as 'container') such as a web browser; they cannot run on their own.
- **Stand-alone client components**—Applications (like Microsoft's Excel and Word) that work as service.
- **Stand-alone server components**—Processes running on servers that provide services in standardized way. These are initiated by remote procedure calls or some other kind of network call. Technologies supporting this include Microsoft's Distributed Component Object Model (DCOM), Object Management Group's Common Object Request Broker Architecture (CORBA) and Sun's Java through Remote Method Invocation (RMI).
- **In-process server components:** These components run on servers within containers. Examples include Microsoft's Transaction Server (MTS) and Sun's Organisation Java Beans (EJB)

A number of different component models have emerged. E.g. Microsoft's Component Object Model (COM). MTS when combined with COM allows developers to create components that can be

distributed in the Windows environment. COM is the basis for ActiveX technologies, with ActiveX Controls being among the most widely used components. Alternative component models include the CORBA Component Model and Sun's EJB.

COM/DCOM, CORBA and RMI are sometimes referred to as distributed object technologies or also termed middleware. (Middleware is a broad term, but a basic definition is software that provides run-time services where by programs/ objects/ components can interact with one another).

Visual tools are now available for designing and testing component-based applications. Components play a significant role in web-based applications.

Advantages of component-based development are:

- This reduces development time as application system can be assembled from prewritten components and only code for unique parts of the system needs to be developed.
- Improves quality by using prewritten and tested components.
- Allows developers to focus more strongly on business functionality.
- Promotes modularity by encouraging interfaces between discrete units of functionality.
- Simplifies reuse and avoids need to be conversant with procedural or class libraries.
- Combining and allowing reusable code to be distributed in an executable format—i.e., no source is required.
- Reduces development cost as less effort is required for designing and building the software.
- Supports multiple development environments due to platform independent components.
- Allows a satisfactory compromise between build and buy options i.e. instead of buying a complete solution, it could be possible to purchase only needed components and incorporate these into a customized system.

Disadvantages:

- Attention to software integration should be provided continuously during the development process.
- If system requirements are poorly defined or the system fails to adequately address business needs, the project will not be successful.

4.3.6 Web-based application development

Web based development has modified client-server architecture and made it more light weight and easy to implement. It has eliminated the need to implement client module on end-user's desktop, and is delivered via internet based technologies. User need to know URL to access the application and if need be the same is delivered on users' desktop or executed from web server. The technology can be deployed within organisation also. For example many organisations have implemented internal user services using intranet portal, which essentially uses internet (web) based technologies.

Historically, software written in one language on a particular platform has used a dedicated application programming interface (API). The use of specialized APIs has caused difficulties in integrating software modules across platforms. Component based technologies such as CORBA and COM that use remote procedure calls (RPCs) have been developed to allow real-time integration of code across platforms. However, using these RPC approaches for different APIs still remains complex. Web-based application development is designed to further facilitate and standardize code module and program integration.

Web-based application development enables users to avoid the need to perform redundant computing tasks with redundant code. For example installing client on all users after making changes or change of address notification from a customer need not be updated separately in multiple databases. For example entering and maintaining same data in contact management, accounts receivable etc. Web application development though is different than traditional developments (e.g. users test and approve the development work), but the risks of application development remain the same.

With web-based application development, an XML language known as Simple Object Access Protocol (SOAP) is used to define APIs. SOAP will work with any operating system and programming language that understands XML. SOAP is simpler than using the more complex RPC-based approach, with the advantage that modules are coupled loosely so that a change to one component does not normally require changes to other components. The second key component of web development is the Web Services Description Language (WSDL), which is also based on XML. WSDL is used to identify the SOAP specification that is to be used for the code module API and the formats of the SOAP messages used for input and output to the code module. The WSDL is also used to identify the particular web service accessible via a corporate intranet or across the Internet by being published to a relevant intranet or Internet web server.

4.4 Summary

Software development is the key to automate business processes using information technology. With changing technologies the SDLC models and methods have undergone many changes. However, the basic risks of SDLC still exist and these are:

- Poor coding techniques.
- Inadequate documentation.
- Inadequate QC and QA (including testing inadequacies).
- Lack of proper change control and controls over promotion into production.
- Inappropriate processes for development processes and deliverables.
- Technical vulnerabilities, and how these could materialize and be controlled/addressed

An IS auditor may not have to master all the development methods but must focus on a risk-based approach in the assessment of SDLC process. The approach should be to identify the business goals and supporting IT goals related to the development and based on these identify the risks. During SDLC audit the focus has to be on application development risks and associated business risks. Some of these controls may look similar for all application development activity. However, these will have to be relevant to the development activity that is taking place in the area which are the subject of audit.

4.5 Questions

1. A SDLC project for updating existing application has been initiated, however project manager has realized that the documentation has not been updated and source code is not available. Which of the following method shall help the project manager?

- A. Business process reengineering
- B. Reverse engineering
- C. Component based development
- D. Agile development method

2. Reusing already developed programs helps project manager in improving productivity. Which of the following methodology is outcome of this concept?

- A. Agile development methodology
- B. Object oriented software development
- C. Component based development
- D. Rapid application development

3. Which of the following is a major weakness of agile development methodology?

- A. High dependence of user interaction
- B. Reduced focus on recording design
- C. Reduced size of development team
- D. Project manager is in role of facilitator

4. The primary advantage of prototyping is that it:

- A. increases user interaction
- B. helps in outsourcing decision
- C. used in rapid application development
- D. helps in finalizing user requirements

5. Which of the following model addresses the weakness of waterfall model related to accommodating changes during development stage?

- A. Spiral model
- B. Incremental model
- C. Validation and verification
- D. Web development method

6. Which of the following activity is most important for IS auditor conducting mid-term review of SDLC?

- A. Ensure risks associated with development method are controlled.
- B. Review appropriateness of development method.
- C. Extrapolate the completion time based on current state.
- D. Perform code review of programs developed so far.

4.6 Answers and Explanations

1. B. Reverse engineering helps in understanding existing system and therefore the primary requirements that can be reengineered to develop new application. Project manager may use any development method depending upon type of application to be developed and deployed.

2. C. Reusing already developed program is most common in software development. However the development model based on this concept is called component based development where program components are already developed and programmer may just use them directly. In Object oriented method Object and classes are reused after customizing. Agile and Rapid development are not primarily developed for reusability.

3. B. The major challenge faced by Agile development is weak documentation of design and related record. Since it heavily depends upon working in interaction with users, where small team of experts captures requirements and develops functional code that can be deployed.

4. D. Prototyping helps in finalizing user requirements where users can review the prototype and confirm if it meets the requirements. This method is used in various models like rapid application development, agile development, spiral model etc.

5. C. Waterfall model requires finalization of earlier phase before beginning next phase. This makes it difficult to accommodate subsequent changes. Validation and verification method helps in overcoming this weakness by introducing iteration during each phase.

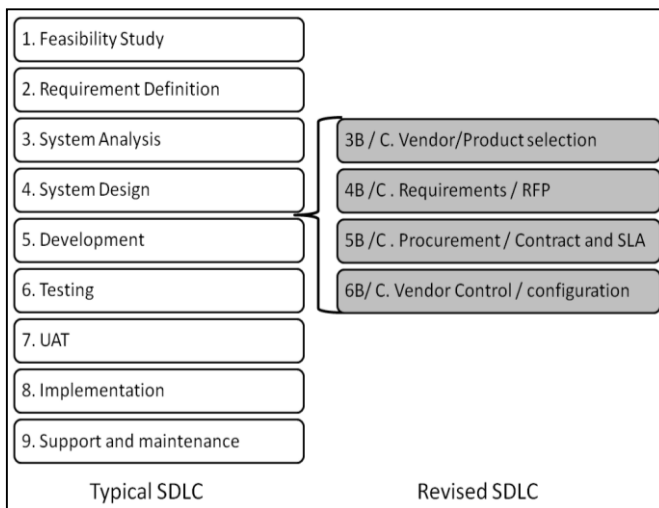
6. A. IS auditor should ensure that objectives of organization in initiating SDLC project are met by confirming that the risks associated with development are controlled.

CHAPTER 5: SYSTEM ACQUISITION FRAMEWORK

Learning objectives

This chapter focuses on steps required to be followed by the project manager if the organisation decide to acquire the software solution. This includes identifying different types of solutions available in market, the techniques on how to analyze them and select the right solution as required. In case organisation decides to outsource the development the steps required to be followed in selecting and monitoring the vendor are discussed. This chapter covers phases 3 B to 6B and 3C to 6C in changed SDLC described in chapter 1.

5.1 Introduction



This chapter provides information on Phase 3B to 6B covering software acquisition processes and 3C to 6C outsourcing of system development (shadowed area).

This chapter discusses the process generally followed by various organisations for software acquisition and outsourcing.

IS auditor primarily should be looking for control aspects associated with outsourcing to ensure that expected benefits can be derived.

Changes in technology have introduced additional phase in traditional SDLC such as software acquisition. A decision for acquiring software may be reached due to various reasons such as availability of commercial software, lack of skilled resources within organisation; the cost of in-house development is higher than benefits of acquiring, focus on core competency, etc. Software acquisition is the process that should occur after the requirements definition phase.

Depending on requirement there could be three cases:

1. **Generic products without customization:** Software is available and can be implemented without customization. These products are also known as Plug-and-play or COTS (Commercial of the shelf) for example MS Office, MS projects etc.
2. **Commercial product with customization:** Software needs to be customized like ERP or core banking products or at lower level customization like Tally.
3. **Outsourced development:** Ready-made software as required is not available. Hence, the organisation intends to outsource development activities based on cost benefit analysis.

1. **Software acquisition decision must be supported by users and users need to be actively involved in evaluation and selection process.**
2. **The feasibility study should contain documentation that supports the decision to acquire the software.**
3. **This chapter describes the acquisition process for application software. Acquisition of supporting software (like operating system, Database and Middleware) is not discussed here since acquisition of these supporting software depends upon primary application, organizational policies and internal standards., However, the processes discussed here can be followed for acquiring these products also.**

Table 5.1 shows the high-level steps in software acquisition process and their applicability for each of three cases mentioned above.

Table 5.1: Software acquisition – comparison of steps

Software Acquisition Steps	Generic products without customization	Commercial product with customization	Outsourced development
Requirement analysis	General requirements	Detail of functionality	Highly granular requirement analysis is required
Gap Analysis	For record	Can be reduced by vendor	Not applicable, as the vendor shall be developing required functionalities
Selection of product	User involvement is necessary	User Involvement is Must	User Involvement is for specifying requirements
Request for Proposal (RFP)	May or May not required	Required	Required
Selection of vendor	General	Specific based on requirements and support	Specific based on requirements, Sustainability and skills
Service level Agreement (SLA)	may not required	Required for support	Essential since the product is specific to organization
User Acceptance (UAT)	may not required	Detailed UAT and sign off for configuration	Detailed UAT and Sig-off for functionalities
Implementation Support	may not required	Required	Required
Maintenance Support	On call	On demand	On going
Ownership of software	License to use	Licensed to use based on contract	Depends upon agreement, organization can own software
Vendor monitoring	Not applicable	Only for support service	Continuous monitoring

5.2 Requirements Analysis

Defining detailed requirement is most essential in case of software acquisition, as selection of product or details of contract for outsourcing development, heavily depends on meeting the maximum or all requirements. This requires involvement of users in thorough and detailed understanding of the system, identifying areas that need to be covered to solve the problem and determination of monitoring requirements to select appropriate solution.

Requirement analysis focuses in achieving the following objectives:

- To consult user management (stakeholders) to determine their expectations.
- To analyze requirements to detect conflicts and determine priorities
- To gather data by various means to ensure requirement gathering is complete.
- To verify that the requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable.

The specific steps which help in achieving the objectives are:

Fact Finding: Application system focuses on two main types of requirements. The first one is service delivery and second one is operational requirements. These may include lower operational costs, better information for managers, smooth operations for users or better levels of services to customers. To assess these needs, the analysts often interact extensively with stakeholders, to determine 'detail requirements'. The fact-finding techniques/tools used by the system analyst include document verification, interviews, questionnaire and observation.

Analysis to understand Present process: Understanding present system and its related problems helps in confirming the requirements from new application/software. Generally this includes identifying rationale and objectives, inputs and data sources, decision points, desired outcomes from application, mandatory and discretionary controls.

Requirements for Proposed Systems: Analysis of functional area and process, the proposed expectations can be clearly defined considering the issues and objectives. The requirements should cover at the minimum the following:

- Outcome to different users from the application.
- Online processing capabilities and expected response time.
- Sources and nature (manual, online etc.) of data to be captured and processed.
- Methods and procedures that show the relationship of inputs and outputs to the database, utilize data communications as, when and where deemed appropriate.
- Work volumes and timings are considered for present and future including peak periods.

5.3 Product selection

Based on requirements, organisations may proceed to select suitable product to meet the requirements. The three options which are considered are:

- **Generic products without customization:** Software is available and can be implemented without customization.
- **Commercial product with customization:** Software needs to be customized
- **Outsourced development:** Software is not available however organisation wishes to outsource development activities based on cost benefit analysis.

In case organisation opts for third option then it can initiate the process for RFP. In first two cases it is likely that more than one product/vendor fits the requirements with advantages and disadvantages. It is best to have adequate participation from various user groups is included when evaluating the product.

The organisations may consider following aspects for evaluating the software product:

- **The agenda-based presentations** are scripted business scenarios that are designed to show how the software will perform certain critical business functions. Vendors are typically invited to demonstrate their product and follow the sample business scenarios given to them to prepare.
- **Checklists or questionnaire:** A most simple but subjective method where criteria are listed as a check list or questions against which functional requirements for various products. Organisation may get this information from vendors as part of request for proposal (RFP) or request for intent (RFI). These responses for different products are validated against requirements. For example, support service checklists may have parameters such as performance; system development, maintenance, conversion, training, back-up, proximity, hardware and software.
- **Point-Scoring Analysis (Functional gap analysis):** Point-scoring analysis provides an objective means of selecting software. This is performed by allotting weight-age for each requirement and then allotting score to the software that meets that requirement. Table 5.2 illustrates a Point Scoring Analysis list.

Table 5.2: Point Scoring Analysis List

Software Evaluation Criteria	Possible points	Software A	Software B	Software C
Does the software meet all mandatory specifications?	10	7	9	6
Will program modifications, if any, be minimal to meet company needs?	10	8	9	7
Does the software contain adequate controls?	10	9	9	8

Software Evaluation Criteria	Possible points	Software A	Software B	Software C
Is the performance (speed, accuracy, reliability, etc.) adequate?	10	7	9	6
Are other users satisfied with the software?	8	6	7	5
Is the software user-friendly?	10	7	8	6
Can the software be demonstrated and test-driven?	9	8	8	7
Does the software have an adequate warranty?	8	6	7	6
Is the software flexible and easily maintained?	8	5	7	5
Is online inquiry of files and records possible?	10	8	9	7
Will the vendor keep the software up to date?	10	8	8	7
Totals	123	94	106	85

- **Public Evaluation Reports:** Organisation may refer to independent agencies that evaluate various software products of different vendors and publish comparison along with rating based on various predefined parameters including survey of current users. (For example, magic quadrant for similar software product by Gartner, Forester etc.). This method has been frequently and usefully employed by several buyers in the past.
- **Proof of Concept (PoC) or Benchmarking Solutions:** Organisations may request vendor to provide a proof of concept (by implementing product in small pilot area within organisation) that the software meets the expected requirements. This helps organisation in evaluating best product that meets the requirements. This is particularly useful for products that has high-cost and requires high level of efforts that it may not be possible to roll back.
- **Acceptability by end users:** This is an important parameter to be considered. Many times software may be able meet maximum functional requirements but users may not accept it. In such situations user acceptability needs to be considered on priority.

5.4 Request for proposal

Once the software is shortlisted organisation may invite request for proposal from the selected vendors. In case it has been decided to outsource the development, organisation may also prepare a RFP. The invitation to respond to an RFP should be published/forwarded to appropriate vendors. Organisations have to carefully examine and compare the vendors' responses using an objective method such as a scoring and ranking methodology. Response from vendors may be evaluated using parameters listed in Table 5.3.

Table 5.3: Parameters for preparing RFP

Item	Description
Software and system requirements	Comparison of product functionalities against requirements based on score point criteria.
Customer References	Validate the Vendor's claims about their product performance and timely completion of work by the vendor from the vendor's customers.
Vendor viability and financial stability	Evaluate the vendor's viability with reference to period for which the vendor is in operation, the period for which the desired product is being used by the existing customers and the Vendor's financial stability on the basis of the market survey and the certification from the customers and on certain supporting documentation from the Vendor
Availability of complete and reliable documentation about the new software	Review the complete set of system documentation provided by the vendor prior to acquisition of the software. The documentation should in detail and precise.
Vendor support	Evaluate what kind of support the vendor provides for the software like onsite maintenance, online updating of upgrades, onsite training to users, automatic new version notifications, 24 x 7 helpline etc.
Response time	Time taken for the vendor to respond and fix in case a problem is reported.
Source code availability	If the software is developed only for the concerned business, the vendor has no right to further sale. The source code must be given by Vendor. In other case, the source code should be deposited with a third party so that the same would be available if the vendor goes out business. The source with the program updates and programs fixes should be included as a part of escrow agreement.
Vendor's experience	Vendor having longer experience in the desired software is more acceptable.
A list of recent or planned enhancements with dates	This will involve review of the vendor's effort to keep the product current.
List of current customers	More the number of customers, greater are the acceptability of the product.
Acceptance testing of product	The vendor should allow the acceptance testing by the users to ensure that the product satisfies the system requirements of the business. This should be done before commitment of the purchase.

5.5 Vendor selection criteria/process

After the RFP responses have been examined, organisation may be able to short list vendors whose product satisfies most or all of the stated requirements in the RFP. In evaluating the best-fit solution and vendor against the given set of business requirements and conditions, a suitable methodology of evaluation should be adopted. The methodology should ensure objective, equitable and fair comparison of the products/vendors (e.g., a gap analysis to find out the differences between requirements and software, the parameters required to modify, cost of product against the benefits derived etc.). Many organisations follow lowest (cost) amongst equal (in meeting requirements) principle.

It is important to keep in mind the minimum and recommended requirements to use the software including:

- Required hardware such as memory, disk space, and server or client characteristics
- Operating system versions and patch levels supported
- Additional tools such as import and export tools
- Databases supported

While selecting the vendor users should concentrate on following criteria:

- **Reliability:** Are the vendor's deliverables (enhancements or fixes) dependable?
- **Commitment to service:** Is the vendor responsive to problems with its product? Does the vendor deliver on time?
- **Commitment to providing training, technical support and documentation for its product:** What is the level of customer satisfaction?

5.5.1 Service Level Agreements (SLAs)

Service Level Agreement (SLA) is formalization of the outsourcing/acquisition activity. This activity follows the vendor selection process that selects the final vendor for supply/develop, implement and support the software product. During this phase organisation and vendor negotiate the terms of contract (SLA) and sign it. Appropriate legal counsel should review the contract prior to its signing. The contract should cover the following items, depending upon terms of requirements:

- Specific description of services, deliverables and their costs
- Commitment dates for deliverables and support
- Commitments for delivery of documentation, fixes, upgrades, new release notifications and training
- Commitments for data migration
- Arrangement for a software escrow agreement or deliverables of source code and system documentation
- Description of the support to be provided during installation/customization
- Criteria for user acceptance

- Provision for a reasonable acceptance testing period, before the commitment to purchase is made
- Allowance for changes to be made by the purchasing company
- Terms of software maintenance
- Allowance for copying software for use in business continuity efforts and for test purposes
- Payment schedule linked to actual delivery dates
- Confidentiality clauses
- Data protection clauses
- Monitoring mechanism and measurement criteria along with reporting commitments. This is particularly important for development and maintenance activities.

Software Licenses: Software license is a contract that grants permission to use software to the organisation that is protected under legal system (like copyright law, patent law, trademark law and any other intellectual property rights), by paying agreed fee. Use of unlicensed software or violations of a licensing agreement expose organisations to possible litigation. Organisation and a software vendor should clearly describe the rights and responsibilities of the parties to the contract. The contracts should cover detail to provide assurances for performance, source code accessibility, software and data security, and other important issues.

5.5.2 Vendor monitoring

Outsourcing helps in improving speed and quality and reducing total costs. Outsourcing also introduces risks, particularly after signing the agreement since vendor becomes a single- or sole-source provider. Proper vendor management can reduce or prevent problems caused by picking a vendor that is unable to achieve the required solution or timescale and by ensuring that contracts address business needs and do not expose the business to unnecessary risk.

Managing the contract involves a monitoring of vendor activities to ensure that deployment efforts are controlled, measured and improved. This includes periodic status reporting, milestones and metrics as agreed with the vendor.

Critical success factors of vendor selection process:

1. Involvement of users.
2. Priority to meeting requirements and not commercials.
3. If requirements meets then the lowest bid must be considered.
4. Organization should maintain the documentation about vendor selection process.

The IS auditor has to understand the RFP and requirements specifications. The review covers:

- Security requirements.
- Process of vendor selection.
- Contents of the contract.
- Monitoring of terms of contract.
- Inclusion of provision of the right to audit the vendor.

5.6 Summary

1. The feasibility study in relation to the software acquisition should contain documentation that supports the decision to acquire the software.
2. The decision is based upon various factors such as cost difference between development and acquisition, availability of the required software readily in the market, the time saved between development and acquisition.
3. A team comprising of technical supports staff and key users should be crated to prepare Request for Proposal (RFP).
4. Organisation should carefully compare and examine the various responses of the Vendor to the RFP, prepare the gap analysis and shortlist the vendors on the basis of such evaluation.
5. The organisation should invite the short listed vendors to have presentation of the product and the processes. The user's participation with feedback must be ensured in such presentation.
6. The last step in the acquisition process is the negotiation and signing of a legal contract with the selected vendor.
7. Managing and control on the implementation of the system is required with the regular status reports.

IS auditors are involved in the software acquisition process to determine whether an adequate level of security controls has been considered prior to any agreement being reached. If security controls are not part of the software, it may become difficult to ensure data integrity for the information that will be processed through the system. Risks involved with the software package include inadequate audit trails, password controls and overall security of the application. To ensure effective mitigation of these risks, IS auditor should ensure that these controls are built into the software application.

5.7 Questions

1. While auditing the software acquisition process the IS auditor PRIMARILY review which of the following to understand the benefits to the business?
 - A. System requirement specifications
 - B. Cost comparison of different products
 - C. Alignment of IT strategy with business
 - D. Vendor with lowest cost has been selected
2. While auditing outsourced software development the IS auditor primarily ensure that:
 - A. vendor selected has experience in similar engagements
 - B. organization has followed established procurement process
 - C. outcome of feasibility study has indicated for outsourcing
 - D. ownership of design and source code has been established
3. Which of the following is primary objective of monitoring activities of vendor hired for software development?

- A. Invoke the penalty clause in contract.
- B. Mitigate risk associated with performance.
- C. Ensure senior management satisfaction.
- D. Monitor third-party resource performance.

4. While acquiring application software the organization has finalized products as follows:

Product	Functional requirements coverage	User acceptability
A	96%	50%
B	88%	75%
C	80%	95%
D	69%	80%

The organization should select product:

- A.
- B.
- C.
- D.

5. Which of the following is a primary concern of management while considering acquisition of new software?

- A. New application does not have long term operational issues.
- B. Vendor for application may not provide source code.
- C. User acceptance testing has been performed but not signed off.
- D. Change management for application is not defined.

6. Compliance with terms of license for software purchased is primarily which type of compliance?

- A. Legal
- B. Contractual
- C. Regulatory
- D. Standard

5.8 Answers and Explanations

1. A. While acquiring software organizations must focus on requirement specifications so as to select most appropriate product. If the products does not meet requirement, it may not be considered.

2. D. While outsourcing the software development the IS auditor must ensure that the ownership of developed software is within the organization. In absence of this provision organization may lose the IPR. Other things are secondary.

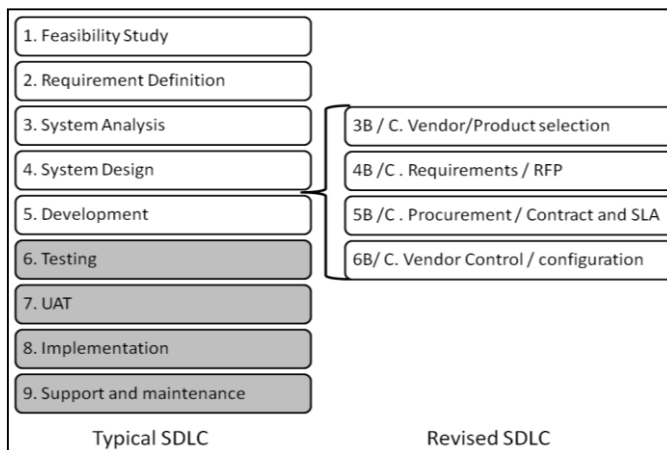
3. B. The primary objective of monitoring vendor activities is that the non-performance by vendor should not impact the organization's benefit realization plan.
4. C. The effective requirements meeting for each product is A = 48% ($96 \times .50$), B = 66% ($88 \times .75$), C = 76 % ($80 \times .95$), D = 55% ($69 \times .80$)
5. D. Absence of change management process is a major hurdle in support and maintenance of application software. Other issues can be managed.
6. B. Terms of software license are governed by the contract between software vendor and purchaser. Hence, it is a contractual compliance.

CHAPTER 6: IMPLEMENTATION AND MAINTENANCE

Learning objectives

This chapter focuses on providing information on implementation methodologies that organisation may adopt depending upon the nature and complexity of solution developed or acquired and nature of services offered by the solutions. The chapter also focuses on providing information on activities that need to be performed before and after implementation (maintenance of application).

6.1 Introduction



This chapter discusses phases 6 to 9 of SDLC

Phase 6 is testing of developed or configured software.

Phase 7 is conducting user acceptance testing (UAT) and sign-off from users. (UAT is discussed in testing section.)

Phase 8 is implementation

methods being used by various organisations.

Phase 9 is change management process required for support and maintenance activities

Application software developed or acquired requires appropriate process for implementing and maintenance in order to realize benefits effectively and efficiently. The best solution to ensure smooth implementation, configuration, change and release management processes need to be implemented. These processes should be focused on reliability, availability and security of production systems. Maintenance generally involves updating and changing IT systems (application and infrastructure) to suit to changing requirement of business. Every change must be assessed, planned, tested, approved, documented, communicated and carried out without any undesirable consequences and minimum downtime for business processes. The IS auditor should be aware of the processes for implementation and change management including controls to ensure segregation of duties between development, test and the production environment.

The change management processes discussed in section 6.4 and configuration management process discussed section 6.5 are common processes used for implementation of changes as well as new application systems.

6.2 Testing

The success of information systems depends upon the quality of software that supports the system. Testing of software before deploying in production to ensure it delivers as per requirements is most essential aspect of quality apart from documentation, compliance with coding standards, version control discipline and user training.

Although testing phase comes much later in the life cycle, planning for testing starts with the commencement of System Development life cycle i.e. during requirement gathering phase. Testing is a process that focuses on correctness, completeness and quality of developed computer software. Testing should systematically uncover different classes of errors in a minimum amount of time with a minimum amount of efforts. The data collected through testing can also provide an indication of the software's reliability and quality. However, testing cannot show the absence of defect, it can only show that software defects are present. There are various types of testing performed during development of life cycle that are discussed in ensuing paragraphs.

6.2.1 Unit Testing

In computer programming, unit testing is a verification and validation method in which a programmer tests whether individual units of source code are fit for use. A unit is the smallest functional part of an application often called as module. It can be an individual program, function, procedure, or may belong to a base/super class, abstract class or derived/child class.

Unit tests are typically written based on requirement specifications and run by testing professionals or software developers to ensure that code meets these requirements and behaves as intended. The goal of unit testing is to isolate each component of the program and show that they are correct. A unit test provides a strict, written contract that the piece of code must satisfy.

There are five categories of tests typically performed on a program unit. Such typical tests are described as follows:

1. **Functional Tests:** Functional Tests check 'whether programs do, what they are supposed to do or not'. The test plan specifies operating conditions, input values, and expected results, and as per this plan, programmer checks by inputting the values to see whether the actual result and expected result match. These test data values are prepared in advance for all possible permutations the data can acquire during live run. This can have two types:
 - a. **Positive test:** Where tester collects the expected values the data can possess. Sometimes tester may use sanitized live data for testing.

- b. **Negative test:** Where tester provides value sets that data should not possess anytime. Here the program should flash the error with suitable message.

For example, if data field is used to store amount and can acquire a value between 0 and 1 crore, positive test should provide expected results and negative test should flash error if values are beyond the specified range.

2. **Performance Tests:** Performance tests are designed to verify the expected performance criteria of program.
There are different performance parameters like response time (time required to receive input and deliver confirmation), execution time (processing of single data value should be less than 100 microseconds), throughput (1000 values must be processed in once second), primary (RAM/CPU) and secondary memory (Storage) utilization and rate of traffic flow on data channels and communication links (number of messages per second).
3. **Stress Tests:** Stress testing is a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results. These tests are designed to overload a program in various ways. The purpose of a stress test is to determine the limitations of the program. (For example if access to web application is expected to be 10000 hits per second, if the program can stand this load and how it behaves when load exceeds or during a sort/search operation, available memory can be reduced to find out whether the program is able to handle the situation.).
4. **Structural Tests:** Structural Tests are concerned with examining the internal processing logic of a software system. Particularly when the program is expected to behave differently depending upon value of data set. Programmer may code for known values and might forget to code for unknown values where program might misbehave. For example tax calculation where depending upon value different rates is applied or if division operation is involved and data set gets value of zero, program may terminate abruptly or go in loop without response.
5. **Parallel Tests:** These are applicable during change management or reengineering where the same test data is used in the new and old system and the output results are then compared.

Methods of Unit Testing

- A. Static analysis testing and
- B. Dynamic testing.

A. Static Testing: Static analysis tests are conducted on source programs and do not normally require executions in operating conditions. Typical static analysis techniques include the following:

- i. **Desk check:** This is done by the programmer to check the logical syntax errors, and deviation from coding standards. As name suggests programmer uses paper and pen to

verify the logic of code by jotting down values of data sets and thinking like computer to arrive at possible values.

- ii. **Structured Walk-through:** Desk check performed with team or peers who scan through the text of the program and explanation try to uncover errors.
- iii. **Code Inspection:** The program is reviewed by a formal committee. Review is done with formal checklists.

B. Dynamic Analysis Testing: Such testing is normally conducted through execution of programs in operating conditions. Typical techniques for dynamic testing and analysis include the following:

- i. **Black Box Testing:** This testing primarily focuses on functionalities as specified in requirements. It assume code set (program/module/function etc.) as a black box without knowledge of internal structure, and focuses on input values and compares expected output for each value. The test designer selects typical inputs including simple, extreme, valid and invalid input-cases and executes to uncover errors. This method of test design is applicable to all levels of software testing i.e. unit, integration, functional testing, system and acceptance. While this method can uncover unimplemented parts of the specification, one cannot be sure that all existent paths are tested. If a module performs a function, which it is not supposed to perform, for example: running of a Trojan code, the black box test does not identify it.
- ii. **White Box Testing:** This testing goes further than black box testing and also tests internal perspective of the code/system/function to design test cases. The tester chooses test case inputs to exercise paths through the code and determines the appropriate outputs. Since the tests are based on the actual implementation, if the implementation changes, the tests probably will need to change, too. It is applicable at the unit, integration and system levels of the testing process. It is typically applied to the unit. While it normally tests paths within a unit, it can also test paths between units during integration, and between subsystems during a system level test. After obtaining a clear picture of the internal workings of a product, tests can be conducted to ensure that the internal operation of the product conforms to specifications and all the internal components are adequately exercised. There are automated tools (like test tools/debuggers etc.) available to conduct this type of testing.
- iii. **Grey Box Testing:** It is a technique that is in between uses black box testing and white box testing. Tester applies a limited number of test cases to the internal workings of the software under test. In the remaining part of the grey box testing, one takes a black box approach in applying inputs to the software under test and observing the outputs.

6.2.2 Integration Testing

Unit testing focuses on testing of different modules/functions and programs that are small part of entire information system being developed. These modules are expected to work together to achieve objectives of information system. For example Internet banking is a system consisting of various functions like saving account management, time deposit management, loan account management, third-party fund transfer, standing instruction, getting statements of accounts etc. While developing programs/functions, each service function is developed separately and tested in unit testing. Now it is necessary to test if these modules/functions work together seamlessly and communicate appropriately during execution. Objective is to evaluate the validity of integration of two or more components that pass information to one another. Integration testing puts together modules that have been unit tested and applies tests defined. There are two approaches for integration testing:

1. Bottom-up Integration: It is the traditional strategy used to integrate the components of a software system starting from smallest module/function/program. It consists of unit testing, followed by sub-system testing. Bottom-up testing is easy to implement as at the time of module testing, tested subordinate modules are available. The disadvantage; however is that testing of major decision / control points is deferred to a later period. For example in above example of internet banking it will test communication between different modules using smallest level of module like saving bank account, fund transfer and then statement of accounts to ensure previous transaction reflects in statement, and so on, however it might not ensure the overall control on passing parameters required for session time out or inactive session

2. Top-down Integration: This starts with the main routine followed by the stubs being substituted for the modules which are directly subordinate to the main module. Considering above example, the testing will start from opening login screen and then login, then selecting function one by one. An incomplete portion of a program code is put under a function (called stub) to allow the function. Here a stub is considered as black box and assumed to perform as expected, which is tested subsequently. Once the main module testing is complete, stubs are substituted with real modules one by one, and these modules are tested. This process continues till the atomic (smallest) modules are reached. Since decision-making processes are likely to occur in the higher levels of program hierarchy, the top-down strategy emphasizes on major control decision points encountered in the earlier stages of a process and detects any error in these processes. The difficulty arises in the top-down method, because the high-level modules are tested with stubs and not with actual modules.

6.2.3 Regression Testing

It is a testing performed during change management when a function/module/program is changed or added to existing software, in order to ensure that new/changed functions executes properly and integrates with other modules as expected. It is required since new data flow paths are established, new I/O may occur and new control logic is invoked. These changes may cause problems with functions that previously worked flawlessly. In the context of the integration testing, the regression tests ensure that changes or corrections have not introduced new faults. The data used for the regression tests should be the same as the data used in the original test.

6.2.4 System Testing

It is a process in which software and other system elements are tested as a whole. System testing begins either when the software as a whole is operational or when the well-defined subsets of the software's functionality have been implemented. The purpose of system testing is to ensure that the new or modified system functions properly. These test procedures are often performed in a non-production test environment. The types of testing that might be carried out with various other objectives described below:

1. **Recovery Testing:** This is the activity of testing 'how well the application is able to recover from crashes, hardware failures and other similar problems'. Recovery testing is the forced failure of the software in a variety of ways to verify that recovery is able to be perform properly, in actual failures
2. **Security Testing:** This is the process to determine that an Information System protects data and maintains functionality as intended. The three basic security concepts that need to be covered by security testing are – confidentiality, integrity, availability. In addition the software may further be tested for user management requirements require i.e. authentication, authorization, and non-repudiation and log maintenance.
3. **Stress or Volume Testing:** Stress testing is a form of testing that is used to determine the stability of a given system or entity based on the requirements and expected data growth. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results. Stress testing may be performed by testing the application with large quantity of data during peak hours to test its performance.
4. **Performance Testing:** Software performance testing is performed on various parameters like response time, speed of processing, effectiveness use of a resources (RAM, CPU etc.), network, etc. This testing technique compares the new system's performance with that of similar systems using available industry benchmarks.

6.2.5 Final Testing

It is conducted if results of system testing are satisfactory and when the system is just ready for implementation. This testing is performed at two levels:

1. At technical level quality assurance testing is performed

2. At functional level user acceptance testing is performed.

Quality Assurance Testing (QAT): QAT focuses on conforming to the quality standards of the organisation accepted before development. It includes documented specifications, technology employed, use of coding standards, and the application meets the documented technical specifications and deliverables. QAT is performed primarily by the technical (IT) department. The participation of the end user is minimal and on request. QAT does not focus on functionality testing.

User Acceptance Testing (UAT): It is a user extensive activity and participation of functional user is a primary requirement for UAT. The objective of UAT is to ensure that the system is production-ready and satisfies all accepted (baselined) requirements. UAT is a formal process and may include:

- i. Definition of test strategies and procedures
- ii. Design of test cases and scenarios
- iii. Execution of the tests
- iv. Utilization of the results to verify system readiness

Acceptance criteria defined along with requirement specifications includes that deliverables must satisfy the predefined needs of the user. A UAT plan must be documented for the final test of the completed system. The tests are written from a user's perspective and should test the system in a manner as close to production as possible. For example, tests may be based around typical predefined, business process scenarios. If new business processes have been developed to accommodate the new or modified system they should also be tested at this point. A key aspect of testing should also include testers seeking to verify that supporting processes integrate into the application in an acceptable fashion. Successful completion would generally enable a project team to hand over a complete integrated package of application and supporting procedures.

1. **UAT is a stage in SDLC where end users finally accept the developed application system. This is required for all situations of acquiring software i.e. software developed in-house, or by outsourced team or purchased and configured by vendor. A formal sign-off generally marks end of development process.**
2. **UAT should be performed in a secure testing or staging environment where both source and executable code are protected to ensure that unauthorized or last-minute changes are not made to the system unless authorized and the standard change management process is followed. In the absence of controls, the risk of introducing unauthorized changes/malicious patches/Trojan horse programs is very high.**
3. **Users should develop test cases or use data of live operations of a specified period to confirm whether the processing of data by new application is providing correct results, has required controls and the reports meet the management requirements.**

Many organizations expects report from IS auditor after tests are completed. The IS auditor should issue an opinion to management as to whether the system meets documented business requirements, has incorporated appropriate controls, and may be migrated to production. This report should also identify and explain the risk that the organization might be exposed by implementing the system.

6.2.6 Other types of Testing

When any complex application/software is intended for general and wide spread use developers want to make sure that product delivers diverse requirements of general users, organisations may consider alpha and beta testing. For example Microsoft performs this type of testing on new product before making it available commercially.

Alpha Testing: This is the first stage, often performed by users within the organisation by the developers, to improve and ensure the quality/functionalities as per users' satisfaction.

Beta Testing: This is the second stage, generally performed after the deployment of the system. It is performed by the external users, during the real life execution of the project. It normally involves sending the product outside the development environment for real world exposure and receives feedback for analysis and modifications, if any.

Automated testing: In software testing, automation of testing is performed using special software (separate from the software being tested) to control the execution of tests and the comparison of actual outcomes with predicted outcomes. Test automation can automate some repetitive but necessary tasks in a formalized testing process already in place, or add additional testing that would be difficult to perform manually.

Integrated Testing: Some organisations rely on integrated test facilities. Test data usually are processed in production-like systems. This confirms the behaviour of the new application or modules in real-life conditions. These conditions include peak volume and other resource-related constraints. In this environment, IS will perform their tests with a set of fictitious data whereas client representatives use extracts of production data to cover the most possible scenarios as well as some made-up data for scenarios that would not be tested by the production data.

Some organisations use a subset of production data in a test environment, such production data may be altered or scrambled to mask the confidential data. This is often the case where the acceptance testing is done by team members who, under usual circumstances, would not have access to such production data. These tools help in building test cases and also generate test data based on conditions. However, using production data may not help in identifying negative test cases.

Accreditation of software: Although it is not type of testing, many organisations insist on certification and accreditation of software. Generally this is done by the software development houses before taking product to market. In case of tailor-made software certification/accreditation

should only be performed once the system is implemented and in operation for some time to produce the evidence needed for certification/accreditation processes. This process includes evaluating program documentation and testing effectiveness. The process will result in a final decision for deploying the business application system.

Security testing: (Application scans and penetration testing) For information security issues, the evaluation process includes reviewing security plans, the risk assessments results along with response decision, and the evaluation of processes to be deployed. The result of security assessment focuses on measuring effectiveness of the security controls. Security testing provides assurance to the business owner.

Security testing of web application for identified external threats (like SQL injection, cross site scripting etc.) is necessary to ensure that the application can sustain an attack by the hacker who is trying to breach the security.

While reviewing testing process IS auditors focus on getting answers to following questions:

1. **Whether the test-suite prepared by the testers includes the actual business scenarios?**
2. **Whether test data used covers all possible aspects of system?**
3. **Whether CASE tools like 'Test Data Generators' have been used?**
4. **Whether test results have been documented?**
5. **Whether tests have been performed in their correct order?**
6. **Whether modifications needed based on test results have been done?**
7. **Whether modifications made have been properly authorized and documented?**

Testers generally perform black box testing (Penetration test) by trying to simulate attacks on hosted application. This is then followed by performing grey box and/or white box testing that includes code review to identify the issues in coding practices that might introduce the vulnerabilities in the application. These can be avoided by including secure coding practices in coding standard developed by the organisations.

6.3 Implementation

Application software developed shall be implemented once it is tested and UAT has been signed off. However the planning for implementation must start much earlier in SDLC, many times after feasibility study. Planning involves:

- Selecting Implementation Strategies
- Preparing for implementation

- Deciding on hardware and ordering (if required) in advance so as to be available in time
- Deciding on site where infrastructure to be made available
- Training
- Conversion of data to suit to the requirements of new application.

6.3.1 Implementation Strategies

Considering the nature of business operation appropriate implementation strategy must be decided, much earlier in SDLC. Generally it is decided once the design is finalized or in case of acquisition once the application is selected. Organisation can adopt one of the four strategies, which are described below:

Cut-off or Direct Implementation / Abrupt Change-Over: This is achieved through an abrupt takeover – an all or no approach. With this strategy, the changeover is done in one operation, completely replacing the old system in one go. Fig 6.1 depicts Direct Implementation, which usually takes place on a set date, often after a break in production or a holiday period so that time can be used to get the hardware and software for the new system installed without causing too much disruption.

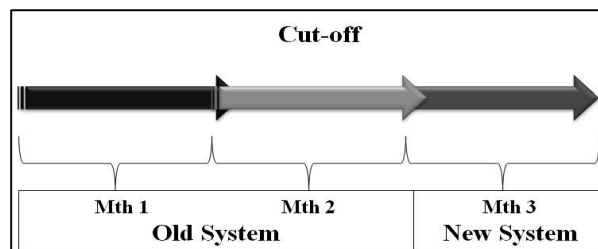


Fig. 6.1: Cut-off or Direct implementation

The challenge in cut-off implementation is that roll-back is most difficult and hence planning must be meticulously done. Also conversion activity must start well in advance and must be properly planned.

Phased Changeover: With this strategy, implementation can be staged with conversion to the new system taking place gradually. This is done based on business operations. For example, converting one function (e.g. marketing) on new system, wait for the same be stabilized and then take another function (Finance/HR/production etc.) If a phase is successful then the next phase is started, eventually leading to the final phase when the new system fully replaces the old one as shown in Fig. 6.2.

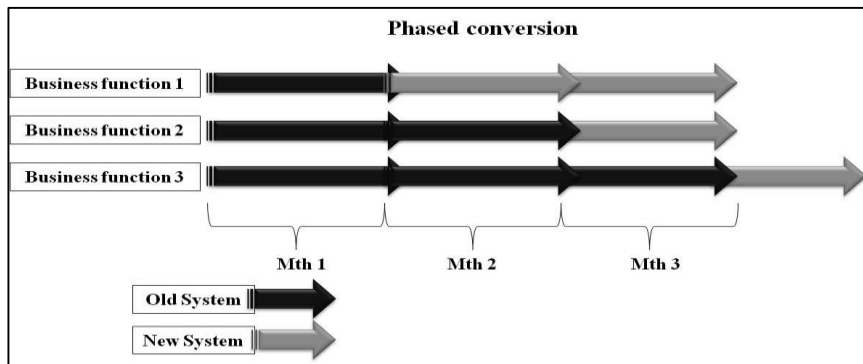


Fig. 6.2: Phased changeover

Phase changeover might require more time to implement however it helps in stabilizing one function before starting another.

Pilot Changeover: With this strategy, the new system replaces the old one in one operational area or with smaller scale. Any errors can be rectified and new system is stabilized in pilot area, this stabilized system is replicated in operational areas throughout the whole system. For example converting banking operations to centralized systems are done at one branch and stabilized. The same process is replicated across all branches. Fig. 6.3 depicts Pilot Implementation.

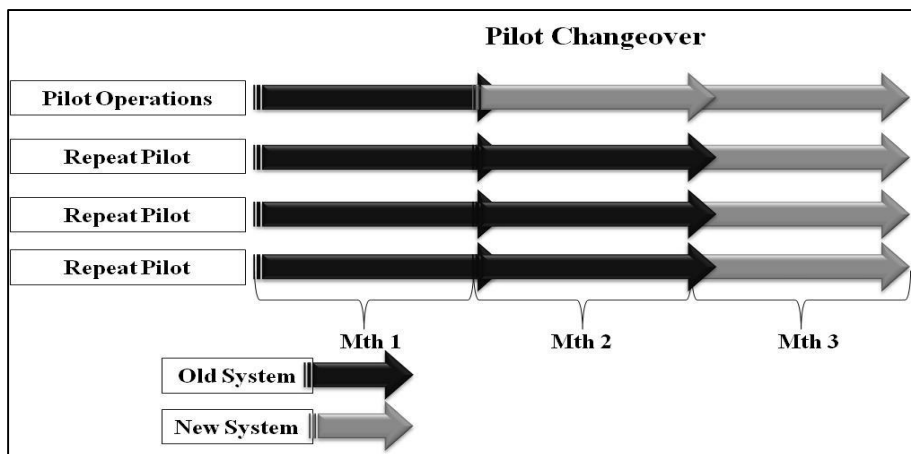


Fig. 6.3: Pilot Changeover

Advantage of pilot implementation is that issues and problems are identified and rectified during pilot run and a stabilized system is implemented thus saving cost and enabling faster implementation.

Parallel Changeover: This is considered the most secure method, time and resource consuming implementation. The new systems is implemented, however the old system also continues to be

operational. The output of new system is regularly compared with old system. If results matches over period of time and issues observed with new system are taken care of, the old system is discontinued. Fig. 6.4 shows parallel implementation.

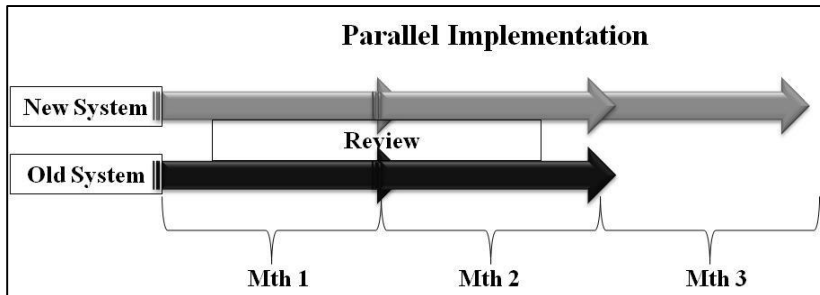


Fig. 6.4: Parallel Changeover

However it is costly and may not be feasible in large and complex systems, since all transactions must be processed twice. Many times users may not be conformable in duplicating the work.

6.3.2 Preparing for implementation

In order to finally deploy or implement the new system in the operating environment, several activities are undertaken. A fully functional as well as documented system is a prerequisite for implementation to begin. Moreover, many other issues like defect removal, maintenances, reengineering may need to be addressed to assure the desirable quality control of the system in operational environment.

The process of ensuring that the information system is operational and then allowing users to take over its operation for use and evaluation is called Systems Implementation. Implementation includes all those activities that take place to convert from the old system to the new. The new system may be totally new, replacing an existing manual or automatic system. Some of the generic key activities involved in system Implementation are:

- Site preparation and hardware installation
- Conversion of data to the new system files;
- Training of end users;
- Completion of user documentation;
- System changeover
- Post implementation review and evaluation

Site preparation and Installation: The hardware required to support the new system is selected prior to the implementation phase. The necessary hardware should be ordered in time to allow for installation and testing of equipment during the implementation phase. An installation checklist should be developed at this time with operating advice from the vendor and system development team. In situations, where people are not experienced in the installation of similar

hardware/platform/equipment, adequate time should be planned to allow completion of required activities.

Site Preparation: An appropriate location as required to provide an operating environment for system (temperature, humidity and dust control specifications) has to be prepared in time.

Installation of New Hardware / Software: Site preparation also includes receiving, installing and connecting the hardware and supporting software (like operating systems, middleware etc.). In case the hardware is available need to be commissioned for the new application as per design requirements.

Equipment Checkout: The equipment must be turned on for testing under normal operating conditions. Though the routine 'diagnostic tests' should be run by the vendor, the in-house implementation team should test the equipment functionalities in actual working conditions.

6.3.3 Training

Operational training to users about system must be planned along with implementation and before going live and depending upon the complexity of application. There are three ways to provide training:

1. **Simulated training:** Where a training instance of application is installed along with live environment and users are requested to explore the application. This type of training is generally performed on-site
2. **Classroom training:** This is controlled simulated training conducted in classroom and is facilitated by trainer.
3. **On the job training:** Conducted in live environment with appropriate guidance from experts.

The quality of training received by the personnel involved with the system in various capacities helps or hinders the successful implementation of information system. When a new system is acquired, which often involves new hardware and software, both users and computer professionals generally need some type of training.

Effectiveness of training can be measured based on changes in number of help desk requests before and after training.

6.3.4 Conversion

Conversion of data is most important activity while implementing new application system or when there is significant change in technology requiring conversion. The conversion activity involves converting data, procedures, documentation from old system to new system. Most important being data conversion.

Data Conversion: The requirement of data conversion depends upon the change. If the new application is replacing manual operation to automated operation it involves:

1. Capturing of data into electronic form
2. Verification of data
3. Uploading into database

In case change is from old system to new system, it involves:

1. Converting electronic data from old format to new format
2. Verification
3. Uploading into new database.

Since data conversion is a type of input, controls on conversions are essential to ensure integrity of data. These controls generally include:

1. **Completeness check:** Using number of records, control totals, batch totals, hash totals. For example verifying number of employees record, checking trial balance before and after conversion etc.
 2. **Accuracy check:** Manual verification or key verification (manual to electronic conversion)
- Unauthorized changes during conversion are one of the sources of frauds.

Procedure Conversion: Changes in application systems may require changes in operating procedures and associated controls. Operating procedures should be carefully completed with sufficient documentation pertaining to operations on how to use the new system. It applies to both computer-operations and functional area operations. Before conversion activities can start, conversion procedures must be defined and personnel involved must be trained to cover input, data files, methods, procedures, output, and internal control.

For example, during manual operation in banking every transaction is verified before being posted to account and then the effect of transaction is reflected in general ledger. However in electronic banking system transactions are flagged with type of transaction and posted to general ledger. Hence verification of transaction is most essential in new system.

System conversion: After on-line and off-line files have been converted and the reliability of the new system has been confirmed for a functional area, daily processing can be shifted from the existing information system to the new one. All transactions initiated after this time are processed on the new system. System development team members should be present to assist and to answer any questions that might develop. Consideration should be given to operating the old system for some more time to permit checking, matching and balancing the total results of both systems.

Scheduling Personnel and Equipment: Scheduling data processing operations of a new information system for the first time is a difficult task for the system manager. As users become familiar with the new system, the job becomes easier to perform and becomes part of the routine work. Schedules should be set up by the system manager in conjunction with departmental managers of operational units serviced by the equipment. The master schedule for next period/month should provide sufficient computer time to handle all required processing.

6.4 Change management process

Application maintenance refers to the process of managing changes in the application and IT triggered or prompted due to changes in processes, regulatory compliances, and strategic changes in business, technology changes and so on. Changes also arise due to issues, problems, incidents faced. In order to handle changes organisation should have defined process. This process generally includes:

1. **Raising change request:** Formal process for requesting change. Anyone can raise the change request with reason for the change, a cost justification analysis, if possible and the expected benefits of the change. An automated process for raising change requests helps in capturing all associated changes and maintaining record of change requests.
2. **Defining requirements:** Defining details of changes required, like functional changes, appearance changes, processing changes. (e.g. change in tax structure may require processing changes, if tax slabs are displayed then appearance changes and so on)
3. **Analysing requirements:** Getting answers to the questions such as: why change is required, when it should be effective, who needs it, where the changes are required, what programs/modules/function is affected, how the changes will be carried out and so on.
4. **Impact analysis:** What will be impact of changes on processes and other related programs that interface with application that need to be changed or how changes in technology shall affect the processing.
5. **Approval of change:** Changes must be approved by the asset owners, i.e. application owners in case of application change and other stakeholders that might be impacted. Sometimes it is difficult to decide who has appropriate authority to approve change due to impact on multiple processes. To overcome such situations organisations forms a change approval board or committee (CAB) consisting of representatives from multiple business functions.
6. **Prioritizing the change requests:** this is required to resolve the conflict due to multiple change requests from different users.
7. **Carrying out changes:** System analyst shall review the changes and decide appropriate resources to carry out changes. Records of all program changes should be maintained. Library management software may help in automating this process and also maintaining audit trail. The maintenance information usually consists of the programmer ID, time and date of change, project or request number associated with the change, and before and after images of the lines of code that were changed. This also helps in preventing and/or detecting unauthorized changes.
8. **System document maintenance:** All relevant system documentation updating sometimes is neglected area during change management. It is essential to ensure the effective utilization and future maintenance of a system, Documentation requiring revision may consist of program and/or system flowcharts, program narratives, data dictionaries, entity relationship models, data flow diagrams (DFDs), operator run books and end-user procedural manuals. In case of infrastructure changes network diagrams.

Data centre block diagrams, electrical and facility diagrams etc. are likely to undergo changes.

9. **Testing the changes:** Changes will be tested as per testing process (Please refer subsection on testing). However for testing changes, following points must be considered:

- Existing functionalities are not affected by the change
- System performance is as expected
- Security vulnerabilities are not introduced

This also includes conducting user acceptance testing and formal sign-off from users/owners. (E-mail, electronic approval in automated system, document etc.)

10. **Releasing changes:** Changes shall be released to production once approved by stakeholders (UAT). Ensure fall-back procedures in place in case operations are affected due to change. Automation of this process shall help management in restricting one person requiring access to production, test and development environment.

11. **Review:** Post implementation/release review may be conducted.

12. **Record maintenance:** Change requests should be maintained in a format that will ensure that all changes associated with primary change requests are considered. This allows the management to easily track the changes to change requests. The process must be formal and maintain record of all approvals and rejections.

For acquired systems vendor may distribute periodic updates, patches or new version of the software. User and systems management should review such changes for impact and appropriateness before implementing.

While reviewing change management IS auditor should ensure that:

- **Access to source program is restricted.**
- **Change requests are approved and record is maintained to trace and track the changes.**
- **Impact assessment is performed before approving changes.**
- **The change request should be documented in standard format covering at the minimum:**
 - **Change specifications, benefit analysis developed and a target date.**
 - **Change form has been reviewed and impact assessment is recorded.**
 - **change request has been approved formally**
- **Verify records of changes for sample changes made and trace end-to-end (from request till closure) confirm that the changes are authorized, approved, and moved to production after UAT.**

Ensure segregation of duties during change management

6.4.1 Emergency Changes

In exceptional situations there may be need to make changes to production to resolve issues in time. This requirement can arise due to one or more reasons like:

- Events/incidents
- Short notice requirement changes (due to external incidents/events: terrorist attacks, natural disasters, etc.)
- Infrastructure failure
- Production issues due to unexpected data conditions

Procedures should focus to ensure that emergency changes can be performed without compromising the integrity of the system. Organisation should have a process for carrying out emergency changes. The process may consist of following steps:

1. Identify need for emergency change (process issue, incident/event etc.)
2. Determine activities involved. Generally it may involve providing all accesses to one person. A special user ID may be created with higher privileges for this purpose and all activities are logged and reviewed.
3. A post-facto change management process must be followed, so as to ensure consistency in documents, source-code library, network diagram etc. as applicable.

The IS auditor has to ensure that emergency changes are handled in a controlled manner.

6.4.2 Implementing Changes into Production

Changes are implemented into production environment once they are approved by the user management (UAT sign-off). The best practices suggest that this implementation should be done by independent team not involved in development or testing of changes. In case of client-server applications or distributed systems, such as point-of-sale systems, the process should be properly documented and implemented over a period of time to ensure:

- Conversion of data
- Training of users
- Support process for changes
- Rollback plan
- All points are updated

6.4.3 Segregation of Duties

Uncontrolled change management has risk associated with unauthorized changes. An unauthorized change occurs due to various reasons:

- Developer has access to production libraries containing programs and data including object code.
- User has not approved change or not aware of the change
- A change procedure has not formally established.
- A change was updated into production without user approval.
- The changes had not been reviewed or tested.
- Developer inserted extra logic for personal benefit (i.e., committed fraud).
- In case of vendor software, changes received were not tested.

In order to control unauthorized changes segregation of duties has to be implemented at organisation level. The typical segregation includes following controls at the minimum:

- Development, test and production environments to be physically separated.
- Developers' team, testing team and production user should not have access to other areas. I.e. developers should not have access to test and production and so on.
- Source code must be maintained by librarian. At least control must be in place to prevent or detect insertion of unauthorized code.
- A separate change control team or release team should be appointed to move source/object code from development to test and from test to production.

It may not be possible for some organisations to implement strict segregation of duties, in such situation appropriate compensating controls should be present to prevent or detect and correct unauthorized changes. Some such situations may arise due to:

1. The developer is also the operator due to small IT department. In this case user management required to ensure proper authorization and monitoring of changes and upgrades made by the programmer.
2. Emergency changes to resolve the issues in production.
3. In case separate release team is not possible, compensating control of enabling user ID of user who moves changes from development to test and/or test to production only after approval and monitoring activities may work as compensating control.
4. Developers should not have write, modify or delete access to production data. Depending on the type of information in production, programmers may not have read-only access to personally identifiable information.

6.4.4 Configuration Management

Configuration management is refers to automated process organisations install to maintain all information assets and work-flows required to maintain them. The backend of such system is a data base called a Configuration management Data Base (CMDB); hence sometimes the system is also referred to as CMDB.

Configuration management system helps in maintaining information about system as collection of configuration items (CI). A CI can be a module/function/program or database instance of IT asset associated with a system and referenced with an ID. Workflows around the CMDB consist of workflows for Change Management, configuration management etc. Change management requests must be formally documented and approved by a change control group within CMDB. CMDB then manages the change process via checkpoints, reviews and sign-off procedures that generates audit trails.

Configuration management sometimes may provide procedures throughout the software life cycle (from requirements analysis to maintenance) to identify, define and baseline software items in the system and thus provide a basis for problem management, change management and release

management. However though it sounds easy, proper implementation of CMDB is a necessary requirement (which must follow SDLC process for acquired Software).

Software configuration management requires following tasks to be performed:

1. Develop configuration management plan.
2. Baseline application and associated assets.
3. Analyze results of configuration control.
4. Develop monitoring of configuration status.
5. Develop release procedures.
6. Define and implement configuration control activities (such as identification and recording of change requests.)
7. Update the configuration status accounting database.

A configuration management tool supports change and release management by supporting following activities:

1. Identification of items affected by a proposed change
2. Help in impact assessment by providing information
3. Recording configuration items affected by changes
4. Implementation of changes as per authorization
5. Registering of configuration item changes when authorized changes and releases are implemented
6. Recording of original configuration to enable rollback if an implemented change fails
7. Preparing a release to avoid human errors and resource costs

6.5 Summary

Implementation of new application follows a similar process required for change and release management. Although change management primarily refers to the maintenance activity in SDLC phases, a large change may have to be initiated to implement change by implementing a SDLC project. In other words a change management process by itself may be considered as a mini-SDLC project. Controls required during implementation and change management are similar and IS auditor has to understand the process of controlling unauthorized changes in software whether it is being developed or configured or maintained.

6.6 Questions

1. Which of the following process during implementation of banking software is most critical to minimize the risk associated with frauds?

- A. Training and awareness
- B. Data conversion
- C. Hardware configuration
- D. Procedure conversion

2. Which of the following is a major concern for IS auditor while auditing implementation phase of SDLC project?

- A. Requirement of resilient infrastructure are captured during implementation
- B. Hardware acquisition has been delayed due delay in procurement process
- C. Organization has contracted multiple network service providers for connectivity
- D. Organization has decided to use existing site for implementing new solution

3. Who among the following should be primarily responsible for approving changes to application system?

- A. Head of IT department
- B. Business process users
- C. Application administrator
- D. Affected business stakeholders

4. Which of the following method is most useful in implementing an ERP application at multiple locations of same organization?

- A. Parallel
- B. Pilot
- C. Phased
- D. Cut off

5. An organization has developed a web based application for the use of internal users to be hosted on intranet. Before finalizing and making it live it was decided to make it available to users for providing feedback. This is an example of:

- A. Internal audit
- B. Alfa testing
- C. Beta testing
- D. User training

6. A major concern associated with using sanitized old production data for testing new application is that:

- A. User may not provide sign off.
- B. Production data may be leaked.
- C. Integration testing cannot be performed.
- D. All conditions cannot be tested.

6.7 Answers and Explanations

1. B. Fraudster manipulated the data being entered into system to commit fraud by exploiting vulnerabilities in the process. Hence, data conversion process must be monitored more closely as compared to other processes.

2. A. Requirement of resilient infrastructure must have been considered during requirement phase, since it affects software development as well as procuring redundant infrastructure. Capturing this requirement during implementation phase will have major impact on benefit realization. Other options are not major concerns, but in fact C is an advantage.
3. D. Changes to application must be primarily approved by application owner, who is also business process owner. However change in application may also require change in dependent systems hence it is best to get approval from all. To facilitate this process generally change approval board is formed that represents all stake holders.
4. B. Pilot is method is most useful, as organization can implement application at one location and run for few days. This will help in finalizing the basic configuration and also learn from post implementation issues. Once successful the same can be replicated at other locations.
5. C. Beta testing is making product available for user for feedback before launching.
6. D. Production data generally may not cover all paths the data can take and hence system cannot be tested for all possible cases. Data leakage is not a major concern since data is sanitized. Options A and C are not concerns.

CHAPTER 7: TRENDS IN TECHNOLOGY IMPACTING SDLC

Learning objective

This chapter provides information on impact of emerging trends on SDLC process. The emerging trends discussed are virtualization, cloud computing, mobile computing, Big data and data analytics. These trends are impacting the decision on technology requirements.

7.1 Introduction

Changes in technology have direct and/or indirect impact on the SDLC phases. With various options available, organisations need to consider use of new technology for effective service delivery and IT must support this service delivery without affecting the security of information assets. In Module 1 we have seen various emerging technologies affecting use of information technology. In this chapter we will consider how some new technologies have impact on SDLC.

We will focus on following technologies:

- Virtualization and cloud computing
- Mobile technology
- Big data and data analytics

7.2 Technology Trends

7.2.1 Virtualization

Virtualization refers to the creation of a virtual machine that acts like a real computer with an operating system. The software that helps in creating virtual machine on the host hardware is called a *hypervisor* or *Virtual Machine Manager* or in short *VMware*. In other words one physical server may host more than one virtual server that supports application. Instead of relying on the old model of “one server, one application” that leads to underutilization of resource, virtual resources are dynamically applied to meet business needs.

Characteristics of virtualizations affecting SDLC

1. **Backup:** It is easier to backup virtual server. When the virtual server boots, it checks the configuration file and then reads from the simulated disk drive, which contains a simulated file-system holding server's operating system software and applications. A backup copy can be created any time when server is not running, by copying disk files, and configuration file. If the virtual server can be installed on another environment by making necessary changes

to configuration file. (i.e. IP and MAC address). The development team needs to define backup procedures according to target environment.

2. **Evaluation of alternates:** Many large projects require evaluation of tools and software. Particularly if alternate solutions are being considered before finalizing suitable solution. Evaluation can be for acquisition of software from different vendors, reusable components or for prototype selection. One can build a series of virtual servers with different solutions or products. It is then easier to compare the requirements against predefined parameters.
3. **Virtualized target for developers:** developers sometimes need to test their code before releasing to testing team; however the developers might be using desktop or laptop for development and might be different from target environment. Using virtualization required target environment may be simulated on developers desktop effectively reducing errors found during final testing or operations.

7.2.2 Cloud computing and sourcing options

The “cloud” in cloud computing is defined as the set of hardware, networks, storage, services, and interfaces that combine to deliver aspects of computing as a service. Webmail service providers like google, Hotmail yahoo etc. depends on cloud technology. Many of us who are using e-mail account with a web-based e-mail service provider like Gmail, Hotmail, Yahoo, etc. are already be cloud service users even without knowing it. You will notice that you are using a computer of any type which may be located anywhere, anytime to access your emails. The email program is running on the server and all your emails including the software is stored on the cloud.

In cloud computing, services are provided over the Internet based technology by dynamically scalable and often virtualized resources. The impact of using ‘cloud’ technology for service delivery affects SDLC process, depending upon which and how the services are being used. The lists of requirements that must be considered are discussed below:

- Application on cloud uses platform independent web based technology like Java, Net, XML, PHP etc. Deployment of services may happen in phased manner, the project manager may consider agile development method to develop and deploy services.
- Client is executed using internet browsers like internet explorer, Google chrome, Mozilla etc. and hence need to be tested for all known browsers. It is necessary to consider security while developing the software, users may or may not use security settings in their browsers. Also not all browsers offer same level of security settings.
- Web application security requirements need to be considered while designing and testing the application.
- Non-functional requirements of performance and response have to be considered while developing the software.
- Licensing issues for utilities and middleware are complex and should be considered. The challenge of licensing has two aspects:

- Who is responsible for procuring licenses? In case organisation uses cloud services offered by service provider for infrastructure only (IaaS), procuring required licenses is not the responsibility of service provider. However in case of PaaS and SaaS, service provider is responsible for procuring licenses.
- Licensing policy of software owner is different and is governed by the contract between provider and purchaser. It is best to involve the software vendor in decision while procuring cloud services.
- In case of procuring SaaS, the software is provided by service provider to multiple clients. Procuring organisation is accountable for security of information processed and stored on cloud and hence the contract and monitoring of terms of contract need to be considered during acquisition phase of SDLC.
- Service provider while offering services must ensure that client organisations are complying with required legal and regulatory requirements and issues related to cross-border compliances are addressed in contract.

Auditing Cloud services

While performing IS audit where auditee has hired third party cloud service provider to host the services, auditor need to evaluate following aspects:

- Business case for using cloud services
- Third party selection process
- Provisions of service level agreement if it covers concerns of business
- Service monitoring mechanism that provides assurance to management
- Mechanism for assurance by service provider on controlling of risks associated
- Third-party independent audit of service provider

Auditor may consider following questions:

- How much security is enough?
- What is the Criticality of the application being hosted on cloud?
- What is Outsourcer's experience with SLA and vendor management?
- What are Country/regional regulations (for e.g., SOX and Europe's data privacy laws), and Industry Regulations (for e.g., GLBA and HIPAA)?
- Does your present security model need to be altered?
- What is the Cloud vendor's policy on vulnerability management – reporting (beyond basic 'Contact Us' links), commitment to following up, promptly responding to reports?
- Is there an independent auditor's report?
- 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?
- What is the impact on compliances?
- What is the impact on security?
- Who owns the data?
- Where does the data reside?
- Who is responsible for compliance and what is the impact on compliance?

- What business continuity and disaster recovery measures are in place in the cloud infrastructure? Does the cloud provider have a backup in place?
- What is the potential implication of employees wanting to sabotage a successful cloud migration strategy?
- What are fall back arrangements on termination of contract?

7.2.3 Mobile Computing

Mobile computing is the name for using of portable devices with computing power connected to the network (mostly wireless), such as PDA, laptops, mobile phones, MP3 players, digital cameras, tablet PC and Palmtops etc. Mobile technology enables organisations to scale up process efficiency by offering access to data anytime, anywhere, anyhow based on access rules defined, on an online and real-time basis thus increasing productivity, customer service, employee satisfaction, etc. Use of mobile devices has inherent risks and these needs to be mitigated by implementing appropriate controls.

Some of the business risks are given below:

- Mobile devices may contain an organisation's sensitive information, like data obtained from business/customer applications, customer private information, corporate e-mails, and documents. The mobile computing devices may be used to provide input to business applications on wireless networks which can impact organisation data on a real-time basis. Loss or theft of organisation information/asset due to virus attacks or malware.
- Exposure due to Information interception through wireless sniffers/intrusion resulting in a loss or breach of sensitive data, privacy impacting organisation reputation and legal implications.
- Propagation of malware resulting in data leakage, data corruption and non-availability of required data.
- Physical damage to devices, data corruption, data leakage, interception of calls and possible exposure of sensitive information.
- Possibility of fraud through remote access and inability to prevent/detect it.
- Copying of critical organisation information by hackers using remote access.
- Lost devices or unauthorized access to unsecured devices allowing exposure of sensitive data, resulting in loss to the organisation, customers or employees

Organisation need to mitigate these risks by using standard risk mitigation options like identifying high-value data elements and providing security, implementing mobile computing security policy, implement specific controls for mobile devices like standard configuration of mobile devices, anti-virus software, user training, encryption etc.

Mobile devices and applications development

Many organisations provide services based on mobile technology. These services uses special application developed to suit to mobile based delivery. New generation smart phones come with separate operating systems (e.g. android, iPod, Microsoft etc.) that run on these phones.

Application need to be developed that can run on these technologies. Many such applications are available for free download and users may not be aware of existence of malware. Organisations that wish to provide mobile based services may initiate projects for developing applications for mobile delivery for existing services. (E.g. Mobile Banking).

This may be essential to ensure capturing of appropriate requirements and that security is built in the application. Organisation may not want to rely on security setting to be done by mobile users. In case new application is being developed which the organisation intends to deploy on mobile devices, SDLC process must capture these requirements before considering feasibility.

7.2.4 Bring your own device (BYOD)

BYOD refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications.

Benefits of BYOD

- **Increased productivity:** Increased productivity comes from a user being more comfortable with their personal device, being an expert user makes navigating the device easier, increasing productivity
- **Employee satisfaction:** BYOD allows user to use the device they have selected as their own rather than one selected by the IT team. It also allows them to carry one device as opposed to one for work and one for personal. Also employee may wish to have devices that are more cutting edge and organisations may not replace these devices as often.
- **Cost savings for the company:** Cost savings can occur on the organisation need not provide mobile devices to employees.

Risks of BYOD

Risks of BYOD are same as risk of mobile computing; however it has higher risk associated with data breach. For example, if an employee uses a smart phone to access the company network and then loses that phone, untrusted parties could retrieve any unsecured data on the phone. Another type of security breach occurs when an employee leaves the company, they do not have to give back the device, so applications and other data may still be present on their device.

A key issue of BYOD which is often overlooked is BYOD's phone number problem, which raises the question of the ownership of the phone number. The issue becomes apparent when employees in sales or other customer-facing roles leave the organisation and take their phone number. Customers calling the number will then potentially be calling competitors which can lead to loss of business.

To mitigate the risks organisation must have a BYOD policy that defines:

- Ownership of information on mobile device
- Which sensitive company information needs to be protected and how
- Education of employees on mobile security.

7.2.5 Big data and Data analytics

Big Data

Big data is a term for the collection of large and complex data that cannot be processed using normal database management tools or traditional data processing applications. The challenges include capture, duration, storage, search, sharing, transfer, analysis, and visualization. Big data requires the use of new or exotic technologies to manage the volume of data. Technologies such as in-line de-duplication, automated tiering of data to get the most efficient usage patterns per kilowatt, and flash or solid-state drives for higher-end performance optimization are expected to increase in importance over the next few years.

The data in big data comes from various sources. It is either historical data or the data collected over period of time that requires analysis or both. For example demographics of population with various attributes like gender, religion, ethnicity, age group, life expectancy, diseases history, birth rate, death rate and so many such attributes and parameter might run in terabytes. There can be another data set capturing consumptions and availability of essential elements like food, liquids, from various countries.

Managing Big data requires special framework technologies like NoSQL databases, Hadoop, MapReduce. These technologies form the core of an open source software framework that supports the processing of large data sets across clustered systems. Primary challenge with big data is design architecture to store the data without affecting integrity (accuracy and completeness) of the data. This is important because most of the times it is stored in denormalized form.

Another challenge is maintaining confidentiality and privacy of the data stored. This is generally controlled by providing access to limited personnel based on need to do basis.

Some examples of big data projects are:

- Turning 12 terabytes of Tweets into improved product sentiment analysis
- Scrutinizing 5 million trade events created each day to identify potential fraud
- Monitoring 100's of live video feeds from surveillance cameras to identify security threats

Risks

Organisations must come to terms with the security challenges they introduce, for example:

- Big data requires data to be stored in denormalized form i.e. schema-less in distributed environments, where data from multiple sources can be joined and aggregated in arbitrary ways, make it challenging to establish access controls
- As the big data consist of high volume, high variety and high velocity data, it makes difficult to ensure data integrity
- Since it is aggregation of data from across the organisation, it also includes sensitive data
- Most existing data security and compliance approaches will not scale to handle big data security.

Risk mitigation

Following controls need to be implemented to minimize the associated risks:

- **Sensitive data identification and classification:** Identification of sensitive data and their relationships with other data sets, so that the right security policies can be implemented.
- **Data access and change controls:** Defining and implementing policies regarding which users and applications can access or change data.
- **Real-time data activity monitoring and auditing:** Enabling logs for sensitive data access with time stamp for monitoring.
- **Data protection:** Consider encrypting confidential data (e.g. credit card details).
- **Vulnerability management:** Identifying weaknesses and initiating remedial action.

Audit questions

Some questions that helps auditor in understanding control implementation.

- Who are running specific big data requests?
- Are users authorized to make requests?
- What jobs users are running?
- Are users trying to download sensitive data or is the request part of a job requirement, for example, a marketing query and credit card details?

The rush for big data benefits is not an excuse for overlooking security.

Data analytics

Organisations use data analytics for various analyses that help management in arriving at right decision. These technologies are useful for analysis of big data, new analytic applications and pattern-based strategies. Organisations will focus on harnessing the power of information by using business intelligence and data analytics tools to monitor and improve performance and costs. IT may be required to focus on developing analytics that enable and track collaborative decision making.

Analytics mean the use of analysis, data, and systematic reasoning to make decisions. What kind of analysis? What kind of data? What kind of reasoning? There are no hard-and-fast answers. Any analytical process can provide a serious, systematic analysis. The most common is statistical

analysis, in which data are used to make inferences about a population from a sample. Variations of statistical analysis can be used for a huge variety of decisions—from knowing reasons of something that happened in the past, to predicting what may happen in the future. Statistical analysis can be powerful, but it's often complex, and sometimes employs untenable assumptions about the data and the business environment.

Benefits of data analytics

- Help manage and steer the business. Analytics give managers tools to understand the dynamics of business, including how economic and marketplace shifts influence business performance.
- Know what's really working. Rigorous analytical testing can establish whether management intervention is causing desired changes, or whether it's simply the result of random statistical fluctuations.
- Leverage previous investments in IT and information to get more insight, faster execution, and more business value in many business processes.
- Cut costs and improve efficiency. Optimization techniques can minimize asset requirements, and predictive models can anticipate market shifts and enable companies to move quickly to slash costs and eliminate waste.
- Manage risk. Greater regulatory oversight will require more precise metrics and risk management models.
- Anticipate changes in market conditions. You can detect patterns in the vast amount of customer and market data coming your way.
- Have a basis for improving decisions over time. If you are using clear logic and explicit supporting data to make a decision, you or someone else can examine the decision process more easily and try to improve it.

Risks

Most risks of big data are also similar to risks of data analytics. However, there are additional risks such as:

- **Logic Errors:** These are related to not being able to collect and analyze appropriate data, or making incorrect assumption.
- **Process Errors:** These are associated with processing incorrect data, missing alternate analysis, incorrect treatment to data resulting in wrong decision.
- **Access control errors:** Data analytics and business intelligence tools help in developing analysis of unstructured data and deploy parameterized report generation for analysis of data. Care must be taken while providing access to report generation modules that the person is eligible to access the data. In absence of such control data breach may occur.

7.3 Summary

Changes in technology are definitely affecting the business environment. However every new technology has its own payload of risks associated. Organisations must ensure that appropriate risk management process is established while considering new technologies while developing solutions for service delivery.

When faced with the paradigm change and nature of services provided through new technologies, IS auditors should consider following key assurance areas:

- **Transparency:** Technology must demonstrate the existence of effective and robust security controls, assuring customers that their information is properly secured against unauthorized access, change and destruction. Is segregation of duties maintained? How are different customers' information segregated? What controls are in place to prevent, detect and react to breaches?
- **Privacy:** With privacy concerns growing across the globe it will be imperative to prove to existing and prospective customers that privacy controls are in place and demonstrate their ability to prevent, detect and react to breaches in a timely manner.
- **Compliance:** Most organisations today must comply with various laws, regulations and standards. New technology must ensure that information must be provided to authorities without compromising other information.
- **Trans-border information flow:** When information can be stored anywhere in the cloud, the physical location of the information can become an issue. Physical location dictates jurisdiction and legal obligation.
- The use of standards and frameworks will help businesses gain assurance around. At the time of writing, there are no publicly available standards for new technologies, however, existing standards should be consulted to address the relevant areas and businesses should look to adjust their existing control frameworks.

7.4 Questions

1. Organizations consider virtualization primarily to:
 - A. Optimize resource utilization
 - B. Eliminate hardware cost
 - C. Implement cloud application
 - D. Reduce license requirements

2. Organization is considering changing the hosting technology for application accessed by internal and external users. Which of the following options has highest security concerns?
 - A. Client-server technology by providing customized client to users.
 - B. Private Cloud hosted within organization and accessed using web.
 - C. Outsourced services provided by third party on public cloud.
 - D. Establish own fiber optics network using service provider.

3. An organization hired third party service provider to provide Software as a Service to internal users. Which of the following document IS auditor should review first?
- A. Service level agreement signed with service provider.
 - B. Business case document approved by the steering committee
 - C. Comparative analysis of requirements for different vendors
 - D. Feasibility study report containing outsourcing recommendations
4. Primary benefit of developing and providing application using mobile technology to customers of organization is to:
- A. Enhance security of data
 - B. Increase usage of technology
 - C. Stay ahead in competition
 - D. Enhance service delivery
5. Which of the following the organization should consider first while allowing users to access organization's data from their own device?
- A. Formulating a policy for use of personal devices
 - B. Selection of encryption appropriate for all devices
 - C. Savings in cost required for acquiring devices
 - D. Define uniform configuration for personal device
6. Which of the following controls are most important for big data application?
- A. Data encryption
 - B. Data classification
 - C. Data access
 - D. Data analysis

7.5 Answers and Explanations

1. A. Virtualization primarily helps in optimizing resources by allowing consolidating hardware and storage for application running on diverse operating systems. Eventually it reduces costs, not eliminate, but that may not be primary objectives. Cloud technology used virtualization to optimize resources. Virtualization may not affect license requirements.
2. C. Public cloud services provided by third party as highest security concerns.
3. B. Business case is the first document IS auditor should review to understand the reasons behind the decision. Business case generally covers feasibility study and requirement analysis. SLA and vendor selection can be reviewed later.
4. D. Using mobile application helps organization to add service delivery channel that enables customers to get information anywhere. It may not enhance security, usage of technology may not be concern for organization and although it may help in match the competition it may not help in leading in market.

- 5. A. Organizations considering BYOD, must first formulate policy for usage of such devices so as to protect the information of organization. Other aspects may be considered based on policy.
- 6. B. Although most important control for big data application are access controls since data is stored in denormalized form, access controls need to be implement at data element level. This can be achieved by data classification. Also encryption controls can be considered for most sensitive data based on classification so that data analysis controls can be implemented effectively.

CHAPTER 8: SDLC REVIEWS AND AUDIT

Learning objectives

This chapter focuses on the process and method required to be followed by IS auditor while auditing the SDLC projects. It covers role of IS auditor as team member of SDLC project where auditor is consultant for including controls. It also covers mid project reviews and post implementation audit of SDLC project.

8.1 Introduction

Every organisation using IT has to adopt a SDLC process to develop and implement the software or to acquire, customize and implement the software. IS auditor has to understand the process each organisation follows and perform the SDLC process audits. The scope of audit might be focused on SDLC or it might be part of larger scope where SDLC processes need to be reviewed.

The IS auditors role in the software acquisition process is to determine whether adequate level of security controls has been considered. This is required to ensure data integrity of the information processed and controls like audit trails, password controls and overall security of the application. The above procedures should be more elaborate and systematic in case where the business is implementing ERP systems giving fully integrated corporate solutions like SAP, Oracle Financials, BAAN, PeopleSoft, JD Edwards etc.

8.2 Role of IS Auditor in SDLC

The IS auditor may be involved in SDLC process:

1. As a project team member as consultant to suggest controls
2. As IS auditor to review the SDLC project
3. As IS auditor to perform Post implementation review

8.2.1 IS Auditor as Team member

The IS Auditor can be associated with SDLC project as team member to perform following activities:

1. As a reviewer for information security requirements to be included in proposed system
2. As a consultant to suggest appropriate controls to be included in proposed solution as well as ensuring security during execution of project.

Generally a question arises about the independence when the auditor is required to perform independent review of SDLC project either mid-project review or post-implementation review. Ideally auditor should avoid performing review in such situations, however, in extreme cases

auditor may perform reviews if the auditor's role is that of consultant of controls and not involved in deciding the controls to be implemented. If auditor has decided and designed the controls it will not be appropriated for the auditor to perform reviews.

8.2.2 Mid-project reviews

The audit of SDLC project can have the following three primary objectives:

1. To provide an opinion on the efficiency, effectiveness, and economy of project management
2. To assess the extent to which proposed application provides for adequate audit trails to evaluate the controls to ensure the integrity of data processed and stored
3. To ascertain the effectiveness of controls embedded within application system.

In order to achieve these goals and provide assurance to management on progress of SDLC project, an IS auditor has to be part of project team to review the progress. IS Auditor typically performs following activities:

- Attend project and steering committee meetings to understand the status of project
- Examine project control documentation to assess possible risks and mitigation plan to ensure expected deliverables
- Interview project team and stakeholders to understand expectations and assess the expected deliverables.
- Ensure 'what project control standards are to be complied with, (such as a formal systems development process) and determining the extent to which compliance is being achieved.
- Examine system documentation such as functional specifications to arrive at an opinion on controls. The auditor's opinion will be based on the degree to which the system satisfies the general control objectives that any information system should meet. A list of such objectives should be provided to the auditor. The auditor should provide a list of the standard controls, over such operational concerns as response time, CPU usage, and random access space availability that the auditor has used as assessment criteria.
- An Auditor may adapt a rating system (for example a scale of 1 to 10, 10 being best) in order to give rating to the various phases of SDLC. For example while rating a Feasibility Study, an auditor can review Feasibility Study Report, interview the personnel, who have conducted feasibility study, understand deliverables and then depending on the content and quality of the Feasibility Study report and interviews, an auditor can arrive at a rating. (Say 7 if scale 1 to 10 is used). After deriving such a rating for all the phases, the auditor can form his/her overall opinion about the SDLC phases.

In order to audit technical work products (such as database design or physical design), auditor may seek opinion of technical experts. Some of the control considerations for an auditor include the following:

- Documented policy and procedures;
- Established Project team with all infrastructure and facilities ;
- Developers/ IT managers are trained on the procedures ;

- Appropriate approvals are being taken at identified mile-stones;
- Development is carried over as per standards, functional specifications;
- Separate test environment for development/ test/ production / test plans;
- Design norms and naming conventions are as per standards and are adhered to;
- Business owners testing and approval before system going live;
- Version control on programs;
- Source Code is properly secured;
- Adequate audit trails are provided in system; and
- Appropriateness of methodologies selected.

While auditing project management, auditor should consider following aspects:

- Project charter
- Roles and responsibilities of different groups / committees (e.g. Project steering committee)
- Adopted project management methodology
- Application Development methodology / model
- Contractual terms with the vendors for purchased applications (E.g. SLAs)
- Contractual terms with the vendors for outsourced services (E.g. SLAs)
- Approvals and sign-offs by the Project steering committee for each SDLC stages
- Deliverables of each SDLC stages
- Minutes of relevant meetings
- Project tracking and reporting documentation
- Resource management
- Ongoing risk management
- Quality Control / Assurance
- Change management
- Data conversion/migration
- Application testing documentation
- Relevant legal, regulatory and policy aspects to be complied with, if any

8.2.3 Post implementation review

Post Implementation Review of SDLC project focuses on finding the answer for the question: "Did the organisation achieve what was required?" It also tries to find out the degree of success from the project, to the extent to which it has met its objectives. A Post-Implementation review should be scheduled some time after the solution has been deployed. Typical periods range from 6 months to 18 months, depending on the type of solution and its environment. The delay is basically to provide sufficient time to be able to measure the benefits from new solution and be able to compare them with business case.

There are two aspects of evaluation:

1. The system is operating as expected without operational issues.
2. The user is satisfied with service delivered by the information system

Typical evaluation covers following aspects:

Development process: Evaluation of the development/acquisition and implementation process is primarily focuses on project execution and ensuring the system was developed on schedule, within budget and meets required quality. The review covers schedules and budgets established in advance against the records of actual performance and cost. However, IS auditor may or may not comment on delay in delivery or budget overrun depending upon the importance of project to the organisation presented in business case.

Operations: The review of issues identified post-implementation and their resolution. Also the benefits of resource utilization as predicted in business case compared against current utilization. For example if the application is expected to support increasing number of concurrent users, are there any operational issues currently observed at lower scale of operations? Is there simulation testing performed to ascertain expected peak performance?

Information Security: System should also need to be evaluated for information security and privacy controls. This aspect of system evaluation is based on the security requirements documented during information gathering, security of infrastructure on which the application is hosted (e.g. hardware baselining, network security, access controls and vulnerability scanning). Evaluation may also include the availability aspect required for continuity (e.g. in case of high availability requirements redundant infrastructure in cluster or replication and readiness of alternate site, updating of BCP documents etc.)

Conversion process: During implementation it is possible that the data converted and migrated to new system might contain obvious errors resulting in erroneous processing or frauds. The conversion processes must be evaluated against the record maintained to ensure the accuracy, completeness and security of data.

IS Auditors should be able to determine if the expected benefits of the new system are realized and whether users are satisfied with the new system. IS Auditors may also review which of the SDLC phases have not met desired objectives and whether any corrective actions were taken.

If there are differences between expectations and actual results, auditors need to determine the reasons for the same. Such discrepancies may be due to incomplete user requirements or any other shortcomings.

8.3 Summary

Successful execution of SDLC project must be reviewed regularly as part of continuous improvement of organisation's project management practices. The IS auditor can play an important role in the process by providing inputs based on review of existing projects. IS Auditor in this case is performing the role of consultant rather than an auditor, as the objective is to implement the learning from review process.

Key factors to be considered by IS Auditor in SDLC process

- Understanding characteristics of system life cycle from initiation till retirement or replacement.
- Understanding and improving project management practices for SDLC projects within organisation.
- The need for adopting latest methodology for information Systems development/acquisition projects based on business focus.
- Understand SDLC phases and activities undertaken in each phase and modifications required depending on the nature of deliverables (new application)
- Requirements analysis is a key component of every IT related project. Capturing appropriate requirements helps in improving time, cost and quality requirements of project. It also helps in minimizing the scope creep situations.
- Building business case with expected benefits and associated risks forms the basis for evaluation of SDLC projects.
- Software Acquisition activities begins with feasibility Study. Although Software Acquisition is not a phase of traditional SDLC but is an important aspect as majority of companies are now buying readymade solutions.
- Outsourcing of SDLC project must be controlled by service level agreements and ongoing monitoring.
- Majority learning are identified in development and implementation phase, where user involvement must be highest possible.
- Mid-project review helps in making corrections in project execution to minimize risks
- Post-implementation review helps in ensuring benefit realization and identifying learning from executed project.

8.4 Questions

1. The primary reason why post implementation review is not performed immediately after implementation is to ensure that auditor can review:
 - A. Change management process based on incidents
 - B. Measure changes customer satisfaction levels
 - C. Compare benefits realized with business case
 - D. Comment of conformance of implementation process
2. While conducting post implementation review of software implemented as IS auditor shall be MOST interested in which of the following metrics? Increasing number of:
 - A. Help desk calls for improving service delivery.
 - B. Operational errors impacting service delivery.
 - C. Change requests approved to add new service.
 - D. Updates required in end user operations manual.
3. While reviewing the prioritization and coordination of SDLC projects and program management, IS auditor shall FIRST ensure that:
 - A. Project selection framework is aligned with IT strategy.

- B. Risks are identified, monitored and mitigated in time.
 - C. Projects are completed within stipulated time and budget.
 - D. Project and program related documentation is available.
4. While reviewing role of senior management in an organization's IT project and program management, IS auditor FIRST ensures that the senior management has:
- A. Allotted appropriate budget and required resources.
 - B. Provided for monitoring of risks associated with projects.
 - C. Defined key performance indicators for each IT project.
 - D. Issued guidelines for implementing framework.
5. Which of the following pair of activities IS auditor cannot perform as team member for software development project?
- A. Conduct the midterm review and recommend controls
 - B. Implement controls and develop integrated test facility
 - C. Develop a control module and perform unit testing
 - D. Implement controls and perform post implementation review
6. Which of the following SDLC project related document shall best provide input on design of controls in application being developed?
- A. Project business case and feasibility study
 - B. PERT, CPM diagrams and Gantt Charts
 - C. Application system detail design document
 - D. Detailed requirements specifications

8.5 Answers and Explanations

1. C. The primary reason for post-implementation review by IS Auditor is to ensure that the organization can start realizing benefits described in business case. Other options are not primary.
2. B. Increasing number of errors affecting service delivery after implementing new application indicates that the application contains bugs that are affecting service delivery and is a major concern. Other options are normal processes and may or may not affect the service delivery.
3. A. Organization must have standard project selection framework as per organization's IT strategy, since that is going to help steering committee in deciding the priority of project selection. Other activities are required for project and program management.
4. D. Except option D other activities are not performed by senior management
5. D. Auditor cannot audit a project where auditor has been actively involved in implementation.
6. C. Detail design document shall best provide information on controls that are being embedded in application being developed. Requirements shall also provide information. However, design shall ensure that requirements are captured in design.

SECTION 3: APPENDIX

IS auditor may use checklist to ensure that review is complete. In order to formalize the auditors' role and practices, a master checklist may be prepared. It is suggested that a master checklist for every audit must be prepared by considering the nature of engagement, type and culture of organisation, objectives of audit and expectation from auditor. Using one checklist for all audits have a risk that auditor may end up in concluding on inappropriate findings and auditor's report may not add value to the organisations.

This is a general checklist. For additional information readers may visit websites of Institute of Internal Auditors (www.theiia.org), ISACA (www.isaca.org) and similar organisations which have done exhaustive research in developing suitable audit programs for various technologies and SDLC projects. The IS Auditor may add more columns (control description, documents inspected, evidence collected, tests performed, result of analysis, conclusion on design, conclusion effectiveness of controls and overall finding) to this checklist to convert it into an audit work paper document..

(Table 8.1) is a sample checklist:

Sl. No.	Checkpoints	SDLC Phase Remark
1.	Whether information system acquisition and / or development policy and procedure documented?	<i>(General questions covers essential information about control environment within organisation)</i>
2.	Whether system acquisition and / or development policy and procedure approved by the management?	General <i>(related to Phase 3 B to 6B)</i>
3.	Whether the policy and procedure cover the following: Problems faced in existing system and need for replacement Functionality of new IS Security needs Regulatory compliance Acceptance Criteria Proposed roles and responsibilities Transition/ Migration to new IS Interfaces with legacy systems Post implementation review Maintenance arrangements.	General <i>(related all phases)</i>

4.	Whether policy and procedure documents are communicated / available to the respective users?	General
5.	Whether policy and procedure documents are reviewed and updated at regular intervals?	General
6.	Whether the organisation has evaluated requirement and functionalities of proposed application?	Phase 1 Feasibility Study Phase 2 requirement definition
7.	Whether the organisation carried out feasibility study in respect of financial, operational and technical feasibility	Phase 1 Feasibility Study
8.	Whether Business case has been prepared listing the benefits against associated risks and approved by management?	Phase 1 and 2 Feasibility study and requirement definition
9.	Whether selection of vendor and acquisition terms considers: Evaluation of alternative vendors Specification on service levels and deliverables Penalty for delays Escrow mechanism for Source codes Customization Upgrades Regulatory Compliance Support and maintenance.	Phase 3B and 3C
10.	Whether the organisation has identified and assigned roles in development activities to appropriate stakeholders?	General
11.	Whether the organisation has a separate development, test and production environments?	General <i>(Mainly related to Phase 6 Testing, Phase 7 UAT and Phase 9 Support)</i>
12.	Whether the IS developed plan is prepared and approved by the management?	Phase 1 Feasibility study Phase 3/4 Analysis and Design

13.	Whether the testing of IS includes: - Confirms the compliance to functional requirements - Confirms the compatibility with IS infrastructure - Identifies bugs and errors and addresses them by analyzing root causes - Escalating functionality issues at appropriate levels.	Phase 6 Testing
14.	Whether the adequate documentation for: - Preserving test results for future reference - Preparation of manuals like systems manual, installation manual, user manual - Obtaining user sign off / acceptance	Phase 6 Testing
15.	Whether the implementation covers the following? - User Departments' involvement and their role - User Training - Acceptance Testing - Role of Vendor and period of Support - Required IS Infrastructure plan - Risk involved and actions required to mitigate the risks - Migration plan	Phase 8 Implementation
16.	If the development activities are outsourced, are the outsourcing activities evaluated based on following practices: - What is the objective behind Outsourcing? - What are the in-house capabilities in performing the job? - What is the economic viability? - What are the in-house infrastructure deficiencies and the time factor involved? - What are the Risks and security concerns? - What are the outsourcing arrangement and fall back method? - What are arrangements for obtaining the source code for the software? - Reviewing the capability and quality of software development activities by visit to vendor's premises? - Review of progress of IS development at periodic intervals.	Phase 1 Feasibility Study and Phase 3C to 6C Phase 7 UAT

Module 5

17.	Whether the organisation carried out a post implementation review of new IS?	General Phase 8 Implementation
18.	Whether a process exists for measuring vendors' performance against the agreed service levels?	Phase 6 C and Phase 9 Support and maintenance
19.	Whether post implementation review results are documented?	Phase 8 Implementation

Module-6

**Business Application
Software Audit**

TABLE OF CONTENTS

MODULE 6: BUSINESS APPLICATION SOFTWARE AUDIT	371
SECTION 1: OVERVIEW	371
Objective:	371
Learning Objectives.....	371
Task Statements.....	371
Knowledge Statements	372
Relationship between Task and Knowledge statements.....	372
Knowledge Statement Reference Guide	374
Mapping of cases to chapters.....	377
SECTION 2: CONTENTS.....	379
Definition:	379
Learning Objective.....	379
Chapter 1: Business Process and Business Application.....	380
Part 1: Enterprises business models.....	380
1.1 Introduction	380
1.2. Business Models and controls	380
1.3 Business Model, Business Process and Business Applications	380
1.3.1 Business Process.....	380
1.3.2 Business Processes and Control Structure	381
1.3.3 Business Applications	381
Definition.....	381
1.4 Business model and risk assessment	381
Introduction	381
1.4.1 Auditing Standards.....	382
ISACA Standards.....	382
ICAI Standards.....	382
Internal Audit Standards	383
1.4.2 Risk assessment for a business application used by organisation	383
1.5 Case Study	383

Conclusion:	386
Case for participants	386
Part 2: Business Application Software as per Enterprises Business Model	387
Learning Objectives.....	387
Introduction.....	387
2.1 Business Application Software: Parameters of selection	387
Key parameters of selection of business application software may be:	387
2.2 Types	388
2.3 Key features and controls for business applications.....	389
Part 3: Case Studies	391
Case for participants	393
2.4 Questions	394
2.5 Answers and Explanations	395
Chapter 2: Application Control	397
Part 1: Application controls review.....	397
Learning Objective.....	397
1.1 Introduction	397
1.1.1 Application controls	397
1.1.2 Internal controls.....	397
1.2 Objectives of application control and key business information requirements	398
1.2.1 Objectives	398
1.2.2 Information Criteria.....	398
1.2.3 Application controls objectives	399
1.2.4 Control practices	400
1. Source Data Preparation and Authorisation.....	400
2. Source data collection and entry	401
3. Accuracy, completeness and authenticity checks	401
4. Processing integrity and validity.....	402
5. Output review, reconciliation and error handling	403
6. Transaction authentication and integrity.....	403

Part 2: Application controls review	405
2.1 Review of application control various business application	405
2.1.1 Need for application control review	405
2.1.2 How to perform application review?	405
2.2 Review of business application controls through use of audit procedures.....	406
2.3 Application controls review for specialised system	406
2.3.1 Artificial Intelligence (AI)	406
IS Auditor's Role	407
2.3.2 Data Warehouse	407
IS Auditor's Role	407
2.3.3 Decision Support System (DSS)	407
IS Auditor's role	408
2.3.4 Electronic Fund Transfer (EFT).....	408
IS Auditor's role	408
2.3.5 E-commerce	409
Risks of E-commerce.....	409
IS Auditor's role	409
2.3.6 Point of Sale System (PoS)	409
IS Auditor's role	409
2.3.7 Automatic Teller Machines (ATM).....	410
IS Auditor's Role	410
Part 3: Cases of Application controls.....	411
3.1 Proper design of source document	411
Case of an educational/vocational institute collecting fees from students	411
3.2 Exception reporting.....	412
What is the benefit?	413
What is the loss if above items are not checked?	414
a. Section 69C of Income Tax Act, 1961: Unexplained expenditure, etc.:	414
3.3 Case for Dependency check:	414
Case of validating two related field of employee database	414

3.4 Reasonableness Check	416
Case of Purchase Order in excess of five times vendor's annual sale	416
3.5 Case to highlight necessity of duplicate check	416
3.6 Obsolete stock reporting	417
3.7 Report on Sales below cost price	417
3.8 Report on TDS deducted but not remitted in time	418
3.9 Questions	419
3.10 Answers and Explanations	421
Chapter 3: Auditing Application Control	423
Part 1: Audit Program for review of application software	423
Learning Objectives.....	423
1.1 Introduction	423
1.2 Why IS Audit?.....	423
Case to highlight "NPA provisioning in system may be wrong	423
1.3 What is IS Audit?	425
1.4 How to perform IS Audit?	426
1.5 Audit mission	426
1.6 Performing an IS Audit.....	427
1.7 Steps of IS Audit	428
1.8 Audit program for key business application.....	429
1.9 Computer Assisted Audit Techniques	429
1.9.1 Needs for CAAT	429
1.9.2 Types of CAAT	430
1. Generalised Audit Software (GAS)	430
2. Specialised Audit Software (SAS)	431
3. Utility Software	431
1.9.3 Typical Steps in using GAS	431
1.9.4 Selecting, implementing and using CAATs	432
1. 10 Continuous Auditing Approach	432

1.10.1 Techniques for Continuous Auditing	433
1. Snapshot	433
2. Integrated Test Facility (ITF)	433
3. System Activity File Interrogation	434
4. Embedded Audit Facilities	434
5. Continuous and Intermittent Simulation	435
1.11 Case on using MS Excel to find Duplicate / Missing Sales Invoice	435
1.11.1 Steps to be performed in above case through use of excel	435
1.11.2 Cases on how to use continuous auditing	437
1. Snapshot	437
2. Integrated Test Facility (ITF)	437
Part 2: Compliance testing and Substantive testing	439
2.1 Compliance Testing	439
2.1.1 Purpose	439
2.2 Substantive Testing	440
2.2.1 Purpose	440
2.3 Relationship between compliance and substantive testing	440
Part 3: Impact of Business application software on Business processes / controls	441
3.1 Case: Highlight need for redefining business process	441
a. To know: Teeming and Lading fraud	441
b. Why this fraud occurs?	441
c. How to control the risk in business application system?	441
1. Organisation using TALLY:	441
2. Organisation using ERP system like SAP:	441
d. What TALLY users need to do?	442
3.2 Procedures to manage changes to business processes and impact on controls	442
Part 4: User Controls	443
4.1 Principles to follow while granting user rights	443
4.2 Creating users for different level of use	443
4.2.1 Key requirement	443

4.2.2 IS Auditor key checkpoints	444
i. Who has the authority to create user rights?	444
ii. Authorisation procedure before creating user rights?	444
iii. Validation of user rights created in system?	444
iv. Process of alteration of user rights?	444
v. Keeping track of user actions?	445
4.3 Creating users for different level of use	445
Case Studies	445
1. User rights review Audit	445
2. GM (F) who left the company	446
Part 5: Database controls	447
5.1 Key features of database	447
5.1.1 Database architecture	447
5.2 Database Security and Control	447
5.3 User creation in database	448
5.4 Structured Query Language	450
5.4.1 Components of SQL	450
5.4.2 Language elements of SQL	451
5.5 SQL commands for reporting	451
Part 6: Financial Reporting and Regulatory requirement in Information Systems	453
6.1 Nature of compliances	453
6.2 Who is responsible for accuracy and authenticity of reports?	454
6.3 Validation of statutory reports from business application software	455
Case on validation of statutory rates in business application software	455
1. PF rates are not properly defined	455
2. TDS rates are not correctly specified	456
Part 7: System Audit Report format as per best practices	459
7.1 Reporting Standards	459
7.1.1 Case to prepare report in specified format	460
7.2 Questions	461

7.3 Answers and Explanations	462
SECTION 3: APPENDIX	465
Appendix 1: Checklist for Application Controls	465
Appendix 2: ATM Audit Checklist	471
Appendix 3: Application Software Checklist.....	471
Appendix 4: User Rights Creation Checklist.....	471
Appendix 5: Review of business application's impact on controls	475
Appendix 6: System Audit Report.....	476
Appendix 7: Sample Audit Report Of Application Software	479

MODULE 6: BUSINESS APPLICATION SOFTWARE AUDIT SECTION 1: OVERVIEW

Objective:

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.

Learning Objectives

- To understand business processes and business application software.
- To understand the business application implemented controls by organisations.
- To provide assurance on business application software and the implemented controls through business application audit.

Task Statements

- 6.1 Assess the enterprise business models by performing preliminary review of effectiveness of the entity's business processes and embedded controls
- 6.2 Assess business processes - risks assessment and control evaluation in the context of business strategy, impact of business application software on Business processes/controls
- 6.3 Assess Business processes by performing preliminary review of adequacy of controls
- 6.4 Identify and document information technology environment and platforms, technology architecture, network, system software and application environment to assess control architecture.
- 6.5 Identify application controls in Data warehouse, Data Mart, DSS, ESS, AI, EFT, etc.
- 6.6 Identify various types of Business Applications like ERP, Banking, Accounting
- 6.7 Prepare audit program for planning and perform review of application software
- 6.8 Identify information systems that are used to process and accumulate transactional data, as well as provide monitoring and financial reporting information and assess the controls.
- 6.9 Review enterprise security policy relating to the identification, authentication and restriction of users to authorized functions and data.
- 6.10 Assess procedures to manage changes to business processes and impact on controls
- 6.11 Review database structure and tables, user creation, access levels and user management.
- 6.12 Evaluate application software configuration and user management features such as user rights and administration and map them with enterprise policies relating to segregation of duties by reviewing user rights granted to specific roles and responsibilities.

- 6.13 Evaluate internal control systems in application software relating to system design, data creation/input, data processing, data flow, data transmission and data storage.
- 6.14 Use reporting, query and SQL features as required for reviewing controls.
- 6.15 Audit specific application software users; assess business system functionality, user rights and segregation of duties levels of authorization, and data security by performing analytical procedures review, compliance testing and substantive testing.
- 6.16 Assess application software controls and identify areas of weaknesses in controls and advise remedial measures
- 6.17 Communicate/Report findings in specific format using standards/best practices as required.
- 6.18 Performing review of application controls as relevant for assurance or compliance assignments.

Knowledge Statements

- 6.1 Enterprise business models
- 6.2 Key features and functionalities of application software
- 6.3 Business processes controls, Analytical procedures, compliance testing and substantive testing
- 6.4 Risk assessment and control evaluation in the context of business strategy
- 6.5 Impact of Business application software on Business processes/controls
- 6.6 Information systems and financial reporting and regulatory requirements for controls.
- 6.7 structure, roles and responsibilities
- 6.8 Application controls in Data warehouse, Data Mart, DSS, ESS, AI, EFT, EDI, etc.
- 6.9 Various types of Business Applications like ERP, Banking, Accounting, etc.
- 6.10 Procedures to manage changes to business processes and impact on controls
- 6.11 Audit program for planning and perform review of application software
- 6.12 Application system software environment at different levels
- 6.13 Database architecture: database structure and tables, user creation and administration, reporting, query and SQL Features
- 6.14 Key business system users, key functionality, user rights and segregation of duties levels of authorization, and data security
- 6.15 Controls at different levels, areas of control weaknesses, risk rating and remedial measures
- 6.16 Report findings in specific format using standards/best practices as required.
- 6.17 Application controls review as relevant for assurance or compliance assignments.

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
6.1 Assess the enterprise business models by performing preliminary review of effectiveness of the organisation's business processes and embedded controls.	1 Enterprise business models
	Key features and functionalities of application software
6.2 Assess business processes: risks assessment and control evaluation in the context of business strategy, impact of business application software on Business processes/controls	3 Business processes controls, Analytical procedures, compliance testing and substantive testing
6.3 Assess Business processes by performing preliminary review of adequacy of controls	4 Risk assessment and control evaluation in the context of business strategy
6.4 Identify and document information technology environment and platforms, technology architecture, network, system software and application environment to assess control architecture.	5 Impact of Business application software on Business processes/controls
6.5 Identify application controls in Data warehouse, Data Mart, DSS, ESS, AI, EFT, EDI	6 Application controls in Data warehouse, Data Mart, DSS, ESS, AI, EFT, EDI
6.6 Identify various types of Business Applications like ERP, Banking, Accounting	7 Various types of Business Applications like ERP, Banking, Accounting
6.7 Prepare audit program for planning and perform review of application software	8 Audit program for planning and perform review of application software
6.8 Identify information systems that are used to process and accumulate transactional data, as well as provide monitoring and financial reporting information and assess the controls.	9 Information systems and financial reporting and regulatory requirements for controls.
6.9 Review enterprise security policy relating to the identification, authentication and restriction of users to authorized functions and data.	10 Application system software environment at different levels
	11 Organisation structure, roles and responsibilities
6.10 Assess procedures to manage changes to business processes and impact on controls	12 Procedures to manage changes to business processes and impact on controls

6.11 Evaluate application software configuration and user management features such as user rights and administration and map them with enterprise policies relating to segregation of duties by reviewing user rights granted to specific roles and responsibilities.	13 Key business system users, key functionality, user rights and segregation of duties levels of authorization, and data security
6.12 Evaluate internal control systems in application software relating to system design, data creation/input, data processing, data flow, data transmission and data storage.	14 Controls at different levels, areas of control weaknesses, risk rating and remedial measures
6.13 Review database structure and tables, user creation, access levels and user management.	15 Database architecture: database structure and tables, user creation and administration, reporting, query and SQL Features
6.14 Use reporting, query and SQL features as required for reviewing controls.	
6.15 Audit specific application software users; assess business system functionality, user rights and segregation of duties levels of authorization, and data security by performing analytical procedures review, compliance testing and substantive testing.	
6.16 Assess application software controls and identify areas of weaknesses in controls and advise remedial measures	16 Application controls review as relevant for assurance or compliance assignments.
6.17 Performing review of application controls as relevant for assurance or compliance assignments.	
6.18 Communicate/Report findings in specific format using standards/best practices as required.	17 Report findings in specific format using standards/best practices as required.

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 of this module.

Topic Heading	Chapter	Part	Para
1 Enterprise business models			
Business Models and controls	1	1	1.2
Key features and functionalities of application software			
Business Models and controls	1	1	1.2
3 Business processes controls, Analytical procedures, compliance testing and substantive testing			
Business Model, Business Process and Business Applications	1	1	1.3
Business Model and Risk Assessment			1.4
4 Risk assessment and control evaluation in the context of business strategy	1		
5 Impact of Business application software on Business processes/controls	1		
6 Application controls in Data warehouse, Data Mart, DSS, ESS, AI, EFT, EDI			
Review of Application Control various business application	2	2	2.1
7 Various types of Business Applications like ERP, Banking, Accounting			
Review of Application Control various business application	2	2	2.1
Review of business application controls through use of audit procedures			2.2
8 Audit program for planning and perform review of application software			
Audit program for key business application	3	1	1.6
9 Information systems and financial reporting and regulatory requirements for controls.			
Nature of compliances	3	6	6.1
Who is responsible for accuracy and authenticity of reports?			6.2
Validation of statutory reports from business application software			6.3
10 Application system software environment at different levels			
Review of Application Control various business application	2	2	2.1
Review of business application controls through use of audit procedures			2.2
Application controls review for specialised system			2.3

11 Organisation structure, roles and responsibilities			
Principles to follow while granting user rights	3	4	4.1
Creating users for different level of use			4.2
Creating users for different level of use			4.3
12 Procedures to manage changes to business processes and impact on controls	3	3	3
13 Key business system users, key functionality, user rights and segregation of duties levels of authorization, and data security			
Review of business application controls through use of audit procedures	2	2	2.2
14 Controls at different levels, areas of control weaknesses, risk rating and remedial measures			
Business Application software: Parameters of selection	2	2	2.1
Compliance Testing	3	2	2.1
Substantive Testing			2.2
Relationship between compliance and substantive testing			2.3
15 Database architecture: database structure and tables, user creation and administration, reporting, query and SQL Features			
Key features of database	3	5	5.1
Database security and control			5.2
User creations in database			5.3
Structured Query Language			5.4
SQL commands for reporting			5.5
16 Application controls review as relevant for assurance or compliance assignments.			
Compliance Testing	3	2	2.1
Substantive Testing			2.2
Relationship between compliance and substantive testing			2.3
17 Report findings in specific format using standards/best practices as required.			
Nature of compliances	3	6	6.1
Who is responsible for accuracy and authenticity of reports?			6.2
Validation of statutory reports from business application software			6.3

Mapping of cases to chapters

The scope of Module 6 is Business Application Software Audit. There are a number of cases (practical case studies) which have been discussed in the module. A chapter wise mapping of the cases is given.

Sl. No	Case Study	Chapter	Part	Para
	CHAPTER 1			
1	To understand the concept of risk assessment of a business application and its impact of other audit procedures to be adopted by auditor.	1	1	1.5
2	Case for participants: Issue to audit: A prepare a risk assessment table to see; "Whether the business application used by organisation <i>restricts negative cash balance</i> ".	1	1	1.5
3	To check whether the application used by the organisation is appropriate for the business purpose.	1	3	
4	Case for participants Audit Objective: To check whether the application used by the organisation is appropriate for the business purpose	1	3	
	CHAPTER 2			
5	a. Proper design of source document: Case of an educational institute collecting fees from students.	2	3	
6	b. Exception reporting: 1. Exception reporting in TALLY. Exception reporting in bank.	2	3	
7	c. Dependency check: Case of validating two related field of employee database	2	3	
8	d. Reasonableness Check: Case of Purchase Order in excess of five times vendor's annual sale	2	3	
9	e. Duplicate Check: Case of double payment made to vendors against one purchase invoice.	2	3	
10	Obsolete stock	2	3	
11	Sales below cost price	2	3	
12	TDS deducted but not remitted in time	2	3	
	CHAPTER 3			
13	To perform IS audit as an exercise needs to precede financial audit	3	1	1.1

Module 6

14	Using MS Excel as an Audit Tool	3	1	
	Case on concurrent audit techniques			
15	Snapshot	3	1	
16	Integrated Test Facility (ITF)	3	1	
17	Embedded Audit Facilities	3, 1	1 /1	
18	To highlight importance of re-defining the business process to suit the requirements of the selected business application.			
19	User Rights Review Audit	3	3	
20	GM (F) leaving the company	3	3	
21	PF rates not properly defined	3	6	
22	Wrong classification of TDS	3	6	
23	To help document a IS audit report for a company's password management policy	3	7	

SECTION 2: CONTENTS

This module has been written with an objective to help participants learn about the business application software, and audit of these business applications. Application software is most critical component of any IT infrastructure used in organisations as this processes the business transactions for all types of organisations. Hence, it is imperative for an IS Auditor to learn the process of performing a business application audit.

This module has three chapters.

- Chapter 1: Deals with business application software's, business processes and business models. The chapter elaborates the nature of business applications that may be used by entities.
- Chapter 2: Deals with application controls in business application software. It further elaborates relevance of application controls in business operations of an organisation.
- Chapter 3: Deals with audit of the business application software. This chapter discusses database controls and user controls. It also provides guidance on how to prepare IS audit reports.

Definition:

Business application software audit module is focused on providing practical guidance to members of ICAI. The module is written with an objective to provide hands on training to members. A DISA should be able to understand how to perform a business application software audit after going through this module.

Learning Objective

- To understand business processes and business application software.
- To understand how business application controls are implemented.
- To provide assurance on business application software and the implemented controls by performing business application software audit.

This module discussed the various business models used by an organisation for their business purposes. There is a direct co-relation between the business model adopted by an organisation and the goals of the organisation. The same co-relation extends to the nature of controls that are put in place by the organisation to achieve its business objectives.

The primary objective of this module is to provide understanding about business processes, business application software and controls implemented in business application software. This will enable IS Auditors to provide assurance or consulting services in the critical area of business application audit.

CHAPTER 1: BUSINESS PROCESS AND BUSINESS APPLICATION

PART 1: ENTERPRISES BUSINESS MODELS

1.1 Introduction

“A business model describes the rationale of how an organization creates, delivers and creates value (economic, social, cultural, or other forms of value). The process of business model construction is part of business strategy.” AS per Oxford Dictionary, it is two different words meaning, “Person’s particular version of product / service, delivery”. A business model can be thus said to be a way an organization delivers its product / service to customers, strategies to do business, infrastructure, trading practices, and operational processes and policies. Business models are a necessary outcome of the vision, mission statements of an organization.

Business models can be varied in nature, like traditional that is sales through retailer or modern that sales through e-commerce. Each business model represents a different business objective for an organisation. It is also important to understand that an organisation is not restricted to a specific business model, an organisation may adopt more than one business model to deliver its product / services.

1.2. Business Models and controls

Each business model shall have a basic control structure built into its processes. The controls structure is also dependent upon the business application software that is being used by the organisation. Control structures are relevant for each business model. The nature of control, the way they are implemented and executed depends upon the business model being put to use. Each business model has its set of risks. The risk associated with the way business model works has a direct link to the nature of controls being put in place.

1.3 Business Model, Business Process and Business Applications

1.3.1 Business Process

Business Process is defined as way / method of arranging a set of activities / tasks to achieve a specific business objective or manufacture a product or deliver a service. Business processes as discussed shall be implemented by an organisation through the business applications it is using.

1.3.2 Business Processes and Control Structure

1. Each business cycle used by an organisation has a defined control structure that has a direct co-relation to the business model used.
2. Organisations have to document business processes and identify key control points.
3. Organisations have to ensure that the key control points are configured in system.
4. IS auditors have to obtain understanding of the above, to assess associated business risk, implemented controls and provide assurance whether the available controls are adequate and appropriate as per business requirements. In case of control weakness, they have to provide recommendations for risk mitigation or performance improvement as required as per scope of assignment.

1.3.3 Business Applications

Definition

“Business Application”, may be defined as applications (meaning computerized software) used by organisation to run its business. The consideration is whether the said application covers / incorporates the key business processes of the organisation. Another important consideration is whether the control structure as available in the Business Application is appropriate to help organisation achieve its goals. Business applications are where the necessary controls needed to run business are put in place. The business processes and related controls are put in place through business applications used by an organisation.

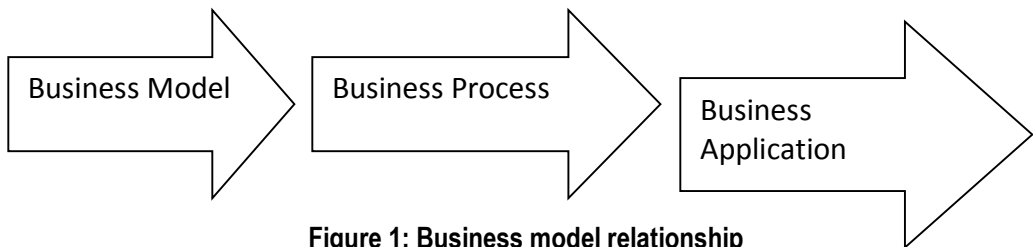


Figure 1: Business model relationship

Organisations use business application as per the business models adopted and the business goals set by management. There are a multitude of business applications and we will discuss some of the critical business applications later in this chapter/module.

1.4 Business model and risk assessment

Introduction

It is critical for an IS Auditor to understand the business model adopted by an organisation so as to get better understanding of risks associated with the business model adopted by the

organisation. Auditing standards issued by standards setting bodies across the world highlight the critical need for performing risk assessment.

1.4.1 Auditing Standards

ISACA Standards

ISACA ITAF, 1201 “Engagement Planning”, identifies risk assessment as one of the key aspects and states that IS audit and assurance professionals, have to;

- Obtain an understanding of the activity being audited. The extent of the knowledge required should be determined by the nature of the enterprise, its environment, areas of risk, and the objectives of the engagement.
- Consider subject matter guidance or direction, as afforded through legislation, regulations, rules, directives and guidelines issued by government or industry.
- Perform a risk assessment to provide reasonable assurance that all material items will be adequately covered during the engagement. Audit strategies, materiality levels and resource requirements can then be developed.
- Develop the engagement project plan using appropriate project management methodologies to ensure that activities remain on track and within budget.

ICAI Standards

SA 200 “Overall Objectives of the Independent Auditor and the conduct of an audit in accordance with standards on Auditing”, Issued by ICAI, requires an auditor to plan an audit and get following information: “The auditor should plan his work to enable him to conduct an effective audit in an efficient and timely manner. Plans should be based on knowledge of the client’s business. Plans should be made to cover, among other things:

- a. Acquiring knowledge of the client’s accounting system, policies and internal control procedures;
- b. Establishing the expected degree of reliance to be placed on internal control;
- c. Determining and programming the nature, timing, and extent of the audit procedures to be performed; and
- d. Coordinating the work to be performed”.

The first step to by an IS auditor is to obtain knowledge about the business of the organisation, do risk assessment and decide on the specific and additional audit procedures to complete the audit. The above steps used in a case discussed below at section 1.5

Internal Audit Standards

SIA 14, on INTERNAL AUDIT IN INFORMATION TECHNOLOGY ENVIRONMENT, as issued by ICAI, states that; “The internal auditor should consider the effect of an IT environment on the internal audit engagement, inter alia:

- a. the extent to which the IT environment is used to record, compile, process and analyse information; and
- b. The system of internal control in existence in the organisation with regard to: the flow of authorised, correct and complete data to the processing centre; the processing, analysis and reporting tasks undertaken in the installation”.

1.4.2 Risk assessment for a business application used by organisation

Risk assessment is a necessary initial procedure to be adopted by IS Auditors, so that they can determine the nature, timing, and extent of the audit procedures to be performed; ISACA ITAF 1202, states IS auditors have to consider subject matter risk, audit risk and related exposure to the enterprise.

1. Subject matter risk, relates to business risk, country risk, contract risks. These are important for an IS auditor to consider but merged with inherent risk (discussed later).
2. Audit risk, is define as auditor reaching incorrect conclusion after an audit. The components of audit risk being *control risk*, *inherent risk* and *detection risk*.
 - Control risk is defined as failure of a control to prevent, detect a material error that exists in system.
 - Inherent risk is defined as risk arising without taking into account a planned action by management to reduce the risk. Simply said it related to nature of transaction / business.
 - Detection risk is defined as failure of an audit procedure to detect an error that might be material individually or in combination of other errors.

The above risk assessment will lead to conclusion and extent of compliance testing and other substantive audit processes to be adopted by the IS Auditors in an audit of business application system. As per COBIT ““Business process controls are activities designed to achieve the broad range of management objectives for the process as a whole. Application controls, on the other hand, are the sub-set of business process controls that relate specifically to the applications and related information used to enable those business processes. “

1.5 Case Study

Objective: To understand the concept of risk assessment of a business application and its impact of other audit procedures to be adopted by auditor.

Issue under consideration: For tax audits done under section 44AB of Income Tax Act, 1961, auditor has to list cash expenses done by an organisation in excess of Rs.20,000/-. These expenses disallowed as a business expense under 40A (3) of the Income Tax Act, 1961.

Business consideration for above issue: Any amount of expense in excess of Rs.20, 000/- in cash shall result in the expense being disallowed as a business expense. The same shall lead to increase in tax liability and related.

Business Applications used: Two different business applications are being considered.

1. Accounting application: The organisation is using TALLY as its business application.
2. ERP Application: The organisation is using SAP as its business application.

A comparative analysis illustrates the impact of business application on audit procedure

Sl. No.	Description	Business Application under consideration	
	Auditor audit shall plan include the following steps: a. acquiring knowledge of the client's accounting system, policies and internal control procedures; b. establishing the expected degree of reliance to be placed on internal control; c. determining and programming the nature, timing, and extent of the audit procedures to be performed;		
	Steps	Accounting Application [TALLY]	ERP Application [SAP]
1	First step: Acquiring knowledge of the client's accounting system, policies and internal control procedures;	Basic configuration in the system does not have an option to restrict payments in excess of Rs.20, 000/-.	The system can be configured to restrict payment in excess Rs.20,000/-
	IMPACT of the above on auditor's assessment of risk.		
	Inherent risk assessment	This increases the <i>inherent risk</i> , vis-à-vis non-compliance with law.	This status keeps the related <i>inherent risk low</i> regarding non-compliance with law.
Sl. No.	Description	Business Application under consideration	

		Accounting Application [TALLY]	ERP Application [SAP]
2	b. establishing the expected degree of reliance to be placed on internal control;	As the necessary control does not exist in business application, the question of reliance on control does not arise.	Auditor may need to apply <i>compliance testing</i> , to check whether the related control is working properly or not. Compliance testing can be through CAATs, as discussed in Module 2.
	Impact on the above on auditor's risk assessment		
	<i>Control risk assessment.</i>	This means auditor shall need to decide on other audit procedures to list such as cash expenses	Compliance test results shall indicate the nature of additional audit procedure.
3	c. determining and programming the nature, timing, and extent of the audit procedures to be performed;	The result of above process means the related <i>risk is higher of cash payments in excess of Rs.20, 000/- being made.</i> Auditor shall need to adopt procedure to arrive at the list.	Positive result of above procedures shall lead IS Auditor to conclude that the <i>risk is lower of cash payments in excess of Rs.20, 000/- being made.</i> Auditor can draw conclusion that no such payments have been made.
4	Additional procedures to be adopted by auditor.	Option 1: Use facility available in the accounting application to generate such list: Alt>F12 in TALLY allows user to define range of item to display. 2. Option: Use report from accounting application and audit the same to generate requisite details.	In case compliance testing results are negative; the resulting <i>control risk</i> shall be assessed as high. IS Auditor shall need to adopt one of the two options given in left column.

Conclusion:

The above case outlines the method, steps and procedure IS auditor needs to undertake for risk assessment of a business application. This helps understand the nature; timing of the additional audit procedures to be taken by IS auditor based on results of risk assessments. This case is referred again in chapter 3 part 1. 5 under heading CAAT: Embedded Audit Tools

Case for participants

Issue to audit: Prepare a risk assessment table to see: "Whether the business application used by organisation *restricts negative cash balance*".

Business relevance: Negative cash balance is indicator that the accounting is not timely, and not as per general business transaction. The same has an implication in Income Tax Act, 1961. Any negative cash balance may be treated as **un-explained expenditure** under section 69C of the act and **added to income of Assessee**.

Participants are expected to draw the risk assessment chart, draw appropriate conclusions and comment upon additional audit procedures to be adopted to identify negative cash balance in books.

PART 2: BUSINESS APPLICATION SOFTWARE AS PER ENTERPRISES BUSINESS MODEL

Learning Objectives

To understand the business application controls implemented in an organisation

Introduction

Business applications are the tool to achieve management goals and objectives. The nature of business enterprise model is a guide to the business application software selects. Each organisation selects the software as per its business goals and needs. The software selection is an important decision for top management to take. Selection of correct application software is quite often most essential as it contributes to success of business.

2.1 Business Application Software: Parameters of selection

Organisation has to put on a piece of paper the business requirements and business goals. Listing of these shall be great help for an organisation to conclude which type and nature of business application it shall use.

Key parameters of selection of business application software may be:

The business goal: Organisation may have varied business objectives, say for example many organisation are customer driven, few may be driven by social causes, other may emphasise capitalist mind-set.

The nature of business: One of the key determinants of the business application software type is the nature of organisation business. Few business may generate daily cash like petrol pumps, departmental store, few other organisation may generate require daily update of sales made like milkman, newspaper agent, few other generate lot of credit sales.

- a. **The geographical spread:** As globalisation has spreads, many Indian companies have been able to reap the benefits by becoming Indian MNC's. Few Indian companies are trying to foray in export market or increase their global footprint. The more the geographical spread of an organisation, more robust business application software is needed. Robustness here is intended to denote the capability of the business application system to work 24/7 as this may become a critical business need, and it may also denote whether the business application system has capability to handle **multiple currency accounting**.
- b. **The volume of transactions:** As the transaction volume increases it is important for organisation to go for business application software that can support business for the next

five years. This is again an important factor to consider, as improper selection can lead to a situation where a customer wants organisation to grow but it cannot grow.

- c. **The regulatory structure at place of operation:** As the number and nature of compliances increase across the world, organisation shall prefer that software which is capable to cater to the compliance requirements. A software company selling a product that is **SOX compliant** is likely to find more buyers than others.

2.2 Types

Business applications can be classified based on processing type (batch, online, real-time) or source (in-house, bought-in) or based on function covered. The most critical way for management is based in function it performs. The discussion is restricted to business applications based on function they perform.

- a. **Accounting Applications:**
Applications like TALLY, TATA EX, UDYOG, used by business entities for purpose of accounting for day to day transactions, generation of financial information like balance sheet, profit and loss account, cash flow statements, are classified as accounting applications.
- b. **Banking Application:**
Today all public sector banks, private sector banks, and including regional rural banks have shifted to **core banking business applications (referred to as CBS)**. Reserve Bank of India guidelines mandating all co-operative banks also to shift to core banking applications by December 013, means 95% plus Indian banks use CBS. CBS used by Indian banks include, FINACLE (by Infosys Technologies Ltd.), FLEXCUBE (By Oracle Financial Services Software Limited, formerly called i-flex Solutions Limited), TCS BaNCS (By TCS Limited), and many more CBS.
- c. **ERP Application:**
These have been created a separate category of business application systems, due to their importance for an organisation. These software called as enterprise resource planning software are used by entities to manage resources optimally and to maximize E³ i.e. economy, efficiency and effectiveness of business operations.
- d. **Payroll Application:**
Many companies across the world are outsourcing these activities to professionals. In India also many CA firms are doing good job on payroll outsourcing. TALLY has a payroll application built into it. ICAI, has made available for its members a payroll application.
- e. **Other Business Applications**
 - i. Office Management Software:
 - ii. Compliance Applications:
 - iii. Customer relationship management Software:
 - iv. Management Support Software:
 - v. Logistics Management Software:
 - vi. Legal matter management

vii. Industry Specific Applications:

The applications detailed above are those which constitute major audit areas for a CA.

2.3 Key features and controls for business applications

Each business application is selected and implemented for a specific business purpose. An IS Auditor has to verify whether the business objective from implementing the business application is achieved or even achievable.

PART 3: CASE STUDIES

Audit Objective: To review whether the application used by the organisation is appropriate for the business purpose.

User: Bank in co-operative sector

Business Application Software: Core banking Solution.

Auditor has to obtain understanding of clients business.

Sl. No.	Description	Business Application under consideration	
	<u>As per SA 200:</u> “Overall Objectives of the Independent Auditor and the conduct of an audit in accordance with standards on Auditing” Issued by ICAI, requires an auditor to plan an audit. <u>Audit shall plan include the following steps:</u> acquiring knowledge of the client’s accounting system, policies and internal control procedures.		
	Steps	Applicable laws	Sample list of guidelines
1	As client is a bank, guideline as specified by Reserve Bank of India (referred to as RBI) shall be applicable. All accounting system needs to be in compliance with the guidelines of RBI.	Reserve Bank of India Act, 1934 Banking Regulation Act , 1949 Companies act, 1956. Co-operative Act for state	Income Recognition and Asset Classification (IRAC) Asset Liability Management Guidelines (ALM) Investment Guidelines (IG) CRR and SLR maintenance Many more guidelines....
Audit Process			
Step 1	Understand the requirement of law		
a.	IRAC Norms	The guidelines state that once an account has been marked as NPA, <i>no further interest charging to be done.</i> Guidelines state that the classification shall be <i>borrower-wise not facility wise, meaning that once an account of a borrower has been marked as NPA all facility extended to the borrower are classified as NPA.</i>	

b.	ALM	Detailed guidelines issue require bank to create ALCO (Asset Liability Committee) and classify each item of balance sheet (both asset and liability), in terms of their maturity.	
c.	Investment Guidelines	Investments need to classified as “Held To Maturity” (HTM), Held for Trade (HFT) and Available for Sale (AFS) HTM investment can be up to limit specified by RBI. Present limit being 5%.	
d.	CRR and SLR	As per RBI, banks need to keep specified percentage of their time and demand liabilities in form of cash, investments, bullion.	
Step	Understanding the system		
	Area of operation	Requirement	Questions to get answers to?
a.	Income Recognition and Asset Classification	No further interest on NPA account.	Whether system has capability to tag an advance as NPA? Whether the system stops calculating interest on account once tagged as NPA?
		NPA borrower wise not facility wise.	To check whether at the time of creation of a new customer, duplicate check is done? To check customer report from system identifies all facility of the customer in the bank? To check whether system generates an exception report for a customer with more than one facility, when one of the facilities is marked as NPA?
b.	Asset Liability Management	Classify each item of balance sheet (both asset and liability), in terms of their maturity.	Whether the CBS used has ALM module? Whether chart of accounts for balance sheet as specified in master, have a field to specify the maturity pattern of account? Whether advance recovery schedule is updated in system? Whether the maturity report from system is as per required format?
	Investment Guidelines	Classification of investment	Whether the CBS used has Investment module? Whether master data has a field to classify investment in specified category? Whether the report generated is as per required format?

		Investment as per RBI specified limits.	Whether system allows update of RBI limits in master data? Whether system generates exception report when the investments made are not as per RBI guidelines?
d.	CRR and SLR.	RBI, guidelines to maintain CRR and SLR investment.	Whether the CBS, has capability to generate the requisite report for CRR and SLR compliance?
Step 3	Drawing conclusions for the audit objective in hand... on next page		

Above is a sample checklist for a detailed audit of business application that an IS Auditor may undertake. Above checklist is focused only on the business validity of the application selected by the organisation. Whether the organisation has proper transaction processing system and control is part of next chapter.

Step 3	Drawing conclusions for the audit objective in hand
	- Answers to the above checklist will help IS Auditor assess whether the CBS selected is appropriate to meet the business requirements of the organisation. - Where the IS auditor reaches a conclusion that many of the requirements are not being met he/she may give any of the following recommendations. First option: Modify the system to meet requirements of law. Second option: Change the system. - In case the management response to option 1 is that system cannot be modified than auditor reaches second option automatically. - Any modifications made are to be validated as per regression testing.

Case for participants

Audit Objective: To check whether the application used by the organisation is appropriate for the business purpose.

Business Application: The one being used by your **client** for accounting purpose.

Area to check: Five key business requirements to be validated.

Audit program for planning and performing audit of business application software is given in Appendix 1: Checklist for application control review.

2.4 Questions

1. Initial adoption of Business Model adopted by an organisation is dependent upon:

- A. Business Applications
- B. Business Objective
- C. Controls in business applications
- D. Business Laws

2. Which of the following is to be reviewed first by an IS Auditor in audit of application software is to understand:

- A. Business Application
- B. Business Controls
- C. Business Model
- D. Business Laws

3. Arrange the following in chronological order

- A. Establishing the expected degree of reliance to be placed on internal control
- B. Determining and programming the nature, timing, and extent of the audit procedures to be performed
- C. Coordinating the work to be performed
- D. Acquiring knowledge of the client's accounting system, policies and internal control procedures

The correct serial order:

- A. A, B, C, D
- B. D, A, B, C
- C. D, C, B, A
- D. B, C, D, A

4. ISACA ITAF 1202, states IS auditor needs the following for an enterprise:

- A. Inherent Risk and Audit Risk.
- B. Detection Risk and Control Risk.
- C. Subject matter risk and Audit risk.
- D. None of above

5. The best definition which fits 'COBIT 5' is that it is a:

- A. Business framework for the governance and management of enterprise IT.
- B. System Audit Tool

- C. Management tool for corporate governance
- D. IT management tool

2.5 Answers and Explanations

1. B. Business Objectives shall be the prime reason for adoption of business models. Other answers may be valid reasons but are never the first reason for adoption of a specific business model. “A **business model** describes the rationale of how an organization creates, delivers, and captures value (economic, social, cultural, or other forms of value). The process of business model construction is part of business strategy.”

2. C. Business Model, needs to be assessed first by IS Auditor. The, b and d, are assessment to be made later on. As an IS Auditor it becomes important to understand the business model adopted by an organisation for a better understanding of risk associated with business model adopted by an organisation.

3. B As per SA 00 SA 200 on “OVERALL OBJECTIVES OF THE INDEPENDENT AUDITOR AND THE CONDUCT OF AN AUDIT IN ACCORDANCE WITH STANDARDS ON AUDITING, the steps to audit as mentioned at point b.

4. B ISACA ITAF 1202, states IS auditor needs to consider subject matter risk and audit risk. Subject matter risk, relates to business risk, country risk, contract risks. Audit risk, is define as auditor reaching incorrect conclusion after an audit. The components of audit risk being *control risk, inherent risk and detection risk*.

5. A. COBIT 5 can be best described as “Business framework for the governance and management of enterprise IT by ‘a’. Other answers are part of COBIT framework but not full Framework.

CHAPTER 2: APPLICATION CONTROL

PART 1: APPLICATION CONTROLS REVIEW

Learning Objective

To understand the implemented business application controls by organisation

1.1 Introduction

Over the last several years, organizations around the world have spent billions of dollars upgrading or installing new business application systems for reasons ranging from tactical goals, such as year 2000 compliance, to strategic activities, such as using technology to establish company differentiation in the marketplace. An application or application system is software that enables users to perform tasks by employing a computer's capabilities directly. These applications represent the interface between the user and business functions. For example, a counter clerk at a bank is required to perform various business activities as part of his job and assigned responsibilities. From the point of view of users, it is the application that drives the business logic. Application controls pertain to individual business processes or application systems, including data edits, separation of business functions, balancing of processing totals, transaction logging, and error reporting. From an organizational perspective, it is important that application controls:

- Safeguard assets
- Maintain data integrity
- Achieve organisational goals effectively and efficiently

1.1.1 Application controls

As per COBIT's management guide: "Application controls are a subset of internal controls that relate to an application system and the information managed by that application. Timely, accurate and reliable information is critical to enable informed decision making. The timeliness, accuracy and reliability of the information are dependent on the underlying application systems that are used to generate process, store and report the information. Application controls are those controls that achieve the business objectives of timely, accurate and reliable information. They consist of the manual and automated activities that ensure that information conforms to certain criteria—what COBIT refers to as business requirements for information. Those criteria are effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability."

1.1.2 Internal controls

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines internal control as: "Internal control is a process, affected by an organisation's board of directors,

management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations"

COSO defines control activities as the policies and procedures that help ensure management directives are carried out.

1.2 Objectives of application control and key business information requirements

1.2.1 Objectives

COBIT states that application controls are intended to provide reasonable assurance that management's objectives relative to a given application have been achieved. Management's objectives are typically articulated through the definition of specific functional requirements for the solution, the definition of business rules for information processing and the definition of supporting manual procedures. Examples include:

- i. **Completeness:** The application processes all transactions and the resulting information is complete.
- ii. **Accuracy:** All transactions are processed accurately and as intended and the resulting information is accurate.
- iii. **Validity:** Only valid transactions are processed and the resulting information is valid.
- iv. **Authorisation:** Only appropriately authorised transactions have been processed.
- v. **Segregation of duties:** The application provides for and supports appropriate segregation of duties and responsibilities as defined by management.

1.2.2 Information Criteria

Key business requirements for information also called as information criteria that these quality parameters need to be present in information generated. These are:

1. **Effectiveness:** Deals with information being relevant and pertinent to the process as well as being delivered in a timely, correct, consistent and usable manner
2. **Efficiency:** Concerns the provision of information through the optimal (most productive and economical) use of resources
3. **Confidentiality:** Concerns the protection of sensitive information from unauthorised disclosure
4. **Integrity:** Relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations

5. **Availability:** Relates to information being available when required by the process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
6. **Compliance:** Deals with complying with the laws, regulations and contractual arrangements to which the process is subject, i.e., externally imposed business criteria as well as internal policies
7. **Reliability:** Relates to the provision of appropriate information for management to operate the organisation and exercise its fiduciary and governance responsibilities

The specific key quality requirements may vary for different organisations based on specific business needs.

1.2.3 Application controls objectives

COBIT provides best practices for application controls which can be used as a benchmark for implementing or evaluating application controls. The COBIT 4.1 control objectives and control practices provides the best collection of controls which are generic and can be customised and used as benchmark for implementation or used as assessment criteria for any application audit. COBIT defines six control objectives for application controls:

1. **Source Data Preparation and Authorisation:** Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Errors and omissions can be minimised through good input form design. Detect errors and irregularities so they can be reported and corrected.
 2. **Source Data Collection and Entry:** Ensure that data input is performed in a timely manner by authorised and qualified staff. Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.
-
1. **Accuracy, Completeness and Authenticity Checks:** Ensure that transactions are accurate, complete and valid. Validate data that were input, and edit or send back for correction as close to the point of origination as possible.
 2. **Processing Integrity and Validity:** Maintain the integrity and validity of data throughout the processing cycle. Detection of erroneous transactions does not disrupt the processing of valid transactions.
 3. **Output Review, Reconciliation and Error Handling:** Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient and protected during transmission; verification,

detection and correction of the accuracy of output occur; and information provided in the output is used.

4. **Transaction Authentication and Integrity:** Before passing transaction data between internal applications and business/operational functions (within or outside the enterprise), check the data for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport

1.2.4 Control practices

Illustrative control practices for the control objectives as per COBIT 4.1 are given below. Under each of the control objectives, there are list of control practices which need to be implemented to meet the control objectives. The control practices are to be customised and implemented as per specific requirements of the organisation. Once the control practices of specific control objective are implemented, then it can be said that the application meets the required control objectives.

1. Source Data Preparation and Authorisation

- i. Design source documents in a way that they increase accuracy with which data can be recorded, control the workflow and facilitate subsequent reference checking. Where appropriate, include completeness controls in the design of the source documents.
- ii. Create and document procedures for preparing source data entry, and ensure that they are effectively and properly communicated to appropriate and qualified personnel. These procedures should establish and communicate required authorisation levels (input, editing, authorising, accepting and rejecting source documents). The procedures should also identify the acceptable source media for each type of transaction.
- iii. Ensure that the function responsible for data entry maintains a list of authorised personnel, including their signatures.
- iv. Ensure that all source documents include standard components, contain proper documentation (e.g., timeliness, predetermined input codes, default values) and are authorised by management.
- v. Automatically assign a unique and sequential identifier (e.g., index, date and time) to every transaction.
- vi. Return documents that are not properly authorised or are incomplete to the submitting originators for correction, and log the fact that they have been returned. Review logs periodically to verify that corrected documents are returned by originators in a timely fashion, and to enable pattern analysis and root cause review.

2. Source data collection and entry

- i. Define and communicate criteria for timeliness, completeness and accuracy of source documents. Establish mechanisms to ensure that data input is performed in accordance with the timeliness, accuracy and completeness criteria.
- ii. Use only pre-numbered source documents for critical transactions. If proper sequence is a transaction requirement, identify and correct out-of-sequence source documents. If completeness is an application requirement, identify and account for missing source documents.
- iii. Define and communicate who can input, edit, authorise, accept and reject transactions, and override errors. Implement access controls and record supporting evidence to establish accountability in line with role and responsibility definitions.
- iv. Define procedures to correct errors, override errors and handle out-of-balance conditions, as well as to follow up, correct, approve and resubmit source documents and transactions in a timely manner. These procedures should consider things such as error message descriptions, override mechanisms and escalation levels.
- v. Generate error messages in a timely manner as close to the point of origin as possible. The transactions should not be processed unless errors are corrected or appropriately overridden or bypassed. Errors that cannot be corrected immediately should be logged in an automated suspense log, and valid transaction processing should continue. Error logs should be reviewed and acted upon within a specified and reasonable period of time.
- vi. Ensure that errors and out-of-balance reports are reviewed by appropriate personnel, followed up and corrected within a reasonable period of time, and, where necessary, incidents are raised for more senior-level attention. Automated monitoring tools should be used to identify, monitor and manage errors.
- vii. Ensure that source documents are safe-stored (either by the business or by IT) for a sufficient period of time in line with legal, regulatory or business requirements.

3. Accuracy, completeness and authenticity checks

- i. Ensure that transaction data are verified as close to the data entry point as possible and interactively during online sessions. Ensure that transaction data, whether people-generated, system-generated or interfaced inputs, are subject to a variety of controls to check for accuracy, completeness and validity. Wherever possible, do not stop transaction validation after the first error is found. Provide understandable error messages immediately to enable efficient remediation.
- ii. Implement controls to ensure accuracy, completeness, validity and compliance to regulatory requirements of data input. Controls may include sequence, limit, range, validity, reasonableness, table look-ups, existence, key verification, check digit, completeness (e.g., total monetary amount, total items, total documents, hash totals),

- duplicate and logical relationship checks, and time edits. Validation criteria and parameters should be subject to periodic reviews and confirmation.
- iii. Establish access control and role and responsibility mechanisms so that only authorised persons input, modify and authorise data.
 - iv. Define requirements for segregation of duties for entry, modification and authorisation of transaction data as well as for validation rules. Implement automated controls and role and responsibility requirements.
 - v. Report transactions failing validation and post them to a suspense file. Report all errors in a timely fashion and do not delay processing of valid transactions.
 - vi. Ensure that transactions failing edit and validation routines are subject to appropriate follow-up until errors are remediated. Ensure that information on processing failures is maintained to allow for root cause analysis and help adjust procedures and automated controls.

4. Processing integrity and validity

- i. Establish and implement mechanisms to authorise the initiation of transaction processing and to enforce that only appropriate and authorised applications and tools are used.
- ii. Routinely verify that processing is completely and accurately performed with automated controls, where appropriate. Controls may include checking for sequence and duplication errors, transaction/record counts, referential integrity checks, control and hash totals, range checks and buffer overflow.
- iii. Ensure that transactions failing validation routines are reported and posted to a suspense file. Where a file contains valid and invalid transactions, ensure that the processing of valid transactions is not delayed and all errors are reported in a timely fashion. Ensure that information on processing failures is kept to allow for root cause analysis and help adjust procedures and automated controls, to ensure early detection or prevent errors.
- iv. Ensure that transactions failing validation routines are subject to appropriate follow-up until errors are remediated or the transaction is cancelled.
- v. Ensure that the correct sequence of jobs has been documented and communicated to IT operations. Job output should include sufficient information regarding subsequent jobs to ensure that data are not inappropriately added, changed or lost during processing.
- vi. Verify the unique and sequential identifier to every transaction (e.g., index, date and time).
- vii. Maintain the audit trail of transactions processed. Include date and time of input and user identification for each online or batch transaction. For sensitive data, the listing should contain before and after images and should be checked by the business owner for accuracy and authorisation of changes made.
- viii. Maintain the integrity of data during unexpected interruptions in data processing with system and database utilities. Ensure that controls are in place to confirm data integrity after processing failures or after use of system or database utilities to resolve operational

problems. Any changes made should be reported and approved by the business owner before they are processed.

- ix. Ensure that adjustments, overrides and high-value transactions are reviewed promptly in detail for appropriateness by a supervisor who does not perform data entry.
- x. Reconcile file totals. For example, a parallel control file that records transaction counts or monetary value as data should be processed and then compared to master file data once transactions are posted. Identify report and act upon out-of-balance conditions.

5. Output review, reconciliation and error handling

- i. When handling and retaining output from IT applications, follow defined procedures and consider privacy and security requirements. Define, communicate and follow procedures for the distribution of output.
- ii. At appropriate intervals, take a physical inventory of all sensitive output, such as negotiable instruments, and compare it with inventory records. Create procedures with audit trails to account for all exceptions and rejections of sensitive output documents.
- iii. Match control totals in the header and/or trailer records of the output to balance with the control totals produced by the system at data entry to ensure completeness and accuracy of processing. If out-of-balance control totals exist, report them to the appropriate level of management.
- iv. Validate completeness and accuracy of processing before other operations are performed. If electronic output is reused, ensure that validation has occurred prior to subsequent uses.
- v. Define and implement procedures to ensure that the business owners review the final output for reasonableness, accuracy and completeness, and output is handled in line with the applicable confidentiality classification. Report potential errors; log them in an automated, centralised logging facility; and address errors in a timely manner.
- vi. If the application produces sensitive output, define who can receive it, label the output so it is recognisable by people and machines, and implement distribution accordingly. Where necessary, send it to special access-controlled output devices.

6. Transaction authentication and integrity

- i. Where transactions are exchanged electronically, establish an agreed-upon standard of communication and mechanisms necessary for mutual authentication, including how transactions will be represented, the responsibilities of both parties and how exception conditions will be handled.
- ii. Tag output from transaction processing applications in accordance with industry standards to facilitate counterparty authentication, provide evidence of non-repudiation and allow for content integrity verification upon receipt by the downstream application.

- iii. Analyse input received from other transaction processing applications to determine authenticity of origin and the maintenance of the integrity of content during transmission.

APPLICATION AND CONTROL OBJECTIVES AND INFORMATION CRITERIA		Information Criteria						
		Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Control Objective	1	S	P	S	P		S	
	2	S	S	S	P		S	
	3	S	P	S	P	S	P	P
	4			P	P	P	P	P
	5	P	S	P	P	P	P	P
	6		S	P	P		P	
P = Primary S = Secondary								

Table to the relationship between the information criteria and how achievement of those criteria can be enabled by various application control objectives. Primary and secondary are the relative importance of the information criteria.

PART 2: APPLICATION CONTROLS REVIEW

An IS auditor has to be aware of the controls that have been put in place in business applications. He / She may have to review the same as a part of auditor's risk assessment procedure. As per SA 200 on "Overall Objectives of the Independent Auditor and the conduct of an audit in accordance with standards on Auditing", compliance procedures are tests designed to obtain reasonable assurance that those internal controls on which audit reliance is to be placed are in effect. As per ISACA ITAF 100 1 "Assertions", IS Audit and assurance professional shall review the assertions against 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.

2.1 Review of application control various business application

2.1.1 Need for application control review

The review is necessary for auditor to draw the following conclusion:

- a. How much reliance he/she can put on entities business application system?
- b. IS Auditor also is also to plan his/her other audit procedures.
- c. In case application controls are found in-effective to achieve the stated business objectives, than IS Auditor need to plan for alternate audit procedure?

2.1.2 How to perform application review?

AS per ISACA ITAF 1205 "Evidences", IS Auditor has to select most appropriate procedure to gather evidence depending on the subject matter being audited: The procedures used to obtain evidence include:

1. Inquiry and confirmation
2. Re-performance
3. Recalculation
4. Computation
5. Analytical Procedures
6. Inspection
7. Observation
8. Other Generally Accepted Methods

2.2 Review of business application controls through use of audit procedures

AS per SA 500, "Audit Evidences", auditor while designing tests of controls shall see whether the controls so put in place are effective.

- a. **Inquiry and confirmation:** IS Auditor may prepare a checklist to enquire and confirm whether the said controls are in place. This process shall evaluate **existence of controls**. A sample checklist for IS Auditor included at end of chapter.
- b. **Re-performance:** IS Auditor may process test data on application controls to see how it responds. This process shall evaluate the **effectiveness of controls**.

2.3 Application controls review for specialised system

Changes in technology are very fast. A separate section for these systems has been incorporated to help IS Auditor put a focused approach to audit of these system.

2.3.1 Artificial Intelligence (AI)

A computer is an electromechanical machine that contains no live elements. However, it is used for simulating human working which involves thinking and reasoning, solving simple and complex problems, calculating, etc. Computer history shows that computers are good at making calculations of repetitive nature speedily. In fact, in the beginning, computers were used mainly for this purpose. The applications of AI can be classified into three major categories:

- i. **Cognitive Science:** This is an area based on research in disciplines such as biology, neurology, psychology, mathematics and allied disciplines. It focuses on how human brain works and how humans think and learn. Applications of AI in the cognitive science are Expert Systems, Learning Systems, Neural Networks, Intelligent Agents and Fuzzy Logic
- ii. **Robotics:** This technology produces robot machines with computer intelligence and human-like physical capabilities. This area includes applications that give robots visual perception, capabilities to feel by touch, dexterity and locomotion.
- iii. **Natural Languages.**

Being able to 'converse' with computers in human languages is the goal of research in this area. Interactive voice response and natural programming languages, closer to human conversation, are some of the applications. Virtual reality is another important application that can be classified under natural interfaces.

IS Auditor's Role

IS auditor has to be conversant with the controls relevant to these systems when used as the integral part of the organizations business process or critical functions and the level of experience or intelligence used as a basis for developing software. The errors produced by such systems would be more critical as compared to the errors produced by the traditional system.

2.3.2 Data Warehouse

Data ware house is defined, "as a Subject-oriented, integrated, time-variant, non-volatile, collection of data in support of management's decision making process. It is a Central Repository of clean, consistent, integrated & summarized information, extracted from multiple operational systems, for on-line query processing."

Data warehousing system is used for getting valuable information for making management decisions. Generally, data is processed by TPS (Transaction Processing System), also known as operational systems. These systems are responsible for day-to-day functioning of business transactions.

Customers depositing and withdrawing money, applying for loans, opening accounts in a bank are examples of Transactions Processing System. The data associated with these transactions is stored in database management system and presented to users or programs whenever required. These systems process data either in a batch mode or in a real-time manner (e.g., when we book a railway seat we are presented with a ticket immediately).

IS Auditor's Role

IS Auditor should consider the following while auditing data warehouse:

1. Credibility of the source data
2. Accuracy of the source data
3. Complexity of the source data structure
4. Accuracy of extraction and transformation process
5. Access control rules
6. Network capacity for speedy access

2.3.3 Decision Support System (DSS)

DSS are information systems that provide interactive information support to managers with analytical models. DSS are designed to be ad hoc systems for specific decisions by individual-managers. These systems answer queries that are not answered by the transactions processing systems. Typical examples are:

1. Comparative sales figures between two consecutive months for different products with percentage variation to total sales.
2. Revenue and Cost projections on the basis of a product mix.
3. Evaluation of different alternatives, leading to the selection of the best one.

IS Auditor's role

As the system shall be used for decision making purpose of the management,

1. Credibility of the source data
2. Accuracy of the source data
3. Accuracy of extraction and transformation process
4. Accuracy and correctness of the output generated
5. Access control rules

2.3.4 Electronic Fund Transfer (EFT)

The electronic mode of payment which has made a lot of impact to the way India does business. All big, medium and small businesses, banks, user's, governments, government departments, logistics, customers, service receivers, service providers, exporters, importers, sellers, buyers, use EFT for their business and personal transaction. LIFE without EFT seems impossible. Immense growth of EFT has led to a new set of risk associated with such transactions. Reserve Bank of India (RBI) has issued detailed guidelines for banks to follow for EFT transactions. RBI has specified in its NEFT guidelines that, Banks need to create procedural guidelines, for the purpose of:

- i. Verifying that a payment instruction, a communication authorising a payment instruction or an NEFT Data File is authorised by the person from whom it purports to be authorised; and
- ii. For detecting error in the transmission or the content of a payment instruction, a communication or an NEFT SFMS message.

IS Auditor's role

The major concern shall be:

1. Authorisation of payment.
2. Validation of receivers details, for correctness and completeness.
3. Verifying the payment made.
4. Getting acknowledgement from the receiver, or alternatively from bank about the payment made.
5. Checking whether the obligation against which the payment was made has been fulfilled.

2.3.5 E-commerce

Other than buying and selling goods on the Internet, E Commerce (Electronic Commerce) involves information sharing, payment, fulfilment and service and support.

Risks of E-commerce

1. Confidentiality of message
2. Id of organisation of the sender
3. Integrity of the message
4. Non Acceptance of confidentiality by receiver
5. Non Repudiation by sender of having sent the message

IS Auditor's role

IS Auditor's responsibility shall be to see whether the transactions have:

1. Authorisation
2. Authentication
3. Confirmation

2.3.6 Point of Sale System (PoS)

As the name indicates, a PoS is intended to capture data at the time and place of transaction which is being initiated by a business user. It is often attached to scanners to read bar codes and magnetic cards for credit card payment and electronic sales. They provide significant cost and time saving as compared to the manual methods. They also eliminate errors that are inherent in manual system (when a user is subjected to make transcription error while entering data from a document into system). POS may involve batch processing or online processing. These are generally observed in the case of big shopping malls or departmental shops.

IS Auditor's role

1. In case there is batch processing, the IS auditor should evaluate the batch controls implemented by the organization.
2. Check if they are in operation,
3. Review exceptional transaction logs.
4. Whether the internal control system is sufficient to ensure the accuracy and completeness of the transaction batch before updating?
5. The relevance of controls is more In the case of online updating system, the IS auditor will have to evaluate the controls for accuracy and completeness of transactions.

6. RBI guidelines regarding “Cash withdrawal at Point of Sale (POS) - Prepaid Payment Instruments issued by banks: need to be validated in case such transactions are taking place.

2.3.7 Automatic Teller Machines (ATM)

An ATM (Automated Teller Machine) is a specialized form of the point of sale terminal. It is designed for unattended use by a customer of a financial institution. The ATMs generally allow cash deposits, cash withdrawals and a range of banking operations like requesting cheque books or account statements. ATMs are generally used for use after the closing hours of the financial institution and can be located either adjacent to the location of the financial institution or at a distant place. The facility of ATM can be within a bank, across local banks and amongst the banks outside a region. ATMs transfer information and money over communication lines. These systems provide a high level of logical and physical security for both the customer and the ATM machine.

IS Auditor's Role

The following are the guidelines for internal controls of ATM system which the auditor shall have to evaluate and report:

- a. Only authorized individuals have been granted access to the system.
- b. The exception reports show all attempts to exceed the limits and reports are reviewed by the management.
- c. The bank has ATM liability coverage for onsite and offsite machines
- d. Controls on proper storage of unused ATM cards, Controls on their issue only against valid application form from a customer, Control over custody of unissued ATM cards, Return of old/ unclaimed ATM cards, Control over activation of PINs
- e. Controls on unused PINs, Procedure for issue of PINs, Return of PINs of returned ATM cards.
- f. Controls to ensure that PINs do not appear in printed form with the customer's account number.
- g. Access control over retrieval or display of PINs via terminals
- h. Mail cards to customers in envelopes with a return address that do not identify the Bank. Mail cards and PINs separately with sufficient period of time (usually three days) between mailings.

As on date, there are more than 1,50,000 ATM machines installations in India. Government of India has already indicated that it wants to further enhance the usage of ATM in India, as this allows bank to reach remote corners without being physically present. This creates a scope to the IS Auditor for a separate ATM Audit. RBI has issued detailed set of instructions for bank to follow. Based on those a separate ATM audit program and checklist is being attached. Please see Appendix: Checklist for ATM audit to understand different areas of an ATM audit.

PART 3: CASES OF APPLICATION CONTROLS

3.1 Proper design of source document

Case of an educational/vocational institute collecting fees from students

Issue: Improper designed source document led to improper accounting.

Impact: A senior faculty left the Institute as incentives / payoffs were not calculated properly by accounts department.

Facts: The vocational institute was being run a PE Pvt. Ltd. (Referred to as PE). PE is engaged in educating CA / CS / CWA students. PE has implemented its fees collection on TALLY. Students while paying the fees were supposed to fill a **pay-in slip** and deposit the fees at the counter. Faculty payoffs are based on fees collected for the subject.

Receipt No. 1111					
Cash /		Cheque Details		Cash details	
Cheque	Date	Name of		1000X	
Name of		Bank		500X	
student		Ch. Number			
Level: Tick	CPT/ FOUNDATION/ IPCC/ FINAL/	Date		100X	
SUBJECT:	EXECUTIVE / PROFESSIONAL			50X	
				20X	
				10X	
				Total	
Student signature		Receiver Signature			

Based on the slip filled above, the cashier used to enter data in TALLY.

Problem: It was found, that one of the subjects in CA and CS has same name Direct Tax Law (DTL). Many students who paid fees for CA DTL got accounted in CS DTL. The result was that at the end of period when all payoffs were cleared TALLY data was used and calculations done.

The fees paid by many CA students were credited of CS students. This resulted in payment dispute and CA Final faculty for PE left the institute in a grudge. The faculty was a respected person; this affected reputation of the Institute.

Action taken: PE management was worried about the development and sought help from an IS Auditor. IS Auditor's mandate was to look for problem and provide a solution.

IS Auditor's Report:

The IS auditor went through the whole fees collection process, the people involved and the present problem. He/she gave a two-step solution to organisation.

First Step: Modify **pay-in-slip**, to include the stream (CA/CS/CWA) as another field.

Second Step: Appoint an Internal Auditor to check whether the payments of fees made by the students have been properly accounted.

Suggested Pay-in-Slip

Receipt No. 1111					
Cash / Cheque		Date		Cheque Details	Cash details
Name of student				Name of	
Stream:	CA / CS /			Bank	1000X
Tick	ICWA			Ch. Number	500X
Level: Tick	CPT/ FOUNDATION/ IPCC/ FINAL/ EXECUTIVE / PROFESSIONAL			Date	100X
SUBJECT:					50X
					20X
					10X
					Total
Student signature		Receiver Signature			

Benefit to PE:

1. A big problem was set right with a simple solution i.e. **proper design of source document.**
2. PE was relieved that such issues won't recur.
3. An Internal Auditor was also appointed to re-check the daily entries made.

3.2 Exception reporting

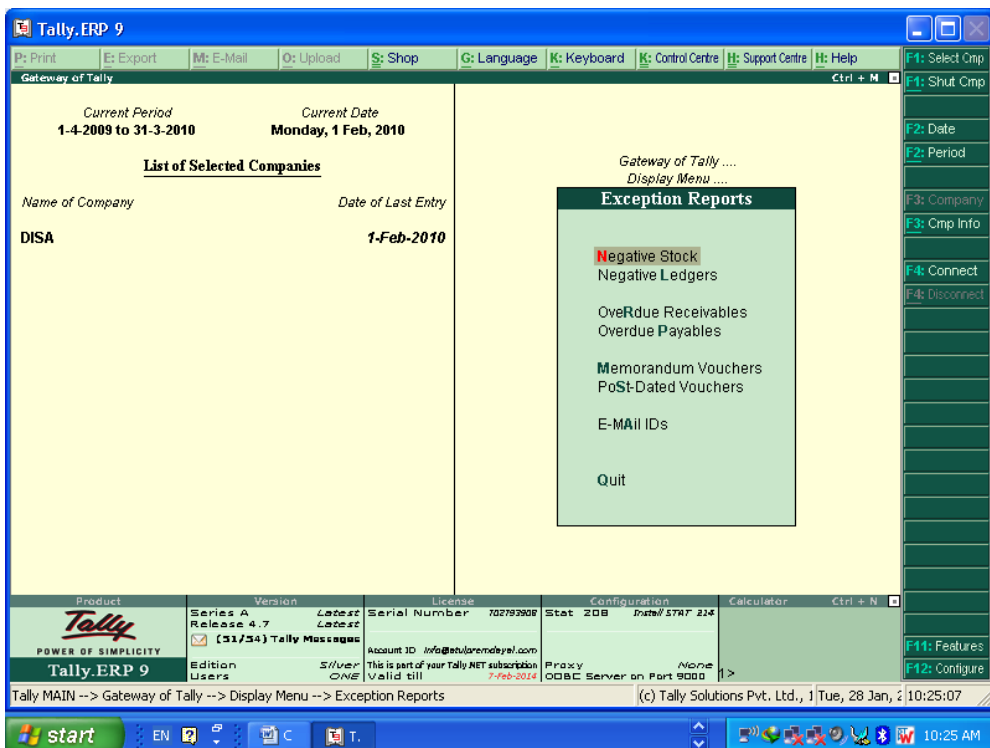
These are special reports generated by business application to highlight issues / items which are not the correct domain. For example: Exception reporting in TALLY:

How to generate the report? The command on GATEWAY OF TALLY: **DISPLAY AND EXCEPTION REPORTS**:

What items are displayed? The screen shot lists items that are reported as exception in TALLY. These include

- Negative Stock
- Negative Ledger and more.

What is the meaning of negative ledger? The word negative ledger means that the ledger account is not its correct **domain**. Correct domain means, for example the domain for **CASH** is **debit**, but if it is **credit**, the system shall show it as **negative ledger**. The same is true for a debtor's ledger with **credit balance** or creditor's ledger with **debit** balance.



What is the benefit?

Users, which include management, auditor's, IS Auditors can directly generate these reports and check as to accuracy of accounting.

What is the loss if above items are not checked?

a. Section 69C of Income Tax Act, 1961: Unexplained expenditure, etc.:

Where in any financial year an Assessee has incurred any expenditure and he offers no explanation about the source of such expenditure or part thereof, or the explanation, if any, offered by him is not, in the opinion of the Assessing Officer, satisfactory, the amount covered by such expenditure or part thereof, as the case may be, may be deemed to be the income of the Assessee for such financial year. **Above negative balance can be treated as Income.**

b. It reflects poor accounting controls, and can lead to losses due to frauds.

Exercise: Kindly comment upon: Q.1 The type of error?

- a. Input
- b. Process
- c. Output
- d. None of Above

Q.2. What is a better solution possible to the above problem?

2. Exception reporting in bank:

Case for participants:

DISA participants are expected to comment on one of the items reported in bank's daily exception reports.

3.3 Case for Dependency check:

Case of validating two related field of employee database

Facts: A company is held guilty of employing underage employees. The authorities send a notice to the company. The notice is based on data submitted by the company as a part of its annual return under labour laws.

The notice states that as per details made available by the company 10 employees have been found to be underage as the time difference between date of birth and date of employment is less than **18 years**. Company responds by saying that it is basically a data entry problem in system from where the said return has been made. The company has to physically parade the 10 employees to the department to convince them that they are not underage.

Action Taken: After so much of embarrassment company decides to appoint an IS Auditor to find the problem and solution.

Tally.ERP 9

Employee Display

Category : **Primary Cost Category**

Name : **ABC**

Display Name in Reports : **ABC**

Under : **Primary**

Date of Joining : **1-Apr-2012**

Define Salary Details : **No**

Date of Resignation / Retirement :

General Info		Payment Details	
Employee Number	:	Bank Name	:
Designation	:	Branch	:
Function	:	Bank A/c Number	:
Location	:	IFS Code	:
Gender	: Female	MICR Code Number	:
Date of Birth	: 1-Apr-2000		
Blood Group	: O Positive		
Father / Mother Name	:		
Spouse Name	:		
Address	:		
Contact Numbers	:		
E-Mail ID	:		

Quit Accept Delete

56/59 Tally Messages

Tally MAIN --> Gateway of Tally --> Payroll Info. --> Employees --> Employee Display

(c) Tally Solutions Pvt. Ltd., 1 Tue, 28 Jan, 2 10:39:52

start EN C T. S.

10:39 AM

Report of IS Auditor:

After studying the system and the problem faced IS auditor suggested the following:

1. System needs to be updated / modified so that it does not allow underage employee updates.
2. An internal system to validate each new addition to employee payroll.

Exercise:

Q.1 the best way to define the error is:

- a. Input error
- b. Process error
- c. Output error
- d. Design error

3.4 Reasonableness Check

Case of Purchase Order in excess of five times vendor's annual sale

Facts: The Company is engaged in manufacturing tyres. While issuing purchase order (PO) to a vendor, the clerk put 100 kgs as quantity instead of 1 kg. The result was that the PO to be made for Rs.2/- lacs was actually made for Rs.200/- lacs i.e. **100 times more**. The same PO was signed by Purchase Manager and delivered to vendor by post. Looking at the PO vendor called back the company and informed that the PO is **more than 5 times annual turnover of vendor himself**.

Errors:

1. **Lack of reasonableness check:** The system must have been created to ensure that such a PO must not be released. It could be having a check on say:
 - a. Maximum quantity that could be entered for purchase, or
 - b. Maximum value a PO could be made.
 - c. Maximum quantity PO that could be sent to a vendor, or
 - d. A better definition by management.
2. Purchase Manager's poor work.
3. No cross check system built in.

Exercise:

Q.1 Reasonableness verification control is a control at which part of application process?

- a. Input
- b. Process
- c. Output
- d. None of above

3.5 Case to highlight necessity of duplicate check

Case of double payment made to vendors against one purchase invoice.

Facts: A company using local made accounting software. While entering transactions, the software allowed user's to create new ledgers by a command ALT+N. The system being used check duplicate ledgers for 100% same name. Any alteration in name or change in case was not tracked. While entering a purchase invoice the data entry operator created a new ledger without checking the existence of previous ledger. Later on it was found that a double payment was made to the vendor as the said purchase was against an advance payment and another payment was released based on new entry.

Errors:

1. Lack of user controls. Data entry operator can create ledger.
2. Lack of **duplicate check**.
3. Lack of internal controls, to see how duplicate entries are in system.

Exercise: Q.1 What is the best solution to the problem?

3.6 Obsolete stock reporting

In TALLY from gateway of tally through the following set of commands company can get report on non-moving / obsolete stock.

Gateway of TALLY: Press **Display**> Press **Inventory books**> Press **Ageing Analysis**: This shall show the following report:

Particulars	Total	<= 45 days	45 to 90 days	90 to 180 days	>= 180 days
	Quantity	Quantity	Quantity	Quantity	Quantity
Cotton					1 more ...
WAX	99,000 Nos.		89 Nos.		98,911 Nos.
Grand Total			89 Nos.		98,911 Nos.

How does the report help?

1. Helps assess the quality of inventory.
2. Basis for valuation of inventory, as non-moving / obsolete stock may be valued at net realizable value.

3.7 Report on Sales below cost price

From GATEWAY OF TALLY following command shall provide the above mentioned report:

- Gateway of TALLY: **Display>Inventory Books>Stock Item**: Then select the item from list and press **F7**, which shows the profit/ loss on items sold. Above details can also be seen through
- Gateway of TALLY: **Display>Account Books>Sales Register**: Then select the month for which sales need to be displayed and press **F7**, which shows the profit/ loss on items sold.

Benefits of the report:

- Management tool for performance analysis.
- Any fraud done can be checked through the same.

3.8 Report on TDS deducted but not remitted in time

Gateway of TALLY: **Display>Statutory Report>TDS Report>Outstandings>TDS Payables**: The following report is displayed:

Tally.ERP 9

P: Print

E: Export

M: E-Mail

O: Upload

S: Shop

G: Language

K: Keyboard

K: Control Centre

H: Support Centre

H: Help

TDS Outstanding

DISA

Ctrl + N

TDS Payable

For 1-Apr-2013

Date	Ref. No.	Nature of Payment	Opening Amount	Due on	Overdue days
1-Apr-2013	Jrnl / 2-1	Payments to Contractors (Other Than Advertisement)	750.00 Cr	7-May-2013	0
			750.00 Cr		

Q: Quit

R: Remove Line

U: Restore Line

U: Restore All

Space: Set

Ctrl + N

56/59 Tally Message

Tally MAIN --> Gateway of Tally --> Display Menu --> Statutory Reports --> TDS Reports --> Outstanding (c) Tally Solutions Pvt. Ltd., 1 Tue, 28 Jan, 13:02:32

F1: Detailed

F2: Period

F3: Company

F6: Age wise

F7: Deductee Type

F8: Other Rep

F9: Inv Rep

F10: Acc Rep

F11: Features

F12: Configure

F12: Range

F12: Value

Benefits of the report:

- Management tool for performance analysis.
- Timely compliance can be ensured.

3.9 Questions

1. Application controls shall include all **except**

- A. Application controls are a subset of internal controls.
- B. The purpose is to collect timely, accurate and reliable information.
- C. It is part of the IS Auditor's responsibility to implement the same.
- D. It is part of business application software.

2. As per Income Tax Act, 1961 and banking norms, all fixed deposit holders of bank need to submit their PAN or form 60/61(a form as per Income Tax Act/Rules). Bank in its account opening form, has not updated the need for form 60/61 in case PAN is not there. This defines which control lapse as per COBIT.

- A. Source Data Preparation and Authorisation:
- B. Source Data Collection and Entry
- C. Accuracy, Completeness and Authenticity Checks
- D. Processing Integrity and Validity

3. In a public sector bank while updating master data for advances given, the bank employee does not update "INSURANCE DATA". This includes details of Insurance Policy, Amount Insured, Expiry Date of Insurance and other related information. This defines which control lapse as per COBIT.

- A. Source Data Preparation and Authorisation:
- B. Source Data Collection and Entry
- C. Accuracy, Completeness and Authenticity Checks
- D. Processing Integrity and Validity

4. Emailed purchase order for 500 units was received as 5000 units.

This defines which control lapse as per COBIT.

- A. Source Data Collection and Entry
- B. Accuracy, Completeness and Authenticity Checks
- C. Output Review, Reconciliation and Error Handling
- D. Transaction Authentication and Integrity

5. An IS Auditor, processes a dummy transaction to check whether the system is allowing cash payments in excess of Rs.20,000/-. This check by auditor represents which of the following evidence collection technique?

- A. Inquiry and confirmation
- B. Re-calculation

Module 6

- C. Inspection
- D. Re-performance

6. While auditing e-commerce transactions, auditor's key concern includes all except:

- A. Authorisation
- B. Authentication
- C. Author
- D. Confirmation

7. RBI instructed banks to stop cash retraction in all ATMs across India from April 1, 013. This was result of few ATM frauds detected. This action by RBI can be best classified as:

- A. Creation
- B. Rectification
- C. Repair
- D. None of above

8. Non – repudiation relates to all terms except one:

- A. Right to deny withdrawn.
- B. Digital Signatures.
- C. E-commerce
- D. None of above

9. Company's billing system does not allow billing to those dealers who have not paid advance amount against proforma invoice. This check is best called as:

- A. Limit Check
- B. Dependency Check
- C. Range Check
- D. Duplicate Check

10. While posting message on FACEBOOK, if user posts the same message again, FACEBOOK gives a warning. The warning indicates which control.

- A. Limit Check
- B. Dependency Check
- C. Range Check
- D. Duplicate Check

3.10 Answers and Explanations

1. C. Represents what auditor's verifies but not that what he/she implements. Rest is part of definition and purpose of application controls.
2. A. is the correct answer as the source data capture is not proper. Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Errors and omissions can be minimised through good input form design.
3. C. This ensures that transactions are accurate, complete and valid. Validate data that were input, and edit or send back for correction as close to the point of origination as possible.
4. D. is the correct answer. As per COBIT, where transactions are exchanged electronically, establish an agreed-upon standard of communication and mechanisms necessary for mutual authentication, including how transactions will be represented, the responsibilities of both parties and how exception conditions will be handled.
5. D. IS Auditor may process test data on application controls to see how it responds.
6. C. Is correct. Others are key concerns of an IS auditor while auditing e-commerce transactions.
7. B. is the right answer. A, is not an answer as action by RBI is based on fraud detection. Repair is done to rectify an error which has occurred in a working system.
8. D. is the correct answer. The other options are related to non-repudiation. A, is definition of word. B, digital signatures create non-repudiation. E-commerce transactions need it (non-repudiation) for execution of contract.
9. B. Dependency check is one where value of one field is related to that of another.
10. D. is the answer as this is a duplicate check.

CHAPTER 3: AUDITING APPLICATION CONTROL

PART 1: AUDIT PROGRAM FOR REVIEW OF APPLICATION SOFTWARE

Learning Objectives

To provide assurance on business application software and the controls put in place, through business application audit.

1.1 Introduction

The role of information System audit has become a critical mechanism for ensuring the integrity of information and the reporting of organization finances to avoid and hopefully prevent future financial fiascos such as Satyam in recent years. Electronic infrastructure and commerce are integrated in business process around the globe. There is a need to control and audit using IS to avoid such kind of scam in near future. Today the business processes are tightly integrated to systems. In few organisations the level of integration is that when systems are **off** business is **off**. In such a scenario it is important to ensure that systems are working properly and nothing is there to affect the working of system. The way businesses are integrated to system, any audit shall be preceded by **system audit**, as proper working of system is necessary to proper working of business. It shall be great risk being taken by a pure financial auditor to submit his/her report without going through the system audit report of the organisation for which financial audit is being done.

1.2 Why IS Audit?

Case to highlight “NPA provisioning in system may be wrong

Issue: NPA provisioning as per RBI guidelines.

Objective: To learn that system audit as an exercise needs to precede financial audit.

Location: Public Sector Bank using a CBS.

Reference: RBI guidelines for **Income Recognition and Asset Classification**.

[RBI/2013-14/62:DBOD.NO.BP.BC.1/21.01.048/2013-14/1. 013]

Specific Point: Provision to be made for sub-standard assets, where the advance as per nature is unsecured. The guidelines state that a provision of @25% has to be made of total out-standing. This is an exception to general rule of provision @15%. The exception is created as the advance

is basically **unsecured in nature**. For example: Credit Card o/s turning sub-standard. This advance is **unsecured in nature**.

Point to remember: The provision is on total o/s, not on the amount of outstanding. As the advance is an **unsecured advance**.

Auditor observation:

Auditor observed that for **credit card outstanding of Rs.1, 00,000/-** the branch had made a provision @15% of out-standing amount, as reflected from system generated Non-Performing-Asset statement. The issue was brought to notice of branch manager. The interaction between the bank employees and the action taken by auditor is shown in the matrix below.

Sl. No.	Query Made to and nature of query.	Response from person at bank	Auditor Action
1	Branch Manager (BM): The provision is not as per RBI guideline.	BM: The bank supplied data to regional office. The calculations have been made the regional office. No fault of branch.	Take to next level
2	Regional Manager (RM): The provision is not as per RBI guideline.	RM: The regional office only fed data in the software supplied by HO . No fault of regional office.	Take to next level.
3	Assistant General Manager (IT) of the bank: AGM (IT): The provision is not as per RBI guideline.	AGM (IT): Accepts the problem in software.	Qualify the main report.

Learning from the above:

1. **For Bank:** Above means that if the banks unsecured sub-standard advances are to the tune of Rs.10/- crore, bank shall be **making short provision of Rs.1/- crore against its NPA's**.

2. **For Auditor:**

a. Branch auditor had to qualify the main audit report.

b. Branch auditor would be within his/her right's to ask bank to supply the **system audit report** of the software being used by the bank for calculating the NPA status and provisions thereon.

3. For us: Case helps us understand that **IS Audit is necessary** in today's business environment as business processes have been integrated into system and lot of decision is being taken through these integrated system.

IS auditing is an integral part of the audit function because it supports the auditor's judgment on the quality of the information processed by computer systems. Initially, auditor with IT audit skills are viewed as the technological resource for the audit staff. The IS auditor's role has evolved to provide assurance that adequate and appropriate controls are in place. The audit's primary role, except in areas of management advisory services, is to provide a statement of assurance as to whether adequate and reliable internal controls are in place and are operating in an efficient and effective manner. Therefore, whereas the management is to ensure, auditors are to assure.

1.3 What is IS Audit?

An information technology audit, or information systems audit, is an examination of the controls within an Information technology (IT) infrastructure. An IS audit is the process of collecting and evaluating the evidence of an organization's information systems, practices, and operations. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively and efficiently 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.

The IT audit's agenda may be summarized by the following questions:

1. Will the organization's computer systems be available for the business at all times when required? (Availability)
2. Will the information in the systems be disclosed only to authorized users? (Confidentiality)
3. Will the information provided by the system always be accurate, reliable, and Timely? (Integrity)

The IS audit focuses on determining the risks that are relevant to information assets, and in assessing controls in order to reduce or mitigate these risks. By implementing controls, the effect of risks can be minimized, but cannot completely eliminate all risks.

As per ISACA ITAF 1007 "Assertions", IS Audit and Assurance professional 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.

Information Systems Audit is often misunderstood as a mere technical audit and a domain of Information Technology professionals. On the contrary, Information Systems 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 information systems audits. Therefore, depending on the audit environment, objectives and scope, the audit

could involve the audit of entire business processes, partially or fully automated, or audit of specified application, technology and related controls.

1.4 How to perform IS Audit?

The fundamental principles of audit do not change with change in the audit subject, however, the perspective of audit and the methods, tools and techniques to achieve the audit objectives do undergo a change. As in a financial audit, audit focus is on the risk arising from inadequate or inefficient controls on recording of transactions which could result in misstatement of financial statements. In an Information Systems Audit the focus is on the risks arising from the use of information technology in carrying out business processes.

ISACA ITAF 1008 “Criteria”, specifies that IS Audit assurance criteria should consider the source for which the IS Audit is being done and the potential audience. For example, when dealing with government regulations criteria based on assertions developed from legislation and regulations shall apply to the subject matter may be most appropriate. Sources of criteria may be:

1. Established by ISACA: These are publicly available criteria.
2. Those established by other expert bodies: Like those created by SYSTRUST certification body.
3. Established by laws and regulations: For example the one discussed in case above relating to RBI guidelines.
4. Developed specifically for IS Audit or Assurance engagement.

Above shall help decide on the key objective for an IS Audit.

Audit Objective: The entire audit program and methodology depends upon the audit objective and scope. The objective of the IS audit is to evaluate an auditee's computerized information system(CIS) in order to ascertain whether the CIS produces timely, accurate, complete and reliable information outputs as well as ensuring confidentiality, integrity, availability and reliability of the data.

1.5 Audit mission

Establishing an IS audit function may be critical in organisations that are specifically dependent on Information Technology. The IS audit function could be established either within the organisation as an internal department or the function could be fully or partly outsourced to an external agency. In either case there are certain fundamental principles that should be taken into consideration. The mission statement defines the primary purpose of the audit function and provides an overview of the focus, priorities, values and principles that will measure audit decisions. It also outlines the value addition that will be provided and clarifies the purpose and meaning for the audit function. IS audit function reviews the reliability and integrity of information, compliance with the policies and regulations, and the processes for safeguarding of assets, as well as to make suggestions for

improvements in operating efficiencies and internal controls? 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. The audit mission statement may vary between various organisations and audit functions.

1.6 Performing an IS Audit

The detailed concepts and practice of IS Audit are covered in detail in Module 3: IS Assurance services. However, some of the key concepts and practice are summarised here in the context of application audit. The standards of IS Audit provided by ISACA in ITAF 1200 on performance standards outlines the following steps for performing an IS audit as under:

- i. **Engagement Planning:** This includes conclusions on 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.
- ii. **Risk Assessment in Planning:** 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. IS audit and assurance professionals shall identify and assess risk relevant to the area under review, when planning individual engagements. IS audit and assurance professionals shall consider subject matter risk, audit risk and related exposure to the enterprise.
- iii. **Performance and Supervision:** IS audit and assurance professionals shall conduct the work in accordance with the approved IS audit plan to cover identified risk and within the agreed-on schedule. IS audit and assurance professionals shall provide supervision to IS audit staff for whom they have supervisory responsibility, to accomplish audit objectives and meet applicable professional audit standards. IS audit and assurance professionals shall accept only tasks that are within their knowledge and skills or for which they have a reasonable expectation of either acquiring the skills during the engagement or achieving the task under supervision. IS audit and assurance professionals shall obtain sufficient and appropriate evidence to achieve the audit objectives. The audit findings and conclusions shall be supported by appropriate analysis and interpretation of this evidence. IS audit and assurance professionals shall document the audit process, describing the audit work and the audit evidence that supports findings and conclusions. IS audit and assurance professionals shall identify and conclude on findings.
- iv. **Materiality:** 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.
IS audit and assurance professionals shall consider materiality and its relationship to audit risk while determining the nature, timing and extent of audit procedures. 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.

- v. **Evidence:** IS audit and assurance professionals shall obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the engagement results. IS audit and assurance professionals shall evaluate the sufficiency of evidence obtained to support conclusions and achieve engagement objectives.
- vi. **Using the Work of Other Experts:** IS audit and assurance professionals shall consider using the work of other experts for the engagement, where appropriate. 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. 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.
- vii. **Irregularity and Illegal Acts:** IS audit and assurance professionals shall consider the risk of irregularities and illegal acts during the engagement. IS audit and assurance professionals shall maintain an attitude of professional scepticism during the engagement. IS audit and assurance professionals shall document and communicate any material irregularities or illegal act to the appropriate party in a timely manner.

1.7 Steps of IS Audit

Gather Information and Plan	
• Knowledge of business and industry • Prior year's audit results • Recent financial information	• Regulatory statutes • Inherent risk assessments
Obtain Understanding of Internal Control	
• Control environment • Control procedures • Detection risk assessment	• Control risk assessment • Equate total risk
Perform Compliance Tests	
• Identify key controls to be tested.	• Perform tests on reliability, risk prevention and adherence to organization
Perform Substantive Tests	

• Analytical procedures • Detailed tests of account	• Other substantive audit procedures
Conclude the Audit	
• Create recommendations.	• Write audit report.

1.8 Audit program for key business application

Detailed checklist for auditing business application software is given in appendix 3.

1.9 Computer Assisted Audit Techniques

CAAT is a significant tool for auditors to gather evidences independently. It provides a mean to gain access and to analyse data for a predetermined audit objective, and report the audit findings with evidences. It helps the auditor to obtain evidence directly on the quality of records produced and maintained in the system. The quality of the evidence collected gives reassurance on the quality of the system processing such transactional evidences.

1.9.1 Needs for CAAT

During the course of the audit an IS auditor should obtain sufficient, relevant and useful evidence to effectively achieve the audit objectives. The audit findings and conclusions have to be supported by appropriate analysis and interpretation of this evidence. Computerised information processing environments pose a challenge to the IS auditor to collect sufficient, relevant and useful evidence, since the evidence exists on magnetic media and can be examined only by using CAATs. With systems having different hardware and software environments, different data structure, record formats, processing functions, etc., it is almost impossible for the auditors to collect evidence and analyse the records without a software tool. Owing to resource constraints and the ever changing audit objectives, it is almost impossible to quickly develop audit capabilities, without using audit software like CAATs.

The ICAI Guidance note on CAAT describes CAATs as important tools for the auditor in performing audits. CAATs may be used in performing various auditing procedures including the following:

- Tests of details of transactions and balances, for example, the use of audit software for recalculated interest or the extraction of invoices over a certain value from the computer records.
- Analytical procedures, for example, identifying inconsistencies or significant fluctuations.
- Tests of general controls, for example testing the setup or configurations of the operating system or access procedures to the program libraries or by using code

- comparison software to check that the version of the program in use is the version approved by management.
- d. Sampling programs to extract data for audit testing
- e. Tests of application controls, for example, testing the functionality of a programmed control
- f. Re-performing calculations performed by the organisation's accounting system.

1.9.2 Types of CAAT

While selecting the CAAT, IS Auditor is faced with certain critical decisions that he / she may be required to make, while balancing on the quality and cost of audit:

- a. Use the audit software developed by the client.
- b. Design and develop his /her own audit software.
- c. Use a standard off the shelf Generalised Audit Software

The first two options require the auditor to be technically competent in programming and its methodology, which may not be his area of expertise. Computer audit software also known as Generalised Audit Programs (GAS) is readily available off-the-shelf software with specific features useful for data interrogation and analysis. The auditor do not require much expertise knowledge to be able to use for auditing purpose

The various types of CAATs can be categorized as follows:

- 1. Generalised Audit Software
- 2. Specialised Audit Software
- 3. Utility Software

A brief description of the types of software is given below:

1. Generalised Audit Software (GAS)

Computer audit software may be defined as: "The processing of a client's live files by the auditor's computer programs". Computer audit software may be used either in compliance or substantive tests. Generalised Audit software refers to generalized computer programs designed to perform data processing functions such as reading data, selecting and analyzing information, performing calculations, creating data files and reporting in a format specified by the auditor. The use of Generalised Audit Software is perhaps the most widely known computer assisted audit technique.

GAS has standard packages developed by software companies exclusively for auditing data stored on computers. These are economical and extensively used by auditors the world over. Available off the shelf, GAS can be used for a wide range of hardware, operating systems, operating environments and database.

Typical operations using GAS include:

- a. Sampling Items are selected following a value based or random sampling plan.
- b. Extraction Items that meet the selection criteria are reported individually.
- c. Totalling the total value and number of items meeting selection criteria are reported.
- d. Ageing Data is aged by reference to a base date
- e. Calculation Input data is manipulated prior to applying selection criteria

2. Specialised Audit Software (SAS)

Specialised Audit software, unlike GAS, is written for special audit purposes or targeting specialized IT environments. The objective of these software to achieve special audit procedures which may be specific to the type of business, transaction or IT environment e.g. testing for NPAs, testing for UNIX controls, testing for overnight deals in a Forex Application software etc. Such software may be either developed by the auditee or embedded as part of the client's mission critical application software. Such software may also be developed by the auditor independently. Before using the organisation's specialized audit software, the auditor should take care to get an assurance on the integrity and security of the software developed by the client...

3. Utility Software

Utility software or utilities though not developed or sold specifically for audit are often extremely useful and handy for conducting audits. These utilities usually come as part of office automation software, operating systems, and database management systems or may even come separately. Utilities are useful in performing specific system command sequences and are also useful in performing common data analysis functions such as searching, sorting, appending, joining, analysis etc. Utilities are extensively used in design, development, testing and auditing of application software, operating systems parameters, security software parameters, security testing, debugging etc.

- a. File comparison: A current version of a file for example, is compared with the previous year's version, or an input file is compared with a processed file.
- b. Production of circularisation letters.

1.9.3 Typical Steps in using GAS

- i. Define the audit objectives
- ii. Identify the tests that the package can undertake to meet the objectives.
- iii. Make out the package input forms for the tests identified.
- iv. Compile the package on the computer, clearing reported edit errors.
- v. If a programmer has been adding coded routines to the package to fill out the input forms or to advice, the programmer's work must be tested.

- vi. Obtain copies of the application filed to be tested.
- vii. Attend the execution of the package against these copy files.
- viii. Maintain security of the copy files and output until the tests have been fully checked out.
- ix. Check the test results and draw audit conclusions.
- x. Interface the test results with whatever subsequent manual audit work to be done.

Refer case at the end of chapter on the above steps:

1.9.4 Selecting, implementing and using CAATs

Computer Assisted Audit Techniques (CAATs) are a significant tool for auditors to gather evidence independently. CAATs provide a means to gain access and analyse data for a predetermined audit objective and to report audit findings with evidence. They help the auditor to obtain evidence directly on the quality of the records produced and maintained in the system. The quality of the evidence collected confirms the quality of the system processing. The following are some examples of CAATs, which can be used to collect evidence:

- ACL, IDEA etc.
- Utility Software such as Find, Search, flowcharting utilities
- Spreadsheets such as Excel
- SQL Commands, OS commands
- Third party access control software
- Application systems
- Options and reports built in as part of the application/systems software
- Performance monitoring tools
- Network management tools, OS utilities
- High end CAATs
- RSAREF, DES, PGP
- TCP Wrapper, SOCKS, TIS Toolkit
- COPS, Tripwire, Tiger
- ISS, SATAN, etc.

1. 10 Continuous Auditing Approach

Continuous auditing is a process through which an auditor evaluates the particular system(s) and thereby generates audit reports on real time basis. Continuous auditing approach may be required to be used in various environments. Such environments usually involve systems that are 4*7 mission critical systems. In the traditional method, the scope for market influence on the information contained in the audit report is less due to

- The time gap between the audit and reporting

- The deficiencies identified in the control systems can be rectified even by the management during the time gap.

1.10.1 Techniques for Continuous Auditing

1. Snapshot

Most applications follow a standard procedure whereby, after taking in the user input they process it to generate the corresponding output. Snapshots are digital pictures of procedures of the console that are saved and stored in the memory. Procedures of the console refer to the application procedures that take input from the console i.e. from the keyboard or the mouse. These procedures serve as references for subsequent output generations in the future. Typically, snapshots are implemented for tracing application software and mapping it. The user provides inputs through the console for processing the data. Snapshots are means through which each step of data processing (after the user gives the input through) is stored and recalled.

Let us consider, for example, a banking transaction. Numerous transactions are effected and processed by various application systems in a banking environment. While all applications are tested before being deployed, in an integrated computing environment, a cash withdrawal at the ATM may be processed by more than one software working in an integrated manner. In the event of some errors in transactions being detected or suspected, snapshot software installed as part of the production environment would continuously take pictures of transactions passing a particular control point e.g. instruction set executed in the memory of the ATM machine for processing withdrawal. Hence the error in code/ instruction can be pinpointed and identified by the snapshot software.

Snapshots are employed in the following:

- They are used for analysing and tracking down the flow of data in an application program, so as to know the underlying logic of the data processing software.
- For documenting the logic, input/output controls (or conditions) of the application program and the sequence of processing.

Snapshots are generally deployed for tracking down the reasons for any disruption in the functioning of application or system software like operating system or database system.

Case at the end of this part: SNAPSHOT for payroll process.

2. Integrated Test Facility (ITF)

Integrated Test Facility (ITF) is a system in which a test pack is pushed through the production system affecting “dummy” entities. Hence this requires dummy entities to be created in the production software. For example, the auditor would introduce test transactions that affect targeting dummy customer accounts and dummy items created earlier for this testing purpose. The approach

could also involve setting a separate dummy organisation using the application software in the live environment. ITF is useful in identifying errors and problems that occur in the live environment and that cannot be traced in the test environment. However the disadvantage in using ITF is that the dummy transactions also append to the live database and hence will impact the results and reports drawn from the live database. It will therefore, be necessary to delete the test transaction from the system once the test is performed. As with all test packs, the output produced is compared with predicted results. This helps to determine whether the programmed procedures being tested are operating correctly.

Case at the end of this part: Stores and Purchase program testing through ITF.

3. System Activity File Interrogation

Most computer operating systems provide the capability of producing a log of every event occurring in the system, both user and computer initiated. This information is usually written to a file and can be printed out periodically. As part of audit testing of general controls, it may be useful for the auditor to review the computer logs generated at various points to build an audit trail. Wherever possible, unauthorised or anomalous activity would need to be identified for further investigation. Where a suitable system activity file is retained on magnetic media, one can select and report exceptional items of possible audit interest such as unauthorised access attempts, unsuccessful login attempts, changes to master records and the like. Similar implementation is also possible by embedding special audit software in application software that maintains continuous transaction logs at various points in the application software. This technique is also referred to as the Systems Control Audit Review File. The files can be further analysed to determine deviations and improper transactions.

4. Embedded Audit Facilities

Embedded audit facilities consist of program audit procedures, which are inserted into the client's application programs and executed simultaneously. The technique helps review transactions as they are processed and select items according to audit criteria specified in the resident code, and automatically write details of these items to an output file for subsequent audit examination.

This technique generally uses one or more specially designed modules embedded in the computer application system to select and record data for subsequent analysis and evaluation. The data collection modules are inserted in the application system or program at points predetermined by the auditor. The auditor also determines the criteria for selection and recording. Automated or manual methods may be used to analyse the data later. This is intended to highlight unusual transactions, which can be later taken up for scrutiny. Please refer to the case of listing cash payments in excess of Rs.20,000/- through use of range function in TALLY discussed in detail in chapter 1.

5. Continuous and Intermittent Simulation

With significant advancements in technologies, business systems are increasingly driven by client-server systems with distributed computing and databases. The components of such systems are networked generally over geographically disparate locations. This has resulted in the need for auditing systems that not only enable continuous auditing of transactions but also have a low overhead on the IT resources of the auditee but without compromising on the independence of such systems. This has resulted in the use of continuous auditing techniques that the client-server environment to enable independent simulation of “suspect” transactions independently by the simulation audit software under the control of the auditor but using the online data of the auditee waiting to be written to the database. **Please note this case is part of PT. Please refer to reference material which includes the publication: Data analysis for an auditor which has detailed case studies on using CAATs. Please also refer to Module-2 which has explanation on CAATs.**

1.11 Case on using MS Excel to find Duplicate / Missing Sales Invoice

Objective: The case is to help understand the steps of using CAATs.

Facts: Company using TALLY has selected manual invoice numbering as an option in TALLY. The option is available when user creates / configures Vouchers.

Problem: Management action of selecting manual invoice numbers, for data entry purpose raises the following risks:

- Duplicate
- Missing invoice number.

IS Auditor's concern: To identify a mechanism to track the missing / duplicate invoice number.

Using Audit tools to achieve the above audit objectives:

- a. Through use of Excel: Discussed here
- b. Through use of IDEA, the generalized audit tool: Part of online demo in **PT**.

1.11.1 Steps to be performed in above case through use of excel

- i. **Define the audit objectives:** To identify duplicate / missing invoice number.
- ii. Identify the tests that the package can undertake to meet the objectives. The objective is to identify duplication / missing invoice number through use of excel.
- iii. Make out the package input forms for the tests identified. No separate input form required. TALLY exports data directly in excel. This is a good control as it reduces the risk of discrepancy occurring during the system hand over process.

Module 6

- iv. Compile the package on the computer, clearing reported edit errors. Display the sales register from TALLY and export the same to excel.
- v. If a programmer has been adding coded routines to the package to fill out the input forms or to advice, the programmer's work must be tested. Not applicable in the instant case.
- vi. Obtain copies of the application file to be tested. Before testing on excel a copy of report kept separately.
- vii. Attend the execution of the package against these copy files.: Execution includes the following steps:
 - *Index the excel sheet in ascending order, based on Invoice Number.*
 - *Insert an additional column to the right side of invoice number.*
 - *Put the rule Invoice number (Row Next)-Invoice number (current row). The same shall appear like:*

	A	B	C
1	Invoice number	Inserted column	Result of command
2	10001	=A3-A2	1.00
3	10002	=A3-A4	1.00
4	10003	=A4-A5	2.00
5	10005	=A5-A6	1.00
6	10006	=A6-A7	0.00
7	10006	=A7-A8	1.00
8	10007	=A8-A9	1.00
9	10008	=A9-A10	
10			

Reading the above: Where the value of column C is other than '1', it means there is a problem with invoice numbering. Above is one way of doing the same in excel, there could be multiple ways of getting the audit conclusions in excel.

- viii. Maintain security of files and output until the tests have been fully checked out: *Important to remember.*
- ix. Check the test results and draw audit conclusions. *Based on above results auditor can draw conclusions.*
- x. Interface the test results with whatever subsequent manual audit work to be done.

1.11.2 Cases on how to use continuous auditing

1. Snapshot

Facts: A software company with more than 1,00,000 employees. Organisation uses payroll software to process salary. The payroll is processed in four distinct steps in system. They are:

- Calculate basic salary: Based on basic input data, like attendance and master data is used here
- Calculate Allowance: Based on basic salary calculated allowances like House Rent Allowances, calculated.
- Calculate deductions: Once Basic Salary and Allowances calculated deductions like TDS, PF etc. made.
- Calculate the net salary: Same based on above calculation.

Audit objective: Management has appointed a system auditor to check whether the payroll system is working properly.

Auditor's use of SNAPSHOT as a technique:

1. This technique allows auditor to capture images of transactions as the same is processed in system.
2. Auditor identifies the transactions for which snapshot shall be taken.
3. Based on the snapshot auditor is able to come to a conclusion about the nature and location or error in payroll process if any.

2. Integrated Test Facility (ITF)

Facts: Company has linked its stores system to its purchase system. In the stores system whenever an items level comes to **re-order level**, system automatically generates a **purchase order**.

Objective: Company appoints an IS Auditor to check whether the same system is working properly or not.

IS Audit process: IS auditor uses the technique of ITF.

IS Audit Steps:

1. Create a dummy organisation. In the given case the dummy organisation is an **issue slip**. The objective is to reduce an items balance below re-order level.
2. Once the dummy organisation is processed in system, auditor checks whether the system triggers a purchase order.
3. If the answer is 'yes', it means the system is working properly.

Points to remember:

1. Items selected for the above test shall be material.
2. Effect of dummy organisation need to be reversed.

PART 2: COMPLIANCE TESTING AND SUBSTANTIVE TESTING

Business application software controls has to be analysed through compliance and substantive testing. These tests are necessary for risk assessment. The evaluation of internal control is accomplished through compliance and substantive testing. The purposes for compliance and substantive testing differ and will be achieved during the fieldwork.

2.1 Compliance Testing

ISACA ITAF 201 Performance Guidelines on “Engagement Planning” states as follows: “Audit and assurance projects should include consideration of internal controls either directly as a part of the project objectives or as a basis for reliance upon information being gathered as a part of the project. Where the objective is evaluation of internal controls, IT audit and assurance professionals should consider the extent to which it will be necessary to review such controls. When the objective is to assess the effectiveness of controls over a period of time, the audit plan should include procedures appropriate for meeting the audit objectives, and these procedures should include compliance testing of controls. When the objective is not to assess the effectiveness of controls over a period of time, but rather to identify control procedures at a point in time, compliance testing of controls may be excluded”.

SA 00 issued by ICAI, “Basic Principles Governing an Audit”, defines compliance procedures as tests designed to obtain reasonable assurance that those internal controls on which audit reliance is to be placed are in effect. A compliance test determines if controls are being applied in a manner that complies with management policies and procedures. The broad objective of compliance test is to provide the 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 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 e.g., to provide assurance that only authorized modifications are made to production programs.

2.1.1 Purpose

Compliance tests are used to help determine the extent of substantive testing to be performed, as stated in Statement of Auditing Standards. Such tests are necessary if the prescribed procedures are to be relied upon in determining the nature, time or extent of substantive tests of particular classes of transactions or balances. Once the key control points are identified, the auditor seeks to develop a preliminary understanding of the controls to ensure their existence and effectiveness. It is achieved through compliance testing. Compliance testing helps an auditor determine that

- The controls exist and are working as expected
- The controls are applied in a manner that complies with policies and procedures.

2.2 Substantive Testing

To obtain evidence of the validity and propriety of accounting treatment of transactions and balances or, conversely, of errors or irregularities therein

SA 00 issued by ICAI, "Basic Principles Governing an Audit", defines substantive procedures are designed to obtain evidence as to the completeness, accuracy and validity of the data produced by the accounting system. A substantive test substantiates the integrity of actual processing and the outcome of compliance testing. Substantive testing is the testing of individual transactions. It provides evidence of the validity and integrity of the balances in the financial statements and the transactions that support these balances. The IS auditors use substantive tests to test for monetary errors directly affecting financial statement balances.

2.2.1 Purpose

Substantive testing procedures focus on broadly two types of tests:

- i. Tests of details of transactions and balance such as recalculating interest to ensure the accuracy of process and effectiveness of controls over the process of the calculation of interest.
- ii. Analysis of significant ratios and trends including the resulting enquiry of unusual fluctuations and items in exceptions e.g. debit balance in deposit accounts, pending items to ensure the controls to prevent or detect such transactions or balances are in place.

2.3 Relationship between compliance and substantive testing

There is a direct correlation between the effectiveness of controls and the extent of substantive testing required. If the auditor after compliance testing concludes that the controls are adequate and are working effectively as expected, then he is justified in reducing the size of his sample for substantive testing. If testing of controls reveals weak controls, he might decide to go for increasing his sample for substantive testing.

Please refer to chapter 2 of module 2: IS Assurance services for more details of compliance testing and substantive testing.

PART 3: IMPACT OF BUSINESS APPLICATION SOFTWARE ON BUSINESS PROCESSES / CONTROLS

As discussed in previous sections, an organisation selects business application to achieve its business goals and objectives. In part 1 of the chapter, the case study has highlighted the importance of selecting the correct business application software. Once an organisation has selected a business application, it needs to implement appropriate business processes or re-define its way of working to ensure that business application software process and organisation own business operations are in sync.

3.1 Case: Highlight need for redefining business process

Objective: To highlight importance of re-defining the business process to suit the requirements of the business application selected to be used.

a. To know: Teeming and Lading fraud

Definition: It is a type of fraud that involves the crediting of one account through the abstraction of money from another account. It can happen when one customer's payment is stolen and another customer's payment is posted to hide the theft.

b. Why this fraud occurs?

If the internal check is lacking then the fraud perpetrator can divert the cash cheque for his/her personal use. As we have read that person in possession must not possess the record of asset. This fraud occurs when a person acts as **cashier as well as ledger writer or enters data**.

c. How to control the risk in business application system?

1. Organisation using TALLY:

In TALLY, as soon as a cash voucher is entered in system, it immediately updates ledger and related financial statements also. The issue to resolve is safeguarding against occurrence of fraud.

Safeguards put in place: In TALLY it is preferred that better **input** controls be put in place to prevent occurrence of fraud by creating specific users with access for specific functions.

2. Organisation using ERP system like SAP:

In SAP, the transaction processing follows a two-step process:

i. **Park of entry:** This step is used to enter and store (park) incomplete documents in the SAP System without carrying out extensive entry checks.

ii. **Posting of entry:** Parked documents can be completed, checked, and then posted at a later date - if necessary by a **different accounting clerk**.

This ensures that same accounting clerk does not receive the cash and also update the records.

d. What TALLY users need to do?

They need to redefine their business process in a manner to prevent the occurrence of above frauds. The redefined business process needs to address the following propositions:

1. There are proper internal check is established, and
2. The business process shall be as per the nature of business of organisation.

3.2 Procedures to manage changes to business processes and impact on controls

During the **procedure conversion performed in the implementation phase of system development** life cycle approach, an organisation needs to prepare a control impact assessment chart. This documentation is important to help identify the following:

Step 1: What is the impact of new business application on the internal controls? This assessment has to be done for all items specified in the “Checklist for Application Control Review of Business Application” (Annexure ‘1’ of this module). An evaluation checklist for impact assessment is given in Appendix-5 “Business Application’s impact on internal controls”.

Step 2: Based on the assessment made at step ‘1’ IS auditor shall check how management has addresses the shortcoming. Management may address the concerns raised by specifying new business process, approval process. All such new business process, approval process need to be validated. For validation IS auditor shall use the checklist given in Appendix 1.

PART 4: USER CONTROLS

The most important aspect of a business application is the user controls. User controls are defined as the rights given to users as per job profile and their rights and duties within the organization. Entitlement of access to an information resource and degree of access is determined according to the job description, functions and role of the user in the organisation.

The “rights of access” is to ensure that user does not gain access to undesired information resources or an undesired mode of access to the information, This is governed by philosophy “need to know and need to do basis” or the principle of least privilege. Principle of least privilege is an important concept in information security. It advocates minimal user profile privileges on computers, based on user’s job necessities. It can also be applied to processes on the computer; each system component or process should have least authority necessary to perform its duties. This is also called the “default deny” principle. All these terms imply that access is available only to users after it has been specifically granted to them, only to perform the job function that has been granted to them. Please refer to the chapter on Logical access controls in Module-4 for more details.

4.1 Principles to follow while granting user rights

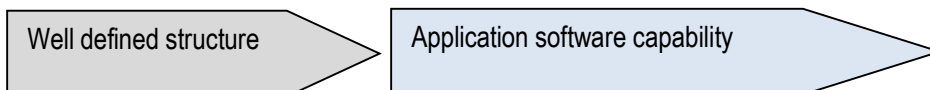
User rights are to be assigned based on following guiding principles:

1. Rights are allocated on the basic philosophy of, “NEED TO KNOW and NEED TO DO
2. Rights need to be allocated based on user’s job profile.
3. Maker and checker distinction need to be followed, for example a user who creates a cash voucher must not be able to modify the same.
4. Asset recorder must be different from person physically holding asset.

4.2 Creating users for different level of use

4.2.1 Key requirement

Proper user rights definition in system has two key requirements.



- a. Well defined management structures with employee roles and responsibility.
- b. Capability of the business application to allow user rights creation

The job of user rights creation, modification and deletion is a critical from internal control perspective.

4.2.2 IS Auditor key checkpoints

It is important for an IS Auditor to check:

i. Who has the authority to create user rights?

IS auditor is also concerned to know the person who has the authority to create users in system. IS auditor needs to evaluate the rights of persons doing this job and how these rights have been granted and monitored.

Case at the end of this part: An accounting software's USER RIGHTS AUDIT.]

ii. Authorisation procedure before creating user rights?

IS Auditor needs to check whether there is a formal user rights approval form/document. The question that need to be answered being

- a. Who triggers the request for user rights creation? Ideally this request has to be generated through HR department.
- b. Whether the form contains all relevant information for the specific user?
- c. Whether the form has been properly filled?
- d. Whether the form has valid authorisation?
- e. Whether forms are marked once user rights are created in system?

iii. Validation of user rights created in system?

IS Auditor needs to evaluate the process how user rights created at step (ii) are validated once they have been put in system. IS Auditor may seek answers to the following questions.

- a. Whether there is a proper cross check mechanism build in organisation to validate the user rights of employee once they have been created?
- b. Whether there is timely validation of user rights and user job profiles? For example this is a cyclical process to be done once each year to see whether the job profile of individual is appropriately reflected in his/her user rights?

iv. Process of alteration of user rights?

IS Auditor is concerned with the process of alteration of rights. The IS Auditor seeks answers to the following questions.

- a. Whether the user right alteration process is linked to job profile of individual?
- b. Who triggers the request for user rights alteration?

- c. Whether the alterations are done through proper validated USER RIGHTS ALTERATION FORMS?
- d. Whether these forms follow the similar authorisation process as done during initial creation of user rights?

v. Keeping track of user actions?

This shall be part audit trail review, dealt in detail at other location in this module.

4.3 Creating users for different level of use

A checklist from TALLY to allow creation of user rights is explained in the case which follows.

Case Studies

1. User rights review Audit

An Internal Auditor asked the company to make available user rights lists as provided by the company in accounting software. Internal Auditor also asked the HR department to make available the hierarchy chart and job profile of the individuals. On comparison of the two documents auditor found the following: There were 50 employees in the company. Details of two employees are:

Designation	HR department profile	Accounting Software rights: Allowed Rights					
	Major responsibility as defined by company	Name of Document / Master	Create	Alter	Delete	Display	Print
Stores Clerk	Prepare Material Receipt Note after validation with PO for quantity, rate, and other terms.	Material Receipt Note	Yes	Yes	Yes	Yes	Yes
		Vendor Master	Yes	Yes	Yes	Yes	Yes
		VAT Rate Master	Yes	Yes	Yes	Yes	Yes
Manager Accounts	Timely and accurate accounting, statutory	Vouchers	Yes	Yes	Yes	Yes	Yes
		Account Masters, including debtors and creditors master.	Yes	Yes	Yes	Yes	Yes

	compliances, timely preparation of financial statements, timely submission of MIS to management.	The person was allowed to do back dated entries 365 days in past.

Exercise for participants: What are the risks and what are the remedies?

2. GM (F) who left the company.

Facts: The Company had a policy of allocating the super-user password to General Manager (Finance). The same defined in the job profile of the GM (F). GM (F) shall be responsible to ensure for allocation, deletion, modification and suspension of user rights based on approvals made available by HR department.

Problem: The GM (F) left the organisation. Another one joined. The new joiner was given another super-user password. Six months after the new joiner, it came to notice of Internal Auditor that all employees of the accounts department have been using the super-user password of the previous GM (F).

Exercise for the participants: What was wrong and how these could be corrected for future?

PART 5: DATABASE CONTROLS

In this chapter we will understand database structure and tables, user creation, access levels and user management. We will also understand how to evaluate internal control systems in application software relating to system design, data creation/input, data processing, data flow, data transmission and data storage. How to use reporting, query and SQL features as required for reviewing controls are briefly discussed.

5.1 Key features of database

5.1.1 Database architecture

Data is defined as collection of different data. Database is like an electronic file cabinet i.e. a collection of computerised data files. Database being a critical system resource needs elaborate controls to be put in place. Data architecture is composed of models, policies, rules or standards that govern which data is collected, and how it is stored, arranged, integrated, and put to use in data systems and in organizations. They are namely;

- (i) **External or user view:** It is at the highest level of the database abstraction. It includes only that portion of database or application programs which is of concern to the users. It is defined by the users or written by the programmers. It is described by the external schema.
- (ii) **Conceptual or global view:** This is reflection of a database as viewed by database administrator. Single view represents the entire database. It describes all records, relationships and constraints or boundaries. Data description to render it independent of the physical representation. It is defined by the conceptual schema,
- (iii) **Physical or internal view:** It is at the lowest level of database abstraction. It is closest to the physical storage method. It indicates how data will be stored, describes data structure, and the access methods. It is expressed by internal schema.

5.2 Database Security and Control

Database Controls could be in terms of:

1. Database Roles and Permissions

- Segregation of duties
- Roles & Permissions allow control of operations that a user can perform on database,

2. Concurrency Control: Addresses conflicts relating to simultaneous accesses

3. **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 Restrict user views of the database.

4. **Stored Procedures:** Database servers offer developers the ability to create & reuse SQL code through the use of objects called as Stored Procedures (Group of SQL statements). This is discussed later.

5.3 User creation in database

Please refer to the eLearning part of module 1 for more details on concepts of database. The objective of Data base security would be Authorized 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;

1. Application programmers
2. Sophisticated users
3. Specialized users
4. Naive users

This user management is achieved through Authorization and access control

Basic model for accessing control involves:

- a. Subjects (Right People)
- b. Objects (Right data)
- c. Access Rights (Right Access)

Subject is allowed **access rights** to **objects**.

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. There is a need to create user and assign some authentication mechanism like a Password.

The screenshot shows the phpMyAdmin interface with the 'Add user' form. The left sidebar contains the phpMyAdmin logo, navigation icons, a '(Recent tables)...' dropdown, 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' (with a dropdown menu and a text input containing 'ISAADMIN'), 'Host' (with a dropdown menu set to 'Local' and a text input containing 'localhost'), 'Password' (with a dropdown menu and a masked text input), and 'Re-type:' (with a masked text input). At the bottom of the section is a 'Generate password:' label, a 'Generate' button, and an empty text input field.

phpMyAdmin

(Recent tables)...

- information_schema
- mysql
- performance_schema
- test

Add user

Login Information

User name: Use text field: ISAADMIN

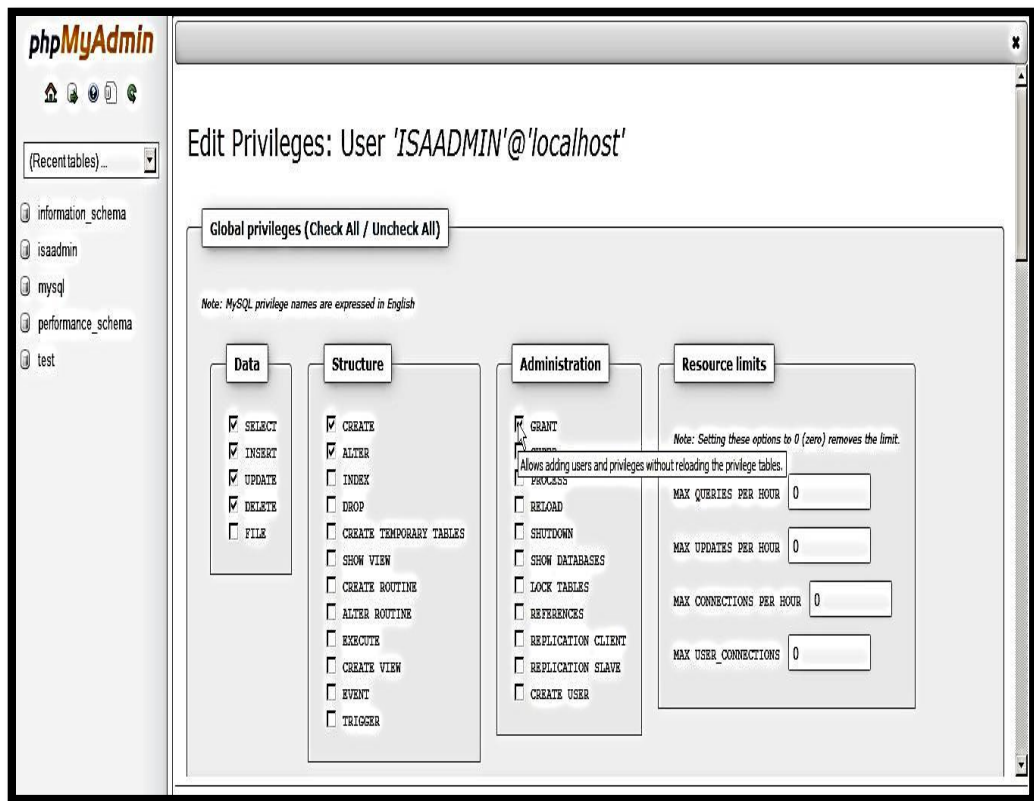
Host: Local localhost

Password: Use text field:

Re-type:

Generate password: Generate

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



5.4 Structured Query Language

A query language is a set of commands to create, update and access data from a database allowing users to raise ad hoc queries / questions interactively without the help of programmers. Structured Query Language (SQL) is a programming language used to manipulate information in relational database management systems (RDBMS).

5.4.1 Components of SQL

- DML or data manipulation language: DML consists of SELECT, UPDATE, INSERT, and DELETE statements.
- DDL or data definition language: DDL is made up of CREATE and ALTER statements.
- DCL or data control language: DCL is comprised of GRANT and REVOKE statements. In recent years DML has been expanded to include the MERGE statement and DDL has had the APPEND statement added.

5.4.2 Language elements of SQL

- a. Clauses, which are in some cases optional, constituent components of statements and queries.
- b. Expressions which can produce either scalar values or tables consisting of columns and rows of data.
- c. Predicates which specify conditions that can be evaluated to Boolean (true/false/unknown) truth values and which are used to limit the effects of statements and queries, or to change program flow.
- d. Queries which retrieve data based on specific criteria.
- e. Statements which may have a persistent effect on schemas and data, or which may control transactions, program flow, connections, sessions, or diagnostics.

5.5 SQL commands for reporting

SELECT Statement Syntax

S.no.	Action	Target	Options to specify
1	Select	Columns	i. Specific columns by name ii. All columns through wildcard
2	From	Tables	Lists "qualified table name
3	Where	Criteria are met	i. Optional ii. Conditions that limit the records to be displayed
4	Group by	Summarize	
5	Order By	Order Results	i. Optional ii. Sorts the query results ASC - ascending order DESC - descending order

The above can be used to generate specified reports directly from database. These are covered in more detail through practical examples in the hands on training of this module.

PART 6: FINANCIAL REPORTING AND REGULATORY REQUIREMENT IN INFORMATION SYSTEMS

6.1 Nature of compliances

As the usage of business application has been increasing in business, so has been the increase of regulatory compliances. Today businesses rely on reports generated from business applications for their statutory compliances. The list of compliances may include:

i. **Taxation related:** TDS, TCS, Excise Duty, Service Tax, VAT, PF, etc.

ii. **Control Related:** Those specified in:

- Section 17(2AA) of Companies Act 1956 (old): Detailing Director's Responsibility Statement, which specifies that directors of the company are responsible to *implement proper internal controls*.
- CARO, 2003 (As amended in 2004), has many clauses where statutory auditor needs to comment upon the *internal controls*.
- SOX compliance: Financial transaction analysis, for example aging analysis for debtors and inventory, capability to drill down un-usual financial transactions.

iii. **XBRL compliance:** Looking to the growth of XBRL compliance in India and governments intention to slowly increase the coverage area of eligible entities, XBRL compliance shall increase in India. Many business application vendors have already started making their software capable of generating XBRL reporting.

iv. **Accounting Standard related:** Accounting standards prescribing the accounting guidance to transactions. It is important that the business applications used are in compliance with the applicable accounting standards.

v. **Compliances as specified in the newly notified Companies act, 2013:**

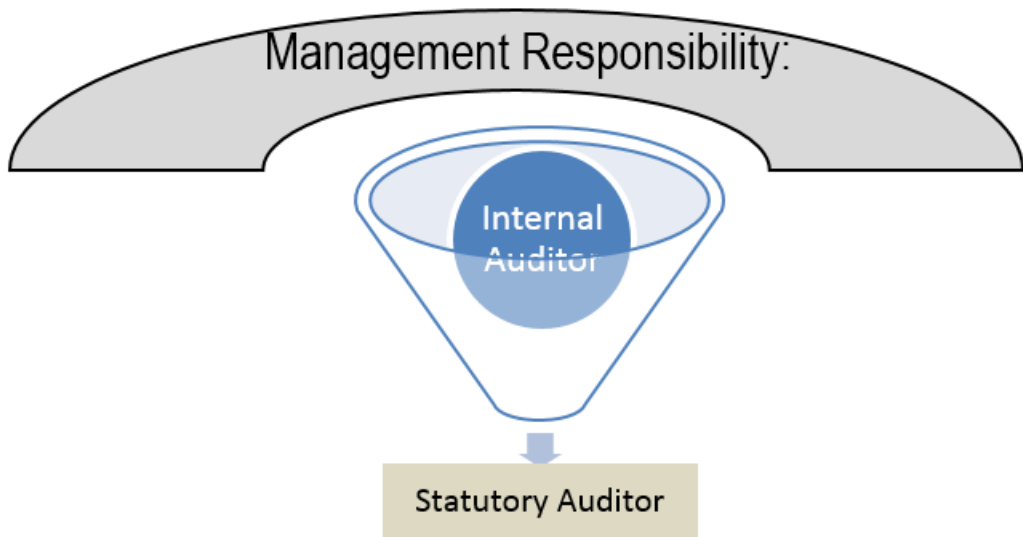
- Maintenance of books in e-form. (Section 128)
- Compulsory Internal Audit: Prescribed companies to have an Internal Auditor. **This provision makes it more important for company to implement proper controls in business application used.** (Section 138)
- Constitution of National Financial Reporting Authority (NFRA). This body has been entrusted with task of framing auditing and accounting standards. (Section 132)

vi. **Compliances requirements from industry specific statutes**

- Banking industry compliances
- Insurance Industry
- Stock market industry

6.2 Who is responsible for accuracy and authenticity of reports?

The responsibility may be defined through the following chart:



- The prime responsibility for accuracy of report generated from the business applications lies with the management.
- The role of internal auditor is to see whether established controls ensure the accuracy of reports.
- Where statutory auditor wishes to use the above reports for his/her documentation, or forms and opinion based on such reports.

SA 580 on "Written Representations", issued by ICAI, state that auditor when decides to obtain written representations as assertions, and to respond appropriately to written representations provided by management or if management does not provide the written representations requested by the auditor.

6.3 Validation of statutory reports from business application software

This requires IS auditor to have an understanding of system, this includes the way it is configured and the way it generates reports. To highlight the above issue two cases are given here.

Case on validation of statutory rates in business application software

1. PF rates are not properly defined

a. **Facts:** Employee's PF Contribution @10% Pay Head Creation. If rate of % defined incorrectly in master configuration, then salary calculated and report will also be affected and shown incorrectly.

b. How to define the rate?

Go to Gateway of Tally > Payroll Info. > Pay Heads> Create> In the Pay Head Creation screen,

- Type Employee's PF Contribution @ 10% as the Name of the Pay Head
- Select Employees' Statutory Deductions in the field Pay Head Type

The screenshot shows the 'Pay Head Alteration' screen in Tally ERP 9. The 'Pay Head Name' is 'Employee PF Contribution @10%'. The 'Pay Head Type' is 'Employees' Statutory Deductions'. The 'Statutory Pay Type' is 'PF Account (A/c No. 1)'. The 'Affect Net Salary' is 'Yes' and 'Name to appear in Payslip' is 'EPF @10%'. The 'Calculation Type' is 'As Computed Value' and 'Calculation Period' is 'Months'. A 'List of Pay Head Types' dropdown menu is open, showing options like 'Not Applicable', 'Bonus', 'Deductions from Employees', etc. The 'Value Basis' is set to '10 %'.

c. What shall be the impact?

- Deduction of PF at wrong rates
- Other liabilities associated with the above.

The screenshot shows the Tally ERP 9 Payroll screen. The main window is titled "Pay Head Alteration" and displays the following information:

Pay Head Info

Name : Employee PF Contribution @ 10%
(alias) :

Pay Head Type : Employees' Statutory Deductions
Statutory Pay Type : PF Account (A/c No. 1)
Under : Current Liabilities

Compute : On Specified Formula
Specified Formula : BASIC PAY

Effective From	From Amount	Amount Upto	Slab Type	Value Basis
1.Apr.2013	6,500.00	6,500.00	Percentage	10 %
			Percentage	0 %

Affect Net Salary : ? Yes
Name to appear in Payslip : EPF @ 10%

Calculation Type : As Computed Value
Calculation Period : Months

Rounding Info

Rounding Method : Normal Rounding Limit :

Opening Balance (on 1.Apr.2013) :

Accept ? Yes or No

Buttons: Out, Accept, Delete, Ctrl + N

Footer: Tally MAIN -> Gateway of Tally -> Payroll Info. -> Pay Heads -> Pay Head Alteration (c) Tally Solutions Pvt. Ltd., 1998-2013 Mon, 20 Jan, 2014 13:02:29

2. TDS rates are not correctly specified

a. Wrong classification of payments and the related section under which payment is to be made.

Default Nature of Payment for professional fees is entered as payment to contractors instead of Fees for Technical Services U/s 194-J.

P: Print	E: Export	M: E-Mail	O: Upload	S: Shop	G: Language	K: Keyboard	K: Control Centre	H: Support Centre	H: Help	F4: New Parent	
Expense Ledgers Setup										Demo	Ctrl + M
Under Group : All Items										For 1-Apr-2013	
S.No.	Name of Ledger	Under	Is TDS Applicable	Default Nature of Payment							
1.	Professional Fess	Indirect Expenses	Yes	Payments to Contractors (Other Than Advertisement)							
2.	Rent	Indirect Expenses	Yes	Winnings From Horse Race							
3.	Commission	Indirect Expenses	No								
4.	Salary	Indirect Expenses	Yes	Fees for Professional Or Technical Services							
5.											

b. Improper classification regarding exemptions:

Income Tax Exemption Limit: Income tax exemption limit is ignored which results in deduction of tax from the first voucher ignoring the basic exemption limit. For example, TDS on interest is deducted only if the amount of interest exceeds Rs. 10000.

<u>P</u> : Print	<u>E</u> : Export	<u>M</u> : E-Mail	<u>O</u> : Upload	<u>S</u> : Shop	<u>G</u> : Language	<u>K</u> : Keyboard	<u>K</u> : Control Centre	<u>H</u> : Support Centre	<u>H</u> : Help	F7: Skip Details	
Income Tax Exemption Setup										Demo	Ctrl + M
Under Group : All Items										For 1-Apr-2013	
S.No.	Name of Ledger	Under	Deductee Type	Ignore Income Tax Exemption	PAN / IT No.						
1.	A	Sundry Creditors	Individual/HUF - Resident	Yes							
2.	A Ltd.	Sundry Creditors	Individual/HUF - Resident	Yes							

c. What shall be the impact?

- Deduction of TDS at wrong rates
- Other liabilities associated with the above

PART 7: SYSTEM AUDIT REPORT FORMAT AS PER BEST PRACTICES

7.1 Reporting Standards

Report is the output of effort taken. Quality of report is the key to success of audit effort. ISACA ITAF 401 guidance on reporting standards states: "The reports produced by IS audit and assurance professionals will vary, depending on the type of assignments performed. Considerations include the levels of assurance, whether IS audit and assurance professionals were acting in an audit capacity, whether they are providing direct reports on the subject matter or reporting on assertions regarding the subject matter, and whether the reports are based on work performed at the review level or the examination level".

1 Audit report format ISACA ITAF 401 on "Reporting" and SA 700 on "Forming an opinion and Reporting on Financial Statements", the audit report need to cover the following." IT audit and assurance professional's report about the effectiveness of control procedures should include the following elements:

- i. Title:
- ii. Addressee
- iii. Description of the scope of the audit, the name of the organisation or component of the organisation to which the subject matter relates, including:
 - a. Identification or description of the area of activity.
 - b. Criteria used as a basis for the IS audit and assurance professional's conclusion.
 - c. The point in time or period of time to which the work, evaluation or measure of the subject matter relates.
 - d. A statement that the maintenance of an effective internal control structure, including control procedures for the area of activity, is the responsibility of management.
- iv. A statement that the IT audit and assurance professional has conducted the engagement to express an opinion on the effectiveness of control procedures.
- v. Identification of the purpose for which the IT audit and assurance professional's report has been prepared and of those entitled to rely on it, and a disclaimer of liability for its use for any other purpose or by any other person.
- vi. Description of the criteria or disclosure of the source of the criteria.
- vii. Statement that the audit has been conducted in accordance with specified IT Audit and Assurance Standards or other applicable professional standards.
- viii. A paragraph stating that because of the inherent limitations of any internal control, misstatements due to errors or fraud may occur and go undetected.

- ix. An expression of opinion about whether, in all material respects, the design and operation of control procedures in relation to the area of activity were effective.
- x. IT audit and assurance professional's signature.
- xi. IT audit and assurance professional's address.
- xii. Date of the IT audit and assurance professional's report. In most instances, the dating of the report is based upon applicable professional standards. In other instances, the date of the report should be based on the conclusion of the fieldwork.

7.1.1 Case to prepare report in specified format

Objective: to help document a system audit report **for a company's password management policy.**

Facts: "Password Management Policy" has been framed as a part of main security policy of the company.

Policy details:

1. Policy Name: "Password Management Policy". The objective is to ensure that the company has no loss due to password mismanagement.

2. Policy Guidelines:

- Password length to be minimum 8 characters.
- Password to be alpha-numeric.
- Password to be changed every 30 days.
- Password not to be shared.

3. Policy design and implementation: Management informed its system developers to implement the above policy as a part of system design.

4. Policy monitoring: Manager (PW) appointed by the company in HR department, having access to password log of system reports to System Administrator. At the end of year management appointed an IS Auditor with the following scope:

- 1. To review policy compliance.
- 2. To suggest:
 - i. Modification in policy
 - ii. Any other aspect for better implementation.

IS Audit steps: *The basic audit steps including those mentioned at chapter 1, IS Auditor used the audit procedures including compliance and substantive procedures. IS Auditor uses the following audit techniques to collect audit evidence.*

- i. **Inquiry:** Interacting with the stakeholders to confirm understanding of the policy and level of compliance by the users.

- ii. **Documentation:** Reviewing the Audit Logs in system. These logs inform which employee logged in on a specific date. Reviewing the attendance records of staff.
- iii. **Observation:** Validating the process by which staff enters their passwords in system.
- iv. **Re-performance:** With the permission of management, IS Auditor tries to create passwords which were **not in line** with the policy.

B. IS Auditor's Findings: Based on the audit done auditor came across the following.

- 1. There were 200 employee data available. Of these 175 are working and 5 have left.
- 2. The password of employee who had left had not been disabled.
- 3. 20 Employees did not change their password every 30 days, as defined in policy. 5 were repeat offenders.
- 4. 50 instances of employee passwords being used when they were absent have been observed.

Please refer to Appendix 6: System Audit Report.

7.2 Questions

- 1. The best way to define the purpose for an IS Audit in one word:
 - A. Assurance
 - B. Activity
 - C. Review
 - D. Performance
- 2. What is the primary basis of audit strategy? It should be based on:
 - A. knowledge.
 - B. life-cycle.
 - C. user-request
 - D. risk assessment.
- 3. Which of the following audit tools is MOST useful to an IS auditor when an audit trail is required?
 - A. Integrated test facility (ITF)
 - B. Continuous and intermittent simulation (CIS)
 - C. Audit hooks
 - D. Snapshots
- 4. Which of the following is the first step in compliance testing? To review:
 - A. access security controls
 - B. input controls
 - C. processing controls
 - D. output controls.

5. The cashier of a company has rights to create bank master in TALLY. This error is a reflection of poor definition for which type of control:

- A. User Controls
- B. Application Control
- C. Input Control
- D. Output Control

6. An employee has left the company. The first thing to do is to:

- A. Hire a replacement employee.
- B. Disable his/her access rights.
- C. Ask the employee to clear all dues/advances.
- D. Escort employee out of company premises.

8. Common features in ISACA ITAF 401, SA 700 and NFRA (National Financial Reporting Authority) is.

- A. Reporting
- B. Auditing
- C. Accounting
- D. Standard

7.3 Answers and Explanations

1. A. The IS audit focuses on determining the risks that are relevant to information assets, and in assessing controls in order to reduce or mitigate these risks. Management gets an assurance about the functioning of controls.

2. D. Audit Strategy is based on risk assessment done by the auditor. Other answers do not represent basis for deciding audit strategy.

3. D. Snapshots is the right answer as in this technique IS auditor can create evidence through IMAGE capturing? A snapshot tool is most useful when an audit trail is required. ITF can be used to incorporate test transactions into a normal production run of a system. CIS is useful when transactions meeting certain criteria need to be examined. Audit hooks are useful when only select transactions or processes need to be examined.

4. A. is the first step towards compliance test. Other steps are more part of application system transaction audit.

5. A. user controls are not properly defined. User controls need to be defined based on NEED TO DO and NEED TO DO basis. The above is reflection of a greater problem of improper assessment user profiles created in the system.

6. B. the first thing to do as soon as an employee leaves the company is to disable his/her access rights in system. This needs to be done to prevent frauds being committed. Other answers may be valid but are not the first thing to do.

C is the correct answer other options are components of SQL.

7. D. ISACA ITAF is a reporting standard by ISACA. SA 700 is a reporting standard by ICAI. NFRA is an authority created in the new Companies act, to prescribe standard for accounting and auditing.

SECTION 3: APPENDIX

APPENDIX 1: CHECKLIST FOR APPLICATION CONTROLS

IS Auditor Review of Application Controls					
	Process/Application Name: Business Process Owner:	Date of review:			
Ref	Control Objective and Control Practices Description	Information Objective			
		Completeness	Accuracy	Validity	Authorisation Segregation of Duties
1	Source Data Preparation and Authorisation Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Check whether the source document is a well-designed input form. Detect errors and irregularities so they can be reported and corrected.				
a	Whether the source documents is designed in a way that they increase accuracy with which data can be recorded, control the workflow and facilitate subsequent reference checking? [Where appropriate, include completeness controls in the design of the source documents.]				
b	Whether the procedures for preparing source data entry, and ensure that they are effectively and properly communicated to appropriate and qualified personnel? [These procedures should establish and communicate required authorisation levels (input, editing, authorising, accepting and rejecting source documents). The procedures should also identify the acceptable source media for each type of transaction.]				
c	Whether the function responsible for data entry maintains a list of authorised personnel, including their signatures?				

d	Whether all source documents include standard components and contain proper documentation (e.g., timeliness, predetermined input codes, default values) and are authorised by management?					
e	Whether application automatically assigns a unique and sequential identifier (e.g., index, date and time) to every transaction?					
f	Whether the document that are not properly authorised or are incomplete to the submitting originators for correction, and log the fact that they have been returned is maintained? Whether review of logs periodically done to verify that corrected documents are returned by originators in a timely fashion, and to enable pattern analysis and root cause review?					
2	Source Data Preparation and Authorisation Establish that data input is performed in a timely manner by authorised and qualified staff. Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.					
a	Whether criteria for timeliness, completeness and accuracy of source documents have been communicated? Whether mechanisms are there to ensure that data input is performed in accordance with the timeliness, accuracy and completeness criteria?					
b	Whether pre-numbered source documents for critical transactions are used? Whether application allows identification and listing of missing source documents?					
c	Whether definition for who can input, edit, authorise, accept and reject transactions, and override errors is there? Whether the same is as per roles and responsibilities of individual and record supporting evidence to establish accountability is maintained?					

d	Whether procedures to correct errors, override errors and handle out-of-balance conditions, as well as to follow up, correct, approve and resubmit source documents and transactions in timely manner are defined?					
e	Whether application system generates error messages in a timely manner and as close to the point of origin as possible? Whether the transactions are processed without errors being corrected or appropriately overridden or bypassed? Whether the errors that cannot be corrected immediately logged in an automated suspense log? Whether error logs are reviewed and acted upon within a specified and reasonable period of time?					
f	Whether errors and out-of-balance reports are reviewed by appropriate personnel, followed up and corrected within a reasonable period of time, and that, where necessary, incidents are raised for more senior attention? Whether automated monitoring tools are used to identify, monitor and manage errors?					
g	Whether all source documents are safe stored (either by the business or by IT) for a sufficient period of time in line with legal, regulatory or business requirements?					
3	Accuracy, Completeness and Authenticity Checks Establish that data input is performed in a timely manner by authorised and qualified staff. Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.					
a	Whether the transaction data are verified as close to the data entry point as possible and interactively during online sessions? Whether the transaction data, whether people-generated, system generated or interfaced inputs, are subject to a variety of controls to check for accuracy, completeness and validity?					

b	Whether controls to ensure accuracy, completeness, validity and compliancy to regulatory requirements of data input put in place? Whether validation criteria and parameters should be subject to periodic reviews and conformation?					
c	Whether access control and role and responsibility mechanisms are established so that only authorised persons input, modify and authorise data?					
d	Whether requirements for segregation of duties for entry, modification and authorisation of transaction data as well as for validation rules defined?					
e	Whether report of transactions failing validation generated? Whether report all errors are generated in a timely fashion?					
f	Whether transactions failing edit and validation routines are subject to appropriate follow-up until errors are remediated? Whether information on processing failures is maintained to allow for root cause analysis and help adjust procedures and automated controls?					
4	Processing Integrity and Validity Maintain the integrity and validity of data throughout the processing cycle. Detection of erroneous transactions does not disrupt the processing of valid transactions.					
a	Whether mechanisms to authorise the initiation of transaction processing and to enforce that only appropriate and authorised applications and tools are used defined and put in place?					
b	Whether processing is completed and accurately performed with automated controls? [For example: Controls may include checking for sequence and duplication errors, transaction/record counts, referential integrity checks, control and hash totals, range checks, and buffer overflow.]					

c	Whether transactions failing validation routines are reported and posted to a suspense file? Whether the errors are reported in timely fashion? Whether the information on processing failures is kept to allow for root cause analysis and help adjust procedures and automated controls, to ensure early detection or to prevent errors?					
d	Whether the transactions failing validation routines are subject to appropriate follow-up until errors are remediated or the transaction is cancelled?					
e	Whether there is a unique and sequential identifier to every transaction (e.g., index, date and time)?					
f	Whether an audit trail of transactions processed. Include date and time of input and user identification for each online or batch transaction maintained? Whether there is a listing of sensitive transactions and before and after images maintained, to check for accuracy and authorisation of changes made?					
g	Whether integrity of data during unexpected interruptions in data processing with system and database utilities, maintained? Whether controls are in place to confirm data integrity after processing failures or after use of system or database utilities to resolve operational problems?					
h	Whether any adjustments, overrides and high-value transactions are reviewed promptly in detail for appropriateness by a supervisor who does not perform data entry?					
i	Whether reconciliation of file totals done? [For example, a parallel control file that records transaction counts or monetary value as data should be processed and then compared to master file data once transactions are posted. Identify report and act upon out-of-balance conditions.]					
5	Output Review, Reconciliation and Error Handling Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient, and protected during transmission; that verification, detection and correction of the accuracy of output occurs; and that information provided in the output is used.					

a	Whether the handling and retaining output from IT applications, follow defined procedures and consider privacy and security requirements? Whether procedures for communicating and follow-up defined for distribution of output?					
b	Whether physical inventory of all sensitive output, such as negotiable instruments taken and compared it with inventory records? Whether there are procedures with audit trails to account for all exceptions and rejections of sensitive output documents?					
c	Whether out-of-balance control totals exist and exceptions reported to the appropriate level of management?					
d	Whether procedure exists to check completeness and accuracy of processing before other operations are performed? Whether reuse of electronic output subject to validation check before re-use?					
e	Whether procedures are defined to ensure that the business owners review the final output for reasonableness, accuracy and completeness? Whether the output is handled in line with the applicable confidentiality classification? Whether the potential errors are logged in a timely manner?					
f	Whether for sensitive output, definition exists as to who can receive it? Whether such output is properly labelled for reorganisation?					

APPENDIX 2: ATM AUDIT CHECKLIST

This is provided as soft copy.

APPENDIX 3: APPLICATION SOFTWARE CHECKLIST

This is provided as a soft copy.

APPENDIX 4: USER RIGHTS CREATION CHECKLIST

EMPLOYEE ACCESS RIGHT'S FORM

Form Sl. No.	1				Date
Name:					
Department / Designation					
Name of Security Level:					
Days allowed for Back Dated Entry:					
Cut- off Date for back Dated Vouchers:					
	Put Y /N only				
Reports / Items to ALLOW / DIS-ALLOW	CREATE	ALTER	DISPLAY	PRINT	Remark
ACCOUNTING STANDARDS					
ACCOUNT MASTERS					
ANNEXURE TO AUDIT REPORT CARO					
ATTENDANCE VOUCHERS					
AUDITING AND ASSURANCE STANDARDS					
AUDIT JOURNALS					
AUDIT LISTINGS					
AUDIT PROGRAMS					

Module 6

AUDIT WORKING PAPERS					
BACK DATED VOUCHERS					
BALANCE SHEET					
BANK BOOKS					
BANK RECONCILIATION					
BATCH GOWDOWN SUMMARY					
BATCH SUMMARY					
CASH FLOW					
CHEQUE PRINTING					
CHEQUE REGISTER					
CLIENT/ SERVER RULE					
COMMODITY WISE PURCHASE					
COMMODITY WISE SALES					
COMPANY FEATURES					
CONNECT COMPANY					
COST CENTER DETAILS					
CST PURCHASE REGISTER					
CST REPORTS					
CST SALES REGISTER					
DAY BOOK					
DEALER EXCISE REPORTS					
DEPOSIT SLIP					
EMPLOYEE VOUCHERS					
EXCISE COMPUTATION					
EXCISE ER-1 REPORT					
EXCISE REPORTS					
FBT REPORTS					
FORM 3CA					
FORM 3CB					
FORM 3CD					
FUNDS FLOW					
GROUP MONTHLY SUMMARY					
GROUP OUTSTANDING					
GROUP SUMMARY					

GROUP VOUCHER DETAILS					
IMPORT DATA					
INTEREST CALCULATIONS					
INVENTORY MASTERS					
INVOICE CONFIGURATION					
JOB WORK ANALYSIS					
JOB WORK ORDER DETAILS					
JOB WORK REGISTERS					
JOB WORK STOCK					
LEDGER MONTHLY SUMMARY					
LEDGER OUTSTANDING					
LEDGER VOUCHER DETAILS					
LOCATION-WISE SUMMARY					
MCA REPORTS					
NOTE SUMMARY					
ORDER DETAILS					
OUTSTANDINGS					
OVERRIDE INVOICE CLASS					
OVERRIDE INVOICE DEFAULTS					
PAYMENT ADVICE					
PAYROLL MASTERS					
PAYROLL REPORTS					
PAYROLL VOUCHERS					
PRICE LIST					
PROFIT & LOSS A/C					
PURCHASE REGISTER					
QUICK SETUP					
RECEIPTS & PAYMENTS					
SALES REGISTER					
SCHEDULE VI					
SERVICE TAX REPORTS					
STATUTORY AUDIT					
STOCK CATEGORY OUTSTANDING					
STOCK CATEGORY SUMMARY					

Module 6

STOCK GROUP OUTSTANDING					
STOCK ITEM MONTHLY DETAILS					
STOCK ITEM OUTSTANDING					
STOCK QUERY					
STOCK SUMMARY					
STOCK VOUCHER DETAILS					
SYNCHRONISATION					
SYNC REPORTS					
TALLY.NET FEATURES					
TAX AUDIT					
TCS REPORTS					
TDS REPORTS					
TRACKING NUMBER DETAILS					
TRIAL BALANCE					
VAT COMPUTATION					
VAT PURCHASE REGISTER					
VAT SALES REGISTER					
VOUCHER REGISTER					
VOUCHERS					
VOUCHING DONE					

Prepared by:

Checked By:

Approved By:

Date of Approval

APPENDIX 5: REVIEW OF BUSINESS APPLICATION'S IMPACT ON CONTROLS

IS Auditor Review of Impact of Business Application on Controls						
	Process/Application Name: Business Process Owner:	Date of review:				
Ref	Changes made to business process due to implementation of business application software. Matrix to evaluate whether the new business application has impact on key information objectives to be achieved.	Information Objective. Put Y, to denote negative impact, and N to denote NO / Positive Impact				
		Completeness	Accuracy	Validity	Authorisation	Segregation of Duties
1	Changes to Source Data Preparation and Authorisation.					
2	Changes to Source Data Preparation and Authorisation.					
3	Accuracy, Completeness and Authenticity Checks					
4	Processing Integrity and Validity.					
5	Output Review, Reconciliation and Error Handling					

For all items labelled as 'Y', IS auditor needs to check how the issue has been addressed.

APPENDIX 6: SYSTEM AUDIT REPORT

Sl. No.	Description	Report	
1	Title:	REPORT ON PASSWORD MANAGEMENT SYSTEM	
2	Addressee	CHIEF INFORMATION OFFICER, XYZ LTD.	
3	Description of the scope of the audit, the name of the organisation or component of the organisation to which the subject matter relates, including:	Scope: System Audit of the Password Management Policy. User rights department in HR department.	
	a. Identification or description of the area of activity	Password Management Policy: Implementation and Compliance	
	b. Criteria used as a basis for the IS audit and assurance professional's conclusion	The mandate of management to comment on <i>compliance</i> , suggest methods to improve compliance	
	c. The point in time or period of time to which the work, evaluation or measure of the subject matter relates	Audit period starts from April 1st, 013 and ends on December 31st, 013.	
	d. A statement that the maintenance of an effective internal control structure, including control procedures for the area of activity, is the responsibility of management	The responsibility of implementing proper and effective internal controls in general and specifically in terms of the policy under audit <i>lies with the management</i> .	
4	A statement that the IT audit and assurance professional has conducted the engagement to express an opinion on the effectiveness of control procedures.	The IS Audit method and approach is to express an opinion on <i>existence, effectiveness and continuity of internal controls put in place by the management</i> .	

5	Identification of the purpose for which the IT audit and assurance professional's report has been prepared and of those entitled to rely on it, and a disclaimer of liability for its use for any other purpose or by any other person	The IS Audit has been conducted to help management identify lacunae's in policy implementation. It does not provide and assurance as to the future viability but is a comment on the present state of affairs. The report is for use by management not for external agency.	
6	Description of the criteria or disclosure of the source of the criteria	The report is based on management request to perform an audit of Password Management System, its effective implementation and monitoring.	
7	Statement that the audit has been conducted in accordance with specified IT Audit and Assurance Standards or other applicable professional standards.	The IS Audit has been conducted as per the ISACA ITAF Standards on System Audit and ICAI SA on Audit.	
8	A paragraph stating that because of the inherent limitations of any internal control, misstatements due to errors or fraud may occur and go undetected.	The audit is done as per mentioned standards. The expression on an opinion is subject to inherent limitation of internal controls. These arising from the fact that implemented controls may fail to prevent, detect mis-statement due to errors and frauds. Audit is subject to its limitation, arising from the fact that audit is done on test basis, leaving a possibility of error or fraud going undetected.	
9	An expression of opinion about whether, in all material respects, the design and operation of control procedures in relation to the area of activity were effective.	Based on the information, explanations provided, we comment that: a. Password Management System has not been implemented properly. B. It fails to achieve the purpose. C. Management needs to take the following actions to improve its performance:	
		i. Policy modification: Policy needs to specifically state, that as employee leaves and organisation his/her password shall be immediately disabled.	

		ii. The attendance system of the organisation needs to be joined to the password system. This is necessary to ensure that a password of absent employee is not misused.	
		iii. Employee training is a must, for proper understanding and implementation of policy.	
		Basis of our recommendation as findings during the audit. Findings are enclosed as an annexure to the report.	
10	IT audit and assurance professional's signature	ABC	
11	IT audit and assurance professional's address	ICAI BHAWAN, NEW DELHI	
12	Date of the IT audit and assurance professional's report. In most instances, the dating of the report is based upon applicable professional standards. In other instances, the date of the report should be based on the conclusion of the fieldwork.	01-Jan-14	
Sl. No.	Annexure to System Audit Report		
1	There were 200 employee data available. Of these 175 are working and 5 have left.		
2	The password of employee who had left had not been disabled.		
3	20 Employees did not change their password every 30 days, as defined in policy. 5 were repeat offenders.		
4	50 instances of employee passwords being used when they were absent have been observed.		
	[IS Auditor may add name and detail of employees]		
5	IT audit and assurance professional's signature	ABC	
6	IT audit and assurance professional's address	ICAI BHAWAN, NEW DELHI	

7	Date of the IT audit and assurance professional's report. In most instances, the dating of the report is based upon applicable professional standards. In other instances, the date of the report should be based on the conclusion of the fieldwork.	01-Jan-14	

APPENDIX 7: SAMPLE AUDIT REPORT OF APPLICATION SOFTWARE

This is provided as soft copy.

Module-7

Business Continuity Management

TABLE OF CONTENTS

MODULE 7: BUSINESS CONTINUITY MANAGEMENT (6%)	491
SECTION: OVERVIEW	491
Objective:	491
Task Statements.....	491
Knowledge Statements	492
Relationship of Task Statements with Knowledge Statements.....	492
Task and Knowledge Statements Mapping	492
Knowledge Statement Reference Guide	494
SECTION 2: CONTENTS.....	499
Chapter 1: Business Continuity Management, Business Continuity Planning and Disaster Recovery Planning.....	499
Learning objectives	499
1.1 Introduction	499
1.2 Definitions of key terms.....	501
1.3 Key concepts of Disaster Recovery, Business Continuity Plan and Business Continuity Management.....	502
1.3.1 Contingency Plan (CP)	502
Components of contingency planning.....	502
1. Business impact analysis (BIA)	502
2. Incident response plan (IR plan)	503
3. Business continuity plan (BCP)	503
4. Disaster recovery plan (DRP).....	503
1.3.2 Business Continuity Plan vs. Disaster Recovery Plan	504
1.3.3 Business Continuity Management.....	504
1.4 Objectives of BCM and BCP	504
1.4.1 Objectives of Business continuity plan:	504
1.4.2 Objectives of Business Continuity Management (BCM)	504
Need for BCM at business Level.....	505
Need for BCM at various levels of IT Environment.	506

1.5 What is a disaster?	506
1.5.1 Types of disasters	507
1. Natural disasters	507
2. Man-made disasters	507
1.5.2 Phases of disaster	507
1. Crisis phase	508
2. Emergency response phase	508
3. Recovery phase	508
4. Restoration phase	508
1.5.3 Examples of disaster	508
1.5.4 Impact of disaster	509
1.6 Summary	510
1.7 Questions	510
1.8 Answers and Explanations	512
Chapter 2: Strategies for Development of Business Continuity plan	515
Learning Objectives	515
2.1 Introduction:	515
2.2 Pre-requisites in developing a Business Continuity Plan	516
2.2.1 Phase 1: Business Impact Analysis	517
2.2.2 Phase 2: Risk assessment and methodology of risk assessment	518
Risk Assessment & Recovery	519
Threats and its type	522
Sample checklist for Risk Assessment	523
Risk Assessment Methods	524
1. Risk Ranking	524
2. Value ranges	525
3. Formulae for comparing risks	525
4. Formula Method for Comparing Risks	526
2.2.3 Phase 3: Development of BCP	526
Business Continuity Team	526

Business Continuity Plan	531
2.2.4 Phase 4: Testing of BCP and DRP	533
Testing the Disaster Recovery Plan	533
Sample Recovery Test agenda	534
BCP Testing	534
2.2.5 Phase 5: Training and Awareness	536
Training the Team	536
Training methods	537
2.2.6 Phase 6: Maintenance of BCP and DRP	538
Role of IS Auditor in testing of BCP:	539
2.3 Incident Handling and Management.	539
2.3.1 Incident Response	539
Incident Response Planning for: Before the Incident	539
Incident Response Planning for: Response during the Incident	540
Incident Response Planning for: After the Incident	540
2.3.2 Incident Classification	540
2.3.3 Norms and procedure for declaring an Incident as a Disaster:	541
Collection of data under IRP	541
Reactions to incidents	541
Incident Notifications	541
Documenting an Incident	541
Incident containment strategies	541
Recovering from incident	542
After action review	542
Incident response plan review and maintenance:	542
2.4 Invoking a DR Phase/BCP Phase	542
2.4.1 Operating Teams of contingency planning	542
2.4.2 DRP scope and objectives	543
2.4.3 Disaster recovery phases	544
2.4.4 Key Disaster recovery activities	544

2.4.5	DRP	545
2.4.6	Disaster Recovery Team	545
	General Responsibilities	545
	General Activities	545
	Administrative Responsibilities	546
	Activities by Phase	546
	Supply Responsibilities	546
	Activities by Phase	546
	Public Relations Responsibilities	547
	Activities by Phase	547
	Management Team Call Checklist	547
	Hardware Responsibilities	547
	Activities by Phase	547
	Software Responsibilities	548
	Activities by Phase	548
	Network Responsibilities	549
	Activities by Phase	549
	Operations Responsibilities	549
	Activities by Phase	549
	Salvage Responsibilities	550
	Activities by Phase	550
	New Data Center Responsibilities	551
	Activities by Phase	551
	New Hardware Responsibilities	551
	Activities by Phase	552
	Resumption of Normal Operations	552
2.5	Documentation: BCP Manual and BCM Policy	552
2.5.1	BCM Policy	553
2.5.2	BCP Manual	553
	Elements of BCP Manual	554

2.6 Data backup, Retention and Restoration practices	556
2.6.1 Back up strategies.....	556
Types of Backup	557
2.6.2 Recovery strategies	557
Strategies for Networked Systems.....	558
LAN Systems	558
Wireless LANs	559
Strategies for Distributed Systems	559
Strategies for Data communications.....	559
Strategies for Voice Communications.....	560
2.7 Types of recovery and alternative sites	561
2.7.1 Mirror Site/ Active Recovery Site	561
Mirror site.....	561
Hot Site	561
Cold Site	562
Warm Site.....	562
2.7.2 Offsite Data protection	562
Data Vaults	563
Hybrid onsite and offsite vaulting	563
2.8 System Resiliency Tools and Techniques.....	563
2.8.1 Fault Tolerance	563
2.8.2 Redundant array of inexpensive disks (RAID)	564
2.9 Insurance coverage for BCP	565
2.9.1 Coverage	565
2.9.2 Kinds of Insurance	565
(a) First-party Insurances: Property damages.....	566
(b) First-party Insurances: Business Interruption	566
(c) Third-party Insurance: General Liability	566
(iv) Third-party Insurance: Directors and Officers	567
2.10 Summary.....	567

2.11 Questions	567
2.12 Answers and Explanations	569
Chapter 3: Audit of business Continuity plan	571
Learning Objectives	571
3.1 Introduction	571
3.2 Steps of BCP Process.....	571
3.2.1 Step 1: Identifying the mission or business-critical functions	572
3.2.2 Step 2: Identifying the resources that support critical functions	572
1. Human Resources	572
2. Processing capability	572
3. Automated applications and data	573
4. Computer-based services	573
5. Physical infrastructure	573
6. Documents and papers	573
3.2.3 Step 3: Anticipating potential contingencies or disasters	573
3.2.4 Step 4: Selecting contingency planning strategies	574
3.2.5 Step 5: Implementing the contingency strategies	574
1. Implementation	574
2. Back up.....	574
3. Documentation	574
4. Assigning responsibility	575
5. No. of BC Plans and responsibility	575
3.2.6 Step 6: Testing and Revising	575
3.3 Audit and Regulatory requirements	575
3.3.1 Role of IS Auditor in BCP Audit.....	575
3.3.2 Regulatory requirements	576
Using COBIT best practices for evaluating regulatory compliances.....	576
MEA03 Monitor, Evaluate and Assess Compliance with External Requirements	576
Process Scope	576
Process Purpose	576

Management Practices	577
3.3.3 Regulatory compliances of BCP	578
Basel Committee on E Banking	578
Indian legislations	578
3.4 Using best practices and frameworks for BCP.....	579
3.4.1 COBIT 5	579
DSS04: Manage continuity	579
Process Scope	579
Process Purpose	579
Management Practices and activities.....	579
BAI04: Manage Availability and Capacity	583
Process Scope	583
Process Purpose	583
Management Practices and activities.....	583
3.4.2 ISO 22301: Standard on Business Continuity Management	585
3.3.3 ITIL	586
3.3.4 SSAE 16	586
3.4.3 Audit Tools and Techniques	586
3.4.4 Service Level Agreement.....	587
3.5 Services that can be provided by an IS Auditor in BCM	587
3.6 Summary	588
3.7 References	589
3.8 Questions	590
3.9 Answers and Explanations	592
SECTION 3: APPENDIX	595
Checklists and control matrix.....	595
Appendix 1: Checklist for a Business Continuity Plan and Audit	595
Appendix 2: RCM and audit guidelines for DRP and BRP	599
Appendix 3: Sample of BCP Audit Finding.....	605

MODULE 7: BUSINESS CONTINUITY MANAGEMENT (6%) SECTION: OVERVIEW

Objective:

Provide assurance or consulting services to confirm whether the Business continuity management (BCM) strategy, processes and practices meet organisation requirements to ensure timely resumption of IT enabled business operations and minimize the business impact of a disaster.

Task Statements

- 7.1 Distinguish between Disaster recovery plan, Business Continuity Plan and BCM.
- 7.2 Evaluate the organisation business continuity plan to assess the adequacy and capability to continue essential business operations during the period of an IT or non-IT disruptions.
- 7.3 Applying industry best practices and regulatory requirements as relevant for BCM such as COBIT/ISO, etc.
- 7.4 Map business continuity management practices to organisation requirements, objectives and budgets.
- 7.5 Review the organisation processes of business resilience in the context of BCM.
- 7.6 Identify the business and operational risks inherent in an entity's disaster recovery/business continuity plan.
- 7.7 Assess the process of business Impact analysis.
- 7.8 Identifying recovery strategies and their adequacy to meet business needs.
- 7.9 Assess impact of RPO/RTO on Computer setup and IT Service Design.
- 7.10 Assess adequacy of operations and end-user procedures for managing disruptions and incident management.
- 7.11 Perform various types of tests for different aspects of Business continuity.
- 7.12 Assess adequacy of documentation and maintenance process of BCM.
- 7.13 Assess service level management practices and the components within a service level agreement.
- 7.14 Review monitoring of third party compliance with the organisation controls as relevant to BCM.
- 7.15 Evaluate adequacy of BCP processes and practices to confirm it meets business continuity requirements.
- 7.16 Evaluate organisation BCM practices to determine whether it meets organisation requirements

Knowledge Statements

- 7.1 DRP, BCP and BCM processes and practices and related documentation.
- 7.2 Industry best practices as relevant such as COBIT, ISO standard for BCP/DRP.
- 7.3 IT deployment in organisations and business continuity requirements at various levels of IT such as hardware, network, system software, database software, application software, data, facilities, human resources, etc.
- 7.4 System resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure, etc.).
- 7.5 Business impact analysis (BIA) related to disaster recovery planning.
- 7.6 Development and maintenance of BCM, BCP and DRP.
- 7.7 Problem and incident management practices (e.g., help desk, escalation procedures, tracking).
- 7.8 Analyzing SLA reports and relevant provisions.
- 7.9 Backup & Recovery strategies, Recovery Window, RPO and RTO.
- 7.10 Data backup, storage, maintenance, retention and restoration practices.
- 7.11 Regulatory, legal, contractual and insurance issues related to BCM.
- 7.12 Types of alternate processing sites and methods (e.g. hot sites, warm sites, cold sites).
- 7.13 Processes used to invoke the disaster recovery plans and BCP as relevant.
- 7.14 Testing methods for DRP/BCP and BCM.
- 7.15 Auditing the BCP-DRP plans.

Relationship of Task Statements with 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 and Knowledge Statements Mapping

Task Statements	Knowledge Statements
7.1 Distinguish between Disaster recovery plan, Business Continuity Plan and BCM and related documentation.	7.1 DRP, BCP and BCM processes and practices.
7.2 Evaluate the organisation business continuity plan to assess the adequacy and capability to continue essential business operations during the period of an IT or non-IT disruptions.	7.2 Industry best practices as relevant such as COBIT, ISO standard for BCP/DRP.
	7.3 IT deployment in organisations and business continuity requirements at various levels of IT such as hardware, network, system software, database software,

	application software, data, facilities, HR, etc.
7.3 Applying industry best practices and regulatory requirements as relevant for BCM such as COBIT/ISO,	7.2 Industry best practices as relevant such as COBIT, ISO standard for BCP/DRP.
7.4 Map business continuity management practices to organisation requirements, objectives and budgets.	7.4 System resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure,)
	7.6 Development and maintenance of BCM, BCP and DRP.
	7.5 Business impact analysis (BIA) related to disaster recovery planning.
7.5 Review the organisation processes of business resilience in the context of BCM.	7.5 Business impact analysis (BIA) related to disaster recovery planning.
7.6 Identify the business and operational risks inherent in an entity's disaster recovery/business continuity plan.	7.5 Business impact analysis (BIA) related to disaster recovery planning.
	7.6 Development and maintenance of BCM, BCP and DRP.
7.7 Assess the process of Business Impact Analysis.	7.5 Business Impact Analysis (BIA) related to disaster recovery planning.
7.8 Identifying recovery strategies and their adequacy to meet business needs.	7.6 Development and maintenance of BCM, BCP and DRP.
	7.7 Problem and incident management practices (e.g., help desk, escalation procedures, tracking).
	7.15 BCM documentation and maintenance processes and procedures.
7.9 Assess impact of RPO/RTO on Computer setup and IT Service Design.	7.9 Backup & Recovery strategies, Recovery Window, RPO and RTO.
	7.10 Data backup, storage, maintenance, retention and restoration practices.
7.10 Assess adequacy of operations and end-user procedures for managing disruptions and incident management.	7.13 Processes used to invoke the disaster recovery plans and BCP as relevant.
	7.9 Backup & Recovery strategies, Recovery Window, RPO and RTO
7.11 Perform various types of tests for different aspects of Business continuity.	7.14 Testing methods for DRP/BCP and BCM.
	7.16 Auditing the BCP-DRP plans and participation in Drills.

7.12 Assess adequacy of documentation and maintenance process of BCM.	7.1 BCM, BCP, DRP and related documentation.
	7.10 Data backup, storage, maintenance, retention and restoration practices.
7.13 Assess Service level management practices and the components within a service level agreement.	7.8 Identifying recovery strategies and their adequacy to meet business needs.
7.14 Review monitoring of third party compliance with the organisation controls as relevant to BCM.	7.11 Regulatory, legal, contractual and insurance issues related to BCM.
7.15 Evaluate adequacy of BCP processes and practices to confirm it meets business continuity requirements.	7.9 Backup & Recovery strategies, Recovery Window, RPO and RTO.
	7.10 Data backup, storage, maintenance, retention and restoration practices
	7.12 Types of alternate processing sites and methods (e.g., Near site, hot sites, warm sites, cold sites)
	7.1 BCM, BCP, DRP and relate documentation.
7.16 Evaluate organisation BCM practices to determine whether it meets organisation requirements.	7.14 Testing methods for DRP/BCP and BCM.
	7.15 Auditing the BCP and DRP plans.
	7.13 Processes used to invoke the disaster recovery plans and BCP as relevant.

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.

KS 7.1 DRP, BCP, BCM processes and practices and related documentation.

Key Concepts	Reference
Understand the difference between BCP, DRP and BCM process	1.1, 1.2, 1.3
Understand the meaning of Disaster, threat.	1.5, 1.5, 1.7

Understand the objectives and need for a BCM.	1.2, 1.3, 1.4

KS 7.2 Industry best practices as relevant such as COBIT, ISO standard for BCP/DRP

Key Concepts	Reference
Understand regulatory requirements and guidance on BCP best practices	3.3 and 3.4
Understand the guidance given by frameworks to facilitate better BCP.	3.3 and 3.4

KS 7.3 IT deployment in organisations and business continuity requirements at various levels of IT such as hardware, network, system software, database software, application software, data, facilities, HR, etc.

Key Concepts	Reference
Understand the BCP Requirements at various level of the IT Infrastructure and the criticality of the functions of each level.	1.2, 1.3, 1.4

KS 7.4 System resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure, etc.)

Key Concepts	Reference
Understand preventive controls that will help in reducing risk of disasters.	2.6 and 2.8

KS 7.5 Business impact analysis (BIA) related to disaster recovery planning

Key Concepts	Reference
Understand the BIA as a key driver of the BCP/DR Process.	1.3, 2.2

KS 7.6 Development and maintenance of BCM, BCP and DRP

Key Concepts	Reference
Understand the process for developing a BCP/DCP.	1.2, 1.3, 1.4, 2.2, 2.4, 2.7

Module 7

Understanding the maintenance process of a BCP/DRP and to check the validity of the plan in updating technologies.	1.2, 1.3, 1.4, 2.2, 2.4, 2.7

KS 7.7 Problem and incident management practices (e.g., help desk, escalation procedures, tracking)

Key Concepts	Reference
Understand the need of having an Incident Management Process.	1.2, 1.3, 1.5, 2.2

KS 7.8 Analyzing SLA reports and relevant provisions

Key Concepts	Reference
Understand the meaning of Service Level Agreement (SLA) and ensure that the services provided by the Vendor are at par to the provisions mentioned in the SLA.	3.2

KS 7.9 Backup & Recovery strategies, Recovery Window, RPO and RTO

Key Concepts	Reference
Understand the Backup and Recovery Strategies, critical recovery time period.	2.2, 2.6, 3.2

KS 7.10 Data backup, storage, maintenance, retention and restoration practices

Key Concepts	Reference
Understand the corrective controls for backup, rerun and restoration practices.	2.6, 3.2, 3.4

KS 7.11 Regulatory, legal, contractual and insurance issues related to BCM

Key Concepts	Reference
Understand the regulatory, legal, contractual issues and compliances related to BCM.	3.3, 3.4
Understand the types of Insurance that is available.	2.9

KS 7.12 Types of alternate processing sites and methods (e.g. hot sites, warm sites, cold sites)

Key Concepts	Reference
Understand the different types of alternate processing points and need for having the correct site.	2.9

KS 7.13 Processes used to invoke the disaster recovery plans and BCP as relevant.

Key Concepts	Reference
Understand the processes to initiate a DR process for restoration of uptime of IT Services at the time of the happening of a critical incident.	2.4, 3.3, 2.9
Understand the process to initiate a BCP following a DR Process for complete restoration of Core Business Operations.	2.4, 3.3, 2.9

KS 7.14 Testing methods for DRP/BCP and BCM

Key Concepts	Reference
Understand the different types of tests for concluding whether the BCP; DR plans are relevant for the entity.	2.2

KS 7.15 Auditing the BCP and DRP plans

Key Concepts	Reference
Understand the Audit of a BCP/DRP Plan.	2.2, 3.3, 3.5
Understanding the Audit of Test of a BCP/DRP Plan.	2.2, 3.3, 3.5

SECTION 2: CONTENTS

CHAPTER 1: BUSINESS CONTINUITY MANAGEMENT, BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

Learning objectives

The objective of this chapter is to provide knowledge about the key concepts of Business Continuity Management (BCM), Business Continuity Planning (BCP), Disaster Recovery Planning (DRP), Incident Responses, Contingency plan and disaster. It is important to understand these concepts as they form the base for the content that is explained in Chapters 2 and 3. DISA candidate is expected to have understanding of the key terms related concepts as this is critical for designing, implementing or reviewing business continuity. A good understanding and working knowledge in this area will help DISAs to provide assurance and consulting services in this area.

1.1 Introduction

Information is said to be the currency of the 21st century and it is considered the most valuable asset of an organisation. This is more so in case of organisations which use and are heavily dependent on Information Technology (IT). Organisations in this modern era run their business based on information which are processed using Information and Communication Technology (ICT). The ICT plays a central role in the operation of the business activities. For example, the stock market is virtually paperless. Banks and financial institutions have become online, where the customers rarely need to set foot in the branch premises. There is a heavy dependence on real time information from information technology assets for conducting business. Information is a critical factor for continued success of the business. This dependence on Information is more explicit in the most organisations which are now dependent on IT for performing their regular business operations. We can understand the criticality of IT by imagining impact of failure or non-availability of IT in case of following types of organisations:

- Bank using Core banking solution with a million accounts, credit cards, loans and customers.
- Companies using centralized ERP software having operations in multiple locations.
- An airline serving customers on flights daily using IT for all operations.
- Pharmacy system filling millions of prescriptions per year (some of the prescriptions are life-saving).

- Automobile factory producing manufacturing hundreds of vehicles daily using automated solution.
- Railways managing thousands of train routes and passengers through automated ticketing and reservation.

The above situations clearly demonstrate the heavy dependence on IT systems. IT can fail due to multiple factors. Hence, organisations should have appropriate contingency plans for resuming operations from disruption. The disruption of business operation can be due to unforeseen man-made or natural disaster and this may lead to loss of productivity, revenue and market share among many other impacts. Hence, organisations have to take necessary steps to ensure that the impact from such disasters is minimized and build resilience which ensures continuity of critical operation in the event of disruptions. Modern organisations cannot think of running their business operations without IT. IT is prone to increased risks which can lead to failure of IT thus impacting operations. Hence, it is becoming increasingly important for organisations to have a business contingency plan for their Information Systems.

The criticality of the plan can be determined based on the level of impact on critical business operations due to failure or non-availability of IT impacting service delivery. The failure of IT could be caused due to any or more of the following:

- Server or network failure
- Disk system failure
- Hacker break-in
- Denial of Service attack
- Extended power failure
- Snow storm, earthquake, tornado or fire
- Spyware, malevolent virus or worm
- Employee error or revenge
- Sabotage or theft

Organisations worldwide are more and more dependent on computers, in assisting and carrying out the decision making processes and in recording business transactions. An organisation is extremely dependent on several I.S. resources like computers, employees, Servers and communication links. If any of these resources are not available, the organisation will not be able to function at its full strength. The longer one or more of these resources are unavailable, the longer it takes the organisation to get back to its original state. Sometimes, organisations can never get back to its original state. As a result, it becomes important to have a tested plan for the disaster

recovery, more importantly, in the information system area to ensure business continuity. The organisations that think ahead have a better chance of survival always.

1.2 Definitions of key terms

The concepts of Business Continuity Management are quite simple to understand. However, to understand and implement BCM or BCP as per needs of organisation requirements, it is know the key terms. Knowledge of definition of these terms will help not only in understanding the topics but also to provide assurance, consulting or implementation services in this area.

Business Continuity Planning: Business continuity planning is the process of developing prior arrangements and procedures that enable an organisation to respond to an event in such a manner that critical business functions can continue within planned level of disruption. The end result of the planning is called a Business Continuity Plan.

Business Continuity Plan: A documented collection of procedures and information that is developed compiled and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical products and services at an acceptable predefined level.

Business Continuity Management: A holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats – if realized – might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stake holders, reputation, brand, and value-creating activities.

Business Impact Analysis: The process of analyzing functions and the effect that a business disruption might have upon them.

Contingency Plan: A plan to deal with specific set of adverse circumstances.

Crisis: An abnormal situation which threatens the operations, staff, customers or reputation of the organisation.

Disaster: A physical event which interrupts business processes sufficiently to threaten the viability of the organisation.

Disaster Recovery Planning: A disaster recovery plan (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.

Emergency Management Team (EMT): This team comprising of executives at all levels including IT is vested with the responsibility of commanding the resources which are required to recover the enterprises operations.

Incident: An event that has the capacity to lead to loss of or a disruption to an organisation's operations, services, or functions – which, if not managed, can escalate into an emergency, crisis or disaster.

Incident Management Plan: A clearly defined and documented plan of action for use at the time of an incident, typically covering the key personnel, resources, services and actions needed to implement the incident management process.

Minimum Business Continuity Objective (MBCO): This refers to the minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during an incident, emergency or disaster. As per ISO 22301:2012, clause 3.28, MBCO is the minimum level of services and/or products that is acceptable to the organizations to achieve its business objectives during a disruption. MBCO is used to develop test plan for testing BCP.

Maximum Acceptable Outage (MAO): This is the time frame during which a recovery must become effective before an outage compromises the ability of an Organization to achieve its business objectives and/or survival. This refers to the maximum period of time that an organization can tolerate the disruption of a critical business function, before the achievement of objectives is adversely affected. MAO is also known as maximum tolerable outage (MTO), maximum downtime (MD). Maximum Tolerable Period Downtime (MTPD).

Resilience: The ability of an organisation to resist being affected by the incident.

Risk: The combination of the probability of an event and its consequence.

Vulnerability: The degree to which a person, asset, process, information, infrastructure or other resources are exposed to the actions or effects of a risk, event or other occurrence.

1.3 Key concepts of Disaster Recovery, Business Continuity Plan and Business Continuity Management

1.3.1 Contingency Plan (CP)

An organisation's ability to withstand losses caused by unexpected events depends on proper planning and execution of such plans. Without a workable plan, unexpected events can cause severe damage to information resources and may affect the business continuity. Contingency planning is an overall process of preparing for unexpected events. Its main goal is to restore normal modes of operation with minimal cost and minimal disruption to normal business activities after unexpected event. It should ideally ensure continuous information systems availability despite unexpected events.

Components of contingency planning

1. Business impact analysis (BIA)

BIA includes tasks like Threat Attack identification and prioritization, Business unit analysis, Attack scenario development, Potential damage assessment, etc. The steps involved in impact analysis

are risk evaluation, defining critical functions in the organisation, identifying critical facilities required for providing recovery of the critical functions and their interdependencies and finally setting priorities for all critical business applications which need to be recovered within defined timelines. The details of this concept have been highlighted in 2.4.

2. Incident response plan (IR plan)

IR Plan includes tasks like incident planning, incident detection, incident reaction, incident recovery etc. Incident Response plan gives an entity a set of procedures and guidelines that is needed by an entity to handle an incident. The details of this concept have been highlighted in 2.8.

3. Business continuity plan (BCP)

BC Plan includes tasks like establishing continuity strategies, planning for continuity of critical operations, continuity management etc. Business Continuity Plan is a plan that contains the steps that would be taken by an entity to resume its business functions during its period of disruption. These plans are executed in parallel with the disaster recovery plans depending on the impact of the disaster. Business Continuity Plans on a whole is about re-establishing existing business processes and functions, communications with the business contacts and resuming business processes at the primary business location.

4. Disaster recovery plan (DRP)

DR Plan includes tasks like plan for disaster recovery, crisis management, recovery operations etc. Disaster Recovery Plan is the set of plans which are to be executed initially at the moment of crisis. These plans include measures to control the disaster, mitigate them and to initiate the recovery of the resources that is needed for the continuity of business. These plans are targeted to initiate/recover the resources that have been affected by a disaster. These are the first plans that would be executed at the time of disaster.

There are three basic strategies that encompass a disaster recovery plan: preventive measures, detective measures, and corrective measures. Preventive measures will try to prevent a disaster from occurring. These measures seek to identify and reduce risks. They are designed to mitigate or prevent an event from turning into a disaster. These measures may include keeping data backed up and off site, using surge protectors, installing generators and conducting routine inspections. Detective measures are taken to discover the presence of any unwanted events within the IT infrastructure. Their aim is to uncover new potential threats. They may detect or uncover unwanted events. These measures include installing fire alarms, using up-to-date antivirus software, holding employee training sessions, and installing server and network monitoring software. Corrective measures are aimed to restore a system after a disaster or otherwise unwanted event takes place. These measures focus on fixing or restoring the systems after a disaster and may include keeping critical documents in the DRP or securing proper insurance policies.

1.3.2 Business Continuity Plan vs. Disaster Recovery Plan

The primary objective of Business Continuity Plan is to ensure that mission critical functions and operations are recovered and made operational in an acceptable time frame. A BCP aims to sustain critical business process during an unplanned interruption period and a DRP is to re-establish the primary site into operation with respect to all business processes of the organisation facing the disaster.

1.3.3 Business Continuity Management

BCM is a holistic process that identifies potential threats and the impacts on normal business operations should those threats actualize. BCM provides a framework to develop and build the organisation's resilience with the capability for an effective response, therefore ensuring that critical objectives are met, safeguarding key stakeholder's interests and the organisation's reputation, brand and value creating activities. The purpose of BCM is to minimize the operational, financial, legal, reputational and other material consequences arising from a disruption due to an undesired event (Basel Committee on Banking Supervision, 2005), minimizing losses and restoring normal, regular operations in the shortest, possible time. Coupled with security measures to protect the organisation's assets, BCM requires plans and strategies that should cater for and allow responses, contingency plans and procedures to recover as quickly as possible. BCM looks at an entirety of the businesses of the entity as a whole. It is a continuous process whereby risks which are inherent to the business are closely monitored and mitigated.

1.4 Objectives of BCM and BCP

1.4.1 Objectives of Business continuity plan:

The primary objective of a Business Continuity Plan (BCP) is to enable an organisation to continue to operate through an extended loss of any of its business premises or functions.

The key objectives of BCP are:

- Manage the risks which could lead to disastrous events.
- Reduce the time taken to recover when an incident occurs and
- Minimize the risks involved in the recovery process.
- Reduce the costs involved in reviving the business from the incident.

1.4.2 Objectives of Business Continuity Management (BCM)

The objective of BCM is to counteract interruptions to business activities and to protect critical business processes from the impact of major failures or disasters. The detailed objectives of BCM are:

- Reduce likelihood of a disruption occurring that affects the business through a risk management process.
- Enhance organisation's ability to recover following a disruption to normal operating conditions.
- Minimize the impact of that disruption, should it occur.
- Protect staff and their welfare and ensure staff knows their roles and responsibilities.
- Tackle potential failures within organisation's I.S. Environment
- Protect the business.
- Preserve and maintain relationships with customers.
- Mitigate negative publicity.
- Safeguard organisation's market share and/or competitive advantage.
- Protect organisation's profits or revenue and avoid financial losses.
- Prevent or reduce damage to the organisation's reputation and image.

Need for BCM at business Level

The need for BCM arises because of the following present day requirements of business

- Need to provide access to potentially millions of new customers.
- Need to ensure security, privacy and confidentiality.
- Need to integrate business processes onto web.
- Need to integrate business partners into key business processes.
- Increased pressure on delivering quality customer service 24x7.
- Emerging pervasive computer devices.

Business and organisations of today depend heavily on Information and Communication Technology (ICT) to conduct business. The ICT plays a central role in the operation of the business activities. For example, the stock market is virtually paperless. Banks and financial institutions have become online, where the customers rarely need to set foot in the branch premises. This dependence on the systems means that all organisations should have contingency plans for resuming operations from disruption. The disruption of business operation can be due to unforeseen manmade or natural disaster that may result into revenue loss, productivity loss and loss of market share among many other impacts. Thus organisations have to take necessary steps to ensure continuity of operation in the event of disruptions. Business continuity is the activity performed by an organisation to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions. These activities include many daily chores such as project management, system backups, change control, and help desk. Business continuity is not something implemented at the time of a disaster;

Business Continuity refers to those activities performed daily to maintain service, consistency, and recoverability.

Need for BCM at various levels of IT Environment.

Disaster Recovery is an essential phase to critical IT Resources. IT Infrastructure generally includes Servers, Workstations, Network and Communication, Operating system software, business applications software, essential utility software, Data Centers, Support Desks, IT Personnel, Disks, Tapes etc. In this technologically driven world, IT Infrastructure has essentially become an integral part of an entity's anatomy. Mail Servers and communication lines like Internet, Phone and Fax are also essentially the important components of the Infrastructure. It is therefore critical to get these components up and running for a successful recovery of the business. Therefore when critical industries like Banks, Insurance Companies, Stock Exchanges, Airline Companies, Railways, Multinational Companies, Government Agencies rely on IT Infrastructure for its daily operations, it is crucial to maintain BCM for such organisations. Software like the Core Banking Systems, SWIFT Financial Messaging Services, Airline Communication Services like AMADEUS, Stock Market Trading Applications, ERP Systems, e-commerce sites and many more are critical where no downtime is tolerated. These applications are used to conduct transactions worldwide and are run only on extensive IT Resources. BCM therefore is a much needed requirement for a quick recovery from a crisis to ensure survival of the business.

1.5 What is a disaster?

BCM or BCP is all about planning in advance to meet future unforeseen events which may impact or disrupt business operations. Disasters are the major source of disruptions. As distinguished from an event which causes disruption for a short period of time and addressed through incident management plan, disaster are of various types and can have varying and serious impact. This section will provide an overview of various types of disasters.

A disaster can be defined as an unplanned interruption of normal business process. It can be said as a disruption of business operations that stops an organisation from providing critical services caused by the absence of critical resources. An occurrence of disaster cannot always be foreseen; hence we need to be prepared for all the types of disasters that can arise, handle them effectively in the shortest time.

Vulnerabilities are also a major cause or source of disasters. Vulnerabilities are weaknesses associated with an organisation's assets. These weaknesses may be exploited by a threat causing unwanted incidents that may result in loss, damage or harm to those assets. Vulnerability in itself does not cause harm; it is merely a condition or set of conditions that may allow a threat to affect an asset. Vulnerability is weakness of an asset or group of assets, which can be exploited by a threat. As part of risk assessment exercise, it is important to understand the various vulnerabilities and threats and coupled with probability, organisation can assess the impact. This will be evaluated

in business impact analysis and mitigated appropriately by implementing appropriate counter measures. In contemporary academia, disasters are seen as the consequence of inappropriately managed risk. These risks are the product of a combination of both hazard/s and vulnerability. Hazards that strike in areas with low vulnerability will never become disasters, as is the case in uninhabited regions.

1.5.1 Types of disasters

A disaster can be natural or man-made (or technological) hazard resulting in an event of substantial extent causing significant physical damage or destruction, loss of life, or drastic change to the environment. A disaster can be defined as any tragic event stemming from events such as earthquakes, floods, catastrophic accidents, fires, or explosions. It can cause damage to life and property and destroy the economic, social and cultural life of people. For a clearer understanding of the concept of disasters, disasters can be classified into two major categories as:

1. Natural disasters
2. Man-made disasters

1. Natural disasters

Natural Disasters are those which are a result of natural environment factors. A natural disaster has its impact on the business's that is present in a geographical area where the natural disaster has struck. Natural disasters are caused by natural events and include fire, earthquake, tsunami, typhoon, floods, tornado, lightning, blizzards, freezing temperatures, heavy snowfall, pandemic, severe hailstorms, volcano etc.

2. Man-made disasters

Man-made disasters are artificial disasters which arise due to the actions of human beings. Artificial disasters has its impact on a business entity specific to which it has occurred. Artificial disasters arising due to human beings Include Terrorist Attack, Bomb Threat, Chemical Spills, Civil Disturbance, Electrical Failure, Fire, HVAC Failure, Water Leaks, Water Stoppage, Strikes, Hacker attacks, Viruses, Human Error, Loss Of Telecommunications, Data Center outage, lost data, Corrupted data, Loss of Network services, Power failure, Prolonged equipment outage, UPS loss, generator loss and anything that diminishes or destroys normal data processing capabilities.

1.5.2 Phases of disaster

It is important to envisage what is the impact when a disaster strikes and decide in advance the action to be taken for various types of disaster scenarios. A typical disaster will consist of some or all of the following phases:

1. Crisis phase

2. Emergency response phase
3. Recovery phase
4. Restoration phase

1. Crisis phase

The Crisis Phase is under the overall responsibility of the Incident Control Team (ICT). It comprises the first few hours after a disruptive event starts or the threat of such an event is first identified; and is caused by, for example:

- Ongoing physical damage to premises which may be life threatening, such as a fire; or
- Restricted access to premises, such as a police cordon after a bomb incident. During the crisis phase, the fire and other emergency evacuation procedures (including bomb threat and valuable object removal procedures) will apply; and the emergency services should be summoned as appropriate.

2. Emergency response phase

The Emergency Response Phase may last from a few minutes to a few hours after the disaster. It will start near the end of, or after, the crisis Phase if there has been one, or when a potentially threatening situation is identified. During the Emergency Response Phase, the Business Continuity Team (BCT) will assess the situation; and decide if and when to activate the BCP.

3. Recovery phase

The Recovery Phase may last from a few days to several months after a disaster and ends when normal operations can restart in the affected premises or replacement premises, if appropriate. During the recovery phase, essential operations will be restarted (this could be at temporary premises) by one or more recovery teams using the BCP; and the essential operations will continue in their recovery format until normal conditions are resumed.

4. Restoration phase

This phase restores conditions to normal. It will start with a damage assessment, usually within a day or so of the disaster, when the cause for evacuation or stopping of operations has ended, normal working will be restarted. During the restoration phase, any damage to the premises and facilities will be repaired.

1.5.3 Examples of disaster

Some examples of disasters and the phases that may impact disaster phases of a business continuity plan are:

Examples of Disaster	Phases
Serious fire during working Hours	All phases in full
Serious fire outside during working hours	All the phases, however, no staff and public evacuation
Very minor fire during working hours	Crisis Phase only, staff and public evacuation but perhaps no removal of valuable objects, Fire Service Summoned to deal with the fire
Gas mail leak outside during working hours, repaired after some hours	Only emergency response phase is appropriate

1.5.4 Impact of disaster

The impact of a disaster can vary and could result in:

- Total destruction of the premises and its contents. For example as a result of a terrorist attack;
- Partial damage, preventing use of the premises. For example through flooding; or
- No actual physical damage to the premises but restricted access for a limited period, such as enforced evacuation due to the discovery nearby of an unexploded bomb.

The impact of a disaster may result in one or more of the following:

- ii. **Loss of human life:** The extent of loss depends on the type and severity of the disaster. Protection of human life is of utmost importance and, the overriding principle behind continuity plans.
- iii. **Loss of productivity:** When a system failure occurs, employees may be handicapped in performing their functions. This could result in productivity loss for the organisation.
- iv. **Loss of Revenue:** For many organisations like banks, airlines, railways, stock brokers, effect of even a relatively short breakdown may lead to huge revenue losses.
- v. **Loss of Market share:** In a competitive market, inability to provide services in time may cause loss of market share. For example, a prolonged non-availability of services from services providers, such as Telecom Company or Internet Service Providers, will cause customers to change to different service providers.
- vi. **Loss of goodwill and customer services:** In case of a prolonged or frequent service disruption, customers may lose confidence resulting in loss of faith and goodwill.
- vii. **Litigation:** Laws, regulations, contractual obligation in form of service level agreement govern the business operations. Failure in such compliance may lead the company to legal litigations and lawsuits.

When considering the impact of a disaster, it should be remembered that it will never happen at a convenient time; and is always unpredictable. There is no way of knowing:

- When it will happen;
- What form it will take;
- How much damage it will cause; or
- How big the impact will be.

However, it is important to envisage various types of scenarios to ensure that the coverage is as comprehensive as feasible covering various types of events with varying impact. Understanding disaster and their impact is the key to successful business impact analysis which will result to preparation of an effective business continuity plan.

1.6 Summary

This chapter has provided an overview of the key concepts relating to management of BCP, DRP and Incident Responses. Together, these are to be implemented as part of Business Continuity management. The ultimate objective of a BCM is to recover from a crisis as fast as possible and at the lowest possible cost. Business Continuity is applicable to organisations of all sizes and types of business. Business Continuity is most crucial to organisations which use IT Resources for their critical business functions. We have also understood that the need for BCP arises due to a disruptive event which could be result in a disaster. Disaster is an event that causes interruption to the ongoing business functions which is either natural or man-made. The phases of a disaster crisis phase, emergency response phase, recovery phase and restoration phase have also been discussed.

1.7 Questions

1. An organisation's disaster recovery plan should address early recovery of:
 - A. All information systems processes.
 - B. All financial processing applications.
 - C. Only those applications designated by the IS Manager.
 - D. Processing in priority order, as defined by business management.
2. Which of the following is MOST important to have in a disaster recovery plan?
 - A. Backup of compiled object programs
 - B. Reciprocal processing agreement
 - C. Phone contact list
 - D. Supply of special forms

3. Which of the following BEST describes difference between a DRP and a BCP? The DRP:
 - A. works for natural disasters whereas BCP works for unplanned operating incidents such as technical failures.
 - B. works for business process recovery and information systems whereas BCP works only for information systems.
 - C. defines all needed actions to restore to normal operation after an un-planned incident whereas BCP only deals with critical operations needed to continue working after an un-planned incident.
 - D. is the awareness process for employees whereas BCP contains procedures to recover the operation.
4. The MOST significant level of BCP program development effort is generally required during the:
 - A. Early stages of planning.
 - B. Evaluation stage.
 - C. Maintenance stage.
 - D. Testing Stage.
5. Disaster recovery planning for a company's computer system usually focuses on:
 - A. Operations turnover procedures.
 - B. Strategic long-range planning.
 - C. The probability that a disaster will occur.
 - D. Alternative procedures to process transactions.
6. An unplanned interruption of normal business process is?
 - A. Risk
 - B. Vulnerability
 - C. Disaster
 - D. Resilience
7. Which of the following strategy does not encompass disaster recovery plan?
 - A. Preventive
 - B. Detective
 - C. Corrective
 - D. Administrative
8. Which of the following is not a fundamental of BCP?

- A. Manage the risks which could lead to disastrous events.
 - B. Minimize the risks involved in the recovery process.
 - C. Reduce the costs involved in reviving the business from the incident
 - D. Mitigate negative publicity
9. Which phase starts with a damage assessment?
- A. Crisis Phase
 - B. Emergency Response Phase
 - C. Recovery Phase
 - D. Restoration Phase
10. Which of the following is of utmost important during an impact of disaster?
- A. Loss of Productivity
 - B. Loss of Revenue
 - C. Loss of Human Life
 - D. Loss of Goodwill & Market Share

1.8 Answers and Explanations

1. D. Business management should know what systems are critical and when they need to process well in advance of a disaster. It is their responsibility to develop and maintain the plan. Adequate time will not be available for this determination once the disaster occurs. IS and the information processing facility are service organisations that exist for the purpose of assisting the general user management in successfully performing their jobs.
2. A. Of the choices, a backup of compiled object programs is the most important in a successful recovery. A reciprocal processing agreement is not as important, because alternative equipment can be found after a disaster occurs. A phone contact list may aid in the immediate aftermath, as would an accessible supply of special forms, but neither is as important as having access to required programs.
3. C. The difference pertains to the scope of each plan. A disaster recovery plan recovers all operations, whereas a business continuity plan retrieves business continuity (minimum requirements to provide services to the customers or clients). Choices A, B and D are incorrect because the type of plan (recovery or continuity) is independent from the sort of disaster or process and it includes both awareness campaigns and procedures.
4. A. A company in the early stages of business continuity planning (BCP) will incur the most significant level of program development effort, which will level out as the BCP program moves into maintenance, testing and evaluation stages. It is during the planning

stage that an IS Auditor will play an important role in obtaining senior management's commitment to resources and assignment of BCP responsibilities.

5. D. It is important that disaster recovery identify alternative processes that can be put in place while the system is not available.
6. C. Disaster is event which interrupts business processes sufficiently to threaten the viability of the organisation. Risk is a combination of the probability of an event and its consequence. Vulnerability is the degree to which a person, asset, process, information, infrastructure or other resources are exposed to the actions or effects of a risk, event or other occurrence. Resilience is the ability of an organisation to resist being affected by the incident.
7. D. There are three basic strategies that encompass a disaster recovery plan: preventive measures, detective measures, and corrective measures. Preventive measures will try to prevent a disaster from occurring. These measures seek to identify and reduce risks. Detective measures are taken to discover the presence of any unwanted events within the IT infrastructure. Their aim is to uncover new potential threats. Corrective measures are aimed to restore a system after a disaster or otherwise unwanted event takes place.
8. D. Mitigate negative publicity is an objective of Business continuity management is to rest all are the fundamental aim of BCP.
9. D. Restoration phase will start with a damage assessment, usually within a day or so of the disaster, when the cause for evacuation or stopping of operations has ended, normal working will be restarted. During the Restoration Phase, any damage to the premises and facilities will be repaired.
10. C. Protection of human life is of utmost importance and, the overriding principle behind continuity plans. Rest all are to be considered later.

CHAPTER 2: STRATEGIES FOR DEVELOPMENT OF BUSINESS CONTINUITY PLAN

Learning Objectives

This chapter forms the core of Business Continuity Management (BCM). The objective of this chapter is to provide understanding on how to design a Business Continuity Plan (BCP). The key steps of BCP such as Business Impact Analysis, performing risk assessment and designing tests for the BCP are explained. BCP requires planning in advance and planning requires extensive documentation and communication so that implementation happens as per plan. Specific aspects of BCP which need to be documented are explained with sample contents, steps and procedures. These cover BCP manual, backup and recovery strategies, recovery and alternate sites, other strategies and types of insurance requirements. Critical events such as how and when to invoke a disaster recovery plan and the specific tasks and responsibilities are explained. This chapter explains what management has to do in case of BCP. A thorough knowledge of these topics will help DISAs will help them to perform a BCP Audit or providing consulting services on any/all aspects of BCP. BCP audit is explained in next chapter.

2.1 Introduction:

An organisation's ability to weather losses caused by unexpected events depends on proper planning and execution of such plans. Without a workable plan, unexpected events can cause severe damage to information resources and assets. Normally businesses that don't have a disaster plan go out of business after a major loss like a fire, a break-in, or a storm. A formal policy provides the authority and guidance necessary to develop an effective Business Continuity plan. The Business Impact Analysis helps to identify and prioritize critical *IT systems and components*. *It also helps to identify the control measures to be in place to reduce the effects of system disruptions*, to increase system availability and to reduce contingency life cycle costs. Developing planned recovery strategies ensures that critical information systems are recovered quickly and effectively following a disruption. Business impact analysis helps organisations in choosing the right recovery strategies. The BCP should contain detailed guidance and procedures to be followed till the restoration of damaged system. *Testing* the plan identifies planning gaps, whereas recovery plan helps in training the personnel for plan activation; both activities improve plan effectiveness and overall organisation preparedness. BCP should be a living document that is updated regularly as per defined policy.

2.2 Pre-requisites in developing a Business Continuity Plan

Regulatory and stakeholder requirements mandate the responsibility on the management of all organisations to ensure that all critical business processes are identified; risks associated with the processes are determined, adequate measures of redundancy are built in and around the processes, to minimize the effect of loss, should there be a disaster. Understanding of regulatory requirements as applicable through various legislations applicable in the international scenario like Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II), Sarbanes-Oxley, HSPD-12, BASEL II, Gramm-Leach-Bliley are essential in developing BCP. Most of the global best practices and frameworks such as COBIT, ISO 27001 and ISO 22301 emphasize the critical need of BCP for organisations.

A BCP cannot be considered as a project which is completed within specified time. BCP has to be a continuous process and has to be an integral part of the day to day business processes. BCP to be effective has to be tested and updated regularly and at least once a year, if not more frequently. Critical business functions may keep changing and hence a plan that does not keep pace with the changes in the organisation is not of any use. Therefore, one may have a working BCP on a given day, but the BCP has to be a continuous affair to ensure success.

The primary objectives of a BCP are to guide an organisation in the event of a disaster and to effectively re-establish critical business operations within the shortest possible period of time with minimal loss of data. The pre-requisite in developing a BCP includes planning for all phases and making it part of business process by assigning responsibility to specific business process owners. The goals of planning the project are to assess current and anticipated vulnerabilities, define the requirements of the business and IT, design and implement risk mitigation procedures and provide the organisation with a BCP that will enable it to react quickly and efficiently in event of a disaster.

The objectives of planning the project is to gain an understanding of the existing and planned future IT environment of the organisation, define the scope of the project, develop the project schedule, and identify risks to the project. In addition, a project sponsor/champion and steering committee should be established. The project sponsor or champion should be a member of senior management team with required authority to push the project to completion. The steering committee should be responsible for guiding the project team. The committee should have members from both functional and IT departments. Further, a project manager and / or a BCP coordinator should be appointed to lead, monitor completion and maintain the project. In implementing a BCP project, the key tasks are:

- Define the scope of the planning effort.
- Develop a plan framework.
- Assemble a project team and conduct awareness sessions.

Just as every organisation is unique, so too is the business continuity planning project. As such each plan should be tailored to the individual organisation, what works for one organisation may not necessarily work for another. The major phases in developing a BCP are:

1. Business Impact Analysis,
2. Risk Assessment,
3. Actual Planning and design of the BCP and the BCP Manual i.e., development of BCP
4. Testing of the BCP,
5. Training and awareness to the employees and
6. Maintenance of the BCP.

2.2.1 Phase 1: Business Impact Analysis

The business impact analysis (BIA) establishes the needs of an organisation for recoverability and sets the requirements for its recovery strategy and ultimately its recovery plan. The BIA also can be used to achieve other objectives within an organisation. Firstly, a BIA can be used to prioritize the recovery sequence of data, infrastructure, etc. Secondly, a BIA can define the minimum operating requirements a business needs to recover operations following a disruption. These things include Information Technology resources, human capital, etc. Thirdly, a BIA presents the value proposition for implementing the appropriate level of recoverability. If it can be demonstrated that a disruption of certain number of minutes, hours or days will have effect on a company's reputation, finances and operations, then simple prudence calls for an organisational response, in the form of both recovery plan and recovery infrastructure, i.e., a plan to prevent disruption or to mitigate its impact. The broad outline of a strategy should be apparent in BIA results. A BIA presents requirements for disaster recovery plans. The narrative outline for a BIA strategy could be as follows:

1. We rely on the 10 data centers to do business.
2. In case of disruption, we would only have 7 data centers available to us.
3. We cannot obtain 3 data centers in a reasonable timeframe.
4. Therefore we need to arrange for alternate data centers in advance of a disruption.

Item number four is the basis of the BIA strategy. Once it is made self-evident that an alternate data center is a requirement, there are other steps an organisation needs to take to properly prepare for a disaster, i.e., size the DR facility, decide on internal vs. outsourced solutions, determine how to get data from one site to another, and so on. The important message of a BIA is that the status quo will not suffice and that some investment is essential. Further analysis will balance the competing imperatives of risk reduction, capital expenditure, service availability, operating expense and P&L impact. If stakeholders do not see the big picture, they surely will not accept the details.

Recovery Strategy Budget Planning								
		Vendor Costs	Hardware Costs	Software Costs	Travel/ Shipping Costs	Labour/ Contract or cost	Testing Costs	Supply Costs
Alternate Site	Cold site							
	Warm Site							
	Hot Site							
	Mobile Site							
	Mirrored Site							
Offsite Storage	Commercial							
	Internal							
Equipment Replacement	SLAs							
	New							
	Existing repairs & use							

BIA is the first phase in Contingency planning process. It provides data about systems and threats faced. It also provides detailed scenarios/effects of attacks. Contingency Planning team conducts Business Impact Analysis in the following stages:

- Threat attack identification and prioritization
- Business unit analysis
- Attack success scenario development
- Potential damage assessment
- Subordinate plan classification
- ◆ The following Issues are to be considered for Business Impact Analysis
 - Different business processes
 - Critical information resources related to critical business processes
 - Critical recovery time period before significant losses are incurred Systems risk ranking

2.2.2 Phase 2: Risk assessment and methodology of risk assessment

Risk Assessment seeks to identify which business processes and related resources are critical to the business, what threats or exposures exist to cause an unplanned interruption of business processes, and what impact accrues due to an interruption. There are various analytical

procedures that are used to determine the risks, threats, and exposures faced by an organisation. These are known by various names, such as Business Impact Analysis (BIA), Application Impact Analysis, Threat and Exposure Analysis, Risk Impact Analysis and so on. While many authors and practitioners maintain subtle differences between these terms, this discussion subsumes all these activities under Risk Assessment.

Risk is an exposure to unwanted loss. In terms of Business Continuity, it is the risk of an incident happening which may result in unwanted loss of an asset or delay in operations.

Risk Assessment is the systematic identification of all risks, their investigation and grading relevant to each other and to the department, so that the management can be given a clear and full understanding of the risks it faces.

Risk Assessment is an important phase in the development of a Business Continuity Plan (BCP). The objective of Risk Assessment are to:

- identify the risks that organisation faces;
- Identify the threat that the organisation would face
- Identify the source of threat
- identify essential operations that must be restarted as quickly as possible after a disaster has taken place;
- identify cost-effective measures that could be introduced to prevent risks or lessen their impact and;
- provide an input for risk management.

All disaster events may not be anticipated or considered. For example, very few organisations considered Tsunami as a major risk in South Asia, before it actually struck.

Risk Assessment & Recovery

The objectives of risk assessment include:

1. **Criticality prioritization:** Identifying business functions or processes and their associated resource requirements. Prioritizing business processes according to their time-sensitivity and criticality.
2. **Estimating the critical recovery time period:** (also called "Recovery Time Objectives" or "Maximum Tolerable Downtime") of the business process. The critical recovery time period is the maximum amount of time allowed for the recovery of the of the business function. This is the amount of downtime of the business process that the business can tolerate and still remain viable. If this time is exceeded, then severe damage to the organisation will result. From the IT point of view, recovery usually means restoring support for the processing and communication functions that are considered to be critical to the business and then restoring support for other non-critical / ancillary systems. From the business perspective, recovery means being able to execute the business functions that are at the key to the survival of the

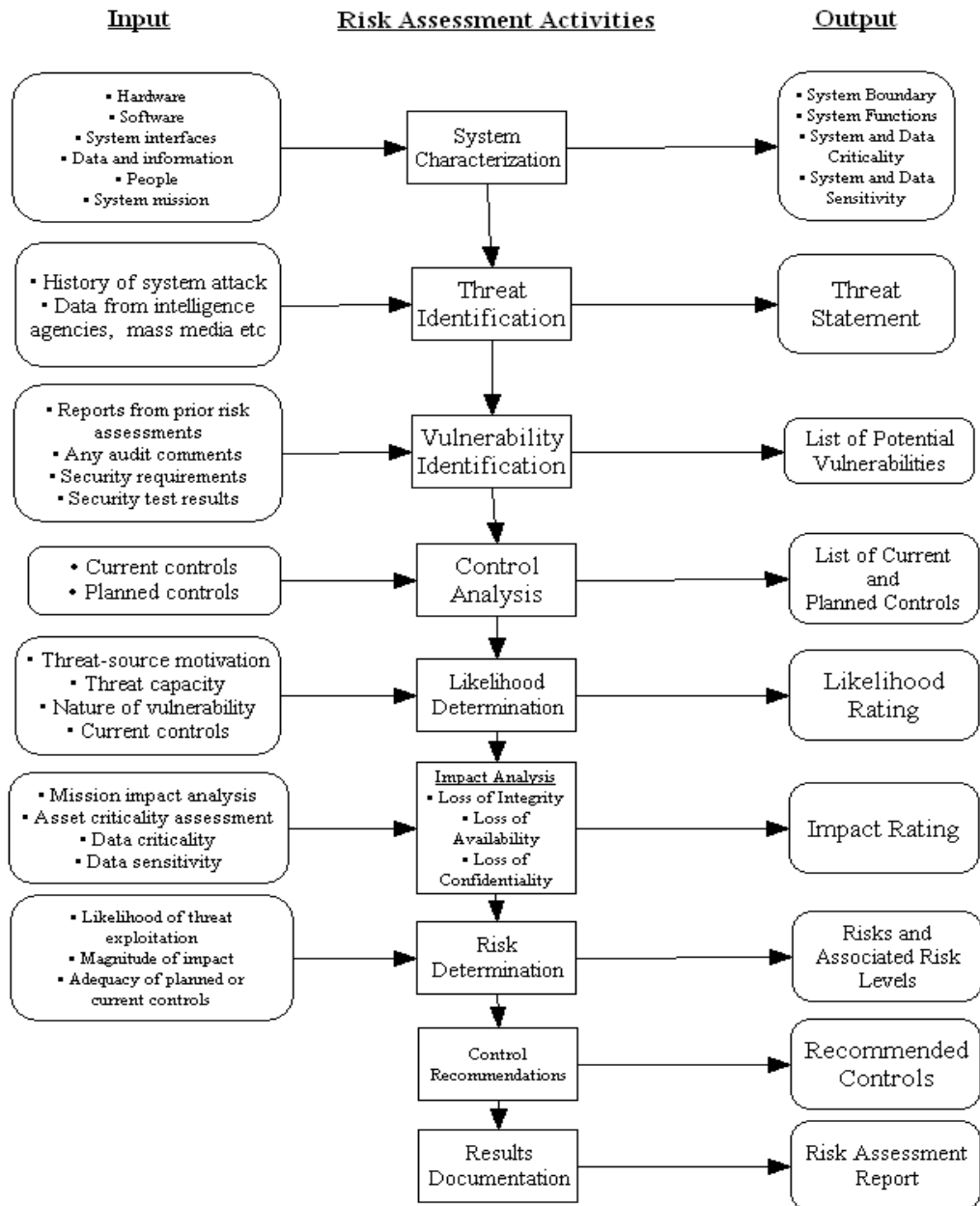
business and then being able to execute the -non-critical/ ancillary functions. Another key factor to consider when defining recovery is the timeframe. Recovery of the function and the system is evaluated considering several time based factors such as:

- i. **Recovery Time Objective (RTO):** RTO is the measure of the user's tolerance to downtime. . It indicates the earliest point in time at which the business operations must resume after disaster. For example: Critical monitoring system must have very low RTO or zero RTO. RTO may be measured in minutes or less.
- ii. **Service Delivery Objective (SDO):** Service Delivery Objective (SDO) is the level of services to be reached during the alternate process mode until the normal situation is restored. This is directly related to the business needs.
- iii. **Recovery Point Objective (RPO):** RPO is a measure of how much data loss due to a node failure is acceptable to the business. A large RPO means that the business can tolerate a great deal of lost data. Depending on the environment, the loss of data could have a significant impact. A rule of thumb is that the lower the RPO, higher the overall cost of maintaining the environment for recovery. An RPO of 5 minutes can lose data up to 5 minutes of data, whereas 0 RPO will have no loss of data. Like RTO / SDO, RPO may vary with services and system. However, it is important to understand the dependencies between the systems and to be taken into consideration while determining the critical systems. These objectives are not closely related – they may both be almost zero, they may both be large, or one may be small but the other large. Once a company decides what RPO and RTO are applicable to an application, the method for backup and recovery of that application becomes much more evident.

Examples of need of various systems in different organisations and scenarios are illustrated here:

- i. A stock exchange trading system must be restored very quickly and cannot afford to lose any data. Since the price of the next trade depends upon the previous trade, the loss of a trade will make all subsequent transactions wrong. In this case, the RTO may be measured as a few minutes or less, but the RPO must be zero.
- ii. A critical monitoring system such as those used by power grids, nuclear facilities, or hospitals for monitoring patients must have a very small RTO, but the RPO may be large. In these systems, monitoring must be as continuous as possible; but the data collected becomes stale very quickly. Thus, if data is lost during an outage (large RPO), this perhaps impacts historical trends; but no critical functions are lost. However, an outage must end as quickly as possible so that critical monitoring can continue. Therefore, a very small RTO is required.
- iii. A Web-based online ordering system must have an RPO close to zero (the company does not wish to lose any sales or, even worse, acknowledge a sale to a customer and then not deliver the product). However, if shipping and billing are delayed by even a day, there is often no serious consequence, thus relaxing the RTO for this part of the application.

- iv. A bank's ATM system is even less critical. If an ATM is down, the customer, although aggravated, will find another one. If an ATM transaction is lost, a customer's account may be inaccurate until the next day when the ATM logs are used to verify and adjust customer accounts. Thus, neither RPO nor RTO need to be small.



Maximum Tolerable outages: Maximum tolerable outage is the maximum time the organisation can support processing in alternate mode. After this point, different problems may arise, especially if the alternate SDO is lower than usual SDO and the information pending to be up-to-date can become unmanageable.

Interruption window: Interruption window is the time the organisation can wait from the point of failure to the critical services/applications restoration. After this time, the progressive losses caused by the interruption are unaffordable.

Threats and its type

The threats, exposure, probability of happening and the loss are documented as part of the Risk Assessment. An analysis of all the business processes that are supported by IT will be carried out to identify the systems / processes that are critical / core to very survival of the business and also to determine the length of time that such processes can survive without IT by not incurring heavy loss. The information should be gathered through standard survey tools or questionnaires and should be documented in a clear and understandable format to be presented to the management. A threat is anything with a potential for adverse effect on an asset, for example fire, unauthorized access to premises. Threats should be assessed to determine:

- How vulnerable the Organisation's assets are to the threats;
- What preventative measures could be taken to lessen the impact of the threats.

The different types of threat an organisation's assets may be at a risk from are as follows:

- Natural
 - Fire
 - Flood
 - Storm
 - Lightning
 - Power Failure
- Deliberate/Intentional
 - Bomb
 - Sabotage
 - Theft
 - Strike

- Accidental
 - Outrage
 - Errors
 - Disclosure

Organisations should also consider threats arising from various issues as:

- Unauthorized access to:
 - Premises
 - Equipment
 - Papers and other resources
 - Computer systems, from outside and inside the premises
- Location of the premises
 - Road, Rail and air traffic
 - Industrial processes
 - Visible targets for terrorism
 - Entrances and Exits
- Shared Premises
 - Should agree who is responsible for what
 - Are legally required to co-operate and co-ordinate during an emergency

Risk assessment has to be a coordinated activity with participation from personnel departments, vendors and interested stakeholders. A sample checklist which can be used for risk assessment is given below:

Sample checklist for Risk Assessment

Areas for Investigation Status	(Y/N) / Comment
Existence of fire and other emergency evacuation procedures	
Existence of bomb threat procedures	
Reliance on telephone, fax, IT equipment	
List of reliable contractors for emergency repairs	
Dependency on specific goods and Services	

Dependency on specific equipment	
Computer data backed up and stored off site	
Compliance with legislation on public health, health and safety, fire precautions	
Compliance with listed building constraints	
Leakages, burst pipes, internal flooding water, oil, gas	
Power isolation devices on electrical systems	

Risk Assessment Methods

If the Risk Management is to be effective, a systematic approach to Risk Assessment should be taken. This means that Risk Assessment should be conducted formally, rather than casually. The following methods will enable a systematic and reliable risk assessment to be carried out:

1. Risk Ranking
2. Value ranges
3. Formulae for comparing risks
4. Computer software if suitable

1. Risk Ranking

The ability of a company to cope with interruption of a business process determines the TOLERANCE of the business process. This tolerance depends on the length of the disruption and may also be linked to the time of the day or month the interruption occurs. In practice, tolerance is usually expressed as a monetary amount – the cost to the company if business process is interrupted for a given unit of time. This cost of interruption is inversely related to the tolerance. The various business processes may be classified on their critical recovery time period.

i. **Critical:** These are functions that cannot be done manually under any circumstances. Unless a company located identical capabilities to replace the damaged capabilities, these functions cannot be performed. These functions have zero or very low tolerance to interruption and consequently, the cost of interruption is high.

ii. **Vital:** These functions can be performed manually but only for a brief period of time. There is relatively higher tolerance to interruption as compared to critical functions and consequently somewhat lower cost of interruption. The function classified as vital can withstand a brief suspension of operations but cannot withstand an extended period of downtime.

iii. **Sensitive:** These processes can be carried out by manual means for an extended period, though with some difficulty. They may require additional staff to perform and when restored, may require considerable amount of time to restore the data to current or usable form.

iv. **Non-Critical:** These processes have a high tolerance to interruption and can be interrupted for an extended period of time with little or no adverse consequences. Very little time is required to restore the data to a current or usable form.

2. Value ranges

To assist in comparison, a range of values should be set for each of the following:

- Asset cost;
- Likelihood of threat happening;
- Vulnerability; and
- Assessment of the risk.

The following ranges can be used:

- A scale of one to five; or
- Very Low, Low, Moderate, High and Very High.

A scale of one to five will produce a more accurate Risk Assessment than a scale of one to three. Ranges greater than five are usually unnecessary and should only be used if a particularly accurate Risk Assessment is required, or a greater distinction between different risks needs to be made.

3. Formulae for comparing risks

To produce more precise results from a Risk Assessment, a formula can be used in conjunction with the value ranges in mentioned above to compare and priorities risks. For example:

$$\text{Risk} = \frac{\text{Asset Cost} + \text{Likelihood} + \text{Vulnerability}}{3}$$

Divide the sum of asset cost, likelihood and vulnerability by three to find the average value. For convenience, the resulting score can then be translated into words to describe the risk, such as:

- 1 -Very Low;
- 2 - Low;
- 3 - Moderate;
- 4 - High;
- 5 -Very High.

Example: The risk of flooding to a premise has been assessed and the following values awarded:

- Asset cost = 5 (the property is highly valued);
- Likelihood = 3 (flood is considered to be a moderate threat because the property is located in the midland); and
- Vulnerability = 2 (because the property is constructed well above the ground level/ Sea level).

Using the formula given above, the score for this particular risk is:

$$\frac{5 + 3 + 2}{3} = 3.3$$

This translates into words as 'Moderate' risk.

4. Formula Method for Comparing Risks

The risk is calculated from the analysis of threats, vulnerabilities and impacts on key assets. Where the risk is unacceptable, steps should be taken to reduce it by applying measures to reduce the impact, threat or vulnerability to an acceptable level. The risk will be determined by an algorithm, based on ascribing values to the risk that is based on the values already ascribed to the threat, vulnerability and impact. There is no universally appropriate formula for this process, but it approximates to: Risk = Threat x Vulnerability x Impact

Thus, a threat, which had a high impact, might still be rated highly although its occurrence would be relatively rare. Conversely, a frequent threat (especially where the organisation was vulnerable) could be rated highly even though its impact was only minor. The example above and the above formulae used are simple and should be adequate for uncomplicated Risk Assessments.

2.2.3 Phase 3: Development of BCP

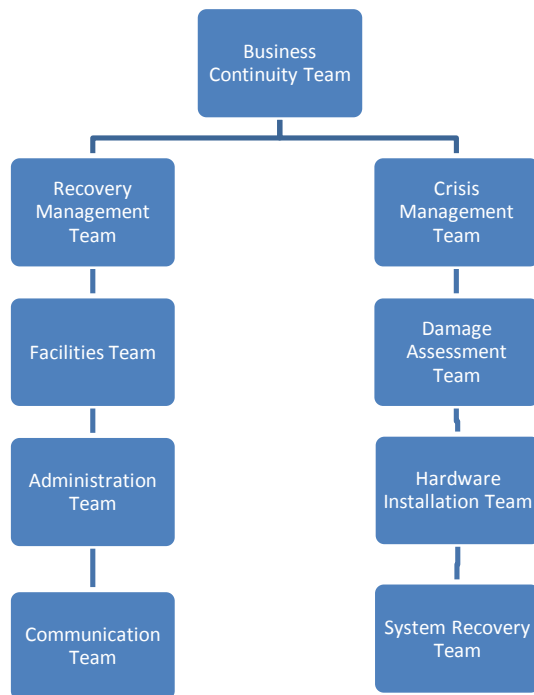
Based on the inputs received from BIA, a detailed plan is then developed. It should ideally address all issues involved in a disruption to business processes and recovery from a disaster. The plan should be documented and written in simple language, so that everyone in the organisation and related to the organisation including, if necessary, third-party vendors etc. understands it. It should be a part of the plan to develop some important teams with clear cut roles and responsibilities. Some of such important teams are:

Business Continuity Team

- i) **Recovery Management Team:** The recovery management team will oversee and manage any recovery exercise. Leaders of all other teams should form part of the management team, to ensure that complete and up-to-date information is presented at all status meetings. The business continuity planning coordinator or administrator will be part of team. Any decisions on revising the recovery process or reacting to changed circumstances will be made by this team. The manager of this team will also report to senior corporate management who are not intimately involved in the process. Even where multiple sites are covered by the plan, the membership of this team will be relatively constant. Only the leaders from the site specific recovery team will vary.

ii) **Crisis Management/Public Relations Team:** Dealing with external agencies or interest groups is an inevitable part of any post-disaster activity. The work performed by this team may extend beyond the provision of detail on what has happened, and what is being done to keep the business in operation. For example, this team may also have to handle:

- notification of death or injury to next of kin;
- dealing with the media;
- liaison with government or regulatory bodies; and
- Handling public concerns if the disaster has health or environmental implications.



Business Continuity Team

To be effective, this team must have all of the necessary information at their disposal and include appropriate senior corporate officials who are comfortable in dealing with the media and relaxed in front of cameras. Mishandling public relations can severely damage an organisation's reputation and cause more harm than the disaster itself.

Dealing with the media is a skill which must be developed, and there are consulting firms which specialize in this service. In addition to being comfortable in the handling of the media, this team must have a predefined plan for issuing statements, an agreed location for making those statements and an understanding of the level of information to be issued. Experience has shown that saying nothing or “no comment” can be more costly to the organisation than providing full and open disclosure. If the media cannot get the information from official sources, it is very good at finding other, not necessarily reliable, information from other sources.

The crisis management team or public relations team must be thoroughly prepared to handle the media and all other external communications. Appropriate spokespersons should be identified and trained. The functionalities of teams under the control of Recovery management team and Crisis management team are elaborated below:

- i) **Hardware Installation Team:** In today's business environment, it is likely that a recovery operation will require the installation of some computer equipment. This may include the ordering and installation of a replacement data center, the installation of the specific terminals and printers required by the impacted business unit, or even the replacement of microcomputers.
- ii) **System recovery Team:** Once the hardware team has completed its job, the system recovery team will be responsible for installing the necessary software, recovering data backup and ensuring that the recovered systems are capable of supporting the critical business functions.
- iii) **Communications Team:** The communications team is responsible for handling the re-routing or re-connection of the essential voice and data communications. Because of the specialized nature of the communications functions, many large and decentralized organisations still maintain a centralized communications group.
- iv) **Facilities Team:** Ensuring a smooth transition to temporary premises, and the refurbishment or replacement of the primary premises is among the responsibilities of the facilities team. This team may also be responsible for equipping the premises with furniture, office supplies and coffee making facilities.
- v) **Administration team:** The various recovery teams will each require administrative support. This will be one of the functions of the administration team. Administration team staff may also be responsible for such matters as staff travel arrangements, catering, petty cash control, telephone services, mail services, and some personnel functions.
- vi) **Damage Assessment Team:** Damage assessment will be one of the first activities performed after a disaster occurs. Depending on the nature of the operations at the

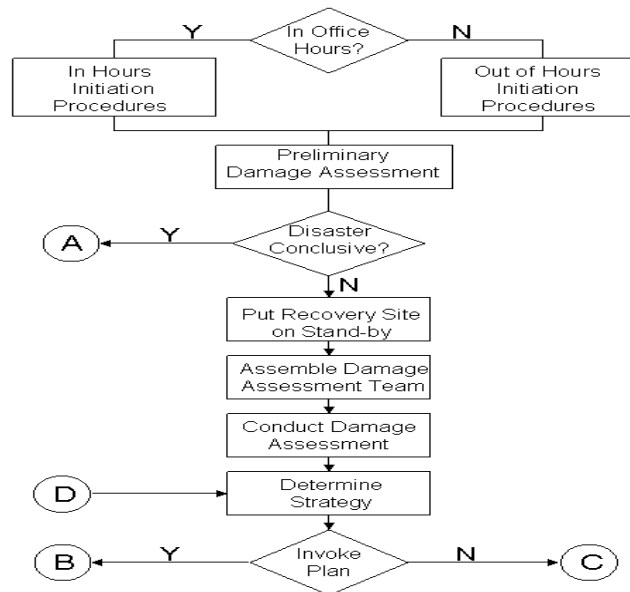
site impacted, the performance of such an assessment may require a number of different skill sets.

vii) Other teams which may be established include:

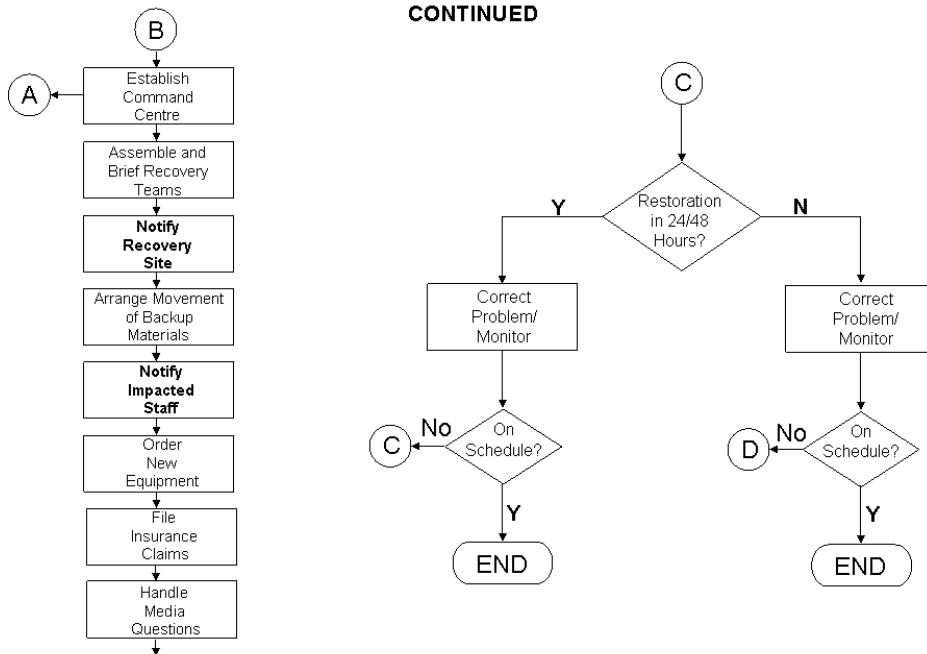
- **Application recovery teams** – to recover specific critical application systems
- **Logistics team** – to assist in team coordination, if staffs are located at geographically separate sites for recovery purpose. This team can handle the distribution of mail and reports, movement of input documents and media, etc.
- **Staff coordination team**- responsible for keeping staff informed of the situation and providing interim financial assistance to families, where required. Employees can be great representatives in times of stress, but can also cause problems if they feel mistreated
- **An insurance team**- responsible for turning the damage assessment information into timely insurance claims
- **User liaison team** – responsible for communications between a data center recovery site and the remote users of that site.

Once the teams have been established and their responsibilities agreed upon, details of the teams should be entered into the plan. This does not require step by step procedures, but an overview of each team's responsibilities and understanding of the interaction required between the teams.

DISASTER NOTIFICATION AND PLAN ACTIVATION



DISASTER NOTIFICATION AND PLAN ACTIVATION CONTINUED



To Detailed Recovery Procedures

Business Continuity Plan

The Business Continuity Plan should minimum encompass the following:

- **Initiation procedures:** Notification procedures will ensure that the organisation's appropriate officials are contacted on a timely basis when a disaster event occurs. These procedures will include contact details all of key personnel and vendors.
- **Preliminary damage assessment:** Once management has been notified of the problem, a preliminary damage assessment should be performed. This need not be a detailed assessment, but will provide an initial indication as to whether the plan needs to be activated.
- **Put recovery site on standby:** Where the BCP involves the use of a commercial recovery center, that site should be put on notice. Most vendors favour being put on notice and appreciate an advance warning.
- **Assemble damage assessment team:** If the preliminary assessment is not conclusive, the full damage assessment team can be assembled. If all staff is on site when disaster strikes, this should be a relatively easy task. However if the incident occurs after office hours it will be necessary to call staff at home to notify all team members of the problem.
- **Conduct damage assessment:** The damage assessment process should be conducted as soon as possible following disaster notification. The assessment of the extent of the damage, possible duration of service disruption, and job processing status will directly impact the subsequent course of recovery action. The assessment process should consider the impact on:
 - The facilities
 - Power and other utilities
 - The environment and
 - Essential equipment
- **Determining strategy:** The identification of the most appropriate strategy will typically require a decision by the recovery management team, based on the damage assessment report. Once an appropriate strategy has been identified, the adoption of that solution must be approved by the senior management.
- **Establish emergency command center:** While it may not be necessary to establish command center for the damage assessment team alone, once the decision has been made to invoke the plan it will be necessary to activate that location. All members of the teams responsible for recovery of the management should assemble at an identified

Emergency Command Centre. This center must be established at a predefined location within easy access of the primary site, but sufficiently far removed that it will not be affected by a disaster event. It is from this site that recovery operations will be directed.

- **Assemble and brief recovery teams:** This effect the notification of all team members to report to the command center. This should include:
 - ✓ Giving details of who is calling
 - ✓ Providing a brief synopsis of disaster status
 - ✓ Instruction to call all staff or alternates on the list of the person being called
 - ✓ Instruction on where to report, when and with what materials and
 - ✓ A record of all calls made should be retained.
- **Notify recovery site:** The recovery to be used including any commercial sites, should be notified of the decision to use the facility and requested to prepare the site in accordance with the contract.
- **Arrange movement of backup materials:** Once the decision is made to move to the recovery site, all of the necessary materials should be recovered from off-site storage and shipped to that location. The shipment of any required special forms from backup supplies should also be coordinated at this time.
- **Notify impacted staff:** Once the recovery operations are under way, the staff that will be impacted but will not be required for recovery activities should also be notified. It is preferable that they receive notification from the organisation rather than from the media.
- **File Insurance claims:** It may not be possible to file the claims immediately, as further damage assessment may still be required However as soon as the necessary information is available, the claims should be prepared.
- **Detail procedures for recovery:** A step by step instructions for recovering systems at recovery site should be written down. Some of instructions are:
 - assemble and check site
 - check off site materials and install equipment
 - test operating system
 - recover applications
 - test applications
 - hire temporary staffs

- update to disaster (if the recovery site is not shadowing all data processed at the primary site, data entry up to the state of disaster will be entered again at the recovery site)
 - process backlog
 - configure networks and test network
 - establish external links
 - redirect mail
 - redirect communications
 - correct problem / monitor
 - establish controls
- **Primary site procedures:** While the detailed recovery procedures are concentrated on alternate facilities to restore the critical business operations, the primary site should be built up again. Steps remain to be taken in that location following the damage assessment and the decision to invoke the plan.
 - **Return to normal operations:** Once the primary site is refurbished or a new primary site available, it is necessary to relocate to that site.
 - **Post recovery reviews:** Once the return to normal operations has been completed and approved, the normal job schedules and operating instructions should be reintroduced. In addition, a review of the recovery operations should be performed to identify any areas in which the plan can be improved. This post mortem should be performed as soon as possible to ensure that concerns and problems experienced are still clear in staffs' minds.

The next step would involve the documentation of the plan which means creation of the BCP Manual. A BCP Manual houses all the relevant steps of the plan that is needed to be followed during a crisis. A BCP manual contains the Disaster Recovery Plans, Business Continuity Plan and the contingency plans. The elements of a BCP Manual are discussed in 2.10.

2.2.4 Phase 4: Testing of BCP and DRP

Testing the Disaster Recovery Plan

The Disaster Recovery Coordinator is responsible for testing of the disaster recovery plan at least annually to ensure the viability of the plan. However, special tests are to be given consideration whenever there has been a major revision to the plan or significant changes in the software,

hardware or data communications have occurred. The objectives of testing the disaster recovery plan are:

1. Simulate the conditions of an ACTUAL Business Recovery situation.
2. Determine the feasibility of the recovery process
3. Identify deficiencies in the existing procedures
4. Test the completeness of the business recovery information stored at the Offsite Storage Location.
5. Train members of the disaster recovery teams

The initial test of the plan will be in the form of a structured walk-through and should occur within two months of the disaster recovery plan's acceptance. Subsequent tests should be to the extent determined by the Business continuity coordinator that are cost effective and meet the benefits and objectives desired.

Sample Recovery Test agenda

Sample Recovery Test Agenda	
1.	What is the purpose of the test?
2.	What are the test objectives?
3.	How will the successful achievement of these objectives be measured?
4.	At the conclusion of the test, collect test measurements from all participants.
5.	Evaluate the test results. Determine if the test was successful or not.
6.	Determine the implications of the test results. Does success for this test imply success in all recovery scenarios?
7.	Update the plan based on results of the test.

BCP Testing

The effectiveness of BCP has to be maintained through regular testing. The five types of tests of BCP are:

1. Checklist test
2. Structured walk through test
3. Simulation test
4. Parallel test
5. Full interruption test

1. **Checklist test:** In this type of test, copies of the plan are distributed to each business unit's management. The plan is then reviewed to ensure that the plan addresses all procedures and

critical areas of the organisation. In reality, this is considered as a preliminary step to real test and is not a satisfactory test in itself.

2. Structured walk through test: In this type of test, business unit management representatives meet to walk through the plan. The goal is to ensure that the plan accurately reflects the organisation's ability to recover successfully, at least on paper. Each step of the plan is walked through in the meeting and marked as performed. Major faults with the plan should be apparent during the walkthrough.

3. Simulation test: In this type of test, all of the operational and support personnel who are expected to perform during an actual emergency meet in a mock practice session. The objective is to test the ability and preparedness of the personnel to respond to a simulated disaster. The simulation may go to the point of relocating to the alternate backup site or enacting recovery procedures, but does not perform any actual recovery process or alternate processing.

4. Parallel test: A Parallel test is a full test of the recovery plan, utilizing all personnel. The difference between this and the full interruption test is that the primary production processing of the business does not stop, the test processing runs in parallel to the real processing. The goal of this type of test is to ensure that critical systems will actually run at the alternate processing backup site. Systems are relocated to the alternate site, parallel processing backup site, and the results of the transactions and other elements are compared. This is the most common type of disaster recovery plan testing.

5. Full interruption test: During a full interruption test, a disaster is replicated event the point of ceasing normal production operations. The plan is implemented Asif it were a real disaster, to the point of involving emergency services. This is a very severe test, as it can cause a disaster on its own. It is the absolute best way to test a disaster recovery plan, however, because the plan either works or doesn't.

Documentation of results: During every phase of the test, a detailed documentation of observations, problems and resolutions should be maintained. This documentation can be of great assistance during an actual disaster. They are also helpful in improving and maintaining the plan as they reveal the strengths and weaknesses of the plan. No test is ever a failure because, however badly it may seem to have gone lessons can still be learnt from it. However, it should be remembered that if a test is not planned properly, it could actually create a disaster. Live tests especially could create disaster if not planned properly because they use real people and real resources in real conditions, probably during normal working hours. Live tests should only be considered after the BCP has been tested in full and all Recovery Team members fully trained. The worst way to test a Plan is to turn off the power suddenly, for example, and tell people to exercise their Recovery Plans, the interruption and delay to normal work could well become a disaster in itself.

Results Analysis: The results of each test should be recorded to identify:

- I. What happened;
- II. What was tested successfully; and
- III. What needs to be changed?

If a test indicates that the BCP needs to be changed, the change should be made and the test repeated until all aspects are completed satisfactorily. When all the components have been tested satisfactorily, the whole BCP is ready for testing. It should not be assumed that because the components work individually there is no need to test the whole BCP. Putting it all together may reveal problems which did not show up in lower level testing. When preparing for testing, the participants should be given all the information and instruction they need.

2.2.5 Phase 5: Training and Awareness

Training the Team

The Disaster Recovery Coordinator is responsible for the coordination of training relating to the disaster recovery plan. The purpose of this training is two-fold:

1. To train recovery team participants who are required to execute plan segments in the event of a disaster.
2. To train the management and key employees in disaster prevention and awareness and the need for DRP.

The training of organisation's user management in disaster recovery planning is crucial. A DRP must have the continued support from organisation's user management to ensure future effective participation in plan testing and updating. It is not solely the responsibility of the Disaster Recovery Coordinator to initiate updates to the disaster recovery plan. User management must be aware of the basic recovery strategy; how the plan provides for rapid recovery of their information technology systems support structure. It is the responsibility of each recovery team participant to fully read and comprehend the entire plan, with specific emphasis on their role and responsibilities as part of the recovery team. On-going training of the recovery team participants will continue through plan tests and review of the plan contents and updates provided by the Disaster Recovery Coordinator.

From the start of the BCP development project, positive action to create awareness of the BCP during the development, testing and training phases should be taken by holding briefings for all staff at an early stage of BCP development to explain the reasons for the BCP and its benefits to everyone and how it will be developed; The organisation should take care that all new staff are briefed about the BCP as a part of their induction to the organisation. It should be remembered that every test also trains the participants. If the full Recovery Teams are not used in each test, the participants should be rotated so that they all gain an adequate experience. At the end of the testing phase, further training and experience requirements should be identified. The Recovery Team leaders should be consulted for their opinions as they should have the best understanding of the present abilities of their Team members.

Training methods

The training methods to be used may include:

1. Walkthrough session
2. Scenario workshop; or
3. Live test simulation

1. Walkthrough Session

For a walkthrough session, the participants sit round a table, each with a copy of the BCP (or appropriate part of the BCP), and 'walk' through it by reading and discussing each part in sequence. Walkthrough sessions should be conducted at a quiet place without interruption because the objective is to identify any weaknesses, errors and omissions by allowing participants' thoughts to flow freely as they go through the plan. The only limit on discussion is that the whole part must be read to the end. All components of the BCP should first be tested using this method as it is highly likely to identify changes needed. One good walkthrough per component is usually sufficient if the suggested changes are then reviewed and agreed by a few of the testers for one Recovery Team. Links with other Teams should be noted and raised during their walkthroughs.

2. Scenario Workshop

This is similar to a walkthrough except that a scenario is devised before the workshop, and the key members of recovery teams are involved, although it is preferable to include all teams.

Scenarios should be designed:

1. around the actual conditions of the premises and its operations;
2. to introduce any possible disaster in a realistic way;
3. to give a good testing of the plan;
4. to include developments that would usually occur during a disaster, for example, changes in safety conditions delaying return to the premises.

Participants should sit round a table at a quiet place without interruption with their copies of the BCP (or appropriate part of the BCP), but instead of reading through the whole BCP, they should role-play their participation in the scenario. As they do so, they should say aloud what they are thinking and doing. The objective is to identify errors, omissions and weaknesses, and to establish whether the plan performs as intended. For this method to be effective, participants must:

1. Accepts the scenario at face value;
2. Become fully involved in the role play; and
3. Voice all their thoughts and imagined actions. Brief interruptions to a participant's spoken thoughts and actions are permitted if other participants have constructive comments or questions.

As the scenario progresses the lead participant(s) may change as appropriate to the timescale of the plan, particularly if the whole BCP is being tested rather than one Recovery Team's Plan. Participants need to be aware of this possibility so that it happens smoothly in the right places.

3. Simulation of a Live Test

The simulation of a live test:

1. is held outside normal working hours so that resources can be used without affecting normal operations;
2. involves the use of the planned and contracted contingencies if this is practical;
3. requires relocation of some staff to another site if appropriate; and
4. has to be as near to real life as possible so that all aspects of the BCP, including contingencies, are tested.

Because it is a test, some shortcuts may be taken, such as sending only a token number of people to the contingency site, or doing only token amounts of work to prove that the operation has been successfully recovered. However, even if shortcuts are used it must still be possible at the end of the test to conclude that all aspects of the BCP are effective. A simulation of a live test, perhaps more than the other methods, needs to be carefully planned to:

1. ensures that the testing is thorough;
2. Avoid confusion when things go wrong; and
3. Prevent any disruption to the real operations.

2.2.6 Phase 6: Maintenance of BCP and DRP

Maintenance of the plans is critical to the success of an actual recovery. The plans must reflect changes to the environments that are supported by the plans. It is critical that existing change management processes are revised to take recovery plan maintenance into account. In areas, where change management does not exist, change management procedures will be recommended and implemented. Many recovery software products take this requirement into account. BCM testing, maintenance and audit testify the organisation BCM to prove the extent to which its strategies and plans are complete, current and accurate; and Identifies opportunities for improvement. Agreements may also need to reflect the changes. If additional equipment is needed, it must be maintained and periodically replaced when it is no longer dependable or no longer fits the organisation's architecture. The BCM maintenance process demonstrates the documented evidence of the proactive management and governance of the organisation's business continuity program; the key people who are to implement the BCM strategy and plans are trained and competent.

The monitoring and control of the BCM risks faced by the organisation; and the evidence that material changes to the organisation's structure, products and services, activities, purpose, staff

and objectives have been incorporated into the organisation's business continuity and incident management plans. Similarly, the maintenance tasks undertaken in development of BCP are to:

- Determine the ownership and responsibility for maintaining the various BCP strategies within the organisation;
- Identify the BCP maintenance triggers to ensure that any organisational, operational, and structural changes are communicated to the personnel who are accountable for ensuring that the plan remains up-to-date;
- Determine the maintenance regime to ensure the plan remains up-to-date;
- Determine the maintenance processes to update the plan; and
- Implement version control procedures to ensure that the plan is maintained up-to-date.

Role of IS Auditor in testing of BCP:

- Ensure that a suitable mechanism exists to update the plan.
- The IS auditor should review the result of the Business Continuity Plan test. The IS auditor should check to see that the results of the test were along anticipated lines. If not, discrepancies between expected outcomes and actual outcomes should be analyzed to find shortcomings in the plan. The IS auditor should examine whether the weaknesses and shortcomings that have been identified during testing have been rectified at a later date.

2.3 Incident Handling and Management.

2.3.1 Incident Response

Incident response (IR) is the set of procedures that commence when an incident is detected. For each attack scenario end case, IR team creates procedures to be deployed during, after, and before the incident. IR planning (IRP) follows these general stages:

- Form IR planning team
- Develop IR policy
- Organize security incident response team
- Develop IR plan
- Develop IR procedures

Incident Response Planning for: Before the Incident

IRP for before the incident consists of both preventative measures to manage risks associated with particular attack and activities to ensure IR team preparedness. Process includes:

- Training the Incident Response Team
- Testing the IR plan

- Selecting and maintaining tools used by the IRT
- Training users of the systems and procedures controlled by the organisation

Incident Response Planning for: Response during the Incident

Most important phase of the IR plan is the reaction to the incident. Each viable attack scenario end case is examined and discussed by the IR team:

- ✓ Trigger (circumstances that cause IR team activation and IR plan initiation) are to be defined.
- ✓ What must be done to react to the particular situation are to be elaborated.
- ✓ How to stop the incident if it is ongoing is also to be addressed along with the way by which the Elimination of problem source can be achieved.

Incident Response Planning for: After the Incident

During this phase, the goal is to return each system to its previous state. IR plan must describe stages necessary to recover from most likely events of the incident. It should also detail other events, like protection from follow-on incidents, forensic analysis, and the after-action review. After-action review (AAR) should explain about the detailed examination of events that occurred from first detection to final recovery.

2.3.2 Incident Classification

Incident classification is the process of evaluating organisational events, determining which events are incident candidates, and then determining whether it is an actual incident or a nonevent. IR design team creates process used to make this judgment; IR team actually classifies events. Incident candidates can be detected and tracked via reports from end users, intrusion detection systems, virus management software, and systems administrators.

Three broad categories of incident indicators are: possible, probable and definite.

Four types of possible actual incidents are: Presence of unfamiliar files, presence or execution of unknown programs or processes, unusual consumption of computing resources and unusual system crashes.

Four probable indicators of actual incidents are: Activities at unexpected times, presence of new accounts, reported attacks and notification from IDS.

Five events of definite indicators of an incident are: Use of dormant accounts, modified or missing logs, presence of hacker tools, notifications by partner or peer and notification by hacker.

Five events which indicate that an incident is underway are: Loss of availability, loss of integrity, loss of confidentiality, violation of policy and violation of law.

2.3.3 Norms and procedure for declaring an Incident as a Disaster:

Collection of data under IRP

Routine collection/analysis of data is required to properly detect/declare incidents. Logs should be enabled, stored off site and in a hardened location. Managing logs include the preparation of the system for amount of data generated, Rotation of the logs on schedule, encryption of logs, the archival and disposal of logs.

Reactions to incidents

How and when to activate IR plans determined by IR strategy organisation chooses to pursue? In formulating incident response strategy, many factors influence an organisation's decision. IR plan designed to stop incident, mitigate effects, and provide data that facilitates recovery. Two general categories of strategic approach for an organisation as it responds to an incident are 1. Protect and forget and 2. Apprehend and prosecute.

Incident Notifications

As soon as IR team determines an incident is in progress, appropriate people must be notified in the correct order. Alert roster is the document containing contact information for individuals to be notified during an incident. There are two ways to activate alert roster namely sequentially and hierarchically. Alert message should contain the scripted description of incident containing enough information for each responder to know what to do on alert process.

Documenting an Incident

Documenting the incident should begin immediately after incident is confirmed and notification process is underway. It should record who, what, when, where, why, and how of each action taken while incident is occurring. The purpose is to make the documentation to serves as case study to determine whether right and effective actions were taken. It helps to prove that the organisation did everything possible to prevent spread of the incident. It can also be used as simulation in future training sessions on future versions of IR plan.

Incident containment strategies

One of the most critical components of IR is stopping incident or containing its scope/impact. Affected areas must be identified. Incident containment strategies focus on two tasks namely stopping the incident and recovering control of the affected systems. IR team can attempt to stop incident and try to recover control by means of several strategies.

Recovering from incident

Once incident is contained and system control regained, incident recovery can begin with the Incident damage assessment (i.e.) immediate determination of the scope of the breach of confidentiality, integrity, and availability of information and information assets. Steps to be taken in the recovery process include Identifying and resolving vulnerabilities, restoration of data, restoration of services and processes, and restoration of confidence across the organisation.

After action review

Ongoing IR plan maintenance includes procedures to conduct after-action reviews, plan review and maintenance; train staffs involved in incident response, and rehearse process that maintains readiness for all aspects of the incident plan. IR team must conduct after-action review that is the detailed examination of events during incident. After Action Review serves as review tool, historical record, case training tool, closure

Incident response plan review and maintenance:

At periodic intervals, an assigned member of management should review the IR plan. When shortcomings are noted, plan should be reviewed and revised to remediate deficiency. Organisation must undertake training programs to ensure a sufficient pool of qualified staff are available to execute the plan when activated. Ongoing and systematic approach to planning requires plans be rehearsed until responders are prepared to perform as expected.

2.4 Invoking a DR Phase/BCP Phase

2.4.1 Operating Teams of contingency planning

Contingency Planning team: This team collects data about information systems and threats, conducts business impact analysis, and creates contingency plans for incident response, disaster recovery, business continuity. The primary role of this team is to conduct research on data that could lead to a crisis and develop actions that would effectively handle these threats.

Incident Response team: This team manages/executes IR plan by detecting, evaluating, responding to incidents. This team is the first team to arrive during the outbreak of an incident. Incident Response Team evaluates the incident, takes the first action to stop the incident. If unsuccessful, then summons the Disaster Recovery Team.

Disaster Recovery team: This team manages/executes DR plan by detecting, evaluating, responding to disasters; re-establishes primary site operations. This team plays its role in reducing the impact of the disaster and executes the steps that are defined in the DR Plan to recover and protect resources that are being impacted by the disaster and to mitigate the disaster itself. If the

impact of the crisis is very high, then the Business Continuity Team steps in parallel to the DR Team and

Business Continuity Team: This team manages/executes BC plan by establishing off-site operations to ensure Business Continuity. Business Continuity Team initiates those responses to the impacts that are being faced by the entity and would bring the entity back to its original level of business functioning. The disaster recovery plan is composed of a number of sections that document resources and procedures to be used in the event that a disaster occurs at the Information Technology Services Locations. Each supported application or platform has a section containing specific recovery procedures. There are also sections that document the personnel that will be needed to perform the recovery tasks and an organisational structure for the recovery process. This plan will be updated on a regular basis as changes to the computing and networking systems are made. Due to the very sensitive nature of the information contained in the plan, the plan should be treated as a confidential document and should be shared with specific employees as per the specific responsibilities they have been assigned.

2.4.2 DRP scope and objectives

The DRP should inform the user about the primary focus of this document like responding to disaster, restoring operations as quickly as possible and reducing the number of decisions which must be made when, and if, a disaster occurs. It should also inform about the responsibility to keep this document current. It should be approved by appropriate authority.

The overall objectives of this plan are to protect organisation's computing resources and employees, to safeguard the vital records of which Information Technology Systems and to guarantee the continued availability of essential Information Technology services. The role of this plan is to document the pre-agreed decisions and to design and implement a sufficient set of procedures for responding to a disaster that involves the data center and its services.

A disaster is defined as the occurrence of any event that causes a significant disruption in Information Technology capabilities. This plan assumes the most severe disaster, the kind that requires moving computing resources to another location. Less severe disasters are controlled at the appropriate management level as a part of the total plan.

The basic approach, general assumptions, and possible sequence of events that need to be followed are stated in the plan. It will outline specific preparations prior to a disaster and emergency procedures immediately after a disaster. The plan is a roadmap from disaster to recovery. Due to the nature of the disaster, the steps outlined may be skipped or performed in a different sequence. The general approach is to make the plan as threat-independent as possible. This means that it should be functional regardless of what type of disaster occurs.

For the recovery process to be effective, the plan is organized around a team concept. Each team has specific duties and responsibilities once the decision is made to invoke the disaster recovery

mode. The plan represents a dynamic process that will be kept current through updates, testing, and reviews. As recommendations are completed or as new areas of concern are recognized, the plan will be revised to reflect the current IT and business environment. **The IS Auditor has to review the process followed for preparation of the DRP and assess whether it meets the requirements of the organisation and provide recommendations on any areas of weaknesses identified.**

2.4.3 Disaster recovery phases

The disaster recovery process consists of four phases which are outlined here:

- Phase 1: Disaster Assessment
- Phase 2: Disaster Recovery Activation
- Phase 3: Alternate Site/Data Center Rebuild
- Phase 4: Return to Primary site

1. Disaster Assessment: The disaster assessment phase lasts from the inception of the disaster until it is under control and the extent of the damage can be assessed. Cooperation with emergency services personnel is critical.

2. Disaster recovery activation: When the decision is made to move primary processing to another location, this phase begins. The Disaster Recovery Management Team will assemble and call upon team members to perform their assigned tasks. The most important function is to fully restore operations at a suitable location and resume normal functions. Once normal operations are established at the alternate location, Phase 2 is complete.

3. Alternate site operation/data center rebuild: This phase involves continuing operations at the alternate location. In addition, the process of restoring the primary site will be performed.

4. Return to primary site: This phase involves the reactivation of the primary site at either the original or possibly a new location. The activation of this site does not have to be as rushed as the activation of the alternate recovery site. At the end of this phase, a thorough review of the disaster recovery process should be taken. Any deficiencies in this plan can be corrected by updating the plan.

2.4.4 Key Disaster recovery activities

The declaring of an incident/event is done by assigned personnel of management. Declaration of a disaster means:

1. Activating the recovery plan
2. Notifying team leaders
3. Notifying key management contacts
4. Redirecting information technology service to an alternate location

5. Securing a new location for the data center
6. Ordering and configuring replacement equipment
7. Reconfiguring the network
8. Reinstalling software and data
9. Keeping management informed
10. Keeping users informed
11. Keeping the public informed

2.4.5 DRP

The DRP should contain information about the vital records details including location where it is stored, who is in charge of that record etc. It contains information about what is stored offsite such as:

1. A current copy of this disaster recovery plan.
2. Copies of install disks for all relevant software and critical software/operating system licenses. These should be stored electronically rather than relying on Internet-downloadable versions. When the software is needed the same version of the software used may not be available on the Internet, or there may be Internet issues that could negatively affect large downloads or may significantly slow down the recovery process.

2.4.6 Disaster Recovery Team

The disaster recovery plan should contain details about Disaster Recovery Management Team and its sub-teams like Administration, Supplies, Public relations etc. and their respective responsibilities. The various types of responsibilities applicable in case of a disaster are explained here covering specific stages.

General Responsibilities

The IT Disaster Recovery Management Team (MGMT) is responsible for the overall coordination of the disaster recovery process from an Information Technology Systems perspective. The other team leaders report to this team during a disaster. In addition to their management activities, members of this team will have administrative, supply, transportation, and public relations responsibilities during a disaster. Each of these responsibilities should be headed by a member of the MGMT team.

General Activities

- Assess the damage and if necessary, declare a disaster (damage assessment forms are included in this plan)
- Coordinate efforts of all teams
- Secure financial backing for the recovery effort

Module 7

- Approve all actions that were not pre-planned
- Give strategic direction
- Be the liaison to upper management
- Expedite matters through all bureaucracy
- Provide counselling to those employees that request or require it

After The Disaster

- Make recommendations on how the disaster recovery plan can be improved

Administrative Responsibilities

The administrative function provides administrative support services to any team requiring this support. This includes the hiring of temporary help or the reassignment of other clerical personnel.

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Notify all vendors and delivery services of change of address

Procedures during All Phases

- Process expense reports
- Account for the recovery costs
- Handle personnel problems

After The Disaster

- Make recommendations on how the disaster recovery plan can be improved

Supply Responsibilities

The supply function is responsible for coordinating the purchase of all needed supplies during the disaster recovery period. Supplies include all computing equipment and supplies, office supplies such as paper and pencils, and office furnishings.

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Purchase supplies required by the teams at the alternate site.

Procedures during Remote Operation/Data Center Rebuild Phase

- Work with procurement to order replacement supplies and expedite shipments
- Ongoing distribution of supplies

Procedures during return to primary site Phase

- Restock supplies at the restored site

After the disaster

- Make recommendations on how the disaster recovery plan can be improved

Public Relations Responsibilities

The public relations function will pass appropriate information about the disaster and associated recovery process to the public and to employees. Every effort should be made to give these groups reason to believe that TAMUCT is doing everything possible to minimize losses and to ensure a quick return to normalcy.

Activities by Phase

All Phases

- Ensure that employees do not talk to the media
- Control information released to the public and to employees
- Interface with organisation's Public Relations or defer to Senior Management
- Publish internal newsletters
- Keep everyone aware of recovery progress

After The Disaster

- Make recommendations on how the disaster recovery plan can be improved

Management Team Call Checklist

The disaster recovery plan should contain disaster recovery management team call checklist. It should specify the contact information about Team leader as well as team members with the details on which functionality he/she can be contacted. The disaster recovery plan should contain details about Technical support Team and its sub-teams like Hardware, Software, Network, Operations etc. and their respective responsibilities.

Hardware Responsibilities

The responsibility of the Hardware Team is to acquire (along with the Facilities Team), configure and install servers and workstations for organisational information Technology users.

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Determine scope of damage for servers and workstations

Module 7

- Order appropriate equipment and supplies (coordinate and work with the Facilities Team for this activity)

Procedures during Remote Operation/Data Center Rebuild Phase

- Set up servers and workstations
- Install software as necessary
- Restore data
- Install additional workstations as they arrive

Procedures during Return Home Phase

- Notify users
- Ensure data is backed up
- Relocate equipment

After The Disaster

- Make recommendations on how the disaster recovery plan can be improved

Software Responsibilities

The responsibility of the Software Team is to maintain the systems software at the alternate site and reconstruct the system software upon returning to the primary site. In addition, the Software Team will provide technical support to the other teams.

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Provide technical support to the other teams
- Build servers and workstations
- Reinstall and configure systems at the primary site
- Test the hardware and software
- Work with appropriate vendors to assist in recovery
- Verify that the systems are performing as expected

Procedures during Remote Operation/Data Center Rebuild Phase

- Provide technical support to the other teams
- Build servers and workstations
- Reinstall and configure systems at the primary site
- Test the hardware and software
- Work with appropriate vendors to assist in recovery
- Verify that the systems are performing as expected

Procedures during Return Home Phase

- Provide technical support to the other teams
- Verify that the system is performing as expected

After The Disaster

- Make recommendations on how the disaster recovery plan can be improved

Network Responsibilities

The Network Team is responsible for preparing for voice and data communications to the alternate location data center and restoring voice and data communications at the primary site.

Activities by Phase

Procedures during disaster recovery activation phase

- Determine the requirements for voice and data communications
- Install the network including lines, routers, switches, controllers and other communications equipment at the alternate location data center
- Test the network.

Procedures during Remote Operation/Data Center Rebuild Phase

- Operate the backup network
- When the replacement equipment arrives at the primary site, install it

Procedures during Relocation Home Phase

- Support the primary site network
- Dismantle the alternate location data center network

After The Disaster

- Make recommendations on how the disaster recovery plan can be improved

Operations Responsibilities

The Operations responsibilities include the daily operation of computer services and management of all backup tapes. When a disaster is declared, the team must secure the correct tapes for transport to the alternate location. Once operations are established at the alternate location, arrangements must be made with an offsite storage service.

Activities by Phase

Procedures during Disaster Recovery Activation Phase

Module 7

- Inventory and select the correct backup tapes
- Transport the tapes to the alternate data center
- Assist all teams in restoring the production environment at the alternate data center

Procedures during Remote Operation/Data Center Rebuild Phase

- Establish a production schedule at the alternate location
- Run the daily schedule at the alternate location
- Perform system and production backups at the alternate location
- Assist other teams in preparing the primary site
- Establish offsite storage at the alternate location

Procedures during Return Home Phase

- Perform system and production backups
- Inventory all tapes at the alternate data center
- Transport all tapes from the alternate data center to the primary site

After The Disaster

- Make recommendations on how the disaster recovery plan can be improved

Technical Support Team Call Checklist

The disaster recovery plan should contain Disaster Recovery Technical Support Team Call Checklist. It should specify the contact information about Team leader as well as team members with the details on which functionality he/she can be contacted. The disaster recovery plan should contain details about Facility Team and its sub-teams like Salvage team, new data center, new hardware team etc. and their respective responsibilities.

Salvage Responsibilities

The Salvage Team is responsible for minimizing the damage at the primary site and to work with the insurance company for settlement of all claims. This depends on a quick determination of what equipment is salvageable and what is not. Repair and replacement orders will be filed for what is not in working condition. This team is also responsible for securing the disaster recovery data center.

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Establish the command center
- Assist in the immediate salvage operations
- Contact Insurance representatives
- Inventory all equipment in the data center. If necessary, involve the vendors.

Procedures during Remote Operation/Data Center Rebuild Phase

- Salvage equipment and supplies
- Settle property claims with the insurance company
- Provide for security at the data center

After The Disaster

- Make recommendations on how the disaster recovery plan can be improved

New Data Center Responsibilities

The New Data Center Team is responsible for locating the proper location for a new data center and overseeing the construction of it. This includes the environmental and security controls for the room.

Activities by Phase

Procedures during Remote Operation/Data Center Rebuild Phase

- Determine the requirements for a new data center
- Work with contractors and university staff on the details
- Oversee the construction of the new data center

Procedures during Return Home Phase

- Ensure that all controls are working as designed

After the Disaster

- Make recommendations on how the disaster recovery plan can be improved

New Hardware Responsibilities

The New Hardware Team is responsible for ordering replacement hardware for equipment damaged in the disaster and installing it in the new or rebuilt data center. Depending on the age of the damaged hardware, replacement may not be one-for-one. All types of hardware are to be handled, including:

1. Servers
2. Printers
3. Switches, Routers, Hubs
4. Work stations
5. Environmental systems
6. UPS Equipment

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Obtain a list of damaged and destroyed equipment

Procedures during Remote Operation/Data Center Rebuild Phase

- Determine what new hardware should be ordered
- Order new hardware
- Arrange for installation and testing of the new hardware

After The Disaster

- Make recommendations on how the disaster recovery plan can be improved

Resumption of Normal Operations

Once the threat has passed, equipment has been repaired or replaced or a new primary site has been built and stocked, the disaster recovery team will assess the situation, declare the disaster over and resume normal operations

2.5 Documentation: BCP Manual and BCM Policy

All documents that form the BCM are to be subject to document control and record control processes. The following documents (representative only) are classified as being part of the business continuity management system:

- The business continuity policy;
- The business continuity management system;
- The business impact analysis report;
- The risk assessment report;
- The aims and objectives of each function;
- The activities undertaken by each function;
- The business continuity strategies;
- The overall and specific incident management plans;
- The business continuity plans;
- SLA with alternate site/mirror site with switchover plans
- Change control, preventative action, corrective action, document control and record control processes;
- Local Authority Risk Register;
- Exercise schedule and results;
- Incident log; and
- Training Program

To provide evidence of the effective operation of the BCM, records demonstrating the operation should be retained as per policy of the organisation and as per applicable laws, if any. These records also include reference to all business interruptions and incidents, irrespective of the nature and length of disruption. This also includes general and detailed definition of requirements as described in developing a BCP. In this, a profile is developed by identifying resources required to support critical functions, which include hardware (mainframe, data and voice communication and personal computers), software (vendor supplied, in-house developed, etc.), documentation (user, procedures), outside support (public networks, DP services, etc.), facilities (office space, office equipment, etc.) and personnel for each business unit.

2.5.1 BCM Policy

While developing the BCM policy, the organisation should consider defining the scope, BCM principles, guidelines and applicable standards for the organisation. They should consider all relevant standards, regulations and policies that have to be included or can be used as benchmark. The objective of this policy is to provide a structure through which:

- Critical services and activities undertaken by the organisation will be identified.
- Plans will be developed to ensure continuity of key service delivery following a business disruption, which may arise from the loss of facilities, personnel, IT and/or communication or failure within the supply and support chains.
- Invocation of incident management and business continuity plans can be managed.
- Incident Management Plans and BCP are subject to ongoing testing, revision and updating as required.
- Planning and management responsibility are assigned to members of the relevant senior management team.

The BCM policy defines the processes of setting up activities for establishing a business continuity capability and the ongoing management and maintenance of the business continuity capability. The set-up activities incorporate the specification, end-to-end design, build, implementation and initial exercising of the business continuity capability. The ongoing maintenance and management activities include embedding business continuity within the organisation, exercising plans regularly, and updating and communicating them, particularly when there is significant change in premises, personnel, process, market, technology or organisational structure.

2.5.2 BCP Manual

An incident or disaster affecting critical business operations can strike at any time. Successful organisations have a comprehensive BCP Manual, which ensures process readiness, data and system availability to ensure business continuity. A BCP manual is a documented description of actions to be taken, resources to be used and procedures to be followed before, during and after an event that severely disrupts all or part of the business operations. A BCP manual consists of

the Business Continuity Plan and the Disaster Recovery Plan. The primary objective of preparing BCP manual is to provide reasonable assurance to senior management of organisation about the capability of the organisation to recover from any unexpected incident or disaster affecting business operations and continue to provide services with minimal impact. Further, the BCP should be comprehensive and anticipate various types of incident or disaster scenarios and outline the action plan for recovering from the incident or disaster with minimum impact and ensuring 'Continuous availability of all key services. The BCP Manual is expected to specify the responsibilities of the BCM team, whose mission is to establish appropriate BCP procedures to ensure the continuity of organisation's critical business functions. In the event of an incident or disaster affecting any of the functional areas, the BCM Team serves as visioning teams between the functional area(s) affected and other departments providing support services.

Elements of BCP Manual

The plan will contain the following elements:

1. **Purpose of the plan:** Included in this section should be a summary description of the purpose of the manual. It should be made clear that the manual does not address recovery from day to day operational problems. Similarly, it must be stressed that the manual does not attempt to foresee all possible disasters, but rather provides a framework within which management can base recovery from any given disaster.
2. **Organisation of the manual:** A brief description of the organisation of the manual, and the contents of each of the major sections, will provide the reader with the direction to the relevant section of the manual in an emergency situation. Any information which is external to the manual but will be required in an emergency should be identified in this section.
3. **Disaster definitions:** It may assist the user of the manual if a definition of disaster classification is provided, together with an identification of the relevance of the plan to that situation. Four types of classification can generally be used:
 - **Problem/Incident:** Event or disruptions that cause no significant damage.
 - **Minor disaster:** Event or disruption that causes limited financial impact,
 - **Major disaster:** Event or disruptions that cause significant impact and may have an effect on outside clients.
 - **Catastrophic disaster:** Event or disruption that has significant impact and adversely affect the organisation's "going concern" status

The BCP manual of each organisation is expected to classify disasters, after taking into account the size and nature of its business and the time and cost associated to each kind of disaster should

be defined as per the requirement of the individual organisation. It should be noted, however, that development of a plan based on each classification is not recommended. The need to invoke the plan should be determined by the length and associated cost of the expected outage and not the classification of the disaster, although there is a direct correlation. These definitions will be most useful for communication with senior management.

4. **Objectives of the plan:** The objectives of the manual should be clearly stated in the introductory section. Typically, such objectives include:
 - Safety/security all personnel. The paramount objective of a BCP is to ensure the safety and security of people (both employees and others who may be affected in the event of a disaster). The safeguarding of assets/data is always a secondary objective.
 - the reduction of confusion in an emergency
 - the identification of critical application systems and / or business functions
 - the identification of all resources, including personnel, required to recover the critical business functions
 - the identification of alternative means of ensuring that the critical business functions are performed and
 - The establishment of a workable plan to recover the critical business functions, and subsequently resume normal operations, as quickly as possible after a disaster.

The list should be expanded as necessary to meet the requirements of any given plan.

5. **Scope of the plan:** In order that there is no confusion as the situations in which the plan will apply, the scope of the plan must be clearly identified. Any limitations must be explained.
6. **Plan approach / recovery strategy:** A step by step summary of the approach adopted by the plan should be presented. For ease of reference, it may be good to provide this overview by means of a schematic diagram. In particular, it may be useful to set up the recovery process as a project plan in this section.
7. **Plan administration:** The introductory section should also identify the person or persons, responsible for the business continuity plan manual, and the expected plan review cycles. These persons will be responsible for issuing revisions which will ensure that the plan remains current. Because the manual will include staff assignments, it is also advisable

that the personnel or human resource function accept responsibility for notifying the plan administrators of all personnel changes which must be reflected in the plan.

8. **Plan management:** Following a disaster, the normal reporting channels and lines of management are unlikely to be strictly adhered to. During a disaster, reporting by exception may be the only feasible way to operate. This does not however negate the requirement for formalized management. The management responsibilities and reporting channels to be observed, during disaster recovery should be clearly established in advance.
9. **Disaster notification and plan activation procedures:** The procedures represent the first steps to be followed when any disaster occurs. It is recommended that the procedures be written in a task oriented manner and provide a logical flow to enable ease of management.

2.6 Data backup, Retention and Restoration practices

2.6.1 Back up strategies

Backup refers to making copies of the data so that these additional copies may be used to restore the original data after a data loss. Various backup strategies are:

- **Dual recording of data:** Under this strategy, two complete copies of the database are maintained. The databases are concurrently updated.
- **Periodic dumping of data:** This strategy involves taking a periodic dump of all or part of the database. The database is saved at a point in time by copying it onto some backup storage medium – magnetic tape, removable disk, Optical disk. The dump may be scheduled.
- **Logging input transactions:** This involves logging the input data transactions which cause changes to the database. Normally, this works in conjunction with a periodic dump. In case of complete database failure, the last dump is loaded and reprocessing of the transactions are carried out which were logged since the last dump.
- **Logging changes to the data:** This involves copying a record each time it is changed by an update action. The changed record can be logged immediately before the update action changes the record, immediately after, or both.

Apart from database backup strategies as mentioned above, it is important to implement email and personal files backup policies. The policy can be like burning DVDs with the folders and documents of importance periodically to more detailed and automated functions. The choice depends and varies with the size, nature and complexity of the situation. For example, individuals are responsible for taking backups of personal files and folders. However, a policy may be there whereby individual users may transfer personal files and folders from the PC to an allocated server space. The data

so transferred in the server will be backed up by the IT department as a part of their routine backup. Email backups should necessarily include the address book backup. However, the most important and critical part of the backup strategy is to include a restoration policy. Restoration of the data from the backup media and devices will ensure that the data can be restored in time of emergency; else a failed backup is a double disaster. The restoration should be done for all backups at least twice a year.

Types of Backup

When the back-ups are taken of the system and data together, they are called total system's back-up. An organisation has to choose the right type of back up for each of the critical components of IS and data to meet specific business requirements. The various types of back-ups are:

- **Full Back up:** A full backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data.
- **Incremental Back up:** An incremental backup captures files that were created or changed since the last backup, regardless of backup type. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space. Normally, incremental backup are very difficult to restore. One will have to start with recovering the last full backup, and then recovering from every incremental backup taken since.
- **Differential Backup:** A differential backup stores files that have changed since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up. Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved. Restoring from a differential backup is a two-step operation: Restoring from the last full backup; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup probably includes files that were already included in earlier differential backups.
- **Mirror back-up:** A mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. Mirror backup is most frequently used to create an exact copy of the backup data.

2.6.2 Recovery strategies

The backup plan is intended to restore operations quickly so that information system function can continue to service an organisation, whereas, recovery plans set out procedures to restore full information system capabilities. Recovery plan should identify a recovery team that will be responsible for working out the specifics of the recovery to be undertaken. The plan should specify

the responsibilities of the various departments and provide guidelines on priorities to be followed. The plan might also indicate which applications are to be recovered first. Members of the recovery team must understand their responsibilities. Again, the problem is that they will be required to undertake unfamiliar tasks. Periodically, they must review and practice executing their responsibilities so they are prepared should a disaster occur. If employees leave the organisation, new employees must be assigned the responsibility immediately and briefed about their responsibilities. The recovery strategies for various types of information systems are outlined here.

Strategies for Networked Systems

Most organisations use networked systems. There is heavy dependence on main server and network in case of networked systems. The recovery strategy would vary depending on the type of network architecture and implementation. For example, LANs can be implemented in two main architectures:

LAN Systems

Peer-to-Peer: Each node has equivalent capabilities and responsibilities. For example, five PCs can be networked through a hub to share data.

Client/Server: Each node on the network is either a client or a server. A client can be a PC or a printer where a client relies on a server for resources. A LAN's topology, protocol, architecture, and nodes will vary depending on the organisation. Thus, contingency solutions for each organisation will be different. Listed below are some of the strategies for recovery of LANs.

1. **Eliminating Single Points of Failure (SPOC):** When developing the LAN contingency plan, the organisation should identify single points of failure that affect critical systems or processes outlined in the Risk Assessment. These single points of failures are to be eliminated by providing alternative or redundant equipment.
2. **Redundant Cabling and Devices:** Contingency planning should also cover threats to the cabling system, such as cable cuts, electromagnetic and radiofrequency interference, and damage resulting from fire, water, and other hazards. As a solution, redundant cables may be installed when appropriate. For example, it might not be cost-effective to install duplicate cables to every desktop. However, it might be cost-effective to install a redundant cable between floors so that hosts on both floors could be reconnected if the primary cable were cut. Contingency planning also should consider network connecting devices such as hubs, switches, bridges, and routers.
3. **Remote Access:** Remote access is a service provided by servers and devices on the LAN. Remote access provides a convenience for users working off-site or allows for a means for servers and devices to communicate between sites.

Remote access can be conducted through various methods, including dialup access and virtual private network (VPN). Remote access may serve as allocation that can access the corporate data

even when they are not in a position to reach the physical premises due to some calamity. If remote access is established as a contingency strategy, data bandwidth requirements should be identified and used to scale the remote access solution. Additionally, security controls such as one-time passwords and data encryption should be implemented, if the communication traffic contains sensitive information.

Wireless LANs

Wireless local area networks can serve as an effective contingency solution to restore network services following a wired LAN disruption. Wireless networks do not require the cabling infrastructure of conventional LANs; therefore, they may be installed quickly as an interim or permanent solution. However, wireless networks broadcast the data over a radio signal, enabling the data to be intercepted. When implementing wireless network, security controls, such as data encryption, should be implemented, if the sensitive information is to be communicated.

Strategies for Distributed Systems

A distributed system is an interconnected set of multiple autonomous processing elements, configured to exchange and process data to complete a single business function. To the user, a distributed system appears to be a single source. Distributed systems use the client-server model to make the application more accessible to users in different locations. Distributed systems are implemented in environments in which clients and users are widely dispersed. These systems rely on LAN and WAN resources to facilitate user access and the elements comprising the distributed system require synchronization and coordination to prevent disruptions and processing errors. A common form of distributed systems is a large database management system (DBMS) that supports organisation wide business functions in multiple geographic locations. In this type of application, data is replicated among servers at each location, and users access the system from their local server. The contingency strategies for distributed system reflect the system's reliance on LAN and WAN availability. Based on this fact, when developing a distributed system contingency strategy, the following methods applicable to system backups should be considered for decentralized systems. In addition, a distributed system should consider WAN communication link redundancy and possibility of using Service Bureaus and Application Service Providers (ASPs).

Strategies for Data communications

- i. **Dial-up:** Using Dial-up as a backup to normal leased or broadband communications lines remains the most popular means of backing up wide-area network communications in an emergency. This approach requires compatible modems at each remote site and at the recovery location. Ideally, the modems should be full duplex modems which will permit transmission and receipt down the same line. The half-duplex option will require two telephone lines for each data line lost.

- ii. **Circuit Extension:** Circuit extension techniques are usually applied to high bandwidth communications services, such as high speed leased lines. This technique builds redundancy into the client's network, by including the recovery site as a defined and serviced node. This is by, where the communications from the remote sites can be directed to the primary site or the recovery site from the carrier's central office. This is effective duplication of equipment and facilities, but with some potential for sharing the costs of the equipment at the recovery site.
- iii. **On-demand service from the carriers:** Many carriers now offer on-demand services which provide the mechanisms to switch communications to the recovery site from the primary site on client notification.
- iv. **Diversification of services:** The use of diverse services provides the best solutions to the loss of a carrier central office. Diversity can be achieved in a number of manners, including: Use of more than one carrier on a regular basis. If the organisation uses two or more carriers, it will likely pay above the odds for its regular service and require investment in some additional equipment. For this approach to communications recovery to work, there must also be some redundancy accommodated following any carrier outage.
- v. **Microwave communications:** The regular communications can be backed up by the use of microwave communications. This could be used to: backup communications from the central office to the primary site, in case of breakage in the land lines; backup communications from the central office to the recovery center; or a backup link from a company controlled communications center direct to the recovery center.
- vi. **VSAT (Very Small Aperture Terminal) based satellite communications:** Companies are increasingly looking to VSAT communications as a cost effective means of communicating large volumes of information. This technique could similarly be used to back up the primary carrier service. The use of this technology requires VSAT terminals to be installed at each remote location and at the recovery center if it does not currently provide such a service.

Strategies for Voice Communications

Many of the techniques and concerns above relate to voice communications as well as data, and this will continue with the expansion of ISDN services for integrated voice and data communications. Other techniques available for voice recovery include:

- I. **Cellular phone backup:** If the regular voice system is inoperative, key employees can be provided with cellular phones as a backup. Given that cellular phones are not run by the major carriers from the same central offices, this also provides coverage for the loss of the central office. Such phones could also be used on an on-going basis and could be

used to balance the load on the main PBX switch. Cellular services can also be extended to data and facsimile transmission.

ii. **Carrier call rerouting systems:** Most of the major carriers now provide customers with call rerouting services such that all calls to a given number can be rerouted to another number temporarily. While this will not be possible in the case of a carrier outage, it can be used for the rerouting of critical business communications following a disaster at a client's offices. Calls can be rerouted to call management service, for example, to support the client in the interim.

2.7 Types of recovery and alternative sites

The traditional focus of BCP/DRP was the recovery of the corporate computer system, which was almost always a mainframe or large minicomputer. Mainframe centric disaster recovery plans often concentrated on replacing an inaccessible or non-functional mainframe with compatible hardware. A backup site or work area recovery (alternate processing site) site is a location where an entity can easily function out of immediately following a disaster. This is an integral part of a DRP or BCP. Types of alternate processing sites are outlined along with some of the widely adopted strategies for centralized system recovery.

2.7.1 Mirror Site/ Active Recovery Site

Mirror site

The single most reliable system backup strategy is to have fully redundant systems called an active recovery or mirror site. While most companies cannot afford to build and equip two identical data centers, those companies that can afford to do so have the ability to recover from almost any disaster. This is the most reliable and also the most expensive method of systems recovery.

Hot Site

A dedicated contingency center, or 'hot site' is a fully equipped computer facility with electrical power, heating, ventilation and air conditioning (HVAC) available for use in the event of a subscriber's computer outage. These facilities are available to a large number of subscribers on a membership basis and use of site is on a 'first come, first served' basis. In addition to the computer facility, these facilities offer an area of general office space and computer ready floor space on which the users can build their own long term recovery configuration. Some of the vendors also offer remote operations facilities for use in tests or emergency. Where the recovery center is in a city other than the subscriber's home location, this can be used to reduce the need to transport staff and resources.

A hot site is a duplicate of the original site of the organisation, with full computer systems as well as near-complete backups of user data. Real time synchronization between the two sites may be used to completely mirror the data environment of the original site using wide area network links and specialized software. Following a disruption to the original site, the hot site exists so that the organisation can relocate with minimal losses to normal operations. Ideally, a hot site will be up and running within a matter of hours or even less. Personnel may still have to be moved to the hot site so it is possible that the hot site may be operational from a data processing perspective before staff has relocated. The capacity of the hot site may or may not match the capacity of the original site depending on the organisation's requirements. This type of backup site is the most expensive to operate. Hot sites are popular with organisations that operate real time processes such as financial institutions, government agencies and ecommerce providers.

Cold Site

A cold site is the least expensive type of backup site for an organisation to operate. It does not include backed up copies of data and information from the original location of the organisation, nor does it include hardware already set up. The lack of hardware contributes to the minimal start-up costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster.

Warm Site

A warm site is a compromise between hot and cold. These sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. Warm sites will have backups on hand, but they may not be complete and may be between several days and a week old. An example would be backup tapes sent to the warm site by courier.

2.7.2 Offsite Data protection

Offsite data protection is the strategy of sending critical data out of the main location as a part of DRP. Data is usually transported off-site using removable storage media such as magnetic tape or optical storage. Data can also be sent electronically via a remote backup service, which is known as electronic vaulting or e-vaulting. Sending backups off-site ensures systems and servers can be reloaded with the latest data in the event of a disaster, accidental error, or system crash. Sending backups off-site also ensures that there is a copy of pertinent data that isn't stored on-site. Off-site backup services are convenient for companies that backup pertinent data on a daily basis. The different types of Offsite Data Protection are outlined here.

Data Vaults

Backups are stored in purpose built vaults. There are no generally recognized standards for the type of structure which constitutes a vault. Commercial vaults fit into three categories:

1. Underground vaults
2. Free-standing dedicated vaults
3. Insulated chambers sharing facilities

Hybrid onsite and offsite vaulting

Hybrid on-site and off-site data vaulting, sometimes known as Hybrid Online Backup, involve a combination of Local backup for fast backup and restore, along with Off-site backup for protection against local disasters. This ensures that the most recent data is available locally in the event of need for recovery, while archived data that is needed much less often is stored in the cloud. Hybrid Online Backup works by storing data to local disk so that the backup can be captured at high speed, and then either the backup software or a D2D2C (Disk to Disk to Cloud) appliance encrypts and transmits data to a service provider. Recent backups are retained locally, to speed data recovery operations. There are a number of cloud storage appliances on the market that can be used as a backup target, including appliances from CTERA Networks, Naquin, StorSimple and Twin Strata.

Alternate Site Selection Criteria					
SITE	COST	HARDWARE EQUIPMENT	TELECOMM UNICATIONS	SET UP TIME	LOCATION
COLD SITE	Low	None	None	Long	Fixed
WARM SITE	Medium	Partial	Partial/ Full	Medium	Fixed
HOT SITE	Medium/ High	Full	Full	Short	Fixed
MOBILE SITE	High	Dependent	Dependent	Dependent	Not Fixed
MIRRORED SITE	High	Full	Full	None	Fixed

2.8 System Resiliency Tools and Techniques

2.8.1 Fault Tolerance

Fault-tolerance is the property that enables a system (often computer-based) to continue operating properly in the event of the failure of (or one or more faults within) some of its components. The basic characteristics of fault tolerance require:

1. No single point of failure.
2. No single point of repair.
3. Fault isolation to the failing component.
4. Fault containment to prevent propagation of the failure.
5. Availability of reversion modes.

In addition, fault tolerant systems are characterized in terms of both planned service outages and unplanned service outages. These are usually measured at the application level and not just at a hardware level. The figure of merit is called availability and is expressed as a percentage. A five nines system would therefore statistically provide 99.999% availability. A spare component addresses first fundamental characteristic of fault-tolerance in three ways:

- i. **Replication:** Providing multiple identical instances of the same system or subsystem, directing tasks or requests to all of them in parallel, and choosing the correct result on the basis of a quorum;
- ii. **Redundancy:** Providing multiple identical instances of the same system and switching to one of the remaining instances in case of a failure (failover);
- iii. **Diversity:** Providing multiple *different* implementations of the same specification and using them like replicated systems to cope with errors in a specific implementation.

2.8.2 Redundant array of inexpensive disks (RAID)

RAID provides fault tolerance and performance improvement via hardware and software solutions. It breaks up the data to write it in multiple disks to improve performance and / or save large files. There are many methods of RAID which are categorized into several levels. There are various combinations of these approaches giving different trade -offs of protection against data Loss, capacity, and speed.

RAID levels: Levels 0, 1, and 5 are the most commonly found, and cover most requirements. Generally, most organisations use RAID-1 to RAID-5 for data redundancy.

Electronic vaulting: Electronic vaulting is a backup type where the data is backed up to an offsite location. The data is backed up, generally, through batch process and transferred through communication lines to a server at an alternate location.

Remote journaling: Remote journaling is a parallel processing of transactions to an alternate site, as opposed to batch dump process like electronic vaulting. The alternate site is fully operational at all times and introduces a very high level of fault tolerance.

Database shadowing: Database shadowing is the live processing of remote journaling, but creates even more redundancy by duplicating the database sites to multiple servers.

2.9 Insurance coverage for BCP

The purpose of insurance is to spread the economic cost and the risk of loss from an individual or business to a large number of people. This is accomplished through the use of an insurance policy. Policies are contracts that obligate the insurer to indemnify the policyholder or some third party from specific risks in return for the payment of a premium. Adequate insurance coverage is a key consideration when developing a BCP and performing a risk analysis. Most insurance agencies specializing in business interruption coverage can provide the organisation with an estimate of anticipated business interruption costs. Most business interruption coverage includes lost revenues following disaster. Extra expense coverage includes all additional expenses until normal operations can be resumed.

2.9.1 Coverage

Insurance policies usually can be obtained to cover the following resources:

- **Equipment:** Covers repair or acquisition of hardware. It varies depending on whether the equipment is purchased or leased.
- **Facilities:** Covers items such as reconstruction of a computer room, raised floors, special furniture.
- **Storage media:** Covers the replacement of the storage media plus their contents – data files, programs, documentation.
- **Business interruption:** Covers loss in business income because an organisations unable to trade.
- **Extra expenses:** Covers additional costs incurred because an organisation is not operating from its normal facilities.
- **Valuable papers:** Covers source documents, pre-printed reports, and records documentation, and other valuable papers.
- **Accounts receivable:** Covers cash-flow problems that arise because an organisation cannot collect its accounts receivable promptly.
- **Media transportation:** Covers damage to media in transit.
- **Malpractice, errors:** Covers claims against an organisation by its customers, and omission e.g., claims and omission made by the clients of an outsourcing vendor or service bureau.

2.9.2 Kinds of Insurance

Insurance is generally divided into two general classes based upon whether the insured is the injured party. Lawyers call these two divisions first-party and third-party insurance. First-party insurance identifies claims by the policyholder against their own insurance. Third-party insurance is designed to protect against claims made against the policyholder and his insurer for wrongs

committed by the policyholder. The most common form of first-party insurance is property damage, while the most common form of third-party insurance is liability.

(a) First-party Insurances: Property damages

Perhaps the oldest insurance in the world is that associated with damage to property. It is designed to protect the insured against the loss or destruction of property. It is offered by the majority of all insurance firms in the world and uses time-tested forms, the industry term for a standard insurance contract accepted industry-wide. This form often defines loss as “physical injury to or destruction of tangible property” or the “loss of use of tangible property which has not been physically injured or destroyed.” Such policies are also known as all risks, defined risk, or casualty insurance.

(b) First-party Insurances: Business Interruption

If an insured company fails to perform its contractual duties, it may be liable to its customers for breach of contract. One potential cause for the inability to deliver might be the loss of information system, data or communications. Some in business and the insurance industry have attempted to mitigate this by including information technology in business recovery/disaster plans. As a result, there has emerged a robust industry in hot sites for companies to occupy in case of fire, flood, earthquake or other natural disaster. Disaster recovery has become a necessity in the physical world. While the role of disaster recovery is well understood in business, the insurance industry was slow to accept the indemnity role relative to insuring data in a business interruption liability insurance context. Insurers are generally aggressive in limiting their own liability and have, in a number of instances, argued that a complete cessation of business is necessary to claim damage.

(c) Third-party Insurance: General Liability

Third party insurance is designed to protect the insured from claims of wrongs committed upon others. It is in parts based on the legal theory of torts. Torts are civil wrongs which generally fit into three categories – intentional, negligent and strict liability. Intentional torts are generally excluded from liability insurance policies because they are foreseeable and avoidable by the insured. Strict liability torts, such as product liability issues, are generally covered under specialized liability insurance. Generally liability policies include comprehensive, umbrella and excess liability policies. Insured parties are exposed to the risk of liability whenever they violate some duty imposed on, or expected of, parties’ relative to each other or society in general. In the cyber environment this can take many forms. If the insured’s computer damages another party’s computer, data connectivity, then the insured may be held liable. A company might be held liable if the computer system was used in connection with a denial-of-service attack. The insured may be also held liable for failing to protect adequately the privacy interests of parties who have been entrusted information to the care of the insured.

(iv) Third-party Insurance: Directors and Officers

Errors and Omissions (E&O) insurance is protection from liability arising from a failure to meet the appropriate standard of care for a given profession. Two common forms of E & O insurance are directors and officers, and Professional liability. Directors and officers insurance is designed to protect officers of companies, as individuals, from liability arising from any wrongful acts committed in the course of their duties as officers. These policies usually are written to compensate the officer's company for any losses payable by the company for the acts of its officer's.

2.10 Summary

We can summarize the following key concepts covered in this chapter:

- The development of a Business Continuity Plan can be done with the support of BCP Policy existing in an organisation. BCP Policy sets the scope of the plan. Development of BCP involves planning BCP as a project includes conducting a Business Impact Analyses, Risk Assessment, testing of the BCP, providing training and awareness and continuous maintenance of the BCP Plan.
- Contingency planning encompass Incident Management planning, Disaster recovery planning and Business Continuity planning.
- The hierarchy for invoking a Business Continuity Plan are: Incident Handling and Response → Disaster Recovery → Business Continuity.
- Business Continuity Management would contain the following minimum documents:
 - Business Continuity Policy which documents the scope for the Business Continuity
 - Business Continuity Manual which documents the step by step process to achieve Business Continuity and details of relevant contacts.
- Backup and Recovery Strategies, Types of Alternative Sites, system resiliency tools and techniques etc., are some strategies which are considered in developing a Business Continuity Plan.
- Insurance is a mode of transferring the risk that arises due to the threats to the Business Continuity. The various types of insurance and coverage have been discussed in this chapter.

2.11 Questions

1. Which of the following control concepts should be included in a complete test of disaster recovery procedures?
 - A. Rotate recovery managers.
 - B. Invite client participation
 - C. Involve all technical staff.
 - D. Install locally stored backup.

2. An advantage of the use of hot sites as a backup alternative is:
 - A. The costs related with hot sites are low.
 - B. That hot sites can be used for a long amount of time.
 - C. That hot sites do not require that equipment and systems software be compatible with the primary installation being backed up.
 - D. That hot sites can be made ready for operation within a short span of time.
3. All of the following are security and control concerns associated with disaster recovery procedures EXCEPT:
 - A. Loss of audit trail.
 - B. Insufficient documentation of procedures.
 - C. Inability to restart under control.
 - D. Inability to resolve system deadlock.
4. Which of the following business recovery strategies would require the least expenditure of funds?
 - A. Warm site
 - B. Empty shell
 - C. Hot site
 - D. Reciprocal agreement
5. Which of the following is NOT a feature of an uninterruptible power supply (UPS)?
 - A. It provides electrical supply to a computer in the event of a power failure.
 - B. It system is an external piece of equipment or can be built into the computer itself.
 - C. It should function to allow an orderly computer shutdown.
 - D. It uses a greater wattage into the computer to ensure enough power is available.
6. Which of the following would warranty a quick continuity of operations when the recovery time window is short?
 - A. A duplicated back-up in an alternate site
 - B. Duplicated data in a remote site
 - C. Transfer of data the moment a contingency occurs
 - D. A manual contingency procedure
7. For which of the following applications would rapid recovery be MOST crucial?
 - A. Point-of-sale

- B. Corporate planning
 - C. Regulatory reporting
 - D. Departmental chargeback
8. Which of the following principles must exist to ensure the viability of a duplicate information processing facility?
- A. The site is near the primary site to ensure quick and efficient recovery is achieved.
 - B. The workload of the primary site is monitored to ensure adequate backup is complete.
 - C. The site contains the most advanced hardware available from the chosen vendor.
 - D. The hardware is tested when it is established to ensure it is working properly.
9. While reviewing the business continuity plan of an organisation, the IS auditor observed that the organisation's data and software files are backed up on a periodic basis. Which characteristic of an effective plan does this demonstrate?
- A. Deterrence
 - B. Mitigation
 - C. Recovery
 - D. Response
10. As updates to an online order entry system are processed, the updates are recorded on a transaction tape and a hard copy transaction log. At the end of the day, the order entry files are backed up onto tape. During the backup procedure, the disk drive malfunctions and the order entry files are lost. Which of the following are necessary to restore these files?
- A. The previous day's backup file and the current transaction tape
 - B. The previous day's transaction file and the current transaction tape
 - C. The current transaction tape and the current hardcopy transaction log
 - D. The current hardcopy transaction log and the previous day's transaction file

2.12 Answers and Explanations

- 1. A. Recovery managers should be rotated to ensure the experience of the recovery plan is spread. Clients may be involved but not necessarily in every case. Not all technical staff should be involved in each test. Remote or off-site backup should always be used.
- 2. D. Hot sites can be made ready for operation normally within hours. However, the use of hot sites is expensive, should not be considered as a long-term solution and does require that equipment and systems software be compatible with the primary installation being backed up.

3. D. The inability to resolve system deadlock is a control concern in the design of database management systems, not disaster recovery procedures. All of the other choices are control concerns associated with disaster recovery procedures.
4. D. Reciprocal agreements are the least expensive because they usually rely on a gentlemen's agreement between two firms.
5. D. A UPS typically cleanses the power to ensure wattage into the computer remains consistent and does not damage the computer. All other answers are features of a UPS.
6. D. A quick continuity of operations could be accomplished when manual procedures for a contingency exist. Choices A, B and C are options for recovery.
7. A. A point-of-sale system is a critical online system that when inoperable will jeopardize the ability of a company to generate revenue and properly track inventory.
8. B. Resource availability must be assured. The workload of the site must be monitored to ensure that availability for emergency backup use is not impaired. The site chosen should not be subject to the same natural disaster as the primary site. In addition, a reasonable compatibility of hardware/software must exist to serve as a basis for backup. The latest or newest hardware may not adequately serve this need. Testing the site when established is essential, but regular testing of the actual backup data is necessary to ensure the operation will continue to perform as planned.
9. B. An effective business continuity plan includes steps to mitigate the effects of a disaster. To have an appropriate backup plan, an organisation should have a process capability established to restore data and files on a timely basis, mitigating the consequence of a disaster. An example of deterrence is when a plan includes installation of firewalls for information systems. An example of recovery is when a plan includes an organisation's hot site to restore normal business operations.
10. A. The previous day's backup will be the most current historical backup of activity in the system. The current day's transaction file will contain all of the day's activity. Therefore, the combination of these two files will enable full recovery up to the point of interruption.

CHAPTER 3: AUDIT OF BUSINESS CONTINUITY PLAN

Learning Objectives

This chapter deals with the regulatory requirements that make it mandatory for an organisation to have Business Continuity Management. Best practices frameworks such as COBIT can be used by adapting it as per organisation requirements to achieve effective Business Continuity Management. This chapter provides details of audit procedures that are to be followed by the IS Auditor. The audit is performed to provide assurance to management on the availability of the required controls which mitigate identified risks. A good understanding of the concepts covered in chapters 1 to 3 will help DISAs to provide assurance and consulting services in the area of BCM, BCP and DRP.

3.1 Introduction

A business continuity plan audit is a formalized method for evaluating how business continuity processes are being managed. The goal of an audit is to determine whether the plan is effective and in line with the company's objectives. A business continuity plan audit should define the risks or threats to the success of the plan and test the controls in place to determine whether or not those risks are acceptable. An audit should also quantify the impact of weaknesses of the plan and offer recommendations for business continuity plan improvements.

3.2 Steps of BCP Process

BCP involves more than planning for a move offsite after a disaster destroys a data center. It also addresses how to keep an organisation's critical functions operating in the event of disruptions, both large and small. This broader perspective on contingency planning is based on the distribution of computer support throughout an organisation. Management of organisations are responsible for implementing BCP. IS Auditor is responsible for validating the required BCP processes are implemented and meet the organisation requirements of BCP. A brief overview of the BCP processes are explained below. The six steps in a BCP process are:

1. Identifying the mission- or business-critical functions.
2. Identifying the resources that support the critical functions.
3. Anticipating potential contingencies or disasters.
4. Selecting contingency planning strategies.
5. Implementing the contingency strategies.
6. Testing and revising the strategy.

3.2.1 Step 1: Identifying the mission or business-critical functions

Protecting the continuity of an organization's mission or business is very difficult if it is not clearly identified. Managers need to understand the organization from a point of view that usually extends beyond the area they control. The definition of an organization's critical mission or business functions is often called a business plan. Since the development of a business plan will be used to support contingency planning, it is necessary not only to identify critical missions and businesses, but also to set priorities for them. A fully redundant capability for each function is prohibitively expensive for most organizations. In the event of a disaster, certain functions will not be performed. If appropriate priorities have been set (and approved by senior management), this could make the difference in the organization's ability to survive a disaster.

3.2.2 Step 2: Identifying the resources that support critical functions

BCP has to address all the resources needed to perform a function, regardless whether they directly relate to a computer. The analysis of needed resources is to be conducted by those who understand how the function is performed and the dependencies of various resources on other resources and other critical relationships. This will allow an organization to assign priorities to resources since not all elements of all resources are crucial to the critical functions. Some of the critical tasks and resources of BCP are explained below.

1. Human Resources

People are perhaps an organization's most obvious resource. Some functions require the effort of specific individuals, some require specialized expertise, and some only require individuals who can be trained to perform a specific task. Within the information technology field, human resources include both operators (such as technicians or system programmers) and users (such as data entry clerks or information analysts).

2. Processing capability

Traditionally contingency planning has focused on processing power (i.e., if the data center is down, how can applications dependent on it continue to be processed?). Although the need for data center backup remains vital, today's other processing alternatives are also important. Local area networks (LANs), minicomputers, workstations, and personal computers in all forms of centralized and distributed processing may be performing critical tasks.

3. Automated applications and data

Computer systems run applications that process data. Without current electronic versions of both applications and data, computerized processing may not be possible. If the processing is being performed on alternate hardware, the applications must be compatible with the alternate hardware, operating systems and other software (including version and configuration), and numerous other technical factors. Because of the complexity, it is normally necessary to periodically verify compatibility.

4. Computer-based services

An organization uses many different kinds of computer-based services to perform its functions. The two most important are normally communications services and information services. Communications can be further categorized as data and voice communications; however, in many organizations these are managed by the same service. Information services include any source of information outside of the organization.

5. Physical infrastructure

For people to work effectively, they need a safe working environment and appropriate equipment and utilities. This can include office space, heating, cooling, venting, power, water, sewage, other utilities, desks, telephones, fax machines, personal computers, terminals, courier services, file cabinets, and many other items. In addition, computers also need space and utilities, such as electricity. Electronic and paper media used to store applications and data also have physical requirements.

6. Documents and papers

Many functions rely on vital records and various documents, papers, or forms. These records could be important because of a legal need (such as being able to produce a signed copy of a loan) or because they are the only record of the information. Records can be maintained on paper, microfiche, microfilm, magnetic media, or optical disk.

3.2.3 Step 3: Anticipating potential contingencies or disasters

Although it is impossible to think of all the things that can go wrong, the next step is to identify a likely range of problems. The development of scenarios will help an organization develop a plan to address the wide range of things that can go wrong. Scenarios are to include small and large contingencies. While some general classes of contingency scenarios are obvious, imagination and creativity, as well as research, can point to other possible, but less obvious, contingencies. The contingency scenarios have to address each of the resources described above.

3.2.4 Step 4: Selecting contingency planning strategies

The next step is to plan how to recover needed resources. In evaluating alternatives, it is necessary to consider what controls are in place to prevent and minimize contingencies. Since no set of controls can cost-effectively prevent all contingencies, it is necessary to coordinate prevention and recovery efforts. A contingency planning strategy normally consists of three parts: emergency response, recovery, and resumption. Emergency response encompasses the initial actions taken to protect lives and limit damage. Recovery refers to the steps that are taken to continue support for critical functions. Resumption is the return to normal operations. The relationship between recovery and resumption is important. The longer it takes to resume normal operations, the longer the organization will have to operate in the recovery mode.

3.2.5 Step 5: Implementing the contingency strategies

Once the contingency planning strategies have been selected, it is necessary to make appropriate preparations, document the strategies, and train employees. Many of these tasks are ongoing.

1. Implementation

Much preparation is needed to implement the strategies for protecting critical functions and their supporting resources. For example, one common preparation is to establish procedures for backing up files and applications. Another is to establish contracts and agreements, if the contingency strategy calls for them. Existing service contracts may need to be renegotiated to add contingency services. Another preparation may be to purchase equipment, especially to support a redundant capability.

2. Back up

Backing up data files and applications is a critical part of virtually every contingency plan. Backups are used, for example, to restore files after a personal computer virus corrupts the files or after a hurricane destroys a data processing center.

3. Documentation

It is important to keep preparations, including documentation, up-to-date. Computer systems change rapidly and so should backup services and redundant equipment. Contracts and agreements may also need to reflect the changes. If additional equipment is needed, it must be maintained and periodically replaced when it is no longer dependable or no longer fits the organization's architecture.

4. Assigning responsibility

Preparation should also include formally designating people who are responsible for various tasks in the event of a contingency. These people are often referred to as the contingency response team. This team is often composed of people who were a part of the contingency planning team.

5. No. of BC Plans and responsibility

There are many important implementation issues for an organization. Two of the most important are firstly: How many plans should be developed and secondly: Who prepares each plan? Both of these questions revolve around the organization's overall strategy for contingency planning. The answers should be documented in organization policy and procedures. Some organizations have just one plan for the entire organization, and others have a plan for every distinct computer system, application, or other resource. However, it is important to ensure coordination between various functional heads responsible for managing critical resources.

3.2.6 Step 6: Testing and Revising

A BC plan has to be tested periodically because there will undoubtedly be flaws in the plan and in its implementation. The plan will become dated as time passes and as the resources used to support critical functions change. Responsibility for keeping the plan updated has to be clearly defined in the BC Plan.

3.3 Audit and Regulatory requirements

Business Continuity Planning (BCP) refers to ability of organisations to recover from a disaster and continue operations with least impact. It is imperative that every organisation whether profit-oriented or service-oriented has a business continuity plan as relevant to the activities of the organisation. It is not enough that organisation has a BCP but it is also important to have an independent audit of BCP to confirm its adequacy and appropriateness to meet the needs of the organisation.

3.3.1 Role of IS Auditor in BCP Audit

In a BCP Audit, the IS auditor is expected to evaluate the processes of developing and maintaining documented, communicated, and tested plans for continuity of business operations and IS processing in the event of a disruption. The objective of BCP review is to assess the ability of the organisation to continue all critical operations during a contingency and recover from a disaster within the defined critical recover time period. IS Auditor is expected to identify residual risks which are not identified and provide recommendations to mitigate them. The plan of action for each type of expected contingency and its adequacy in meeting contingency requirements is also assessed

in a BCP audit. BCP of an organisation is also to be reviewed to a limited extent for the assessment of an auditee organisation from the perspective of going concern.

3.3.2 Regulatory requirements

A business continuity plan audit should provide management an evaluation of the organisation's preparedness in the event of a major business disruption. It should identify issues that may limit interim business processing and restoration of same. It should also provide management with an independent assessment of the effectiveness of the business continuity plan and its alignment with subordinate continuity plans. The business continuity plan audit should be programmed to cover the applicable laws, standards and Frameworks etc. Understanding of the applicable Regulatory requirements are essential while doing the audit of any BCP environment to ensure whether the information technology arrangement related to Business continuity and disaster recovery plans are in conformity with the applicable Laws and regulations. It is also necessary to understand whether the information technology related to BCP/DRP arrangements are supporting the business compliance with external laws and regulations. Hence before designing the audit scope and programs all external compliance requirements are to be identified and External compliance requirements are adequately addressed. This can be ensured by adopting the following management practices as suggested by COBIT 5 Process MEA03 Monitor, Evaluate and Assess Compliance with External Requirements. COBIT stands for Control Objectives for Information and Related Technology. Given below are some relevant extracts from COBIT 5: Enabling process which are relevant and can be adapted for implementing or reviewing BCP processes of any organisation.

Using COBIT best practices for evaluating regulatory compliances

MEA03 Monitor, Evaluate and Assess Compliance with External Requirements

Process 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 organisation compliance.

Process Purpose

Ensure that the organisation is compliant with all applicable external requirements.

Management Practices

1. 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. This will be achieved by doing following activities:

- Assign responsibility for identifying and monitoring any changes of legal, regulatory and other external contractual requirements relevant to the use of IT resources and the processing of information within the business and IT operations of the organisation.
- Identify and assess all potential compliance requirements and the impact on IT activities in areas such as data flow, privacy, internal controls, financial reporting, industry-specific regulations, intellectual property, health and safety.
- Assess the impact of IT-related legal and regulatory requirements on third-party contracts related to IT operations, service providers and business trading partners.
- Obtain independent counsel, where appropriate, on changes to applicable laws, regulations and standards.
- Maintain an up-to-date log of all relevant legal, regulatory and contractual requirements, their impact and required actions.
- Maintain a harmonized and integrated overall register of external compliance requirements for the organisation.

2. 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. This can be achieved by doing following activities:

- Regularly review and adjust policies, principles, standards, procedures and methodologies for their effectiveness in ensuring necessary compliance and addressing organisation risk using internal and external experts, as required.
- Communicate new and changed requirements to all relevant personnel.

3. Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements. This is ensured by adopting the following activities:

- Regularly evaluate organisational policies, standards, procedures and methodologies in all functions of the organisation to ensure compliance with relevant legal and regulatory requirements in relation to the processing of information.
- Address compliance gaps in policies, standards and procedures on a timely basis.
- Periodically evaluate business and IT processes and activities to ensure adherence to applicable legal, regulatory and contractual requirements.
- Regularly review for recurring patterns of compliance failures. Where necessary, improve policies, standards, procedures, methodologies, and associated processes and activities.

4. 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. To ensure this management practice the following activities are to be ensured:

- Obtain regular confirmation of compliance with internal policies from business and IT process owners and unit heads.
- Perform regular (and, where appropriate, independent) internal and external reviews to assess levels of compliance.
- If required, obtain assertions from third-party IT service providers on levels of their compliance with applicable laws and regulations.
- If required, obtain assertions from business partners on levels of their compliance with applicable laws and regulations as they relate to intercompany electronic transactions.
- Monitor and report on non-compliance issues and, where necessary, investigate the root cause.
- Integrate reporting on legal, regulatory and contractual requirements at an organisation wide level, involving all business units.

3.3.3 Regulatory compliances of BCP

Regulatory requirements play an important role in outlining the need for BCP for organisations which provide critical services. These regulations also provide generic guidelines for implementing BCP. Some of the sample laws and regulations that are applicable are given here:

Basel Committee on E Banking

The Basel Committee on E-Banking outlines the principles for electronic banking as; “Banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services”. The Committee underlines that banks should also ensure that periodic independent internal and/or external audits are conducted about business continuity and contingency planning. These requirements are spelt out in Appendix VI relating to “Sound Capacity, Business Continuity and Contingency Planning Practices for E-Banking”.

Indian legislations

There are various Indian legislations such as the Information Technology Act, Indian Income Tax act, Central Sales Tax act, State VAT Acts, Services tax act, Central excise act etc. which require data retention for specific number of years. Organisations which have to comply with these requirements have to ensure that they have a proper business continuity plan which meets these requirements. The Reserve bank of India provides regular guidelines to financial institutions covering various aspects of IT deployment. These guidelines cover business continuity and disaster recovery procedures for various types of business operations which are dependent on IT environment.

Bank Audit

The Long Form Audit report in the case of statutory audit of banks contains two key points relating to business continuity and disaster recovery which need to be evaluated and commented by the statutory auditor.

- Whether regular back-ups of accounts and off-site storage are maintained as per the guidelines of the controlling authorities of the bank?
- Whether adequate contingency and disaster recovery plans are in place for loss/encryption of data?

The first point may be irrelevant in case of audit of branches where core banking solution is implemented. However, a general review of the contingency and disaster recovery plans has to be made by auditor and required comments provided. In case of internal audit or concurrent audit of banks, there are specific areas of BCP which need to be reviewed by the auditors.

3.4 Using best practices and frameworks for BCP

3.4.1 COBIT 5

COBIT 5 is a framework of business governance. It provides a set of best practices for Governance and management of Organisation IT. Best practices pertaining to BCM can be selected and adapted as required. Below is an extract of management practices and activities from COBIT which is applicable to BCP.

DSS04: Manage continuity

Process 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 organisation.

Process Purpose

Continue critical business operations and maintain availability of information at a level acceptable to the organisation in the event of a significant disruption.

Management Practices and activities

1. **Define the business continuity policy, objectives and scope:** Define business continuity policy and scope aligned with organisation and stakeholder objectives.

- Identify internal and outsourced business processes and service activities that are critical to the organisation operations or necessary to meet legal and/or contractual obligations.

- Identify key stakeholders and roles and responsibilities for defining and agreeing on continuity policy and scope.
- Define and document the agreed-on minimum policy objectives and scope for business continuity and embed the need for continuity planning in the organisation culture.
- Identify essential supporting business processes and related IT Services.

2. Maintain a continuity strategy: Evaluate business continuity management options and choose a cost-effective and viable continuity strategy that will ensure organisation recovery and continuity in the face of a disaster or other major incident or disruption.

- Identify potential scenarios likely to give rise to events that could significant disruptive incidents.
- Conduct a business impact analysis to evaluate the impact overtime of a disruption to critical business functions and the effect that a disruption would have on them.
- Establish the minimum time required to recover a business process and supporting IT based on an acceptable length interruption and maximum tolerable outage.
- Assess the likelihood of threats that could cause loss of business continuity and identify measures that will reduce the likelihood and impact through improved prevention and increased resilience.
- Analyze continuity requirements to identify the possible strategic business and technical options.
- Determine the conditions and owners of key decisions that will cause the continuity plans to be invoked.
- Identify resource requirements and costs for each strategic technical option and make strategic recommendations.
- Obtain executive business approval for selected strategic options.

3. Develop and implement a business: continuity response. Develop a business continuity plan (BCP) based on the strategy that documents the procedures and information in readiness for use in an incident to enable the organisation to continue its critical activities.

- Define the incident response actions and communications to be taken in the event of disruption. Define related roles and responsibilities, including accountability for policy and implementation.
- Develop and maintain operational BCPs containing the procedures to be followed to enable continued operation of critical business processes and/or temporary processing arrangements, including links to plans of outsourced service providers.
- Ensure that key suppliers and outsource partners have effective continuity plans in place. Obtain audited evidence as required.
- Define the conditions and recovery procedures that would enable resumption of business processing, including updating and reconciliation of information databases to preserve information integrity.

- Define and document the resources required to support the continuity and recovery procedures, considering people, facilities and IT infrastructure.
- Define and document the information backup requirements required to support the plans, including plans and paper documents as well as data files, and consider the need for security and off-site storage.
- Determine required skills for individuals involved in executing the plan and procedures.
- Distribute the plans and supporting documentation securely to appropriately authorize interested parties and make sure they are accessible under all disaster scenarios.

4. **Exercise, test and review the BCP:** Test the continuity arrangements on a regular basis to exercise the recovery plans against predetermined outcomes and to allow innovative solutions to be developed and help to verify over time that the plan will work as anticipated.

- Define objectives for exercising and testing the business, technical, logistical, administrative, procedural and operational systems of the plan to verify completeness of the BCP in meeting business risk.
- Define and agree on with stakeholders exercises that are realistic, validate continuity procedures, and include roles and responsibilities and data retention arrangements that cause minimum disruption to business processes.
- Assign roles and responsibilities for performing continuity plan exercises and tests.
- Schedule exercises and test activities as defined in the continuity plan.
- Conduct a post-exercise debriefing and analysis to consider the achievement.
- Develop recommendations for improving the current continuity plan based on the results of the review.

5. **Review, maintain and improve the continuity plan:** Conduct a management review of the continuity capability at regular intervals to ensure its continued suitability, adequacy and effectiveness. Manage changes to the plan in accordance with the change control process to ensure that the continuity plan is kept up to date and continually reflects actual business requirements.

- Review the continuity plan and capability on a regular basis against any assumptions made and current business operational and strategic objectives.
- Consider whether a revised business impact assessment may be required, depending on the nature of the change.
- Recommend and communicate changes in policy, plans, procedures, infrastructure, and roles and responsibilities for management approval and processing via the change management process.
- Review the continuity plan on a regular basis to consider the impact of new or major changes to: organisation, business processes, outsourcing arrangements, technologies, infrastructure, operating systems and application systems.

6. Conduct continuity plan training. Provide all concerned internal and external parties with regular training sessions regarding the procedures and their roles and responsibilities in case of disruption.

- Define and maintain training requirements and plans for those performing continuity planning, impact assessments, risk assessments, media communication and incident response. Ensure that the training plans consider frequency of training and training delivery mechanisms.
- Develop competencies based on practical training including participation in exercises and tests.
- Monitor skills and competencies based on the exercise and test results.

7. Manage backup arrangements: Maintain availability of business critical information.

- Backup systems, applications, data and documentation according to a defined schedule, considering:
 - Frequency (monthly, weekly, daily, etc.)
 - Mode of backup (e.g., disk mirroring for real-time backups vs. DVD-ROM for long-term retention)
 - Type of backup (e.g., full vs. incremental)
 - Type of media
 - Automated online backups
 - Data types (e.g., voice, optical)
 - Creation of logs
 - Critical end-user computing data (e.g., spreadsheets)
 - Physical and logical location of data sources
 - Security and access rights
 - Encryption
- Ensure that systems, applications, data and documentation maintained or processed by third parties are adequately backed up or otherwise secured. Consider requiring return of backups from third parties. Consider escrow or deposit arrangements.
- Define requirements for on-site and off-site storage of backup data that meet the business requirements. Consider the accessibility required to back up data.
- Roll out BCP awareness and training.
- Periodically test and refresh archived and backup data.

8. Conduct post-resumption review: Assess the adequacy of the BCP following the successful resumption of business processes and services after a disruption.

- Assess adherence to the documented BCP.
- Determine the effectiveness of the plan, continuity capabilities, roles and responsibilities, skills and competencies, resilience to the incident, technical infrastructure, and organisational structures and relationships.

- Identify weaknesses or omissions in the plan and capabilities and make recommendations for improvement.
- Obtain management approval for any changes to the plan and apply via the organisation change control process.

BAI04: Manage Availability and Capacity

Process 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.

Process Purpose

Maintain service availability, efficient management of resources, and optimization of system performance through prediction of future performance and capacity requirements.

Management Practices and activities

1. Assess current availability, performance and capacity and create a baseline: Assess availability, performance and capacity of services and resources to ensure that cost-justifiable capacity and performance are available to support business needs and deliver against SLAs. Create availability, performance and capacity baselines for future comparison.

- Consider the following (current and forecasted) in the assessment of availability, performance and capacity of services and resources: customer requirements, business priorities, business objectives, budget impact, resource utilization, IT capabilities and industry trends.
- Monitor actual performance and capacity usage against defined thresholds, supported where necessary with automated software.
- Identify and follow up on all incidents caused by inadequate performance or capacity.
- Regularly evaluate the current levels of performance for all processing levels (business demand, service capacity and resource capacity) by comparing them against trends and SLAs, taking into account changes in the environment.

2. Assess business impact: Identify important services to the organisation, map services and resources to business processes, and identify business dependencies. Ensure that the impact of unavailable resources is fully agreed on and accepted by the customer. Ensure that, for vital business functions, the SLA availability requirements can be satisfied.

- Identify only those solutions or services that are critical in the availability and capacity management process.
- Map the selected solutions or services to application(s) and infrastructure (IT and facility) on which they depend to enable a focus on critical resources for availability planning.
- Collect data on availability patterns from logs of past failures and performance monitoring. Use modelling tools that help predict failures based on past usage trends and management expectations of new environment or user conditions.
- Create scenarios based on the collected data, describing future availability situations to illustrate a variety of potential capacity levels needed to achieve the availability performance objective.
- Determine the likelihood that the availability performance objective will not be achieved based on the scenarios.
- Determine the impact of the scenarios on the business performance measures (e.g., revenue, profit, customer services). Engage the business line, functional (especially finance) and regional leaders to understand their evaluation of impact.
- Ensure that business process owners fully understand and agree to the results of this analysis. From the business owners, obtain a list of unacceptable risk scenarios that require a response to reduce risk to acceptable levels.

3. Plan for new or changed service requirements: Plan and prioritise availability, performance and capacity implications of changing business needs and service requirements.

- Review availability and capacity implications of service trend analysis.
- Identify availability and capacity implications of changing business needs and improvement opportunities. Use modelling techniques to validate availability, performance and capacity plans.
- Prioritize needed improvements and create cost-justifiable availability and capacity plans.
- Adjust the performance and capacity plans and SLAs based on realistic, new, proposed and/or projected business processes and supporting services, applications and infrastructure changes as well as reviews of actual performance and capacity usage, including workload levels.
- Ensure that management performs comparisons of actual demand on resources with forecasted supply and demand to evaluate current forecasting techniques and make improvements where possible.

4. Monitor and review availability and capacity: Monitor, measure, analyses, report and review availability, performance and capacity. Identify deviations from established baselines. Review trend analysis reports identifying any significant issues and variances, initiating actions where necessary, and ensuring that all outstanding issues are followed up.

- Establish a process for gathering data to provide management with monitoring and reporting information for availability, performance and capacity workload of all information-related resources.
- Provide regular reporting of the results in an appropriate form for review by IT and business management and communication to organisation management.
- Integrate monitoring and reporting activities in the iterative capacity management activities (monitoring, analysis, tuning and implementations).
- Provide capacity reports to the budgeting processes.

5. Investigate and address availability, performance and capacity issues: Address deviations by investigating and resolving identified availability, performance and capacity issues.

- Obtain guidance from vendor product manuals to ensure an appropriate level of performance availability for peak processing and workloads.
- Identify performance and capacity gaps based on monitoring current and forecasted performance. Use the known availability, continuity and recovery specifications to classify resources and allow prioritization.
- Define corrective actions (e.g., shifting workload, prioritizing tasks or adding resources, when performance and capacity issues are identified).
- Integrate required corrective actions into the appropriate planning and change management processes.
- Define an escalation procedure for swift resolution in case of emergency capacity and performance problems.

For more information, please www.isaca.org/cobit.

3.4.2 ISO 22301: Standard on Business Continuity Management

ISO 22301 specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to prepare for, respond to and recover from disruptive events when they arise. The requirements specified in ISO 22301 are generic and intended to be applicable to all organisations (or parts thereof), regardless of type, size and nature of the organisation. The extent of application of these requirements depends on the organisation's operating environment and complexity. Following the new structure of the ISO Guide 83, ISO 22301 is organized into the following main clauses:

- Clause 4: Context of the organisation
- Clause 5: Leadership
- Clause 6: Planning
- Clause 7: Support
- Clause 8: Operation
- Clause 9: Performance evaluation

- Clause 10: Improvement

For more information, please www.iso.org.

3.3.3 ITIL

Information Technology Infrastructure Library (ITIL), a UK body, is a collection of best practices in IT service management, consisting of a series of books giving guidance on the provision of quality IT services. ITIL is drawn from the public and private sectors internationally, supported by a comprehensive qualification scheme and accredited training organisations. ITIL is the most widely adopted approach for IT Service Management in the world. It provides a practical, no-nonsense framework for identifying, planning, delivering and supporting IT services to the business. It includes descriptions of best practice in information security management as well as other related disciplines. For more information, please visit: www.itil-officialsite.com.

3.3.4 SSAE 16

Statement on Standards for Attestation Engagements (SSAE) No. 16, known as SSAE 16, has been put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). SSAE 16 is an “attest” standard that closely mirrors its international “assurance” equivalent, ISAE 3402, which was issued by the International Auditing and Assurance Standards Board (IAASB), a standard-setting board of the International Federation of Accountants (IFAC). SSAE 16 is issued by AICPA. It is generally applicable when an auditor (called the “user auditor”) is auditing the financial statements of an entity (“user organisation”) that obtains services from another organisation (“service organisation”). The service organisations that provide such services could be application service providers, bank trust departments, claims processing centers, Internet data centers, or other data processing service bureaus. . For more information, please visit: www.ssae16.org

3.4.3 Audit Tools and Techniques

The objective of BCP audit is to provide assurance to management on adequacy of BCP process and DRP procedures, identify control gaps, ensure regulatory compliance and ensure business process owners are accountable for their plans and testing. The best audit tool and technique is a periodic simulation of a disaster. Other audit techniques would include observations, interviews, checklists, inquiries, meetings, questionnaires and documentation reviews. These tools and methods may be categorized as explained here.

- Automated Tools:** Automated tools make it possible to review large computer systems for a variety of flaws in a short time period. They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, lack of integrity of the system software, etc.

- ii. **Internal Control Auditing:** This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance of laws and regulations.
- iii. **Disaster and Security Checklists:** A checklist can be used against which the system can be audited. The checklist should be based upon disaster recovery policies and practices, which form the baseline. Checklists can also be used to verify changes to the system from contingency point of view.
- iv. **Penetration Testing:** Penetration testing can be used to locate vulnerabilities in the network.

3.4.4 Service Level Agreement

A service level agreement is an agreement between the organisation and the customer. The SLA details are the services(s) to be provided. The IT organisation could be an internal IT department or an external IT service provider, and the customer is the business. The business may acquire IT services from an internal IT organisation, such as email services, an intranet, an organisation resource planning (ERP) system, etc. the business may acquire IT services from an external IT service provider, such as internet connectivity, hosting of a public website. The SLA describes the services in nontechnical terms, from the viewpoint of the customer.

During the term of the agreement, it serves as the standard for measuring and adjusting the services. Service levels are often defined to include hardware and software performance targets (such as user response time and hardware availability) but can also include a wide range of other performance measures. Such measures might include financial performance measures (such as year to year incremental cost reduction), human relationship measures (such as resource planning, staff turnover, development and training) or risk management measures (compliance with control objectives).

The IS auditor should be aware of the different types of measures available and should ensure that they are comprehensive and include risk, security and control measures as well as security and control measures as well as efficiency and effectiveness measures.

Where the functions of a BCP are outsourced, the IS auditor should determine how management gains assurance that the controls at the third party are properly designed and operating effectively. Several techniques can be used by management, including questionnaires, onsite visits or an independent third-party assurance report such as an SSAE 16 SOC 1 report or SOC 2 or SOC 3 report.

3.5 Services that can be provided by an IS Auditor in BCM

1. **Management Consultancy Services** in providing guidance in drafting of a BCP/DRP. CAs can provide insight to the organisation on the development of a BCP/DRP. Appropriate

guidance in drafting a BCP such as scoping of the BCP as per the policy etc. Development of a BCP Manual.

2. Management Consultancy Services in designing and implementing a BCP/DRP. CAs can provide guidance in the actual design of the BCP that is relevant to the organisation's nature and size. They can assist the management in implementing the BCP in the organisation. They can design the phases for implementation of the BCP and thus ensure correct and effective implementation of the BCP in the organisation.
3. Designing Test Plans and Conducting Tests of the BCP/DRP. CAs can design plans that can be used by the management for regular testing of the BCP. He can also evaluate the tests that have been conducted by the management.
4. Consultancy Services in revising and updating the BCP/DRP. Maintenance of the BCP is a periodic process. Technologies evolve and the Business Environment often changes and hence it is necessary to revise and update the BCP.
5. Conducting Pre Implementation Audit, Post Implementation Audit, General Audit of the BCP/DRP.
A Chartered Accountant can provide assurance whether the BCP would suffice to the organisation.
6. Consultancy Services in Risk Assessment and Business Impact Analysis. Conducting a proper Business Impact Analysis and assessing the risks that are present in the organisation's environment is really crucial for the correct development of the BCP/DRP. CAs can help in the development stages by conducting BIA and Risk Assessment for the organisation.
7. CAs can be involved in any/all areas of BCP implementation or review. These areas could be pertaining to:
 - a. Risk Assessment
 - b. Business Impact Assessment
 - c. Disaster Recovery Strategy Selection
 - d. Business Continuity Plan Development
 - e. Fast-track Business Continuity Development
 - f. BCP / DRP Audit, Review and Health-check Services
 - g. Development and Management of BCP / DRP Exercises and Rehearsals
 - h. Media Management for Crisis Scenarios
 - i. Business Continuity Training

3.6 Summary

A BCP is not merely about information Technology Assets but is also about people reactions in case of a crisis. In a crisis, people have to assume responsibilities that are different from their normal day to day tasks. This requires a series of coordinated actions on the part of the personnel involved. A BCP is rarely a standalone document. It is, usually, part of a set of documents... There may be a separate plan, the Cyber Incident Response Plan, to take care of threats like computer

viruses and network intrusions. An Occupant Emergency Plan (OEP) may be in use for the evacuation of premises during a fire or medical emergencies. Insurance is yet another tool that supplements BCP. Monetary losses can be minimized by transferring certain risks to an insurance company on the payment of a premium. A BCP that exists on paper without being tested serves no useful purpose. The worst possible way to "test" is to see whether it works during a real disaster. Ideally, while framing the objectives of the BCP, the organisation spells out the "acceptance criteria", that is, the tests that will validate the BCP. Testing a BCP can be a complex undertaking as many personnel will have to carry out the tests even while continuing with normal operations.

After the completion of Chapter 3, we can summarize the broad coverage as follows:

- IS Auditor has to understand BCP processes and key activities for each of the key processes. This chapter has provided an overview of the BCP processes.
- Regulations such as the Sarbanes Oxley Act, HIPAA, and BASEL 2 make it mandatory for an organisation to have Business Continuity Management. Standards such as ISO 22301, 27000 etc. and Frameworks such as COBIT, ITIL lays down the steps that could be followed by the management of the organisation to have efficient Business Continuity Management Practices.
- Audit Process that are to be followed by an IS Auditor. A control is placed always against an identified risk by the management. It is essential for an IS Auditor to verify the controls that have been put in place by the management for adequacy and existence. IS auditor has to follow the standard auditing procedures and guidance notes (if any) issued by the governing bodies (Like ICAI in case of Chartered accountants, ISACA in case of certified information system auditors etc.) while discharging their duties.

3.7 References

www.icai.org

www.isaca.org

www.csoonline.com

www.thebci.org

www.aicpa.org

www.iso.org

www.bsigroup.org

3.8 Questions

1. An IS auditor reviewing an organisation's information systems disaster recovery plan should verify that it is:
 - A. Tested every 1 month.
 - B. Regularly reviewed and updated.
 - C. Approved by the chief executive officer
 - D. Approved by the top management
2. Which of the following would an IS auditor consider to be the MOST important to review when conducting a business continuity audit?
 - A. A hot site is contracted for and available when needed.
 - B. A business continuity manual is available and current.
 - C. Insurance coverage is sufficient
 - D. Media backups are performed on a timely basis and stored off-site.
3. Which of the following findings would an IS auditor be MOST concerned about when performing an audit of backup and recovery and the offsite storage vault?
 - A. There are three individuals with a key to enter the area
 - B. Paper documents are also stored in the offsite vault
 - C. Data files, which are stored in the vault, are synchronized
 - D. The offsite vault is located in a separate facility
4. A company performs full back-up of data and programs on a regular basis. The primary purpose of this practice is to:
 - A. Maintain data integrity in the applications.
 - B. Restore application processing after a disruption.
 - C. Prevent unauthorized changes to programs and data.
 - D. Ensure recovery of data processing in case of a disaster.
5. Which of the following procedures would an IS auditor perform to BEST determine whether adequate recovery/restart procedures exist?
 - A. Reviewing program code
 - B. Reviewing operations documentation
 - C. Turning off the UPS, then the power
 - D. Reviewing program documentation

6. An IS auditor performing a review of the back-up processing facilities would be MOST concerned that:
 - A. Adequate fire insurance exists.
 - B. Regular hardware maintenance is performed.
 - C. Offsite storage of transaction and master files exists.
 - D. Backup processing facilities are fully tested.
7. Which of the following offsite information processing facility conditions would cause an IS auditor the GREATEST concern?
 - A. Company name is clearly visible on the facility.
 - B. The facility is located outside city limits from the originating city.
 - C. The facility does not have any windows.
 - D. The facility entrance is located in the back of the building rather than the front.
8. Which of the following methods of results analysis, during the testing of the business continuity plan (BCP), provides the BEST assurance that the plan is workable?
 - A. Quantitatively measuring the results of the test
 - B. Measurement of accuracy
 - C. Elapsed time for completion of prescribed tasks
 - D. Evaluation of the observed test results
9. An IS auditor conducting a review of disaster recovery plan (DRP) at a financial processing organisation has noticed that existing DRP was compiled two years ago by a systems analyst using information from operations department. The plan was presented to CEO for approval but it is not yet approved. The plan has never been updated, tested or circulated to key management and staff, though interviews show that each would know what action to take for their area in the event of a disruptive incident. The IS auditor's report should recommend:
 - A. The deputy CEO be censured for his failure to approve the plan.
 - B. A board of senior managers be set up to review the existing plan.
 - C. The existing plan be approved and circulated to all key management and staff.
 - D. An experienced manager coordinates the creation of a new plan or revised plan within a defined time limit.
10. Which of the following would be of MOST concern for an IS auditor reviewing back-up facilities?
 - A. adequate fire insurance exists.
 - B. regular hardware maintenance is performed.
 - C. offsite storage of transaction and master files exists.

D. backup processing facilities are fully tested.

3.9 Answers and Explanations

1. B. The plan must be reviewed at appropriate intervals, depending upon the nature of the business and the rate of change of systems and personnel, otherwise it may quickly become out of date and may no longer be effective (for example, hardware or software changes in the live processing environment are not reflected in the plan). The plan must be subjected to regular testing, but the period between tests will depend on nature of the organisation and relative importance of IS. Three months or even annually may be appropriate in different circumstances. Although the disaster recovery plan should receive the approval of senior management, it need not be the CEO if another executive officer is equally, or more appropriate. For a purely IS-related plan, the executive responsible for technology may have approved the plan. the IS disaster recovery plan will usually be a technical document and relevant to IS and communications staff only.
2. D. Without data to process, all other components of the recovery effort are in vain. Even in the absence of a plan, recovery efforts of any type would not be practical without data to process.
3. C. More than one person would need to have a key to the vault and location of the vault is important, but not as important as the files being synchronized. Choice A is incorrect because more than one person would typically need to have a key to the vault to ensure that individuals responsible for the offsite vault can take vacations and rotate duties. Choice B is not correct because the IS auditor would not be concerned whether paper documents are stored in the offsite vault. In fact, paper documents such as procedural documents and a copy of the contingency plan would most likely be stored in the offsite vault.
4. B. Back-up procedures are designed to restore programs and data to a previous state prior to computer or system disruption. These backup procedures merely copy data and do not test or validate integrity. Back-up procedures will also not prevent changes to program and data. On the contrary, changes will simply be copied. Although backup procedures can ease the recovery process following a disaster, they are not sufficient in themselves.
5. B. Operations documentation should contain recovery/restart procedures so that operations can return to normal processing in a timely manner. Turning off the UPS and then turning off the power might create a situation for recovery and restart, but the negative effect on operations would prove this method to be undesirable. The

review of program code and documentation generally does not provide evidence regarding recovery/restart procedures.

6. C. Adequate fire insurance and fully tested backup processing facilities are important elements for recovery, but without the offsite storage of transaction and master files, it is generally impossible to recover. Regular hardware maintenance does not relate to recovery.
7. A. The offsite facility should not be easily identified from the outside. Signs identifying the company and the contents of the facility should not be present. This is to prevent intentional sabotage of the offsite facility should the destruction of the originating site be from malicious attack. The offsite facility should not be subject to the same natural disaster that affected the originating site. The offsite facility must also be secured and controlled just as the originating site. This includes adequate physical access controls such as locked doors, no windows and human surveillance.
8. A. Quantitatively measuring the results of the test involves a generic statement measuring all the activities performed during BCP, which gives the best assurance of an effective plan. Although choices B and C are also quantitative, they relate to specific areas or an analysis of results from one viewpoint, namely the accuracy of the results and the elapsed time.
9. D. The primary concern is to establish a workable disaster recovery plan which reflects current processing volumes to protect the organisation from any disruptive incident. Censuring the deputy CEO will not achieve this, and is generally not within the scope of an IS Auditor to recommend anyway. Setting up a board to review the plan, which is two years out of date, may achieve an updated plan, but is not likely to be a speedy operation and issuing the existing plan would be folly without first ensuring that it is workable. The best way to achieve a disaster recovery plan in a short timescale is to make an experienced manager responsible for coordinating the knowledge of other managers, as established by the audit interviews, into a single, formal document within a defined time limit.
10. C Adequate fire insurance and fully tested backup processing facilities are important elements for recovery, but without the offsite storage of transaction and master files, it is generally impossible to recover. Regular hardware maintenance does not relate to recovery.

SECTION 3: APPENDIX

CHECKLISTS AND CONTROL MATRIX

Appendix 1: Checklist for a Business Continuity Plan and Audit

Process Objectives:

- To seamlessly recover from the disaster situation.
- To reduce the impact of the damage of the assets, in turn reducing the data loss.
- To assure compliances
- To sustain operations so that customer service and corporate image can be maintained.

Using this Checklist:

This checklist is to be used by the IS Auditor who is conducting the BCP Audit. This checklist covers the entire BCP Process but it has to be customized as per the specific needs of the assignment. An IS Auditor can use this checklist as a basis for recording observations and for collecting evidences for the Audit engagement. This is checklist is an illustrative example as to how an IS Auditor could conduct a BCM Audit at an organisation. It can be taken as a base for conducting such audit engagements.

Sl. No	Checkpoints/Particulars
Policy and Procedure	
1.	Is business continuity plan documented and implemented?
2.	Whether the scope and objectives of a BCP are clearly defined in the policy document? (Scope to cover all critical activities of business. Objectives should clearly spell out outcomes of the BCP)
3.	Whether there exist any exceptions to the scope of BCP i.e. in terms of location or any specific area, and whether the management has justifications for exclusion of the same.
4.	What is the time limit for such exclusion and what is the current strategy of covering such exclusions
5.	Are the policy and procedure documents approved by the Top Management? (Verify sign off on policy and procedure documents and budget allocations made by the management for a BCP)
6.	Does the business continuity plan ensure the resumption of IS operations during major information system failures? (Verify that the IS disaster recovery plan is in line with strategies, goals and objectives of corporate business continuity plan).
7.	Are users involved in the preparation of business continuity plan?

Sl. No	Checkpoints/Particulars
	(Managerial, operational, administrative and technical experts should be involved in the preparation of the BCP and DRP).
8.	Does the policy and procedure documents include the following - List of critical information assets. - List of vendor for service level agreements. - Current and future business operations. - Identification of potential threats and vulnerabilities. - Business impact analysis. - Involvement of technical and operational expert in preparation of BCP and Disaster recovery plans. - Recovery procedure to minimize losses and interruptions in business operations. - Disaster recovery teams. - Training and test drills. - Compliance with statutory and regulatory requirements
9.	Are the BCP policy and procedures circulated to all concerned? (Verify availability and circulation of the BCP & DRP to all concerned, including onsite and offsite storage).
10.	Is the business continuity plan updated and reviewed regularly? (Verify minutes of meeting where policy and procedures are reviewed. Verify amendments made to the policy and procedure documents due to the change in business environment).
Risk Assessment	
1.	Has the management identified potential threats/vulnerabilities to business operations? (Verify the business environment study report. Risk Assessment Report?)
2.	Are the risks evaluated by the Management? (Verify the probability or occurrence of the threat / vulnerability review carried out by the management).
3.	Has the organisation selected the appropriate method for risk evaluation?
4.	Has the organisation carried out the assessment of internal controls? (Verify the internal controls mitigating the risk).
5	Has the organisation taken an appropriate decision on the risks identified? (Verify the decision-making on the options - accepted, reduced, avoided or transferred – for the risks identified).
6.	Are the risk assessment carried out at regular interval? (Verify the review frequency.)
Business Impact Analysis	
1.	Does the organisation carry out business impact analysis (BIA) for business operations?

Sl. No	Checkpoints/Particulars
2.	Has the organisation identified a BIA team?
3.	Are RTO and RPO defined by the management?
4.	Whether the SDO has been defined based upon RTO & RPO
5.	Whether the organisation has measured BIA? (Impact of risks on business operations can be measured in the form of business loss, loss of goodwill etc.)
6.	Is the business impact analysis carried out at a regular interval?
Development and Implementation of the BCP and DRP	
1.	Has the organisation prioritized recovery of interrupted business operations? (Prioritization of activities is based on RTO and RPO)
2.	Has the organisation identified the various BCP and DRP Teams? (Verify employees are identified, informed and trained to take an action in the event of disaster).
3.	Are the responsibilities for each team documented? (Verify the roles and responsibilities assigned to employees for actions to be taken in the event of incident/disaster)
4.	Does the BCP document(s) include the following? Scope and objective. Roles and responsibilities of BCP and DRP Teams. Incident declaration. Contact list. Evacuation and stay-in procedure. Activity priorities. Human resource and welfare procedure. Escalation procedures. Procedure for resumption of business activities. Media communication. Legal and statutory requirements. Backup and restore procedures. Offsite operating procedures
5.	Are the copies of up-to-date BCP Documents stored offsite?
6.	Does the offsite facility have the adequate security requirements? (Verify the logical access, physical access and environmental control of the offsite).
7.	Does the BCP include training to employees? (Verify the evidences of training given).
8.	Whether the organisation has an adequate media and document backup and restoration procedures? (Verify the backup and restoration schedules adopted by the organisation)

Sl. No	Checkpoints/Particulars
9.	Are logs for backup and restoration maintained and reviewed? (Verify the logs maintained and review of the same by an independent person).
10.	Whether the media library has an adequate access control? (Verify the physical and logical access controls to the media library).
11.	Are the BCP and DRP communicated to all the concerned? (Verify availability and circulation of BCP & DRP to all concerned, including Onsite and offsite storage).
Maintenance of BCP and DRP	
1.	Whether the business continuity plan is tested at regular interval?
2.	Has the organisation reviewed the gap analysis of testing results? (Review process that includes a comparison of test results to the planned results).
3.	How has the organisation decided to reduce the gaps identified, what is the time limit set for addressing the same?
4.	Has the organisation got a testing plan? (Verify copy of test plan and updates).
5.	Are test drills conducted at appropriate intervals?
6.	Do organisation documents and analyses have testing results? (Verify the corrective copies of test results and analysis of the report).
7.	Has the organisation prepared action points to rectify the testing results? (Verify the corrective action plan for all problems encountered during the test drill).
8.	Does the organisation carry out retesting activity for action points? (Verify the evidences of retesting activities).
9.	Does the organisation review the BCP and DRP at regular intervals?
10.	Whether a review of the BCP includes following? BCP policy and procedure Scope and exclusion of BCP Inventory of IS assets Validating assumption made while risk assessment and preparation of BCP and DRP Risk assessment Business impact analysis Back up of system and data Training to employees Test drills

Appendix 2: RCM and audit guidelines for DRP and BRP

The risk control matrix (RCM) can be used by IS Auditors for identifying the relevant risks, implemented controls and steps to audit specific areas. This is a sample risk control matrix which can be adapted as required. The list of risks provides the key areas which are generally applicable for organisations. The relevant controls mitigate the risks.

Risk	Control	Audit Guidelines/Procedure
Non Existence of a Disaster Recovery/Business resumption Plan / improper planning methodologies used to create a DR/BCP could lead to a failure in resumption of critical business function.	The organisation should take steps in formulating a Business Continuity Policy. The policy should contain details regarding the methodologies used in formulating a DRP/BCP. Periodic.	• Identification and prioritization of the activities which are essential to continue functioning. • The plan is based upon a business impact analysis that considers the impact of the loss of essential functions. • Operations managers and key employees participated in the development of the plan. • The plan identifies the resources that will likely be needed for recovery and the location of their availability. • The plan is simple and easily understood so that it will be effective when it is needed. • The plan is realistic in its assumptions.
Insufficient Backup processes could lead to data not being backed up correctly and restoration of data would not be possible. Backups without data pertaining to the software environment would lead to data being restored but not possible to render such retrieved data due to lack of software.	Processes should include periodic backup of data which also involves storing data of the software those are dependent to render the files. Backups should be followed periodically and in the manner prescribed in the Business Continuity Policy and signoffs should be obtained along with notification from the backup utility.	• Determine if information backup procedures are sufficient to allow for recovery of critical data. • Determine if copies of the plan are safeguarded by off-site storage. • Review information backup procedures in general. The availability of backup data could be critical in minimizing the time needed for recovery. • Determine if the disaster recovery/ business resumption plan covers procedures for

		disaster declaration, general shutdown and migration of operations to the backup facility.
Insufficient testing of the BCP could lead to difficulties at the time of actual disaster.	Testing and revisions should be a part of the Policy. Test Plans drafted should be executed and reports regarding the tests should be maintained.	•Determine if a test plan exists and to what extent the disaster recovery/business resumption plan has been tested. • Determine if a testing schedule exists and is adequate (at least annually). Verify the date of the last test. Determine if weaknesses identified in the last tests were corrected.
Lack of Required Resources those are essential to execute a DRP/BCP will lead to a failed execution.	The required resources should be procured and preserved. The resources needs to be reviewed periodically and changed as there could be wear and tear due to efflux of time. The required resources should be in accordance to the BCP/DRP.	•Determine if resources have been made available to maintain the disaster recovery/business resumption plan and keep it current. •Have resources been allocated to prevent the disaster recovery/ business resumption plan from becoming outdated and ineffective?
BCP/DRP without correct review of the existing plans, Business Impact Analysis and Risk Assessment would lead to the formulation of a weak and ineffective Plan.	BCP/DRP which has been made for the organisation should be relevant and adequate to the size and nature of the organisation. Sufficient Risk Assessment and Business Impact Analysis should be performed and documented while revising/formulating a BCP/DRP.	•Obtain and review the existing disaster recovery/ business resumption plan. •Obtain and review plans for disaster recovery/ business resumption testing and/or documentation of actual tests •Obtain and review the existing business impact analysis. •Gather background information to provide criteria and guidance in the preparation and evaluation of

		disaster recovery/ business resumption plans. •Gain an understanding of the methodology used to develop the existing business impact analysis. •Determine if recommendations made by the external firm who produced the business impact analysis have been implemented or otherwise addressed.
Irregular revision of the BCP/DRP would lead to an outdated plan being executed and would be ineffective thus leading to losses and closure of the organisation.	Timely revision of the BCP/DRP should be carried out. Correct versioning of the plans should be present and the plans of the older versions should be archived and kept away from the latest version.	•Determine if the plan is dated each time that it is revised so that the most current version will be used if needed. •Determine if the plan has been updated within past 12 months.
Employees and other personnel who are ignorant of the plans would lead to lack of co-ordination, chaos and confusion during execution of the BCP/DRP.	Employees should be given periodic briefing about the BCP/DRP. Roles and Responsibilities of each employee should be allotted for smooth execution of BCP. Relevant documents should be made available and kept at strategic areas of the organisation.	•Interview functional area managers or key employees to determine their understanding of The disaster recovery/ business resumption plan. Do they have a clear understanding of their role in working towards the resumption of normal operations? •Determine all the locations where the disaster recovery/ business resumption plan is stored. Are there a variety of locations to ensure that the plan will survive disasters and will be available to those that need them?
Loss of life to the employee is a very serious matter and	Employees should be given a first preference while	• Have key employees seen the plan and are all

loss if any is a seriously bad for the image of the company	planning the DRP/BCP. Loss of material can be tolerable but loss of life should be avoided.	employees aware that there is such plan? ii) Have employees been told their specific roles and responsibilities if the disaster recovery/ business resumption plan is put into effect? • Does the disaster recovery/ business resumption plan include contact information of key employees, especially after working hours? • Does the disaster recovery/ business resumption plan include provisions for people with special needs? • Does the disaster recovery/ business resumption plan have a provision for replacement staff when necessary?
Buildings, electricity, telecommunications, storage facilities, water and other infrastructure if not well provisioned will be a hindrance during the recovery stages.	As feasible by the organisation, adequate measures like having an alternative site fully equipped should be made available. Rent Agreements/leases to the alternative facility should be maintained. Adequate transport and telecommunication facilities should be available.	• Does the disaster recovery/ business resumption plan have a provision for having a building engineer inspect the building and facilities soon after a disaster so that damage can be identified and repaired to make the premises safe for the return of employees as soon as possible? • Does the disaster recovery/business resumption plan consider the need for alternative shelter, if needed? Alternatives in the immediate area may be affected by the same disaster. • Review any agreements for use of backup facilities.

		• Verify that the backup facilities are adequate based on projected needs (telecommunications, utilities, etc.). Will the site be secure? • Does the disaster recovery/business resumption plan consider the failure of electrical power, natural gas, toxic chemical containers, and pipes? • Are building safety features regularly inspected and tested? • Does the plan consider the disruption of transportation systems? This could affect the ability of employees to report to work or return home. It could also affect the ability of vendors to provide the goods needed in the recovery effort.
Inadequate IT Environment at the alternative site could lead to late resumption of the Business.	Care should be taken that alternative IT Infrastructure should be made available at the Alternative site. Provision for Maintenance of the alternative IT Infrastructure should be present.	• Determine if the plan reflects the current IT environment. • Determine if the plan includes prioritization of critical applications and systems. • Determine if the plan includes time requirements for recovery/availability of each critical system, and that they are reasonable. • Does the disaster recovery/business resumption plan include arrangements for emergency telecommunications? • Is there a plan for alternate means of data transmission if the computer network is interrupted? Has the security

		of alternate methods been considered?
Inadequate details about the administration during the time of crisis will lead to execution hindrances. Inadequate Incident Response teams could lead to a higher chaos and lack of coordination.	BCP Policy should contain details regarding administration during Crisis, Incident Management, essential records to be preserved for future use. BCP Policy should provide for the protection of critical assets, documents. BCP Policy should provide for the correct storage for such documents.	• Does the disaster recovery/ business resumption plan cover administrative and management aspects in addition to operations? Is there a management plan to maintain operations if the building is severely damaged or if access to the building is denied or limited for an extended period of time? • Is there a designated emergency operations center where incident management teams can coordinate response and recovery? • Have essential records been identified? Do we have a duplicate set of essential records stored in a secure location? • To facilitate retrieval, are essential records separated from those that will not be needed immediately? • Has executive management assigned the necessary resources for plan development, concurred with the selection of essential activities and priority for recovery, agreed to back-up arrangements and the costs involved, and are prepared to authorize activation of the plan should the need arise.
Lack of preservation of key business contacts and creation of special reserves could result in an	Ensure that the BCP Policy provides for preservation of contacts either through backups and the	• Does the disaster recovery/ business resumption plan include the names and numbers of

ineffective BCP/DRP Execution.	management policy has provides for creation of special reserves for BCP/DRP crisis.	Suppliers of essential equipment and other material? •Does the disaster recovery/ business resumption plan include provisions for the approval to expend funds that were not budgeted for the period? Recovery may be costly.

Appendix 3: Sample of BCP Audit Finding

Max Infotech should have an alternate disaster recovery site and documented procedures and policies for disaster recovery.

Observation

Max Infotech does not have an alternate disaster recovery site. Also documented Disaster Recovery Plan (DRP) and business continuity plan are not there.

Exposure

The DRP is a key plan ensuring availability of resources critical to the business operations. In the absence of documented procedures and policies for the same, it may be difficult to recover from a disaster resulting in non-availability of data and applications to the users for unacceptable period of time thereby interrupting business processes and impacting the business.

Cause

This is due to lack of documented Disaster Recovery Plan (DRP).

Recommendation

Ensure that the Max Infotech has an alternate disaster recovery site and a documented procedures and policies for disaster recovery. This document should include:

- Provision for back up and restoration of resources identified as critical to recovery;
- Provision for back up and off-site location of non-critical application software, data files and system software to facilitate their restoration following the recovery of critical application;
- Frequency of back up and off-site rotation and number of generations maintained, of production data files including databases;
- Back up and off-site copies of system software, updated or replaced with each upgrade or revision;

Module 7

- Off-site copies of systems, program, user and operations documentation updated to reflect system revision;
- Instructions on how to restore from back-up copies of program and data files.