Technical Guide on
Information System Audit

Celebrating the 60th Year of Excellence

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

Technical Guide on Information System Audit

Committee on Information Technology

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA

(Set up by an Act of Parliament)

New Delhi

Second Edition : January, 2009

Email : cit@icai.org

Website : www.icai.org

Price : Rs 250/- (with CD)

ISBN : 978-81-88437-60-3

Published by : The Publication Department on behalf of Smt. Indu Arora, Secretary, Committee on Information Technology, 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.

January/2009/1000 Copies

FOREWORD TO SECOND EDITION

The Committee on Information Technology (CIT) has been constituted by the Institute of Chartered Accountants of India to identify the emerging professional opportunities in the Information Technology sector for members and prepare them to face the threats and challenges ahead through suitable courses/ seminars/ workshops and professional guides. Since its inception, the Committee has proactively considered the contemporary requirements and initiated steps to suitably equip the members in terms of knowledge and skills to face the challenges ahead and convert them into professional opportunities.

Information Technology, in the emerging economic scenario, has risen from a humble role of business enabler to business driver. Enterprises and governments are making increasing use of IT to better manage their activities, manage their core business functionality and offer value added services to their clients. The IT responsiveness and efficiency within the process flow, within the enterprise and with its customers/ vendors are the deciding factors for an organisation to compete and survive in the global village. It is often found that typical IT implementations leave a lot to be desired with respect to necessary checks and balances (controls), efficiency and effectiveness and last, but not the least, disaster recovery planning/ business continuity planning.

Sarbanes Oxley Act and its Indian counterpart – Clause 49 of the Listing Agreement to the Indian Stock Exchange require the directors to certify the existence and operation of sufficient internal controls. As the Internal Controls are now increasingly implemented through computer systems, the need for Information System Audit is on the increase apart from heightened business risks considering emerging business scenario and increasing deployment of IT to manage business. The Committee introduced the Post Qualification Course on Information Systems Audit in the year 2000 to suitably equip the profession to offer value added services in the area of Information System Audit.

I am pleased with the ardent efforts put in by the Committee on Information Technology for coming out with this informative *Technical Guide on Information System Audit,* second edition. I am sure that the members will be immensely benefited by this timely publication that aims to contribute to a better

understanding and dissemination of information in this vibrant business field and provide a framework to undertake Information System Audits.

I appreciate the efforts put in by Shri Atul C. Bheda, Chairman, Committee on Information Technology, members of the Committee and Committee Secretariat towards this challenging responsibility.

New Delhi **CA. Ved Jain**

December 22, 2008 President

PREFACE TO SECOND EDITION

The Committee on Information Technology introduced the post qualification course on Information Systems Audit in the year 2000 to provide the necessary training and development to the members to offer value added services in this emerging field. The need for Information System Audits by enterprises is on the increase considering the emerging requirements of Sarbanes Oxley Act and Clause 49 of the listing Agreement to the Indian Stock Exchange, which require certification by the directors for existence and operation of sufficient Internal Controls. As the Internal Controls today are implemented through the Information Systems to manage the business activities, there is an increasing need for Information System Audits in the country and abroad. The Committee is indeed very grateful to the members in coming forward in unprecedented large numbers to develop competencies in this emerging field.

The Committee on IT has endeavored to further equip members to provide value added services to their clients in the area of Information System Audit by providing this revised edition of *Technical Guide on Information System Audit* such that they have a framework and requisite support. This guide aims to enhance the knowledge of ISA qualified members to perform Information Systems Assurance/ Systems and Process Assurance Services. In addition to providing an introduction to the processes and procedures to be followed, this guide provides illustrative checklists for conducting Information System Audits.

I would like to add a word of caution on use of this technical guide, including checklists. This guide is a generic document that has to be suitably adapted to the specific requirements of a particular assignment.

I am grateful to CA. Ravi Pandit, for having, contributed the basic draft of this technical guide. I express my gratitude to CA. Ved Jain, President and CA. Uttam Prakash Aggarwal, Vice President for their whole hearted support and guidance in coming out with this guide and endeavors of the Committee. I also acknowledge the guidance, support and contribution of the members of the Committee on Information Technology in finalising this guide. I also thank Smt. Indu Arora, Secretary to the Committee, Shri Ravi K. Arora, Jt. Director and committee secretariat for working hard to release this very useful publication for the ISA Members.

I am confident that members will be immensely benefited by this timely and sincere effort of the Committee. This revised publication would contribute to better understanding and dissemination of information in this crucial domain and members will feel assured and better equipped to offer value added services in this emerging field.

Shri Atul C. Bheda

December 19, 2008 — Chairman

New Delhi — Committee on Information Technology

FOREWARD TO FIRST EDITION

In the emerging scenario of global village and technological revolution, it is a challenging task for the Institute members to keep abreast with developments and convert threats into challenges and survive/ grow in the globalised world.

The Committee on Information Technology (CIT) has been established to identify the emerging professional opportunities in the Information Technology sector for members and prepare them to face the threats and challenges ahead. Since its inception, the Committee has proactively considered the modern day requirements and initiated steps to suitably equip the members in terms of knowledge and skills to face the challenges ahead.

There is increasing need for the *Information System Assurance Services* as businesses are increasingly using information technology to service their core business functionality without having sufficient checks and balances leading to increasing business risks. Hence the need for Information System Audit by Chartered Accountants with DISA post qualification.
There has been an increasing need for a framework for Information System Audit. Indeed, it is a pleasure for me to know that the CIT has come out with this informative *Information Systems Audit - Technical Guide*. I am confident that members will be benefited by this timely and sincere effort of the Committee. This publication would contribute to better understanding and dissemination of information in this critical area and members will feel more confident and better equipped to carry out their jobs.

I would like to place on record my deep appreciation for the efforts put in by Shri Harinderjit Singh, Chairman, Committe~ on Information Technology, members of the Committee and Secretary of the Committee for this commendable job.

Sunil Goyal
President

New Delhi
January 24, 2005

PREFACE TO FIRST EDITION

In today's age, there is a seamless integration of business process, internal controls, accounting, systems and IT. In this scenario, our members have to provide assurance and their value add services to clients. With this background, the Committee on Information Technology (CIT) of The Institute of Chartered Accountants of India was established in the year 2000 to identify the emerging professional opportunities in the Information Technology sector for members and prepare them to face the related challenges ahead. This technical guide is one of the initiatives of the CIT to equip our members to perform the assignments relating to Information Assurance audits and other related value add services The guide contains subjects like an introduction to the Information System Audit, Information System Audit mandate, defining auditee's requirements, planning for Information System Audit, audit risk assessment, documentation, conduct of Information System Audit, use and documentation of CAAT. The highlight of the guide is the sample checklists for practical guidance Also included in is a copy ofthe RBI Checklists for Computer Audit, in the formation of which the ICAI was a member.

I would like to add a word of caution on use of this technical guide, including checklists. This guide is a generic document that has to be suitably adapted! tailored to the specific requirements of a particular assignment.

I am grateful to Shri V. Jawahar, Co-opted Member to the Committee on Information Technology, to have contributed the basic draft of this technical guide. In this regard, I also acknowledge the guidance and contribution of our President, Shri Sunil Goyal, FCA, Vice President, Shri Kamlesh S. Vikamsey, FCA, all the members of the Committee on Information Technology and Shri RaviArora, Secretary, CIT.

I am sure that this Technical Guide on Information Technology would be of immense help to the members in providing the Information Assurance Services, a value added service, whose demand is on the increase by the day and as usual I look forward to your feedback and suggestions to improve the same.

Harinderjit Singh
Chairman
Committee on Information Technology

New Delhi
January 24, 2005

CONTENTS

1	**INTRODUCTION**	**1**
1.1	Need for Information System Audit	1
1.2	Information System Auditing Standards	4
1.3	Auditing Guidelines	6
2	**AUDIT PREPARATION AND PLANNING**	**7**
2.1	Business understanding	7
2.2	Audit Scope & Charter	9
2.2.1	Contents	10
2.2.2	Purpose	10
2.2.3	Responsibility	10
2.2.4	Authority	11
2.2.5	Accountability	11
2.2.6	Exclusions	13
2.2.7	Effective Communication with Auditee	13
2.3	Audit Planning	13
2.3.1	Audit Requirements	14
2.3.2	Materiality	17
2.3.3	Assessment of Internal Controls	18
2.4	Risk Based Approach	18
2.4.1	Selection of a Risk Assessment Methodology	20
2.4.2	Use of Risk Assessment	21
2.4.3	Risk Assessment Documentation	24
2.5	Audit Staffing	25
2.5.1	Auditor Independence	26

2.5.2 Due Professional Care 28
2.5.3 Competence 30
2.6 Using work of other experts 31
2.6.1 Rights of Access to the Work of Other Experts 32
2.6.2 Planning Considerations 32
2.6.3 Independence and Objectivity 32
2.6.4 Professional Competence 33
2.6.5 Scope of Work and Approach 33
2.6.6 Level of Review Required 33
2.6.7 Review of Other Expert's Work Papers 33
2.6.8 Review of Other Expert's Report(s) 34
2.6.9 Implementation of Recommendations 35
2.7 Audit Schedule 35
2.8 Communication of Audit Plan 36
2.9 CAAT (Computer Assisted Auditing Techniques) 38
2.9.1 Types of CAATs 40
2.9.2 Planning Steps 42
2.9.3 Arrangements with the Auditee 42
2.9.4 Testing the CAATs 43
2.9.5 Security of Data and CAATs 43
2.9.6 Mandate to Use CAATs 44
2.9.7 Documentation & Relying on Experts 44
2.9.8 Reporting 45
2.9.9 Continuous Online Audit Approach 46
3 Conducting the Audit 49
3.1 Audit Methodology 49
3.2 Pre-Audit Activities 49

3.2.1 Audit Team Finalization 50
3.2.2 Communication and Logistics Arrangements 50
3.2.3 Data Gathering 51
3.2.4 Sampling 51
3.2.5 Materiality & Evidence Gathering 53
3.3 Information System Audit Process 56
3.3.1 Opening Meeting 56
3.3.2 Reviewing the documents 56
3.3.3 Interviewing the Key Personnel 57
3.3.4 Conducting the walkthroughs 57
3.3.5 Testing of IS Controls 57
3.3.6 Closing Meeting 58
3.4 Documenting Observations and Findings 58
3.5 Audit Report – Preparation & Distribution 59
4 FOLOW-UP ACTIVITIES 61
4.1 Usage of Audit Reports 61
4.2 Reporting of Information System Audit Report 61
4.3 Follow Up Audit Procedure 62
5 INFORMATION SYSTEM AUDITS 65
5.1 IT General Controls (ITGC) Audit 66
5.1.1 Overview 66
5.1.2 Evolution of ITGC 67
5.1.3 Auditing IT General Controls 68
5.1.3.1 Logical Access Control 69
5.1.3.2 SDLC (System development life cycle) controls 72
5.1.3.3 Change Management Controls 75

5.1.3.4 Physical and Environmental security controls 76
5.1.3.5 Data backup and recovery controls 78
5.1.4 ITGC Audit Scope 79
5.1.5 ITGC Audit Checklist Reference 80
5.2 Application Control Audit 81
5.2.1 Overview 81
5.2.2 Risks 81
5.2.3 IT Application Controls 82
5.2.3.1 Input Controls 82
5.2.3.2 Data Validation Edit Controls 82
5.2.3.3 Processing Controls 84
5.2.3.4 Output Controls 84
5.2.3.5 Data File Controls 85
5.2.4 Auditing Software Acquisition Control 86
5.2.5 Application System Documentation 90
5.2.6 Application Controls Audit Checklist References 91
5.3 Network Security Audit 91
5.3.1 Overview 91
5.3.2 Network Audit Objectives 93
5.3.3 Network Vulnerabilities 93
5.3.3.1 Interception 93
5.3.3.2 Availability 93
5.3.3.3 Access/Entry Points 93
5.3.4 Controls 94
5.3.4.1 Physical Access Controls 94

5.3.4.2 Network Monitoring 94
5.3.4.3 Access/Entry Points 95
5.3.5 Auditing Network Security 96
5.3.6 Mobile Computing and Wireless Networks 96
5.3.7 Network Audit Approach 99
5.3.8 Network Audit Checklist Reference 101
5.4 Data Migration Audit 102
5.4.1 Overview 102
5.4.2 Data Migration Risks 102
5.4.3 Audit Process 103
5.4.3.1 Understanding the data migration requirements 104
5.4.3.2 Data mapping strategy and plans review 106
5.4.3.3 Planned operational changes review 107
5.4.3.4 Implementation readiness review 108
5.4.3.5 Pre-migration Sample Test 109
5.4.3.6 Data Conversion Verification 109
5.4.3.7 Overall audit analysis of the implementation 110
5.4.4 Data Migration Audit Checklist Reference 110
5.5 Business Continuity Management Audit (BCM) 110
5.5.1 Overview 110
5.5.2 BCM Activities 112
5.5.2.1 Policy and procedure 112
5.5.2.2 Risk assessment 113
5.5.2.3 Business Impact Analysis (BIA) 115

5.5.2.4 Development and Implementation of BCP and DRP 116
5.5.2.5 Training 122
5.5.2.6 Maintenance 122
5.5.3 BCM Audit Scope 123
5.5.4 BCM Audit Checklist Reference 124
5.5.5 BCM Audit Formats and Templates 124
5.6 E- Commerce Audit 124
5.6.1 Overview 124
5.6.2 Types of e-commerce 126
5.6.2.1 Through the Internet 126
5.6.2.2 Through Dedicated networks 127
5.6.2.3 Electronic Payments 128
5.6.3 Risks in E-Commerce 128
5.6.3.1 Authenticity 129
5.6.3.2 Non-Repudiation 129
5.6.3.3 Timing 129
5.6.3.4 Data Integrity 129
5.6.3.5 Interception of Data 130
5.6.3.6 Identity Theft 130
5.6.3.7 Business Interruption 130
5.6.3.8 Corruption of Data 131
5.6.3.9 Lack of Authentication 132
5.6.3.10 Loss of Privacy/Confidentiality 132
5.6.3.11 Frauds in e commerce 133
5.6.4 E-Commerce Audit Approach 133
5.6.4.1 Evaluate the Business Aspects 135

5.6.4.2 Detailed Risk Assessment 136
5.6.4.3 Change Management Process 136
5.6.4.4 Identification and Authentication 137
5.6.4.5 Data Validations and Authorisations 137
5.6.4.6 Data Storage Integrity 138
5.6.4.7 Protection against External IS Threats 139
5.6.4.8 Compliance with Privacy Regulations and Best Practices 140
5.6.4.9 Third-party Services 140
5.6.5 Reporting 141
5.6.6 E-commerce Audit Checklist Reference 141
5.7 Data Centre Audit 141
5.7.1 Overview 141
5.7.2 The audit process 142
5.7.2.1 Audit Preparation 142
5.7.2.2 Establishing Audit Objectives 142
5.7.2.3 Performing the Review 143
5.7.2.4 Data Centre Documentation 154
5.7.3 Data Centre Audit Checklist Reference 154

Annexures

Annexure I : Audit Checklists 155
Annexure II : Formats and Templates 232
Annexure III : Glossary and Abbreviations 239

1

INTRODUCTION

1.1 Need for Information System Audit

1.2 Information System Auditing Standards

1.3 Auditing Guidelines

1.1 Need for Information System Audit

Information systems are very important for running any large business. Earlier computer systems were used to merely record business transactions, but now they are actually used for taking business decisions for the enterprise. They are complex and have many components coming together to make a complete business solution. Their usage into accounting systems changed the way data was stored, retrieved and controlled. In such a complex scenario, senior management and business managers are concerned about information systems.

IT auditing is the future of the accounting profession. In today's world, company dynamics / financial state is determined by the use of computers. The rise in information technology usage is rapid and must be utilized for organizational success. The role IT auditors play maybe unknown to most but it impacts the lives of all. IT auditing adds security, reliability and accuracy to the information systems. Without IT auditing, we would be unable to safely shop on the internet or control our identities. As history continues, we will continue to see the rise of this up and coming profession.

Information Technology has changed the business environment in the following significant ways.

1. It has increased the ability to capture, store, analyze and process tremendous amounts of data and information and has impacted what one can do in business in terms of information and as a business enabler. IS has empowered the business decision-maker many times over. It also has become a primary enabler to various production processes and service processes. It has become a critical component of business processes. There is a residual effect in that the increased use of technology has resulted in increased budgets, increased successes and failures and increased awareness of the need to control.

2. Technology has impacted controls significantly. While control objectives have in large part remained constant, except for some that are technology-specific, technology changes have altered the way systems should be controlled. Safeguarding assets as a control objective remains the same, whether manual or automated. However, the manner through which the control objectives are met is decisive.

3. Technology has impacted the auditing profession in terms of how audits are performed (information capture and analysis, control concerns) and the knowledge required to draw conclusions regarding operational or system effectiveness, efficiency and integrity, and reporting integrity. Initially, the impact was focused on dealing with a changed processing environment. As the need for auditors with specialized skills regarding technology grew, so did the beginning of the information systems auditing profession.

The first use of a computerized accounting system was at General Electric in 1954. During the period of 1954 to the mid-1960s, the auditing profession was still auditing around the computer. At this time only, mainframe computers were used and few people had the skills and abilities to program computers. This began to change in the mid-1960s with the introduction of new, smaller and less expensive machines. This increased the use of computers in businesses and with it came the need for auditors to become familiar with EDP concepts in business. Along with the increase in computer use, came the rise of different types of accounting systems. The formation and rise in popularity of the Internet and

E-commerce have had significant influences on the growth of IT audit. The Internet influences the lives of most of the world and is a place of increased business, entertainment and crime. IT auditing helps organizations and individuals on the Internet find security while helping commerce and communications to flourish.

The term information assurance means safeguarding the collection, storage, transmission and use of information. The ultimate goal of information assurance is to protect users, business units and enterprises from the negative affects of corruption of information or denial-of-service attacks. For example, if the personnel data in a human resource database are valid in the sense that they could be correct, but are in fact not correct, there may be no negative impact on the information system, but the enterprise may suffer when people get the wrong amount of money in their pay check or the check is sent to the wrong address. Similarly, if an order for an engine part in a supply and logistics system is lost in the part of the system that dictates which pallets get loaded onto the wrong boat to the wrong destination, the information system continues to operate, but the supply service is denied to the person requiring the parts. Naturally, if the information systems processing, storing or communicating the information become corrupt or unavailable, that may also affect the enterprise as a whole, but simply protecting the systems without protecting the information, processing and communication is not adequate.

Computer based systems audit functions do not undermine the importance of traditional internal controls such as separation of duties but are implemented differently. Compared to the manual internal control systems, collecting of evidence on the reliability of internal controls is often more complex in the computer based information systems. Computer controls are often more critical than manual controls.

Evaluation of the reliability of the controls in computer systems is often more complex than in the manual systems. Greater numbers of more complex controls need to be considered. Other sciences such as traditional auditing, computer science, management and behavioural science are the basis of the principles and practice of information systems auditing.

1.2 Information System Auditing Standards

Information System Audit Standards provides audit professionals a clear idea of the minimum level of acceptable performance essential to discharge their responsibilities effectively.

The specialised nature of information systems (IS) auditing and the skills necessary to perform such audits require standards that apply specifically to Information System Auditing. Standards define mandatory requirements for Information System Auditing and reporting.

They inform:

- Information System Auditors of the minimum level of acceptable performance required to meet the professional responsibilities

- Management and other interested parties of the profession's expectations concerning the work of practitioners

The Institute of Chartered Accountants of India has issued AASs covering various aspects. Although these standards are primarily concerned with the audit of financial information, they can be adapted for the purposes of Information System Audit depending on its scope and objectives.

The following AASs issued by the Institute of Chartered Accountants of India can be adapted for the Information System Audits:

4. Basic Principles Governing an Audit

5. Objective and scope of the Audit of Financial Statements

6. Documentation

7. The Auditor's responsibility to consider detect / error in an Audit of financial Statements

8. Audit Evidence

9. Risk Assessment and Internal Controls

10. Relying Upon the Work of an Internal Auditor
11. Audit Planning
12. Using the Work of an Expert
13. Using the Work of Another Auditor
14. Representations by Management
15. Responsibility of Joint Auditors
16. Audit Materiality
17. Analytical Procedures
18. Audit Sampling
19. Going Concern
20. Quality control for Audit Work
21. Audit of Accounting Estimates
22. Subsequent Events
23. Knowledge of Business
24. Consideration of Laws and Regulations in and audit of Financial Statements
25. Initial Engagements Opening Balances
26. Related Parties
27. Audit considerations relating to Using Service organisations
28. Comparatives
29. Terms of Audit Engagement
30. Communication of Audit Matters With Those Charged with Governance
31. The Auditor's Report on Financial Statements

32. Auditing in a Computer Information Systems Environment

33. External Confirmations

34. Engagements to compile Financial Information

35. Engagements to Perform Agreed upon Procedures regarding Financial Information.

1.3 Auditing Guidelines

Guidelines provide guidance in applying Information System Auditing Standards. The Information System Auditor should consider them in determining how to achieve implementation of the standards, use professional judgment in their application and be prepared to justify any departure.

Several well known organizations have given practical and useful information on Information System Audit and few are given in Annexure as below.

- ISACA
- ISO 27001
- IIA
- ITIL

2

AUDIT PREPARATION AND PLANNING

2.1	Business Understanding
2.2	Audit Scope and Charter
2.3	Audit Planning
2.4	Risk Based Approach
2.5	Audit Staffing
2.6	Using work of other experts
2.7	Audit Schedule
2.8	Communication of Audit Plan
2.9	CAAT (Computer Assisted Auditing Techniques)

2.1 Business Understanding

The Information System Auditor should develop an audit plan taking into consideration:

- The objectives of the auditee relevant to the audit area, and
- Its technology infrastructure.

Before starting any Information System Audit, the Information System Auditor should plan his work to meet the audit objectives. In this planning stage, the Information System Auditor gathers relevant organizational information for creating their audit plan. The preliminary review should identify an organization's strategy and responsibilities for managing and controlling its IT Infrastructure and computer applications. An auditor should study

an organization's compute application systems e.g. accounting system to establish which applications are significant for the organization's objectives.

In addition to giving the Information System Auditor an understanding of the organisation's operations and its IS requirements, this will assist the Information System Auditor in determining the significance of the IS resources being reviewed as they relate to the objectives of the organisation. The Information System Auditor should gain an understanding of the types of systems, transactions and practices that have a significant effect on the specific organisation, function, process or data that is the subject of the audit. Knowledge of the organisation should include the business, financial and inherent risks facing the organisation as well as conditions in the organisation's marketplace. It should also include the extent to which the organisation relies on outsourcing to meet its objectives. The extent of the knowledge of the organisation and its processes required by the Information System Auditor will be determined by the nature of the organisation and the level of detail at which the audit work is being performed. The Information System Auditor may require specialised knowledge when dealing with unusual or complex operations. The Information System Auditor should use this information in identifying potential problems, formulating the objectives and scope of the work, performing the work and considering actions of management for which the Information System Auditor should be alert.

Where appropriate, the Information System Auditor should also consider the area under review and its relationship to the organisation (strategically, financially and/ or operationally) and obtain information on the strategic plan, including the IS strategic plan. The Information System Auditor should have an understanding of the auditee's information architecture and the auditee's technological direction to be able to design a plan appropriate for the present and, where appropriate, future technology of the auditee.

A more extensive knowledge of the organisation and its processes will ordinarily be required when the audit objective involves a wide range of information system functions rather than when the

objectives are for limited functions. For example, a review with the objective of evaluating control over an organisation's payroll system would ordinarily require a more thorough understanding of the organisation than a review with the objective of testing controls over a specific program library system.

This preliminary investigation will prepare an Information System Auditor for the following:

- Understand the issues and current risks of the business.
- Speak to the management intelligently about the business and gain their confidence as an auditor.
- Identify the issues that may require special attention in an audit through a cursory evaluation of controls.
- Understand the materiality of risks and potential control weaknesses.
- Know how to go about developing an audit scope that will add value to the business process by focusing on the risks most meaningful to management.

2.2 Audit Scope & Charter

The Information System Auditor must have a clear mandate to perform the Information System Audit function. This is usually documented in the audit charter. In case, the audit charter exists for the entire audit function and Information System Audit is a part of the same, then the IS mandate should be a separate part of bigger audit.

For an internal information systems audit function, an audit charter is prepared for the ongoing activities. The audit charter will be subject to an annual review or more often, if the responsibilities are varied or changed. The audit charter or engagement letter should be reviewed to ensure that the purpose, responsibility and scope have not changed. The audit charter should explicitly contain the aspects of authority, responsibility and accountability. The charter must formally establish the position of the audit function within the organization and also describe the ways in

which it is intended to contribute to the organisation's overall mission and goals. An engagement letter may be used by the internal Information System Auditor to further clarify or confirm involvement in specific assignments.

For an external Information System Audit, an engagement letter is normally prepared for each audit or non-audit assignment. The audit charter or engagement letter should be detailed enough to communicate the purpose, responsibility and limitations of the audit function or audit assignment.

2.2.1 Contents

The audit charter should clearly address the four aspects of purpose, responsibility, authority and accountability. Aspects to consider are set out in the following sections.

2.2.2 Purpose

- Role
- Aims/goals
- Mission statement
- Scope
- Objectives

2.2.3 Responsibility

- Operating principles
- Independence
- Relationship with external audit
- Auditee requirements
- Critical success factors
- Key performance indicators

- Risk assessment
- Other measures of performance

2.2.4 Authority

- Right of access to information, personnel, locations and systems relevant to the performance of audits
- Scope or any limitations of scope
- Functions to be audited
- Auditee expectations
- Organisational structure, including reporting lines to board and senior management
- Grading of Information System Audit staff

2.2.5 Accountability

- Reporting lines to senior management
- Assignment performance appraisals
- Personnel performance appraisals
- Staffing/career development
- Auditee rights
- Independent quality reviews
- Assessment of compliance with standards
- Benchmarking performance and functions
- Assessment of completion of the audit plan
- Comparison of budget to actual costs
- Agreed actions, e.g., penalties when either party fails to carry out his responsibilities

The audit charter forms a sound basis for communication with auditees and should include references to service level agreements for such things as:

- Availability for unplanned work
- Delivery of reports
- Costs
- Response to auditee complaints
- Quality of service
- Review of performance
- Communication with auditees
- Needs assessment
- Control risk self-assessment
- Agreement of terms of reference for audits
- Reporting process
- Agreement of findings

The Information System Auditor should consider establishing a quality assurance process (e.g., interviews, customer satisfaction surveys, assignment performance surveys) to understand Auditee needs and expectations relevant to the Information System Audit function. These needs should be evaluated against the charter for improving the service or changing the service delivery or audit charter, as necessary.

The charter should state the auditor's right to have access to records, facilities, and personnel in the conduct of his work. The charter must also establish the right of the head of thInformation System Audit function to have direct access to the Audit Committee and to the Board of Directors.

2.2.6 Exclusions

The charter must also establish the audit functions responsibility in relation to providing advice to the management about how well the organisation is attaining the asset safeguarding, data integrity, effectiveness and efficiency objectives. At the same time, it must state that the management has the primary responsibility for controls within an organisation and for taking corrective actions on the basis of the advice of the Information System Auditors.

2.2.7 Effective Communication with Auditee

Effective communication with auditee involves:

- Describing the service, its scope, availability and timeliness of delivery
- Providing cost estimates or budgets if they are available
- Describing problems and possible solutions for them
- Providing adequate and readily accessible facilities for effective communication
- Determining the relationship between the service offered and the needs of the auditee

2.3 Audit Planning

An audit plan is a detailed outline of the auditor's plans and procedures in conducting an audit. The objective of the audit plan is to assist the auditor in conducting an effective and efficient audit. A good, detailed, documented audit plan is very necessary for a successful audit.

The audit plan gives details of the audit objectives and steps the auditor must take, to ensure all important issues in the audit are covered. The audit plan includes:

- The auditor understands the client.

- Potential audit risks.
- A basic framework for how the audit resources (budgeted audit hours) are to be allocated throughout the audit.
- Audit procedures to be performed.

2.3.1 Audit Requirements

Defining the scope and objectives of an audit is the first formal step of an audit engagement. It sets the stage and identifies the key areas of investigation. Normally, the audit scope and objectives definition is done jointly by the management of the business and its processes with the Information System Auditor. The more input Information System Auditor can get from the management related to their insight into the inherent risks of the processes, the controls in place, and the challenges they face on a daily basis, the more valuable and relevant the audit report will be.

It is necessary in planning of an audit to discuss the objectives of the auditee relevant to the audit area and the technology infrastructure. Actually, at this stage, Information System Auditor has already started the audit and he is informally interviewing the auditee and forming an opinion of the control environment as he plans the audit and seeks their input. Part of the planning process will encompass understanding the business requirements and environment as input to materiality decisions made when planning an audit. Based on the assigned objectives, he should present the plan to the client, seek their concurrence, and entertain their suggestions for modification of the scope. Sometimes, he should be asking for documentation or contours of the process to better understand the technology being used or the actual workflow.

Depending on whether this is a cyclical audit or not, Information System Auditor should be looking for opportunities for adding value to the Information System Audit. He should think of how he might do things differently this time or how he can scale the scope down to something digestible in the time frame allotted to the audit. In all cases, it is important for management to understand how the risks can affect the business and how the controls might help make their jobs better or more profitable. It is important for

Information System Auditor to make the Auditee's understand the seriousness of IT Risks. If they do not agree with or even fail to understand the reasoning behind controlling risks to meet the business needs, then Information System Auditor has a different kind of risk on his hands that may need to be addressed off-line with senior management.

Risk assessment and prioritization of identified risks are all necessary steps in defining audit scope and objectives. As he identifies the risks and controls, both potential and existing, the Information System Auditor will need to consider the extent to which they will need to test existing controls in order to place reliance upon them. If the scope requires reliance on controls over a period of time, he will need to plan on gathering evidence and testing procedures across that period of time to test the effectiveness of the controls. Preliminary evaluation of these controls will be necessary to plan his testing and resource needs properly. For example, historic data may need to be reviewed through logs or other audit documentation and will therefore take additional time or testing processes.

One of the important tasks an auditor must do when planning the audit is to develop a **working budget**. The IT auditor must know the capabilities of the audit staff assigned to the project. In addition to budgeted time needed to perform the audit, the IT auditor should also budget time needed to train the audit staff (if needed) and allow time for any error correction step.

The scope and objectives are normally presented to management in writing and formally presented in an audit engagement or kick-off meeting. Depending upon the preliminary agreements that may already have taken place, management may negotiate terms and conditions at this meeting. In this meeting, they should layout the concerns that need to be reviewed and the assurances they are seeking as a result of this engagement. This also is the time for deciding how ongoing communications will be managed during the course of the engagement in terms of frequency, length, detail of updates, and who should be the contacts.

Once the Information System Auditor is assigned a particular Information System Audit with a broad idea of the scope and the

objectives defined, he will need to formally plan the same which typically involves the following:

- Notifying the client and prepare a schedule and pre-audit meetings
- Defining the scope and objectives
- Understanding the process and its technical components
- Determining the corresponding business processes on which to focus
- Understanding and validating the inherent risks and threats of the processes and components with the client
- Determining the desired controls or risk mitigating and validating expected controls and current residual risk with the client
- Identifying management tools that would validate or report on the proper functioning of the controls
- Performing a risk and control analysis to document the risk exposures and corresponding auditing priorities of the audit program components and their relevance to the scope and objectives
- Creating an audit program that incorporates the risk control analysis, gathers the evidence needed to determine the sufficiency of the existing controls and risk mitigates, and identifies the weaknesses
- Finalizing staff resource and skill requirements
- Determining the time allocation for the components of the audit based on the materiality of the risks, the various tasks associated with testing each component, and the skill level of the staff
- Establishing the framework of the work papers and fieldwork documentation

In order to evaluate whether an Information System Audit has been successful. The auditor must first identify the intended scope

and objectives of the audit to test management's assertions on their information systems. To meet the audit objectives, and to ensure that audit resources will be used efficiently, the auditor will need to establish levels of materiality. The auditor should consider both qualitative and quantitative aspects in determining materiality. An assessment of risk should be made to provide a reasonable assurance that all material items will be adequately covered during the audit work. This assessment should identify areas with relatively high risk of existence of material problems.

2.3.2 Materiality

In assessing materiality, the Information System Auditor should consider the following:

- The aggregate level of error acceptable to management, the IT auditor, and appropriate regulatory agencies.
- The potential for the cumulative effect of small errors or weaknesses to become material.

While establishing materiality, the auditor should also audit non-financial items such as physical access controls, logical access controls, and systems for personnel management, manufacturing control, design, quality control, and password generation.

While planning the audit work to meet the audit objectives, the auditor should identify relevant control objectives and determine, based on materiality, which controls should be examined. Internal control objectives are placed by management and identifies what the management strives to achieve through their internal controls.

Where financial transactions are not processed, the following identifies some measures the auditor should consider when assessing materiality:

- Criticality of the business processes supported by the system or operation.
- Cost of the system or operation (hardware, software, third-party services)
- Potential cost of errors.

- Number of accesses/transactions/inquiries processed per period.
- Penalties for failure to comply with legal and contractual requirements.

2.3.3 Assessment of Internal Controls

Any Information System Audit should include assessment of the internal controls either as a part of the audit subject or as a basis for reliance being gathered as a part of the audit.

Where the objective is evaluation of internal controls. Information System Auditor 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. However, if 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.

When the Information System Auditor evaluates internal controls for the purpose of placing reliance on control procedures in support of information being gathered as part of the audit, the Information System Auditor should ordinarily make a preliminary evaluation of the controls and develop the audit plan on the basis of this evaluation.

During a review, the Information System Auditor will consider the appropriateness of this evaluation in determining the extent to which controls can be relied upon during testing. For example, in using computer programs to test data files, the Information System Auditor should evaluate controls over program libraries containing programs being used for audit purposes to determine the extent to which the programs are protected from unauthorised modification.

2.4 Risk Based Approach

While planning the audit, the auditor decides what level of audit risk (the risk of reaching an incorrect conclusion based on the

audit findings) he or she is willing to accept. The more effective and extensive the audit work is, the less the risk that a weakness will go undetected and the auditor will issue an inappropriate report. Audit risk is dependent on the auditors assessed levels of inherent risk (the susceptibility of an audit area to error which could be material, assuming there are no related internal controls), control risk (the risk a material weakness will not be prevented or detected by internal controls), and detection risk (the risk substantive tests will not detect an error which could be material). These risks are determined when the auditor performs a risk assessment of the organization.

Many information systems are used in any organizations. There are different applications for different functions and activities and many computer installations at different geographical locations. The auditor is faced with the questions of what, when and how to audit, frequently. The answer to this is to adopt a risk-based approach.

While there are risks inherent to information systems, these risks impact different systems in different ways. The risk of non-availability even for a few minutes could be serious for a health care system at an advanced hospital. The risk of unauthorized modification can be a source of frauds and potential losses to an online banking system. A batch processing system or a data consolidation system may be relatively less vulnerable to some of these risks. The technical environments on which the systems run may also affect the risk associated with the systems.

The steps that can be followed for a risk-based approach to make an audit plan are:

1. Take an Inventory of the information systems in use in the organization and categorize them.

2. Determine which of the systems impact critical functions or assets, such as money, materials, customers, decision making, and how close to real time do they operate.

3. Assess what risks affect these systems and the severity of the impact on the business.

4. Rank the systems based on the above assessment and decide the audit priority, resources, schedule and frequency.

The auditor then can draw up a yearly audit plan that lists the audits to be performed during the year as per the schedule, and the resources required.

The level of audit work required to meet a specific audit objective is a subjective decision made by the Information System Auditor. There are two types of risks that an Information System Auditor faces, the risk of reaching an incorrect conclusion based on the audit findings (audit risk) and the risk of errors occurring in the area being audited (error risk). Whatever decision he is taking, he should document the risk assessment methodology used for an audit.

2.4.1 Selection of a Risk Assessment Methodology

Information System Auditor has a choice of many risk assessment methodologies, computerised and non-computerised. These range from simple classifications of high, medium and low, based on the Information System Auditor's judgment, to complex and apparently scientific calculations to provide a numeric risk rating. The Information System Auditor should consider the level of complexity and detail appropriate for the organisation being audited.

However, **a**ll risk assessment methodologies rely on subjective judgments at some point in the process (e.g., for assigning weightings to the various parameters). The Information System Auditor should identify the subjective decisions required in order to use a particular methodology and consider whether these judgments can be made and validated to an appropriate level of accuracy.

In deciding the most appropriate risk assessment methodology, the Information System Auditor should consider the following:

- The type of information required to be collected (some systems use financial effect as the only measure - this is not always appropriate for Information System Audits)

- The cost of software or other licenses required to use the methodology
- The extent to which the information required is already available
- The amount of additional information required to be collected before reliable output can be obtained, and the cost of collecting this information (including the time required to be invested in the collection exercise)
- The opinions of other users of the methodology, and their views of how well it has assisted them in improving the efficiency and/or effectiveness of their audits
- The willingness of management to accept the methodology as the means of determining the type and level of audit work carried out

No single risk assessment methodology can be expected to be appropriate in all situations. Conditions affecting audits may change over time. Periodically, the Information System Auditor should re-evaluate the appropriateness of the chosen risk assessment methodologies.

2.4.2 Use of Risk Assessment

The selected risk assessment techniques are used by the Information System Auditor in developing the overall audit plan and in planning specific audits. Risk assessment, in combination with other audit techniques, should be considered in making planning decisions such as:

- The nature, extent, and timing of audit procedures
- The areas or business functions to be audited
- The amount of time and resources to be allocated to an audit

The Information System Auditor should consider each of the following types of risk to determine their overall level:

- Inherent risk

- Control risk
- Detection risk

Inherent Risk

Inherent risk is the susceptibility of an audit area to error which could be material, individually or in combination with other errors, assuming that there were no related internal controls. For example, the inherent risk associated with operating system security is ordinarily high since changes to, or even disclosure of, data or programs through operating system security weaknesses could result in false management information or competitive disadvantage. By contrast, the inherent risk associated with security for a stand-alone PC, when a proper analysis demonstrates it is not used for business-critical purposes, is ordinarily low.

Inherent risk for most Information System Audit areas is ordinarily high since the potential effect of errors ordinarily spans several business systems and many users. In assessing the inherent risk, the Information System Auditor should consider both pervasive and detailed IS controls. This does not apply to circumstances, where the Information System Auditor's assignment is related to pervasive IS controls only. At the pervasive IS control level, the Information System Auditor should consider to the level appropriate for the audit area in question:

- The integrity of IS management and IS management experience and knowledge
- Changes in IS management
- Pressures on IS management which may predispose them to conceal or misstate information (e.g. large business-critical project over-runs and hacker activity)
- The nature of the organisation's business and systems (e.g., the plans for electronic commerce, the complexity of the systems, and the lack of integrated systems)
- Factors affecting the organisation's industry as a whole (e.g., changes in technology, and IS staff availability)

- The level of third party influence on the control of the systems being audited (e.g., because of supply chain integration, outsourced IS processes, joint business ventures, and direct access by customers)
- Findings from and date of previous audits

At the detailed IS control level, the Information System Auditor should consider the level appropriate for the audit area in question:

- The findings from and date of previous audits in this area
- The complexity of the systems involved
- The level of manual intervention required
- The susceptibility to loss or misappropriation of the assets controlled by the system (e.g., inventory, and payroll)
- The likelihood of activity peaks at certain times in the audit period
- Activities outside the day-to-day routine of IS processing (e.g., the use of operating system utilities to amend data)
- The integrity, experience and skills of the management and staff involved in applying the IS controls

Control Risk

Control risk is the risk that an error which could occur in an audit area, and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. For example, the control risk associated with manual reviews of computer logs can be high because activities requiring investigation are often easily missed owing to the volume of logged information. The control risk associated with computerised data validation procedures is ordinarily low because the processes are consistently applied.

The Information System Auditor should assess the control risk as high unless relevant internal controls are:

- Identified
- Evaluated as effective
- Tested and proved to be operating appropriately

Detection Risk

Detection risk is the risk that the Information System Auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors. For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high because logs for the whole period of the audit are not available at the time of the audit. The detection risk associated with identification of the lack of disaster recovery plans is ordinarily low since existence is easily verified.

In determining the level of substantive testing required, the Information System Auditor should consider both:

- The assessment of inherent risk
- The conclusion reached on control risk following compliance testing

The higher the assessment of inherent and control risk, the more audit evidence the Information System Auditor should normally obtain from the performance of substantive audit procedures.

2.4.3 Risk Assessment Documentation

The Information System Auditor should consider documenting the risk assessment technique or methodology used for a specific audit. The documentation should ordinarily include:

- A description of the risk assessment methodology used
- The identification of significant exposures and the corresponding risks
- The risks and exposures the audit is intended to address

- The audit evidence used to support the Information System Auditor's assessment of risk

2.5 Audit Staffing

Part of planning Information System Audits involves making auditor assignments, schedules, individual audit timing, and skill requirements. All this should be juggled to satisfy the plan requirements. Aligning the audit and technical skill requirements with the skills of the available staff and the development goals of the team members require thought and management skills. The Auditor in Charge (AIC), who will lead the individual audit, must be knowledgeable of the technology, risks, and audit techniques unique to the subject and be able to provide guidance and developmental assistance for staff auditors assisting in the fieldwork. The AIC will be responsible for the final product and will approve all the work papers, testing, and results.

The AIC will represent the audit department through the presentation of the final report and ensure that the opinions rendered represent both the risks and controls adequately. Their communication skills (both verbal and written) must be well developed enough to give management the sense that the audit effort is well managed and under control at all times.

As the field is relatively young, not all jurisdictions have developed a pre-defined skill set that is required when evaluating the qualifications of IT audit personnel. Since auditors will be responsible for evaluating the controls affecting the recording and safekeeping of assets, it is recommended that IT personnel having a detailed knowledge regarding information systems with a general understanding of accounting principles should be suitable for the Information System Audit assignment.

Still, there may be a requirement for skill sets that are not available from the existing staff. Opportunities for partnering with the IS department experts are ideal for building relationships and educating IS staff members on the practices while obtaining knowledge of technical subject matters, as long as independence can be maintained. In addition, opportunities for formal training and individual staff auditor development also exist. Care must be taken to ensure that the end result does not misrepresent the

overall audit effort as inexperienced and unprofessional. Partnering with the external auditors to gain technical knowledge also is a viable option that pays off for the companies external auditors because it enables them to more easily rely on the internal audits assessment of controls. Additional planning time may need to be allocated to an audit where skills need to be developed before the audit can be conducted professionally.

The auditee organization should take sufficient care to expect the following minimum expectations from the Information System Auditors.

Auditor Independence: In all matters related to the audit, the Information System Auditor should be independent of the auditee in both attitude and appearance. The Information System Audit function also should be independent of the area or activity being reviewed to permit objective completion of the audit assignment.

Due professional care: The Information System Auditor should exercise due professional care, including observance of applicable professional auditing standards, in conducting the audit assignments.

Competence: The Information System Auditor should be professionally competent, having the skills and knowledge to conduct the audit assignment and he should maintain professional competence through appropriate professional education and training.

2.5.1 Auditor Independence

- Information System Auditor should be independent of the auditee in both attitude and appearance. If independence is impaired in fact or appearance, the details of the impairment should be disclosed to the appropriate parties.

- The Information System Audit function should be independent of the area or activity being reviewed to permit objective completion of the audit assignment.

- The audit charter or engagement letter should address independence and accountability of the audit function.

- Independence should be regularly assessed by the Information System Auditor, and management and the audit committee as appropriate.

The trade-off between non-audit role in an IS initiative and the independent audit of the IS initiative or the related function should be the decision of the audit committee or equivalent governance body. Aspects that are likely to influence the decision include:

- Potential alternative resources for either role
- Perception of the relative value added by the conflicting activities
- Potential for educating the IS team so that future initiatives could benefit
- Career development opportunities and succession planning for the Information System Auditor
- Level of risk attached to non-audit role
- Effect on the visibility, profile, image, etc., of the Information System Audit function
- Effect of the decision on the requirements of external auditors or regulators, if any
- The provisions of the Information System Audit charter

Disclosure Requirements: Where the independence of Information System Audit management and/or staff, with reference to an audit of an IS initiative and or the related function, could be or could be seen to be impaired by a non-audit role in the IS initiative, the Information System Auditor should disclose it in the audit report, sufficient information about the non-audit role as well as the actions taken to provide a reasonable assurance of objectivity. This will enable the users of the audit report to understand the likely extent of the impairment, if any, and the measures taken to mitigate its effects . Information that the Information System Auditor should consider disclosing includes aspects such as:

- Names and the seniority of the Information System Audit management and staff involved in the IS initiative in non-audit role

- Nature, timing and extent of their non-audit involvement in the IS initiative

- Reasons for their involvement in the non-audit role in the IS initiative as well as in the audit of the IS initiative or the related function

- Steps taken to provide an assurance that objectivity has not been materially impaired in the course of the audit work and the reporting process

- The fact that the potential impairment of the independence has been highlighted to the audit committee or equivalent governance body and their concurrence obtained before undertaking the non-audit role

2.5.2 Due Professional Care

The Information System Auditor should exercise due professional care, including observance of applicable professional auditing standards, in conducting the audit assignments.

The Information System Auditor should maintain the highest degree of integrity and conduct, and not adopt any methods that could be seen as unlawful, unethical or unprofessional to obtain or execute audit assignments.

- The standard of due care is the level of diligence that a prudent and competent expert would exercise under a given set of circumstances. Due professional care applies to an individual who professes to exercise a special skill, such as Information System Auditing. Due professional care requires the individual to exercise that skill to a level commonly possessed by practitioners of that speciality.

- Due professional care applies to the exercise of professional judgment in the conduct of the work performed. Due professional care implies that the professional approaches

matters requiring professional judgment with proper diligence.

- Due professional care should extend to every aspect of the audit, including but not restricted to the evaluation of audit risk, accepting audit assignments, formulation of audit objectives, the establishment of the audit scope, planning the audit, conducting the audit, allocation of resources to the audit, selection of audit tests, evaluation of test results, audit documentation, conclusion of audit, reporting and delivery of audit results. In doing this, the Information System Auditor should determine or evaluate:
    - The type, level, skill and competence of audit resources required to meet the audit objectives
    - The significance of identified risks and the potential affect of such risks on the audit
    - The audit evidence gathered
    - The competence, integrity and conclusions of others upon whose work the Information System Auditor places reliance

The Information System Auditor should maintain an independent and objective state of mind in all matters related to the conduct of the IT audit assignment. The auditor should appear honest, impartial and unbiased in addressing audit issues and reaching conclusions.

The Information System Auditor should conduct the audit with diligence while adhering to professional standards and statutory and regulatory requirements. The Information System Auditor should have a reasonable expectation that the Information System Audit assignment can be completed in accordance with established Information System Audit standards and other appropriate professional, regulatory or industry standards, and will result in the Information System Audit being able to express a professional opinion. The Information System Auditor should disclose the circumstances of any non-compliance in a manner consistent with the communication of the audit results.

The Information System Auditor should have a satisfactory assurance that management understands its obligations and responsibilities in providing appropriate, relevant and timely information required in the performance of the audit assignment and to ensure the co-operation of relevant personnel during the audit.

The Information System Auditor should serve the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and should not engage in acts discreditable to the profession.

The Information System Auditor should maintain the privacy and confidentiality of the information obtained in the course of his/her duties unless a disclosure is required by legal authority. Such information should not be used for personal benefit or released to inappropriate parties.

The Information System Auditor should exercise due professional care while informing appropriate parties of the results of the work performed.

The intended recipients of the audit reports have an appropriate expectation that the Information System Auditor has exercised due professional care throughout the course of the audit. The Information System Auditor should not accept an assignment unless adequate skills, knowledge and other resources are available to complete the work in a manner expected of a professional.

2.5.3 Competence

The Information System Auditor should be professionally competent, having the skills and knowledge to conduct the audit assignment. The Information System Auditor should maintain professional competence through appropriate continuing professional education and training.

The Information System Auditor should provide a reasonable assurance that sufficient professional competencies (skills, knowledge and experience relevant to the planned assignment) are made available prior to the commencement of the work. If not,

the Information System Auditor should decline or withdraw from the assignment.

If needed, the Information System Auditor should meet the continuing professional education or development requirements of a recognised audit-related professional designations or else should have sufficient formal education, training and work experience.

Where the Information System Auditor leads a team to conduct a review, the Information System Auditor must provide a reasonable assurance that all the members have the appropriate level of professional competency for the work they perform.

2.6 Using work of other experts

The interdependency of customers' and suppliers' processing and the outsourcing of non-core activities mean that an Information System Auditor (internal or external) will often find that parts of the environment being audited are controlled and audited by other independent functions or organisations. This guideline sets out how the Information System Auditor should comply with the above standard in these circumstances. Compliance with this guideline is not mandatory, but the Information System Auditor should be prepared to justify any deviation from it.

Information System Auditors should consider using the work of other experts in the audit when there are constraints that could impair the audit work to be performed or potential gains in the quality of the audit. Examples of these are the knowledge required by the technical nature of the tasks to be performed, scarce audit resources and limited knowledge of specific areas of audit. An 'expert' could be an Information System Auditor from the external accounting firm, a management consultant, an IT expert or expert in the area of the audit who has been appointed by top management or by the Information System Audit team. An expert could be internal or external to an organisation as long as independence and objectivity is maintained.

2.6.1 Rights of Access to the Work of Other Experts

The Information System Auditor should verify that, where the work of other experts is relevant to the Information System Audit objectives, the audit charter or engagement letter specifies the Information System Auditor's right of access to this work.

2.6.2 Planning Considerations

When the Information System Auditor does not have the required skills or other competencies to perform the audit, the Information System Auditor should seek competent assistance from other experts; however, the Information System Auditor should have good knowledge of the work performed but is not expected to have a knowledge level equivalent to the experts.

When an Information System Audit involves using the work of other experts, the Information System Auditor should consider their activities and their effect on the Information System Audit objectives whilst planning the Information System Audit work. The planning process should include

- Assessing the independence and objectivity of the other experts
- Assessing their professional competence and qualifications
- Obtaining an understanding of their scope of work, approach, timing and quality control processes, including assessing if they exercised due care in creating working papers and retaining evidence of their work
- Determining the level of review required

2.6.3 Independence and Objectivity

The processes for selection and appointment, the organisational status, the reporting line and the effect of their recommendations on management practices are indicators of the independence and objectivity of other experts.

2.6.4 Professional Competence

The qualifications, experience, resources and credentials of other experts should all be taken into account in assessing professional competence.

2.6.5 Scope of Work and Approach

Scope of work and approach ordinarily will be evidenced by the other expert's written audit charter, terms of reference or letter of engagement.

2.6.6 Level of Review Required

The nature, timing and extent of audit evidence required will depend upon the significance and scope of the other expert's work. The Information System Auditor's planning process should identify the level of review that is required to provide sufficient/ reliable, relevant and useful audit evidence to achieve the overall Information System Audit objectives effectively. The Information System Auditor should review the other expert's final report, audit programme(s) and audit work papers. The Information System Auditor should also consider whether supplemental testing of the other expert's work is required.

2.6.7 Review of Other Expert's Work Papers

The Information System Auditor should have access to all work papers created by the expert, supporting documentation and reports of other experts, where such access does not create legal issues.

Where the expert's access to records creates legal issues and, hence, such access is not available, the Information System Auditor should appropriately determine and conclude the extent of use and reliance on the expert's work.

In reviewing other expert's work papers, the Information System Auditor should perform sufficient audit work to confirm that the other expert's work was appropriately planned, supervised,

documented and reviewed, to consider the appropriateness, sufficiency of the audit evidence provided by them, and to determine the extent of use and reliance on the expert's work. Compliance with relevant professional standards should also be assessed. The Information System Auditor should assess whether the work of other experts is adequate and complete to enable the Information System Auditor to conclude on the current audit objectives and document such conclusion.

Based on the assessment of the work of other experts' work papers, the Information System Auditor should apply additional test procedures to gain sufficient and appropriate audit evidence in circumstances, where the work of other experts does not provide sufficient and appropriate audit evidence.

If additional test procedures performed do not provide sufficient and appropriate audit evidence, the Information System Auditor should provide appropriate audit conclusion and include scope limitation, wherever required.

2.6.8 Review of Other Expert's Report(s)

The Information System Auditor should perform sufficient reviews of the other expert's final report(s) to confirm that the scope specified in the audit charter, terms of reference or letter of engagement has been met; that any significant assumptions used by the other experts have been identified; and that the findings and conclusions reported have been agreed upon by management.

It may be appropriate for management to provide their own report on the audited entities, in recognition of their primary responsibility for systems of internal control. In this case, the Information System Auditor should consider management's and the expert's reports together.

The Information System Auditor should assess the usefulness and appropriateness of reports issued by the other experts, and should consider any significant findings reported by the other experts. It is

the Information System Auditor's responsibility to assess the effect of the other expert's findings and conclusions on the overall audit objective, and to verify that any additional work required to meet the overall audit objective is completed

If an expert is engaged by another part of the organisation, reliance may be placed on the report of the expert. In some cases, this may lessen the need for Information System Audit coverage even though the Information System Auditor does not have access to supporting documentation and work papers. The Information System Auditor should be cautious in providing an opinion on such cases.

The Information System Auditor's views/comments on the adoptability and relevance of the expert's report should form a part of the Information System Auditor's report if the expert's report is utilised in forming the Information System Auditor's opinion.

2.6.9 Implementation of Recommendations

Where appropriate, the Information System Auditor should consider the extent to which management has implemented any recommendations of other experts. This should include assessing if management has committed to remediation of issues identified by other experts within appropriate time frames and the current status of remediation.

2.7 Audit Schedule

Schedules of individual audits, resources, the start and finish deadlines, and possible overlap of each audit all must be reconciled when developing a master Information System Audit schedule for the Information System Audit plan. Remember that time also must be allocated for vacations, training, departmental meetings, and other overhead-related time. Time allocation for an individual audit should include time for planning, fieldwork review, report writing, and post-audit follow-up. It is usually wise to set aside some time in reserve for unplanned issues that come up during the course of the year, either due to new risks or business

issues that will require more work to satisfy the risk/control investigation that is warranted.

Clients should be given the opportunity to provide input into the final scope and goals of an audit plan and to the individual audits. There may be local concerns or newly emerging risk issues that the planning process was not aware of or did not account for that can be addressed by seeking out this input. Business unit management also should be given the courtesy of advance scheduling notice so that the disruption of the business processes is minimized.

Audit management may take the approach that audits should contain the element of surprise to ensure that the audit truly represents the actual control conditions by implementing their audits unannounced and capitalizing on the element of surprise. In some cases, gathering evidence before announcing an audit may be necessary to establish a known condition where IT management chronically disregards established controls. A poor control environment is not often correctable by advance notice of an audit. However, you may be able to fix up some issues cosmetically, but correcting the root problems requires basic process changes that advance notice will not enable an auditee to address. In fact, if the overall goal of the audit is to help the business and its management implement proper controls, improve performance, and assist with reaching the organizations common goals, then having the IS processes unit prepare for an audit by tightening the controls achieves much of this by itself. Actually, it is more of a win-win scenario because the internal audit team then can report to management that controls are in place as desired, and the process and the business overall can benefit from the improved control position.

2.8 Communication of Audit Plan

Once all of the relevant technical processes are identified and the extent of the involvement of these processes is understood for the purposes of planning the audit, they can be separated into logical subdivisions of the audit program. These divisions are based on

the expertise required, geographical divisions, managerial responsibility divisions, or some method that worked well in the prior audit approaches. Evidence of approval by the audit management with their assessment of risks and planned scope and objectives should be well documented in this section.

The audit program is a high-level description of the audit work to be performed. It is a series of audit steps designed to meet the audits objectives by identifying the process-related risks, determining the controls that are in place to mitigate that risk, and testing those controls for effectiveness and sufficiency to successfully mitigate the risk to an acceptable level. The collection of all audit steps that must be performed to reach the desired conclusions is called the audit program. This program should be prepared in advance of the fieldwork and include sections for testing, evaluation, and conclusions for all of the significant risk areas that were identified and approved for inclusion in the audits scope and objectives. As dictated by the style and format used by your audit organization, assignments, and the work allocation of auditors of particular sections will be documented in the audits program sections of the work papers.

Some programs are organized by process, thus exploring all of the risks and control objectives for a particular process. This is a useful way of developing an audit program when different managers are accountable for separate processes, because it enables the audit to focus on areas divided by a manager and provides a vehicle for prioritizing risks for a single process.

Another organizational style is by risk or control objective. In this manner, a particular risk can be fully explored across all relevant processes and functions, thus enabling an aggregate view of the impact of a particular control objective. This type of audit program approach typically is used by upper management in order to understand the impact of changes or the exposure that requires a broad corporate view of a particular issue.

Provisions for tracking risk/control weaknesses and for aggregating them in a summary format also should be planned for

in work paper layout. In addition, standard locations for making notes on program steps, such as when noting the percentage of steps complete, filling out the auditor date of completion and management review, and making comments, should be part of the format adopted in an audit program. Each section should provide an approach that would enable a reasonably competent third-party auditor to follow through with your process and draw the same conclusions. Tying the testing and related findings directly back to the risks and drawing conclusions and making recommendations that support the business needs is the best way to ensure this is done.

Planning Memo

A planning memo outlines for the auditee the tone and course of action the IT audit manager plans to take. The memo outlines for the auditee the areas within the audit the auditor is planning to spend most of their time, and it gives the auditee the opportunity to voice any concerns.

2.9 CAAT (Computer Assisted Auditing Techniques)

As the use of information systems to record, transact and process data, increases in the organizations, the Information System Auditor needs to utilise IS tools to adequately assess risk considering the need to audit large number of transactions. With data volumes growing and Management expectations on assurances becoming more specific, random verifications and testing is not satisfactory. The use of audit software ensures complete scrutiny of selected transactions, and pointed identification and zeroing in on erroneous/exceptional transactions, even when data volumes are huge. And all this can be done in a fraction of the time required with manual methods.

The use of computer-assisted audit techniques (CAATs) serves as an important tool for the Information System Auditor to evaluate the control environment in an efficient and effective manner. The use of CAATs can lead to increased audit coverage, more

thorough and consistent analysis of data, and reduction in risk. CAATs include many types of tools and techniques, such as generalised audit software, customised queries or scripts, utility software, software tracing and mapping, and audit expert systems.

Information System Auditor uses CAAT for getting one or more of the following benefits:

- Reduced level of audit risk.
- Greater independence from the auditee.
- Broader and more consistent audit coverage.
- Faster availability of information.
- Improved exception identification.
- Greater flexibility of run times.
- Greater opportunity to quantify internal control weaknesses.
- Enhanced sampling.
- Cost savings over time.

When planning the audit, the Information System Auditor should consider an appropriate combination of manual techniques and CAATs. In determining whether to use CAATs, the factors to be considered include:

- Computer knowledge, expertise, and experience of the Information System Auditor
- Availability of suitable CAATs and IS facilities
- Efficiency and effectiveness of using CAATs over manual techniques
- Time constraints
- Integrity of the information system and IT environment

- Level of audit risk.
- Ease of use, both for existing audit staff and future staff.
- Training requirements.
- Complexity of coding and maintenance.
- Flexibility of uses.
- Installation requirements.
- Processing efficiencies (especially with a PC CAAT).
- Effort required in bringing the data files and their co-relation into the CAATs for analysis.

CAATs may be used in performing various audit procedures including:

- Tests of details of transactions and balances
- Analytical review procedures
- Compliance tests of IS general controls
- Compliance tests of IS application controls
- Penetration testing

The Information System Auditor must have an understanding of the capabilities and limitations of the CAATs so that the same may be used effectively and efficiently. Before utilising CAATS, an Information System Auditor must document the need and also indicate how the use of CAATs would serve the objective of the audit.

2.9.1 Types of CAATs

Following types of CAATs are available in the market

1. **Generalised audit software** has the capability to directly read and access various database platforms, flat file systems and

ASCII formats. Information System Auditors use this type software typically for the following functions:

- File access enables the reading of different record format and file structures.
- File reorganization- enables an indexing, sorting, merging and linking with another file to get meaningful information
- Data selection - enables global filtration condition and selection criteria.
- Statistical functions enable sampling, stratification and frequency analysis.
- Arithmetical functions enable arithmetic operators and functioning.

2. **Utility software** provides evidence to the auditors about system control effectiveness. It is generally a subset of software, for example, database management system's generated report.

3. **Test data**: Test Data is used for testing logic error in a program and whether the program meets its objectives.

4. **Expert Systems**: Information System Auditors use expert systems, which is built on the knowledge base of the experienced auditors and gives direction and valuable information for carrying out the audit.

While using CAATs, the Information System Auditor must consider the following concerns.

- The integrity, reliability and security of the CAATs.
- The integrity of the information systems and security environment.
- The confidentiality and security of the data as required by the client.

2.9.2 Planning Steps

The major steps to be undertaken by the Information System Auditor in preparing for the application of the selected CAATs are:

- Set the audit objectives of the CAATs
- Determine the accessibility and availability of the organisation's IS facilities, programs/system and data.
- Determine resource requirements, i.e., personnel, CAATs, processing environment (organisation's IS facilities or audit IS facilities).
- Obtain access to the organisation's IS facilities, programs/system, and data, including file definitions.
- Document CAATs to be used, including objectives, high-level flowcharts, and run instructions.
- Define the procedures to be undertaken (e.g., statistical sampling, recalculation, confirmation, etc.).
- Define output requirements.

2.9.3 Arrangements with the Auditee

Data files, such as detailed transaction files, are often only retained for a short period of time; therefore, the Information System Auditor should make arrangements for the retention of the data covering the appropriate audit time frame.

Access to the organisation's IS facilities, programs/system, and data, should be arranged for well in advance of the needed time period in order to minimise the effect on the organisation's production environment.

The Information System Auditor should assess the effect that changes to the production programs/system may have on the use of the CAATs. In doing so, the Information System Auditor should consider the effect of these changes on the integrity and

usefulness of the CAATs, as well as the integrity of the programs/system and data used by the Information System Auditor.

2.9.4 Testing the CAATs

The Information System Auditor should obtain a reasonable assurance of the integrity, reliability, usefulness, and security of the CAATs through appropriate planning, design, testing, processing and review of documentation before placing reliance upon the CAATs. The nature, timing and extent of testing are dependent on the commercial availability and stability of the CAATs.

2.9.5 Security of Data and CAATs

Where CAATs are used to extract information for data analysis, the Information System Auditor should verify the integrity of the information system and IT environment from which the data are extracted.

CAATs can be used to extract sensitive program/system information and production data that should be kept confidential.

The Information System Auditor should safeguard the program/system information and production data with an appropriate level of confidentiality and security. In doing so, the Information System Auditor should consider the level of confidentiality and security required by the organisation owning the data and any relevant legislation.

The Information System Auditor should use and document the results of appropriate procedures to provide for the ongoing integrity, reliability, usefulness, and security of the CAATs. For example, this should include a review of program maintenance and program change controls over embedded audit software to determine that only authorised changes were made to the CAATs.

When the CAATs reside in an environment not under the control of the Information System Auditor, an appropriate level of control

should be in effect to identify changes to the CAATs. When the CAATs are changed, the Information System Auditor should obtain assurance of their integrity, reliability, usefulness, and security through appropriate planning, design, testing, processing and review of documentation before reliance is placed on the CAATs.

2.9.6 Mandate to Use CAATs

Information System Auditors should take care to mention the use of CAATs in their Audit Mandate, if required, to avoid issues/ problems later and ensure availability of data for analysis.

2.9.7 Documentation & Relying on Experts

Work Papers: The step-by-step CAATs process should be sufficiently documented to provide adequate audit evidence. Specifically, the audit work papers should contain sufficient documentation to describe the CAATs application, including the details set out in the following sections.

Planning Documentation should include:

- CAATs objectives.
- CAATs to be used.
- Controls to be exercised.
- Staffing and timing.

Execution Documentation should include:

- CAATs preparation and testing procedures and controls
- Details of the tests performed by the CAATs
- Details of inputs (e.g., data used, file layouts), testing periods, processing (e.g., CAATs high-level flowcharts, logic) and outputs (e.g., log files, reports)
- Listing of relevant parameters or source code

Audit Evidence Documentation should include:

- Output produced.
- Description of the audit analysis work performed on the output.
- Audit findings.
- Audit conclusions.
- Audit recommendations.

2.9.8 Reporting

The objectives, scope and methodology section of the report should contain a clear description of the CAATs used. The description of the CAATs used should also be included in the body of the report, where the specific finding relating to the use of the CAATs is discussed.

If the description of the CAATs used is applicable to several findings, or is too detailed, it should be discussed briefly in the objectives, scope and methodology section of the report and the reader referred to an appendix with a more detailed description.

Use of Work of another Auditor/ Expert Rights of Access: The Information System Auditor should ensure that, where the work of other auditors or experts is relevant to the Information System Audit objectives, the audit charter or engagement letter specifies the Information System Auditor's right of access to this work.

Planning Considerations: When an Information System Audit involves using the work of other auditors or experts, the Information System Auditor should consider their activities and their effect on the Information System Audit objectives while planning the Information System Audit work.

The planning process should include

- Assessing the independence and objectivity of the other auditors or experts.
- Assessing their professional competence.
- Obtaining an understanding of their scope of work and approach.
- Determining the level of review required.

2.9.9 Continuous Online Audit Approach

CAATs have the ability to improve audit efficiency, particularly in paperless environment through continuous online auditing techniques. The Information System Auditor must develop audit techniques that are appropriate for use with advanced computerized systems. Information System Auditors may use one or more of the following five types of automated evaluation techniques:

- Systems Control Audit Review File (SCARF) and Embedded Audit Modules (EAM): The use of this technique involves embedding specially written audit software in the organization's host application system so that the application systems are monitored on a selective basis.
- Snapshots: This technique involves taking what might be termed pictures of the processing path that a transaction follows from the input to the output stage. With the use of this technique, transactions are tagged by applying identifiers to input data and recording selected information about what occurs for the auditor's subsequent review.
- Audit hooks: This technique involves embedding hooks in application systems to function as red flags and induce Information System Auditors to act before an error or irregularity gets out of hand.
- Integrated Test Facilities (ITF): In this technique, facilities are set up and included in an auditee's production files. The

Information System Auditor can make the system process either live transactions or test transactions during regular processing runs and have these transactions update the records of the dummy entity. The operator enters the test transactions simultaneously with live transactions that are entered for processing. The auditor then compares the output with the data that have been independently calculated to verify the correctness of the computer processed data.

- Continuous and Intermittent Simulation (CIS): The computer system, during a process run of a transaction, simulates the instruction execution of the application. As each transaction is entered, the simulator decides whether the transaction meets certain predetermined criteria and if so, audits the transaction. If not, the simulator waits until it encounters the next transaction that meets the criteria.

3

CONDUCTING THE AUDIT

3.1	Audit Methodology
3.2	Pre-Audit Activities
3.3	Information System Audit Process
3.4	Documenting Observations and Findings
3.5	Audit Report – Preparation & Distribution

3.1 Audit Methodology

Audit Methodology is the set of procedures to perform the scheduled audit and achieve the audit objectives.

Audit Methodology also describes the format of the Audit Report and guidelines about completing and gathering the work-papers. Work-papers include the Templates to test the Internal Controls and evidences collected during the audit. Most of the work-papers and/or evidences are in the form of electronic format (Screenshots / diagrams / flowcharts etc.) which should be gathered and preserved to conclude the audit while preparing the final report of the audit.

3.2 Pre-Audit Activities

Although Audit Planning, as discussed earlier, covers all the major areas, following activities need to be reviewed and finalized before the actual audit.

- Audit Team Finalization
- Communication and Logistics Arrangements
- Data Gathering

- Sampling
- Materiality & Evidence Gathering

3.2.1 Audit Team Finalization

Information System Auditor should ensure that Audit Team members are available during the audit schedule and their skill sets are matched with the Audit Profile

It is a good practice that, if Audit Team has 4/5 auditors then, at least 2 Auditors are familiar with the Auditee organization and the site / location, which means, 2 members from the Audit Team were involved during the previous audits of that organization / site.

3.2.2 Communication and Logistics Arrangements

Information System Auditor must send a reminder at least 15 days before the scheduled audit date. The following should be included in the reminder –

1. Audit Scope – Although the Audit Scope is well defined in the Audit Charter, confirmation about the readiness of Auditee is necessary before conducting the audit. Hence, while obtaining the confirmation Information System Auditor should include main facets of the scope like Applications, Locations and Exclusions

2. Other requirements – Information System Auditor should ensure that Auditee is aware about the other requirements of Auditors like –

    - Availability of the respective staff
    - Physical Access to the Facility
    - Conference Room to be booked for Auditors
    - Telephone and Internet Arrangement
    - Access to the different IS applications as a GUEST User

- Access to the different IS Applications to use the auditing tool and/or CAATs

3. Logistics Arrangements – Information System Auditor should ensure that following logistics arrangements have been made and confirmation about the same should be obtained before travelling.

    - Travel Arrangements – Bus / Train / Flight bookings
    - Accommodation Arrangements – Hotel / Guest House
    - Pick-up and Drop arrangements to / from accommodation facility to / from office and/or station / airport

3.2.3 Data Gathering

While preparing for the audit, the entire audit team should go through following documents –

- Organization's Web Site
- Organization's Annual Report
- Previous Audit Report
- Previous Audit Checklists and Work Papers
- Any other Related Documents / Material

3.2.4 Sampling

Information System Auditors use sampling when time and cost considerations preclude a total verification of all transactions or events in a predefined population. The population consists of the entire group of items that need to be examined. The subset of the population members is called a sample. Sampling is used to infer characteristics about a population, based on the results of examining the characteristics of a sample of the population. There are two general approaches to audit sampling / statistical and non statistical. Within these two general approaches, they are two

primary methods that are used by the auditors, attribute sampling and variable sampling.

Attribute sampling, generally applied in compliance testing situations, deals with the presence or absence of the attribute and provides conclusions that are expressed in rates of incidence. Variable samples, generally applied in substantive testing situation, deals with population characteristic that vary, such as rupees and weights, and provides conclusion related to deviation from the norms.

Attribute sampling refers to three different, but related types of proportional sampling.

1. Attribute sampling is sampling model that tries to estimate the rates (percent) of occurrence of specific quality (attribute) in a population.

2. Stop and go sampling is a model that helps prevent excessive sampling of an attribute by allowing an audit test to be stopped at the earliest possible moment. It is used when the Information System Auditors believes that relatively few errors will be found in a population.

3. Discovery sampling is the model that can be used when the expected occurrence rate is extremely low. This model is used when the objective of the audit is to seek out fraud, circumvention of regulation and other irregularities.

Variable sampling refers to a number of different types of quantitative sampling models:

1. Stratified mean per unit model is one in which the population is divided into groups and samples are drawn from various groups.

2. Un-stratified mean per unit model is one, where by a sample mean is calculated and projected as an estimated total.

3. Difference estimation model is used to estimate the total difference between the audited values and the non-audited values based on differences obtained from sample observations.

The main steps used by an Information System Auditor in the construction and selection of a sample for an audit test include:

- Determining the objectives of the test.
- Defining the population to be sampled.
- Determining the sampled method i.e. attribute versus variable.
- Calculating the sample site.
- Selecting the sample.
- Evaluating the sample from audit perspective.

3.2.5 Materiality & Evidence Gathering

Information System Auditors should assess the materiality and plan their audit effectively by focusing their efforts on high risk areas and assess the severity of any errors or weaknesses found.

The assessment of what is material is a matter of professional judgment and includes consideration of the effect on the organization as a whole of errors, omissions, irregularities and illegal acts, which may arise as a result of control weaknesses in the area being audited.

The Information System Auditor should consider both qualitative and quantitative aspects in determining materiality.

Information is material if its misstatement (omission or erroneous statement) could influence the decisions of its users. Materiality depends upon the size and nature of the item, judged in the particular circumstances of its misstatement. The auditor should normally establish levels of materiality in such a way that the audit work will be sufficient to meet the audit objective and will use audit resources efficiently.

In assessing the materiality, the Information System Auditor should consider the aggregate level of error acceptable to the management, Information System Auditor, and various regulatory

agencies and potential for the cumulative effect of minor errors or weaknesses to become material.

Basing on the materiality, the Information System Auditor should identify the controls to be examined. With respect to a specific control objective, a material control is a control or group of controls without which control procedures do not provide a reasonable assurance that the control objective will be met. Where the Information System Audit objective relates to systems or operations that process financial transactions, the value of the assets controlled by the systems or the value of the transactions processed should be considered in assessing materiality.

Financial auditors, generally, measure materiality in monetary terms. Information System Auditors may audit non-financial items such as physical access controls, logical access controls, program change controls, manufacturing controls, design controls, quality controls, password generation, credit card protection, patient care etc.

In the case of assessing the materiality for non-financial transactions, the following are the examples of measures to assess the materiality:

- Criticality of the business processes supported by the system or operation.
- Cost of the system or operation.
- Potential cost of errors.
- Number of accesses/transactions/inquiries processed per period.
- Nature, timing and extent of reports prepared and files maintained.
- Nature and quantities of materials handled.
- Service level agreements/ requirements and cost of potential penalties.

- Penalties for failure to comply with legal and contractual, public health and safety requirements.

Evidence is any information used by the Information System Auditor to determine whether the entity or data being audited follows the established audit criteria or objectives. Audit evidence may include the Information System Auditors observations, notes taken from interviews, material extracted from correspondence and internal documentation or the results of audit test procedures. While all evidence will assist the Information System Auditor in developing audit conclusions, some evidence is more reliable than others.

While evaluating the evidence, Information System Auditors should keep the following points in mind:

- Independence of the provider of the evidence.
- Qualifications of the individual providing the evidence.
- Objectivity of the evidence.

The Information System Auditor should apply good judgment to determine which material is directly appropriate to the objectives of the audit and which is not. Both quality and quantity of evidence must be assessed by the Information System Auditor. These two qualities are referred to as competent (quality) and sufficient (quantity). Evidential matter is competent when it is valid and relevant. Audit judgment is used to determine when sufficiency is achieved in the same manner that is used to determine the competency of evidential matter.

Gathering of evidential matter is the key step in the audit process. The Information System Auditor should be aware of the various forms of evidence and how are they gathered and reviewed.

The Information System Auditors normally use the following techniques for gathering evidence:

- Reviewing IS Organization Structures.
- Reviewing IS Documentation Standards.

- Interviewing the Appropriate Personnel.
- Observing the processes and Employee Awareness.

3.3 Information System Audit Process

3.3.1 Opening Meeting

During the Initial Phase of the audit, this meeting is conducted, to get introduced to the Top Management and Auditee. Audit Scope, Objective and entire Audit Plan is discussed during the meeting

3.3.2 Reviewing the documents

An Information System Auditor reviews the following documents to get an overview and understanding about the different processes in the organization

- Policies – Are the management guidelines which should be approved by the Top Management and should be reviewed at least once in each year?
- Procedures – Are the detailed documents based on the policies set by the top management. ?. Procedures contain the detailed information about the process. All the procedures should be approved by the management and should be reviewed at least once in each year
- Flowcharts – Pictures are worth a thousand words when it comes to understanding the interactions of various processes and how the transaction flow has the dependencies and branches that run in various directions
- Audit Logs and Screenshots – Every organization implements the monitoring control over the processes and preserves the evidence of the same, in the form of system screenshots and system logs. This gives an added confidence to the Information System Auditor about the monitoring control established by the management

3.3.3 Interviewing the Key Personnel

Information System Auditor conducts the meetings and interviews each Dept. / Unit Head as well as with the key personnel working in the operations, to know the following –

- To understand the employee's awareness towards organization's IS policies and procedures
- Reporting Hierarchy and relationship to understand implementation of SOD (Segregation Of Duties) control
- To gain the knowledge of the entire process and the flow of the data / transactions in the organization

3.3.4 Conducting the walkthroughs

Walkthroughs are conducted to understand the implementation of different processes and gain the evidence for the compliance and/or deviations if any. Walkthroughs include the physical round around the facility, meeting and interacting with the employees, going through the documentations maintained, either Input Forms or Output Forms, by the operations people.

3.3.5 Testing of IS Controls

Testing of Controls involves the following –

- Obtaining the population and conducting the compliance tests either on the entire population and/or on selected samples from the population
- If any auditing tools are to be used, then the testing is conducted by using the utilities of those tools

Testing is performed to determine whether the controls are working. Testing is a scientific process which involves, understanding a process and the expected results. Testing also focuses on, whether these results are control related or actual computational results and performing the work to see if the results support the hypothesis. The testing of a large amounts of transactions or data is usually not possible due to time and cost constraints. Hence, sampling is done on the population and

ensure a sufficient quality and quantity to extrapolate the results of the testing into a reliable conclusion on the entire population.

Testing of the controls, ensures the Design Effectiveness as well as Operational Effectiveness of the controls

Substantive Testing - This type of testing is used to substantiate the integrity of the actual processing. It is used to ensure that processes, not controls, are working as per

The design of the control and produce the reliable results.

Compliance Testing – A compliance test determines if controls are working as designed. As per the policies and procedures, compliance testing results into the adherence to these management directives.

3.3.6 Closing Meeting

Information System Auditors discuss all the Observations, Gaps (Non-Conformities) with the Top Management and recommend the possible solutions for the gaps observed during the audit.

3.4 Documenting Observations and Findings

Information System Auditors must maintain proper documentation of their work as these are the record of the work performed by them and the evidence supporting their findings and conclusions. Documentation is meant to –

- Prove the extent to which an Information System Auditor has complied with guidelines and standards to assist in the planning, performance and review of audits.
- Facilitate third party reviews.
- Evaluate the quality assurance program of the Information System Audit function.
- Extend support in circumstances such as insurance claims, fraud cases and lawsuits. Assist in the professional development of the staff.
- Information System Auditors must ensure that at least the minimum level of documentation is maintained as a record of

the planning and preparation of the audit scope and objectives.

- Expedite Audit Program.
- Audit steps performed and the evidence gathered.
- Audit observations, findings, conclusions and recommendations.
- Complete Report issued.
- Facilitate Supervisory review

The extent of the documentation maintained by an Information System Auditor depends on the needs of the audit and would normally include:

- The Information System Auditor's understanding of the area to be audited and its environment.
- The understanding of the information processing systems and the internal control environment.
- The author and source of the audit documentation and the date of completion.
- Audit evidence, its source and the date of completion.
- The auditee's response to the recommendations.

Information System Auditors must ensure that the documentation they maintain includes information required by standards and guidelines issued by the professional bodies like ICAI, ISACA, ITGI etc., law, government guidelines, and that such documentation is clear, complete and understandable by the reviewer.

3.5 Audit Report – Preparation & Distribution

Audit report is prepared after the completion of the audit of all the in-scope locations / sites and after consolidation of all the observations and/or findings.

Information System Auditor includes following while preparing audit report –

- Background – The section describes the Business as well as IT environment of the organization

- Scope – Audit scope along with any exclusions are mentioned under this section
- Audit Methodology
- Executive Summary – It is the summary of all the Major Findings, to which Information System Auditor wants an immediate attention of the top management
- Conclusion and Roadmap – Audit is concluded and if the management have asked for the further roadmap, it is depicted under this section
- Detail Findings – All findings and observations should be listed in the following fashion –
- Observation and/or finding
- Policy / procedure section which will relate to the observation / finding
- Risk Areas
- Recommendation
- Annexure(s) –
- Audit Profile,
- List of personnel interviewed,
- List of Evidences verified / obtained
- Disclaimer

Report Distribution – Information System Auditor distributes the report to the respective personnel, strictly as per the Audit Charter. Audit Report is a confidential report and under top management discretion to distribute the report, further down the line, in the organization.

4

FOLLOW-UP ACTIVITIES

4.1 Usage of Audit Reports

4.2 Reporting of Information System Audit Report

4.3 Follow Up audit Procedure

Ultimately, the value of an audit lies in the improvements made to the business situation brought about as a result of the audit. Where no such improvements take place, the audit may well have been a waste of time, resources, and money. Improvements will only take place where the individual authorized and empowered to take an effective action has been convinced that some form of action is appropriate to improve the control situation.

4.1 Usage of Audit Reports

Variety of individuals will use audit reports for a variety of purposes. Executive management will typically use an audit report to gain an insight into the overall status of internal controls within a given business area and for the organization as a whole. Operational management uses audit reports to determine the adequacy and effectiveness of specific controls in achieving specific performance and control objectives. Other agencies may use audit reports to gain insight into the inner workings of specific operations and the degree of reliance that can be placed on the outputs of those business areas.

4.2 Reporting of Information System Audit Report

In general, auditors communicate the over all findings together with recommendations for actions to be taken using the audit

report. These reports are sent to those individuals who are in a position to take an effective action or ensure that corrective actions are taken. Senior executives within the organization may also receive either copies of the report or summaries of the reports. Results of the audit are usually reported orally in the form of interim reports and closing conferences as well as in writing.

After the reporting of findings and recommendations, the Information System Auditor should request and evaluate relevant information to conclude whether appropriate action has been taken by management in a timely manner.

4.3 Follow Up Audit Procedure

A follow-up process should be established by an Information System Audit function to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action. Responsibility for these follow-activities may be defined in the audit charter of the function.

It is, unfortunately, a truism that people do not do what is expected, they do what is far from stringent. The Information System Audit executive should establish a follow-up process to monitor progress and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action. These two alternatives lead to different follow-up activities. Where management chooses to *take appropriate action on the audit findings*, auditors must find out what action was taken and determine if it was appropriate. They would typically issue follow-up reports normally directed to the recipients of the original report and the key focus must be on the attainment of the control objectives, not necessarily on the implementation of audit recommendations. Where management *accepted the risk of not taking action*, no follow-up report may be required. Given the mixed nature of audit findings, it is to be expected that management will implement some recommendations and accept some risks. This should be noted in the follow-up report.

Follow-up reports are normally directed to the recipients of the original report and the key emphasis is on the resolution of the

audit findings, not necessarily on the implementation of specific audit recommendations. It may well be that, subsequent to the audit report being issued, management circumstances may have changed in terms of risk prioritization or resource availability and an alternative course of action has been implemented leading to achievement of the same control objectives.

Where the auditor feels that the alternative course of action has not adequately addressed the control objective, the auditor will need guidelines for rejecting auditee's corrective measures. Under the circumstances care should be taken not to attempt to force audit preferences on management. The audit focus should be on control objectives and principles; management should focus on the controls themselves. To do otherwise is to risk becoming the approver. Management must decide, not the auditor. Where a management action is rejected, the auditor must take care never to attack the individuals concerned. The auditor must avoid becoming emotionally involved in disagreements. Auditor should state specifically in rejections, why the rejection has occurred and which control objectives are still threatened.

The auditor will commonly review auditee responses and corrective actions, evaluate the adequacy of those responses and corrective actions, and report follow-up findings. Follow-up actions will vary significantly for differing audits in terms of the breadth, degree of focus, depth, and extent of follow-up examination. Practical considerations such as time available must be taken into consideration.

Auditors tend to be optimists as far as time is concerned and follow-ups are often used to take shortcuts. In many cases, follow-ups are completely omitted. In order to reduce the time required for follow up, the auditor should attempt to:

- Follow up as many steps as possible during the audit itself
- Review written responses prior to the review
- Review only the documentation of corrective action for less critical findings
- Do not perform audit work at all on minor items

- Limit follow-up tests to only the problems noted

It is not necessary that the follow-up be done by the original auditor or audit team. In some lower risk cases, all that may be required is confirmation from management that the agreed action has been taken. In other cases, the audit committee itself may seek reassurance from management that agreed actions have been implemented.

If the management's proposed actions to implement reported recommendations have been discussed with, or provided to, the auditor, these actions should be recorded as a management response in the final report.

The nature, timing and extent of the follow-up activities should take into account the significance of the reported finding and impact if corrective action is not taken. The timing of Information System Audit follow-up activities in relation to the original reporting should be a matter of professional judgment dependent on a number of considerations, such as the nature or magnitude of associated risks and costs to the entity.

Where the management provides information on action taken to implement recommendations and the Information System Auditor has doubts about information provided, appropriate testing or other procedures should be undertaken to ascertain the true position or status concerning the follow-up activities.

A report on the status of follow-up activities, including agreed recommendations not implemented, may be presented to the committee if one has been established, or alternatively to the appropriate level of entity management.

As a part of the follow-up activities, the Information System Auditor should evaluate whether findings if not implemented are still relevant

5

INFORMATION SYSTEM AUDITS

5.1	**IT General controls (ITGC) Audit**
5.2	**Application control Audit**
5.3	**Network Security Audit**
5.4	**Data Migration Audit**
5.5	**Business Continuity Management Audit (BCM)**
5.6	**E- Commerce Audit**
5.7	**Data Centre Audit**

Information System Audits are classified under seven different areas for better understanding. Areas of Information System Audit are ITGC audit which covers the general controls in IS department such as access controls, change management and system development etc. Application control audit covers the areas of input, processing and output controls. Network security audit covers the areas of access, functioning of network and mobile devices security. Data Migration audit covers data mapping, data conversion and operational changes relating to the same. BCM audit covers the risk assessment, business impact analysis, preparation of BCP and DRP, backup and maintenance of BCP and DRP. E- Commerce audit covers area of risks, authorisation, data transfer, and access in relation to e-commerce activities. Data centre audit covers change management, equipments, backup and environment controls in relation to data centre.

5.1 IT General Controls (ITGC) Audit

5.1.1 Overview

IT controls are specific to IT processes designed and developed to support the business processes. Due to the pervasive use of Information Systems now-a-days, it is important that controls are in place.

IT General Controls are those controls that are pervasive to all systems, processes, and data for any organization or IT environment. The objectives of ITGCs are to ensure the proper development and implementation of applications, as well as the integrity of programs, data files, and computer operations.

The most common ITGCs:

- Logical Access Controls – Infrastructure and Applications
- SDLC (System development life cycle) Controls.
- Change Management controls.
- Physical and Environmental Controls.
- Data backup and recovery controls.
- Computer operation controls.

IT environments have continued to increase in complexity with ever greater reliance on the information produced by IT systems and processes. The recent emergence of regulations aiming to restore the investor confidence has placed a greater emphasis on internal controls and often requires independent assessments of the effectiveness of internal controls.

- Ensure that systems are developed, configured, and implemented to achieve management's objectives.
- Ensure that changes to programs and related infrastructure components are requested, prioritized, performed, tested, and implemented in accordance with management's objectives.

- Ensure that production systems are processed completely and accurately in accordance with management's objectives, and that processing problems are identified and resolved completely and accurately to maintain the integrity of financial data.

- Ensure that only authorized access is granted to programs and data upon authentication of a user's identity.

5.1.2 Evolution of ITGC

Information technology controls have been given increased prominence in the companies listed in the United States by the Sarbanes-Oxley Act. The Sarbanes-Oxley (SOX) Act came in effect from 2002.

The requirement of SOX is that the chief executive (CEO) and chief financial officers (CFO) of the public companies should attest the accuracy of financial reports (Section 302) and should establish adequate internal controls over financial reporting (Section 404). SOX has an increased focus on IT controls, as it focuses the Internal Control over financial processing and reporting as per the section 404 of SOX.

COBIT (Control Objectives for Information Technology) framework is widely for SOX compliance, in spite of its wider scope. The 2007 SOX guidance from the PCAOB (Public Company Accounting Oversight Board) and SEC (Securities and Exchange Commission) state that IT controls should only be part of the SOX 404 assessment to the extent that specific financial risks are addressed, which significantly reduces the scope of IT controls required in the assessment.

The focus is on KEY controls (those that specifically address risks), and not on the entire systems / processes. IT controls which fall under the scope of a SOX 404, may include –

- Application (transaction processing) controls, in the processes AP (accounts payable, payroll), GL (general ledger), AR (accounts receivable etc.), that address the identified financial reporting risks.

- IT General Controls which supports the main programs functions and ensure the reliability of the financial reports. E.g. change control and security controls

- IT operations controls, which ensure that, problems within the financial transaction processing are identified and corrected.

5.1.3 Auditing IT General Controls

Information System Auditor will have to see the following, towards the assessment of the key controls –

- To understand the organization's Internal Control Environment and the processes related to financial reporting

- To Identify the IT systems, which are contributing towards processing the financial data i.e. Initiation, Authorization, Processing, Summarization and Reporting

- To identify the key controls which address specific financial risks

- To understand the design and implementation of Internal Controls and its continued effectiveness

- To verify the documentation and testing results of these IT controls

- To ensure that IT controls are updated and changed, to address the necessary and corresponding changes in internal control or financial reporting processes

- Periodic monitoring mechanism of IT controls for effective operation over time.

Information System Auditor must be able to identify the areas where technology plays a critical part. Information System Auditor should be able to sense that IT controls can have a direct or indirect impact on the financial reporting process. E.g. IT application controls which will ensure the completeness of transactions have direct impact on financial statements. Access controls, on the other hand, exist within these applications or

within their supporting systems, such as databases, networks and operating systems, are equally important, but do not have a direct impact on financial reporting. Application controls are generally aligned with a business process that gives rise to financial reports.

5.1.3.1 Logical Access Control

Logical Security means unique user ID and password access, authentication, access rights and authority levels, which should be able to safeguard the organization's systems. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation. The other term for the Logical Security is "User Management". It typically includes the areas like access modes , user types , role based access and passwords

Access Modes – Read only – It provides the users with the capability to view, copy, and print the information but would not be able to alter / modify it, such as delete from, add to, or insert in it any way.

Read and Write – Users are allowed to view and print as well as add, delete, and modify the information. Logical access control can be further refined "read/write" access such that a user has read-only ability for one field of information but the ability to write to a related field. E.g. In the banks the user can see the account information for a customer and is allowed to change certain fields if required i.e. address and contact details of the customer and the user can not change the account no., customer's name and account balance.

Execute – It is the most common activity performed by the users in relation to the applications and programs. e.g. using a word processor, spreadsheet or a database etc. Users would not ordinarily be given read or write capabilities for an application, however, since it would appear in a format that is unintelligible to most users. It might be desirable, though, for software programming specialists to be able to read and write applications.

Logical access control should be able to meet the crucial requirement of preserving the integrity of the information,

protecting it against improper modification and remains available for all to view it.

User Types – In the system, usually two user types are found – General User and Elevated and/or Super User

General User – is the user who has restricted access to the system may be only to the little functionalities or to the few screens of the application. General user usually enters the data, views it for the completeness and correctness and prints it whenever it is required. E.g. Clerks in the Banks, Data Entry Operators in the industry

Elevated / Super User – is the user, who has the ability to change / modify any of the following. (e.g. Sysadmin, DBA etc.)

- Access Rights of the General Users
- System Parameter Settings
- Access to System Data

Usually Super Users are the functional heads / managers of the respective departments and given an additional access privileges, either to authorize the transactions and/or change the system parameters (e.g. Tax Rates)

Role based Access – A role is a functions or a job assignment. E.g. Data entry clerk,Purchase officer, Project leader, Programmer etc. The access rights are grouped and defined under the role name, which becomes easier to assign the access rights to a particular user and also restricts use of those access rights to the individuals. An individual may be authorized for more than one role, but may be required to act in a single role at a time. Changing roles may require logging out and then in again, or entry of a special role-changing command. E.g. An individual who is logged on in the role of a System Administrator can perform operations that would be denied to the same individual acting in the role of an ordinary user. While defining the roles in the system and assigning them to the different users, “Segregation of Duties” (SOD) must be considered. The process of defining roles and their relationships should be based on a thorough analysis of the way in which an

organization operates and should include input from the business process owners in the organization. Role based access is used in Core Banking Solutions packages and in ERP (Enterprise Resource Planning)

Passwords – Passwords in the authentication key to login into the system. Following are the requirements while setting the passwords –

- Combination Alphanumeric characters
- Password length restrictions
- Use of Upper case and special characters
- Password expiry – 45 / 90 days
- Not being able to use the past four or five changed passwords
- After 3/5 unsuccessful attempts the account should get locked

The best practices followed in the industry about the passwords –

- System default passwords are changed after the implementation of the system
- User awareness is created about NOT sharing the passwords
- Passwords of Elevated Users are stored in the sealed envelops, to be able to access the system in case of emergency

Information System Auditor should review the User Management policies and procedures to ensure following –

- Process of grating the access to the new user
- Process of user access of terminated employees and/or employees on long leave

- Process of grating the access to the existing users, in case of change in role
- Periodic monitoring mechanism, to review the access rights of all the users from appropriateness and SOD point of view

5.1.3.2 SDLC (System development life cycle) controls

SDLC process begins with, how new systems or modifications to the current systems are requested, prioritized, actually designed, development of the source code to perform the functions desired, testing of the system developed and/or modified, training of employees to use the new/modified system, and the final system implementation.

SDLC is a systematic approach to problem solving and is composed of several phases, each comprised of multiple steps –

1. Feasibility Study
2. Analysis
3. Design
4. Implementation
5. Testing
6. Evaluation
7. Maintenance

Information System Auditor should consider the following influencing SDLC:

- In-house design and development of the system (using internal resources)
- Design and development of the system by using fully or partly the outsourced resources located onsite or offsite
- Off the shelf available packages implemented as-is without any customization

- Off the shelf available packages implemented as-is with some customization

At times, large complex applications may involve a combination of the above.

Information System Auditor should be aware of implications of following risks, while auditing SDLC

- Adoption of inappropriate SDLC for the application system
- Inadequate controls in the SDLC process
- User requirements and objectives not being met by the application system
- Lack of involvement of all the stakeholders
- Lack of management support
- Inadequate project management
- Inappropriate technology and architecture
- Change in scope
- Time over-runs
- Budget over-runs
- Insufficient attention to security and controls
- Performance criteria not being met
- Inappropriate resourcing / staffing model
- Incomplete documentation
- Inadequate contractual protection
- Inadequate adherence to the development methodologies
- Insufficient attention to interdependencies on other applications and processes

- Inadequate configuration management
- Insufficient planning for data conversion/migration and cutover

SDLC Audit Scope – Information System Auditor should consider the following scenarios while finalizing the SDLC Audit Scope and review relevant SDLC stages

- Pre-implementation review – Information System Auditor should study the proposed SDLC model and the related aspects to assess the appropriateness and the potential risks and provide the necessary risk mitigation recommendations to the management.
- Parallel / concurrent reviews – Information System Auditor should review the relevant SDLC stages, as they are happening, to highlight risks/issues and provide necessary risk mitigation recommendations to the appropriate management.
- Post-implementation reviews – Information System Auditor should review the relevant SDLC stages after their completion to highlight issues faced and provide recommendations for downstream corrections (if possible) and to serve as a learning tool for the future.

Auditing SDLC – Information System Auditor should consider following aspects while auditing and evaluating SDLC phases

- 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. Service Level Agreements –SLAs)
- Contractual terms with the vendors for outsourced services (E.g. Service Level Agreements –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

5.1.3.3 Change Management Controls

The Change Management Process ensuring that all changes to the IS infrastructure are carried out in a planned and authorized manner. Information System Auditor should review the change management process, to ensure that the following risks can be mitigated:

- Malicious code is not being used by the users
- Sensitive data is not lost
- Security features that are inbuilt into the system are always turned on
- Error free financial reporting

Program Change Management policy and procedure must address the following –

- Source Code Changes – This is related to the change in the program which will affect the functionality of the program
- Data Changes – The data changes are requested directly into the databases due to, may be the data changes are not possible from front-end data entry screens and/or access to the data changes is restricted to special user group
- Changes in Key Parameter Values – Changes in the values of the Key Parameters may affect the financial reporting of the organization (e.g. Tax Rate) and/or may affect the security features inbuilt into the system (e.g. Audit Logs ON / OFF)
- Changes to scheduled jobs – Change management procedure for changes to scheduled jobs.
- Changes to End user computing – Spreads sheets developed by users for specific functions and if shared by multiple users.
- Emergency Changes – The policy stating the situations wherein the changes can be made into the systems by overriding the usual process, must be documented clearly

A change management control system address the analysis, application, and review of changes to the applications / systems.

5.1.3.4 Physical and Environmental security controls

Physical and Environmental Security equipments are purchased and commissioned / installed in the facility. Information System Auditor will have to review the process of the following –

- Procurement and commissioning / installing the equipment in the facility
- Periodic Monitoring mechanism of all such external parties.
- Annual Maintenance Contracts (AMC) are in place

- Periodic maintenance is being conducted regularly
- Breakdown calls are attended as per SLA mentioned under AMC
- The documentation for all the above is maintained
- Performance is evaluated annually for each external party, before renewing the AMC

Physical access controls

- Employee Access – Photo Ids, Electronic Card keys, Cipher Key Locks, Biometric
- Visitors Access – Manual logging register is maintained
- Access to the sensitive / critical areas like Server Rooms and Data Centers – Dead-man Doors, Alarm system, Not advertising the sensitive areas like DRP sites
- Monitoring Mechanism – Security Guards, CCTV
- Periodic Review of Monitoring Mechanisms – Visitors Logs, CCTV Logs, Access Logs of Server Rooms on holidays and/or after office hours should be verified monthly
- AMCs for all third parties like Security Guards, CCTV, Electronic Card system / biometric etc. should be in place and monitored

Environmental controls –

- Water and Smoke Detectors
- Fire Extinguishers
- Fire Suppression Systems
- Fire-proof Flooring, walls and ceiling for Server Rooms and/or Data Centers
- Humidity / Temperature Control

- Electrical Power –
- Electrical Surge Protectors
- Air conditioning
- Wiring running through adequate conduits and electrical panels
- Alternate electric power sources (UPS and D.G. Sets)
- Documented and tested emergency building evacuation plan

5.1.3.5 Data backup and recovery controls

Review of the ability of the current process to provide for periodic (daily, weekly and annually) backup of all information systems (O.S. , Applications, Databases and other files) or those considered vital. Also includes a review of restoration (usually done yearly) of systems/data. Off-site rotation involves when/where/how the backup media (Tapes / CDs) are moved to a physically and environmentally secure facility, other than the current facility for safekeeping.

Data back-up and recovery controls are covered in detail under 5.7 Data Center Audit

- Computer operation controls – Computer Operations term is related to Mainframe Systems (e.g. IBM OS/390) – how work is performed by computer Operations personnel, known as “Operators” and the computer operations procedures (known as run-books) followed to provide control on “production” systems being run daily / weekly / monthly / annually. Operators are also the personnel responsible for the backup of mainframe systems.
- Mainframe systems are diminishing now-a-days and hence Computer Operations Controls are referred as Job Scheduling Controls.
- A Job Scheduler is a software application, which processes the unattended background executions, synonymously known as batch processing.

- Features of a Job Scheduler –
- An interfaces to define the workflows and/or job dependencies
- Priorities to control the execution order of unrelated jobs
- Automatic submission of executions of jobs / Transaction Batches
- An interfaces to monitor the executions of jobs / Transaction Batches

Most operating system platforms such as Unix and Windows provide basic job scheduling capabilities (E.g. Unix – Cron). Usually batch processing is done into DBMS, Backup applications, and ERPs, with the help of a Job Scheduler. E.g. Appworx is used with Oracle Apps ERP

Information System Auditor should review the following controls related to a Job Scheduler –

- Jobs should be monitored for completeness
- Abandoned jobs should be resolved in a timely manner
- Access to Job Schedulers should be restricted to appropriate operations personnel

5.1.4 ITGC Audit Scope

Information System Auditor may finalize the ITGC Audit Scope based on the following factors –

Sarbanes-Oxley Compliance – SOX section 404 states the fundamental requirements about the internal control evaluation and reporting. While auditing SOX 404 compliance, Information System Auditor should consider the following risks and controls prominently

- Those that exists through technology
- Those that impact the integrity of processing and/or data

General controls are the controls which impact all the applications irrespective of the technology and environment. Along with General controls, the specific application controls like the controls designed and implemented in the business areas (e.g. Segregation of Duties) and the controls inbuilt into the application for error checking and validation of key fields should be considered.

COBIT (Control Objectives for Information Technology) framework published by ITGI and ISACA, composed of IT General Controls, objectives, risks and controls and can be used as a guidance for SOX 404 compliance.

High Level IT Security Review – Many organizations conduct the High Level IT Security Review to know the present status of establishment of IT Controls and short-fall areas where controls needs to be strengthened. Primarily, such reviews are conducted when either the client would like to know the present status of IT Security to finalize the contract or organization would like to go for the certification (e.g. ISO 27001) and would like to decide the entire road map after assessing the IT Security Status.

Apart from IT General Controls listed above, all the areas listed under Audit Checklist are touched upon to get an idea about the IT Security status and overall awareness among the employees in the organization.

5.1.5 ITGC Audit Checklist Reference

Refer to the checklists as per following details –

- Logical access controls – Infrastructure and Applications – checklist no. 4
- SDLC (System development life cycle) controls – checklist no.8
- Program change management controls – checklist no.5.2
- Physical security controls – checklist no.3
- Data backup and recovery controls – checklist no.5.3

5.2 Application Control Audit

5.2.1 Overview

Application Control Audit is conducted, to ensure that, processes and components of the system performing in an appropriate manner, are efficient, and are adequately controlled. The controls built into the application, should provide a reasonable assurance about the data processing that is valid, accurate, reliable, timely, and secure.

IT application or program controls are fully-automated (i.e., performed automatically by the systems) designed to ensure the complete and accurate processing of data, from input through output. These controls vary based on the business purpose of the specific application. These controls may also help ensure the privacy and security of data transmitted between applications.

Application software is the software that processes business transactions. The application software could be a payroll system, a retail banking system, an inventory system, billing system or, possibly, an integrated ERP (enterprise resource planning) system. It is the application software that understands data with reference to their business context. The rules pertaining to the business processes are implemented in the application software.

Most users interact with the computer systems only through the application software. The application software enables and also limits the actions that a user can do.

It is very important to subject application software to a thorough audit because the business processes and transactions involving money, material and services flow through the application software package.

5.2.2 Risks

Application level risks at the system and data level include such things as:

- System availability risks relating to the lack of system operational capability

- System security risks relating to unauthorized access to systems and/or data
- System integrity risks relating to the incomplete, inaccurate, untimely, or unauthorized processing of data
- System maintainability risks relating to the inability to update the system when required in a manner that continues to provide for system availability, security, and integrity
- Data risks relating to its completeness, integrity, confidentiality, privacy and accuracy

5.2.3 IT Application Controls

IT application controls include input control, data validation and edit controls, processing controls, output controls and data file controls, as below.

5.2.3.1 Input controls

These are controls that ensure all data from sources is fed into the application system correctly and completely. Some control examples are as below.

a) **Logging all Transactions –** All transactions are logged and the same are reconciled to source documents for accuracy.

b) **Log of Transmission** –All relevant transmissions are logged to enable review.

c) **Documentation** – Written procedures for handling different situations are made available for ensuring error-free inputs.

d) **Marking Source Document** –The source document is marked, as it is processed, to avoid duplicate entry.

5.2.3.2 Data Validation Edit Controls

These are controls that ensure correct data from sources is fed into the application system. Some control examples are as below.

a) **Sequence/Serial Number Check:** Out of sequence or duplicate numbers are rejected

b) **Limit Checks:** Predetermined limits on the data fields are checked

c) **Range Checks:** Values in the data fields is checked to be between two limits

d) **Validity Check:** Verification of the data field is performed, either through software or manually, to verify that no errors are present and/or that it adheres to a standard e.g. Sex Code can only be M or F

e) **Reasonableness check:** Values in the data field should conform to specified criteria e.g. Salary can't be 1 million dollars

f) **Table Check/Lookup:** A table check constraint specifies a search condition that is enforced for each row of the **table** on which the **table check** constraint is defined e.g. Zip code is checked against the table for validity

g) **Key Check/Verification:** Same data is entered by another employee and keys verify whether the data entered previously was correct

h) **Completeness Check:** The data field is checked for completeness of data e.g. Check for a Null value in the primary field or check for minimum characters required for a password

i) **Duplicate Checks:** The primary field should be unique and should not have any duplicates e.g. No duplicate in fields such as cheque number and invoice number

j) **Logical Checks:** A relationship logic check is done between two fields which are related by a logic e.g. Date of marriage should be at least 18 years after date of birth

k) **Check Digits:** A check digit is a form of redundancy check used for error detection. It typically consists of a single digit computed from the other digits in the message.e.g. Normally in a bank account number the last digit is the check digit.

5.2.3.3 Processing Controls

These are controls that ensure correct processing of all data input into the application system. Some control examples are as below.

a) **Manual Recalculations:** Recalculations are done manually on sample transactions and the results are compared with actual outputs.

b) **Run-to-run totals:** Batch totals of input data and processed data are compared to each other.

c) **Reasonable checks of calculated amounts:** A predetermined reasonable logic check is done on the data in the given field e.g. Salary can't be more than +/- 20% of the last month's value.

d) **Limit checks:** A predetermined check is done on the data field which will not accept any data which is outside given limits e.g. the number of months in the year must be between 1 and 12 only.

5.2.3.4 Output Controls

These are controls that ensure correct and controlled outputs from the application system. Some control examples are as below.

1. **Logging of sensitive information**

   In this control, the sensitive output is logged and traced, until it is filed properly or shredded and reconciliation of logs at regular interval is carried out

2. **Critical Forms Generation**

   Critical forms, such as pre-printed cheques, are logged, stored safely and controlled

3. **Report Distribution**

   Report distribution is only to authorized persons and it is delivered as per the schedule only

4. Retention Period

Reports are retained as per the organizational policy and destroyed, as required under the policy

5. Error Handling in Reports

Error reports should be promptly delivered to the dept. concerned. They should be subsequently reviewed and corrective actions taken.

6. Receipt Report Verification

Sensitive reports should be signed for on delivery and receipts should be kept on record

5.2.3.5 Data File Controls

These are controls on the data files in the application system. Some control examples are as below.

1. Prior and Later Image Reporting

This control is also known as before-and-after image reporting. In this control, the snapshot of data before and after any transactions is taken.

2. Error Reporting Follow-up and Handling

All of the error reports should be followed up properly and the error correction should be reviewed by a person other than the one who initiated the process

3. Media Labeling (Internal/External)

External Labeling is done to ensure proper media are used. Internal labeling, like tape headers, is done to reconfirm if the media used is correct

4. Source Documentation Preservation and Retention

Preservation and Retention of source documentation is required for verification, troubleshooting and restructuring

of the data. So Source documentation is maintained as per the policy of the organization

5. One-for-One Checking

Every source document must agree with the computer-processed document

6. Security of Data File

Unauthorized people should not have access to data files and access should be as per the authorization level

7. Preprinted/Pre-recorded Inputs

Certain information, e.g. company's name and branch name, should be preprinted

Additional application control components include both preventive and detective. Although both control types operate within an application based on programmed or configurable system logic, preventive controls perform as the name implies — that is, they prevent an error from occurring within an application. An example of a preventive control is an input data validation routine. The routine checks are to make sure that the data entered is consistent with the associated program logic and only allows correct data to be saved. Otherwise, incorrect or invalid data is rejected at the time of data entry.

Detective controls also perform as the name implies — that is, they detect errors based on predefined program logic. An example of a detective control is one that discovers a favourable or unfavourable variation between a vendor invoice price and the purchase order price.

Application controls, particularly those that are detective in nature, are also used to support manual controls used in the environment. Most notably, the data or results of a detective control can be used to support a monitoring control. For instance, the detective control described in the previous paragraph can note any purchase price variances by using a program to list these exceptions on a report. Management's review of these exceptions can then be considered a monitoring control.

5.2.4 Auditing Software Acquisition Control

Software Acquisition Control Audit should typically cover the following areas:

- Adherence to business rules in the flow and accuracy in processing
- Validations of various data inputs
- Logical access control and authorization
- Exception handling and logging

Adherence to business rules in the flow and accuracy in processing is checked by the typical two checks given below.

1. **Test Data/ Test Check**

   It is used for a given specific program. In this check, a dummy/simulated transaction is run through the real program. This type of check does not require many resources but it might not check all transactions and permanent files, master file or history file etc. cannot be checked.

2. **Base Case System Evaluations**

   This check uses Data-sets (developed as Base Case) which typically come as part of the testing program. It can be used for periodic validations to ensure that the system is functioning as expected.

The steps to be performed in carrying out a typical Software Acquisition review are as below:

- Study and review of documentation relating to the application. Many times, the Information System Auditor may find situations where documentation is not available or is not updated. In such cases, the auditor should obtain technical information about the design and architecture of the system through other means.

- Study key functions of the software at work by observing and interacting with the operating personnel during work. This gives an opportunity to see how processes actually flow and also observe associated manual activities that could act as complementary controls.

- Run through the various menus, features and options to identify processes and options for conformance to business rules and practices. (Studying the documentation before this can significantly hasten the activity.) To illustrate with an example, it is a well accepted rule in financial accounting that once an accounting transaction has been keyed in and confirmed on the system to update the ledgers, it should not be edited or modified. The correct method would be to pass a fresh reversal transaction to correct errors, if any. However, if the Information System Auditor observes that there is an option in the software to "edit/modify transactions," this would be noted as a control deficiency for correction.
  This kind of run-through can be done more effectively if a development/test system is made available to the Information System Auditor. In the absence of such a facility, the auditor only can watch the system run by the system administrator and make notes. The auditor is advised not to do any testing on a production system as this could affect adversely a "live" system.

- Validate every input to the system against the applicable criteria. Such validations go a long way in eliminating errors and ensuring data integrity. Apart from simple validations for numeric, character and data fields, all inputs should be validated with range checks, permissible values, etc. Validation checks that are built on application-specific logic can act as powerful controls not only for ensuring data accuracy but also to prevent undesirable data manipulations. The Information System Auditor can check validations by actually testing them out in the development/test system. Alternatively, looking at the database definitions, the associated triggers and stored procedures would be the way for a technically savvy Information System Auditor to review the validations.

- Verify access control in application software. This consists of two aspects--the inherent design of the access control module and the nature of access granted to various users and its maintenance. Every application software has a number of modules/options/menus that cater to the different functionality provided by the software. Different users will need access to various features based on their responsibilities and job descriptions. All access should be strictly based on 'the need to know and do principle'. The design of the access control module may be of varied types. Most software would check a combination of user id and passwords before allowing access. Access may be controlled for each module, menu option, each screen or controlled through objects. Often the matrix of users versus the options/actions becomes too large and complex to maintain hence it is normal to define certain roles for different classes of employees and group them together and assign them similar access. The Information System Auditor should review the design of the access control module keeping in mind the criticality of the functions/actions possible in the software and evaluate whether the design provides the level of control and granularity to selectively and strictly allows access as per the job requirements of all the users. Having done this, the auditor should proceed to verify whether all existing users have appropriate access as evidenced by their job descriptions and whether access to certain critical activities are allowed only to select personnel duly authorized. It also is necessary to verify who has administrator/super user rights and how such rights are used / controlled. Ideally no one in the IT/development group should have any access to the production data. All actions on the data by the super user should be logged and verified by the data owners regularly.

- Verification of how errors and exceptions are handled. In many activities software provides options and ways to reverse transactions, correct errors, allow transactions under special circumstances, etc. Each one of these is special to the business and based on the rules and procedures defined by the organization for these. The Information System Auditor needs to see how the software handles these. Are

these circumstances properly authorized in the software? Does it capture the user id and time stamp for all transactions to provide suitable trails? Are the exceptions and critical activities like updates to global parameters logged for independent review later?

- Correction of any weaknesses found at the end of an applications review in the software that could lead to errors or compromises in security. These would need to be corrected by either changes in design and/or some recoding. While this would be addressed by the IT department, the user or owner of the application from the functional area would want to know if any of these weaknesses have been exploited by anyone and whether there have been any losses. To provide an answer to this question, the Information System Auditor should download all the data for the period in question and run a series of comprehensive tests using an audit software and determine if any error or fraud really occurred .

- Evaluation of the environment under which the application runs. The audit of the application software alone is not enough. Generally, it is prudent to conduct a security review of the operating system and the database in which the application runs while doing an application review.

Transactional and support applications require control reviews from time to time based on their significance to the overall control environment. The frequency, scope, and depth of these reviews should vary based on the application's type and impact on financial reporting, regulatory compliance, or operational requirements, and the organization's reliance on the controls within the application for risk management purposes.

5.2.5 Application System Documentation

Ideally the following documentation should be available with the application software.

1. Feasibility study document

2. System Development Methodology Document

a. Overall methodology

b. User requirements

3. Functional Design Detail and Specification Document

   a. Explains the application in detail

   b. Key control of the applications

4. Program changes document

   a. Change or modification to program

   b. Authorization of changes

5. User manual

   a. Helps to understand the system from the user's perspective

   b. Weaknesses in the program can usually be noted from this document

6. Technical Reference

Vendor-supplied manual/s are necessary for in-depth understanding and troubleshooting

5.2.6 Application Controls Audit Checklist References

Please refer to serial no. 8.4 of audit check list no. 8 – Information System Acquisition, Development and Maintenance, given in Annexure 1

5.3 Network Security Audit

5.3.1 Overview

Today's business systems need to exchange data with each other. Systems need to be integrated and must establish fast and reliable communication that is as widespread as the organization and its business dealings. Information systems need to reach out to

users, vendors, customers and partners (irrespective of their location).

In the early days of networking, computer networks involved the connection of several computers into one single network. In today's environment networking encompasses networks of networks encompassing hundreds or even thousands of individual workstations. Today every computer in the world is, connected to every other computer through the Internet. Such connectivity has the propensity to provide access or communication paths for anyone to any system in the absence of any measures to prevent such access. But we are trying to separate the individual computers and systems with the help of standards and technical solutions.

The influence of networking technologies on information systems (IS) and its auditing is being felt increasingly which in turn is influencing the nature of information systems in the modern organizations. This is truer in respect to the e-commerce.

A network can be very simple as a small local area network (LAN) connecting a few computers inside a single room or a building, or it could be a complex one that connects computers at factories and offices spread over a number of cities or even countries. A network is also connected with other networks, such as the networks of customers or vendors or a public network like the Internet.

The focus of this chapter has been to sketch a basic approach to network security audit, and not to provide specific audit and technical guidelines. Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become ``wired'', an ISO Auditor need to understand the basics of networking in today's world. It is not possible to give all the information and details of networking world in one chapter. However, books and searches on the Internet can provide checklists pertaining to evaluating the configurations of most commonly used devices and security products.

5.3.2 Network Audit Objectives

The primary objectives of the Network Audit are to determine whether:

- the networks and associated component are configured, tested and reliable prior to being placed into production;
- the network's resources are appropriately monitored;
- Adequate controls are in place to ensure the security and recoverability of the networks.

5.3.3 Network Vulnerabilities

The basic vulnerabilities associated with a network can be grouped into three broad categories:

5.3.3.1 Interception

The data that are transmitted over the network pass through some medium that consists of a carrier and other equipment, often in the physical control of other third parties. These data could be intercepted. Once intercepted, there is a risk of undesirable disclosure, i.e., someone stealing data or modifying the intercepted data, resulting in loss of integrity and consequent other, more material losses.

5.3.3.2 Availability

As networks proliferate, more and more users are remote and access their applications over the network, crossing hundreds or thousands of miles. If network connectivity fails or becomes unavailable for any reason, there would be a serious interruption to business and consequent damages.

5.3.3.3 Access/Entry Points

The network takes a computer system beyond the box into the world. The network makes the system available to users across geographical boundaries, resulting in a lot of conveniences and efficiencies. At the same time, the same network provides the feasibility for access to the system from anywhere. A single

vulnerability in the network can make all the information assets in the network vulnerable to intruders. The network provides many points of entry for intruders, interceptors and malicious code-like viruses, worms and Trojan horses. Considering that a major benefit of a network is its ability to provide access from anywhere in the universe, it becomes very difficult to devise controls around this access.

5.3.4 Controls

Following are the typical controls available to manage the risks.

5.3.4.1 Physical Access Controls

For compromising the network, especially on the dedicated, proprietary networks, physical access to the equipment and/or the cabling is required. Good physical access controls at data centres and offices, and physical security over telecommunication equipment can limit the interception through sniffing. The Information System Auditor should evaluate physical security, including all the points where the communication links terminate and where the network wiring and distributions points are located. However, there are limitations to the effectiveness of such controls, especially with increasing wireless communication.

The most effective control to interception is encryption. When data are encrypted, even if they are intercepted, disclosure or modification cannot occur unless the scrambled data can be decrypted. Today, there exist many methods of encryption and many combinations of its use. Encryption can be done either by the application or at the communication level by a device such as a router, switch or a multiplexer. A virtual private network (VPN) is an example of the usage of encryption to tunnel data securely over a public or shared network. The use of digital certificates and digital signatures is another example.

5.3.4.2 Network Monitoring

The control to ensure availability and reliability of a network is through good network architecture and monitoring. The design of the network should ensure that between every resource and an access point there are redundant paths and automatic routing to

switch the traffic to the available path without loss of data or time. Every component in the network needs to be fault-tolerant or built with suitable redundancies. Complex and widespread networks need to be monitored and managed. This is often done by using network management software. The establishment of a network operations centre (NOC) with software tools and a service desk often staffed 24/7 provides this capability. Such tools provide data for capacity management. They also ensure that the networks provide adequate bandwidth to enable the data to move along without bottlenecks and with the speed required by the users and applications. The Information System Audit review should cover all these aspects.

5.3.4.3 Access/ Entry Points

Most controls in a network are built at the points where the network connects with an external network. These controls seek to limit the type of traffic that can come in or go out and also the origin and destination of the traffic. For example, to provide access to a web server that is inside the network to customers all over the world for placing orders, the network should accept only a certain type of traffic (HTTP) and not the kind of traffic that tries to log into the server (telnet). In another situation where a partner or vendor provides, for example, system development or maintenance services over a dedicated network from a fixed location, the network may allow traffic only from those systems with specific addresses. Such controls are implemented through suitable configuration of the rule base in a firewall and/or through access control lists in the routers. Antivirus software and intrusion detection systems can detect viruses and other malicious code at these entry points and take detective and corrective action. In addition to being at the gateways, the strategic positioning of such control devices/software and tools at critical hosts and segments of the network can enhance security further based on requirements determined by the risk assessment. The operating systems of the servers where critical resources are hosted need to be hardened and the access controls in applications also need to be controlled and maintained securely.

5.3.5 Auditing Network Security

The Information System Auditor needs to study and understand the network under review. This can be done in the following steps.

- Review network diagrams (LAN, WAN, MAN etc.) to understand the network infrastructure. This should include the gateways, firewalls, routers, switches, hubs, servers, modems etc.
    - The network diagram is a diagram that shows all the cabling and equipment available on the network. The auditor should, if required and possible, verify physically the correctness and the accuracy of the diagram. Large networks evolve and change constantly with changing business needs and a diagram that is not updated is useless.
    - The Information System Auditor should ascertain what processes exist in the organization to update and maintain the network diagram accurately.
    - The use of a software tool to generate this diagram ensures some degree of accuracy.
    - In any network, there will be locations where there is a concentration of resources, such as a Data Centre where ERP servers, mail servers, etc., are hosted and many points such as manufacturing plants, sales offices etc., from which these resources are accessed. While smaller networks may have only one such location, complex networks may have many hosting points where critical resources are located.
    - The network diagram could also provide input on the type of devices and protocols used on the network.
    - The network diagram and its details provide the most important input for the audit, and the auditor should keep referring to it throughout the audit.
- Review physical and logical access controls

- Protection to network assets should be related to the risks associated with the assets as determined by a systematic risk assessment. The auditor needs to have a good idea of the critical assets, systems and services that need to be secured. Typically, one would want to protect enterprise systems including ERPs, mail servers and other internal applications, web servers that host applications that are accessed by customers and vendors, and the network and its components. In this context, the security and access mechanisms surrounding the applications and the servers (the OS and database) also need to be robust.

- Threats from inside are as serious as the ones from outside. The auditor needs to evaluate whether both are adequately handled. To secure systems from internal threats, all host based security such as application and OS-level security needs to be evaluated.

- The next step is to determine the persons who have access to the systems on the network and how. Are only employees accessing the system? Can customers and vendors also access the systems? Do they have access to the system from outside the office? Do customers access the system via the Internet or do they perform remote logins to the enterprise systems? All these factors have a significant impact on security.

- Study the network design, strategies, segmentations of routers and switches and WAN for configuration and protocols

  - At a minimum level, every network today is connected to the Internet through an Internet service provider. The primary reason for connecting to the Internet is to enable receipt and dispatch of mail and to enable browsing by employees. Enterprises may also have other reasons to connect to the Internet, such as e-commerce web sites through which the company's vendors, customers and partners collaborate, place

orders or exchange other information. Dedicated connections to the networks of other partners may also exist. The gateways through which each of these connections is made are potential entry points for the external world.

- The auditor at this point should identify the demarcation between the internal network and the external network. Based on step 2, the Information System Auditor may already know which systems are accessed only by internal users, which are accessed from the external world or the Internet and which are accessed only by the external users. Such categorization would also help an auditor conclude the effectiveness of the design of the demilitarized zone and the positioning of security products like firewalls and intrusion detection systems. A major effort would be to separate the internal network from the external world at the gateways.

- The first step is looking at the gateways as the potential points through which entry can be gained by the unauthorized or malicious code. The controls are implemented through well designed and secure network architecture, choice of protocols and encryption mechanisms, choice and configuration of network devices such as routers, and additional defences including firewalls, antivirus and intrusion detection systems. Evaluating every one of these requires a specialist knowledge, and the auditor would do well to ensure that the audit team evaluating network security consists of experts who have the specific knowledge of the protocols, the network devices and the software deployed at the network.

- Study the applicable policies, standards, procedures and guidance on network

  - It is necessary for the Information System Auditor to evaluate the processes associated with the management of all these security components. Configurations need to be maintained through suitable

change management procedures, logs need to be scrutinized and acted upon, incidents have to be managed and learning and preventive action documented. Good security does not come from mere investments in complex and expensive tools and software alone. It requires a capable Information System Auditor to review the systematic management of the security tools through well-defined processes.

- Study the network organization, personnel involved and their duties and responsibilities

Security products are constantly evolving. Many are developing multiple capabilities and morphing into hybrid products that provide fire walling, antivirus and intrusion detection and correction all in one. Once the Information System Auditor is clear about the need, role and limitations of each of these, the specific knowledge about them can be acquired or hired.

5.3.6 Mobile Computing and Wireless Networks

Mobile and wireless computing are becoming very important in worldwide business operations. Mobile and wireless computing refer to the use of wireless communication technologies and portable computing devices to access network-based applications and information from a wide range of computing devices. The increasing use of this technology and the proliferation of new portable devices with Internet access expand the frontiers of an organisation and the Information System Auditor now needs to understand this technology to identify the associated risks.

The term wireless computing means the ability of computing devices to communicate in a form to start a local area network without cabling infrastructure (wireless). This involves the usage of technologies converging around IEEE 802.11x and other wireless standards and radio band services.

With the advent of wireless technology for transmitting data and voice, the well-known and relied upon controls instituted using parameter devices are disappearing. Controls like the physical security controls, such as security guards, cameras and locks that

were effective in protecting wired networks and data transmissions are not very relevant.

The risks and threats associated with attacks against wireless networks are widespread including:

- Attacks where message traffic is captured and analysed and encryption keys cracked,
- Resource theft, where Internet access is obtained that in return is used as a launch pad for other attacks, i.e., cyclical redundancy check
- Denial-of-service due to signal interference and the propagation of threat from viruses and worms

The term mobile computing enables this concept to devices that enable new powerful applications and expand an enterprise network to reach places in circumstances that were not possible by other means. It is comprised of cellular phones, laptops and other mobile and mobile-enabled technologies.

Mobile devices have now computing and storage capability and they can be used to store, process and access applications and data. They are semi-independent devices that process data in an independent form and periodically connect to a central system or a network to exchange data or applications with other systems, or they can be used as client nodes that access and/or update data stored in another remote system on a real-time basis (they may act as peers as well as in a hierarchy).

- Together with the mobile computing devices, the following points of security vulnerability exist: the mobile device, the wireless channel, and the network connection between the wireless web servers and the back-end transaction servers.
- Hand held devices and wireless local area networks (WLAN) are more vulnerable to potential viruses and the ability for wireless signals to be picked up by third parties.
- So to overcome these vulnerabilities, stricter security policies, WLAN security standards, the use of encryption

technology, and end-to- end security solutions are very necessary.

5.3.7 Network Audit Approach

- Information about the likely use of mobile devices, identifying where they are used for business transaction and data processing and/or for personal productivity purposes (i.e., Internet browsing, mail, calendar, address book, to-do list) and about hardware and software technologies used should be gained by the Information System Auditor.

- Sufficient information about the risk analysis, along with the likelihood of occurrence and probable impact of the event, performed by the entity to evaluate the impacts of its mobile computing environment should be gained by the Information System Auditor. .

- The Information System Auditor should get information about the policies and procedures used to manage mobile computing, involving deployment, operation and maintenance of aspects, such as communications, hardware, application software, data security, systems software and security software. Typical examples of the areas to cover are device configuration, physical control, approved software and tools, application security, network security, contingency plans, backup and recovery.

- Personal interviews, documentation analysis (such as business case and protocols documentation) and wireless infrastructure testing should be used appropriately in gathering, analysing and interpreting the data.

- Where third-party organisations are used to outsource IS or business functions, the Information System Auditor should review the terms of the agreement, evaluating the appropriateness of the security measures they enforce and the right of the organisation to periodically review the environment of the third party involved in the service it provides.

- The Information System Auditor should also review previous examination reports and consider their results in the planning process

5.3.8 Network Audit Checklist Reference

Refer to the Checklist No 5 - Operations and Incident Management Checklist for network audit and Mobile Computing Audit

5.4 DATA MIGRATION AUDIT

5.4.1 Overview

According to the Wikipedia, data migration is "the transferring of data between storage types, formats or computer systems… it is required when organizations or individuals change computer systems or upgrade to new systems."

For IS Practitioners, data migration is a very challenging, but often neglected area in IS operations. Information is a very important asset of any organization which is extracted from data. But in practice, data migration is, most of the times a function associated with applications. In fact, data migration is always a part of some bigger application project. Perhaps, because of this the data migration gets neglected, resulting in the deadline for actual go-live date for new applications also getting delayed.

- Data migration could be also required on a regular basis due to changes in Server and storage consolidation, Technology upgrades etc.
- Data migration is one of biggest challenges in IS Operations.
- The data migration project is used for enhancing and cleansing the legacy data. So the data available from the legacy systems needs to be enhanced and properly cleaned, before it can be used in the modern powerful systems.
- Businesses need data for running their business and any interruptions are not tolerated and it affects the operations. So the data should be converted, cleansed and made

available in the new application or location in the shortest possible time and with great accuracy.

- Business, technical and operational requirements put difficult and challenging conditions on the migration process.
- Resource demands like staff, processing power, bandwidth and risks like application downtime, performance impact to production environments, technical incompatibilities, and data corruption/loss make data conversion process very challenging.

5.4.2 Data Migration Risks

Following are the Risks in the Data Migration activities

- Data corruption
- Data loss
- Application downtime
- Performance degradation
- Technical incompatibilities

5.4.3 Audit Process

Because of the above constraints and the importance of data for running businesses, the data conversion strategy and planning should be time-bound and foolproof. There is very little scope for making mistakes in this project. Auditors should be associated with the data migration process from the initial planning stage itself, till the completion of the project.

Depending on the size, complexity and time frame of the Data Migration project, the audit plan also should be finalized during the strategy stage itself. Reporting of audit results should be more frequent and flexible. For example, if the auditors feel it is important to communicate concerns, they can do so throughout the project; otherwise, they will normally produce written pre-implementation and post-implementation audit reports, which will not add any value to the organization. By being involved early in

the Data Migration Project, auditors can informally raise questions and suggestions that influence a project without actually making formal audit recommendations. Conversion audits should be done in lockstep with the project planning and frequent and timely reporting of the findings. Being involved early in the project initiative is vital to developing a good understanding of the project's issues, challenges, and risks, as well as what management is doing to address them.

5.4.3.1 Understanding the data migration requirements

Information System Auditors should study the application and its criticality for business with all the stakeholders. They should review with both the project's IT team and the business units the scope of the initiative, supporting project plans, high-level implementation plans and schedules, and proposed implementation programs and project controls.

The objective of this step, also is to identify the business and operational requirements that impact the migration process.

- IT staff defines available network bandwidth and CPU cycle load, allowable downtime, and migration schedule
- Database and system administrators define application and database requirements in terms of the content, structure etc.
- Business owners define the requirements and importance of, specific applications and types of data i.e. whether numeric or characters etc.
- Security and compliance groups define security i.e. data should not get stolen or misplaced while in transit and compliance requirements i.e. certain fields need to be retained for compliance purposes and so a secure back-up of the source data should be kept in a secure place.

Simultaneously, auditors should also finalize the data migration audit plan by modifying the generic audit process to reflect the actual IT project's objectives, issues, and assurance needs. The high-level risk assessment would further guide the data migration audit-planning process.

Information System Auditor should complete an assessment of the project plans, implementation and testing plans, and the planned data-conversion program specifications. Auditors should provide feedback about their assessment of the implementation approach to the project's management team. The project team and management are under intense pressure of schedules that show early progress and they may overlook many aspects. So they will benefit from receiving an independent assessment of the project efforts and plans from the Information System Auditors. Having Information System Auditors review the early project efforts further assures stakeholders that all important aspects of the project have been considered in planning.

Information System Auditors should study the number of tiers and sources for the source data and the destination.

- Single-tier migration is a migration in which all source data is migrated onto one or more devices within a single tier, which is also the primary storage. Within a single-tier migration, the storage vendor could be same or different.

- Data layout:

    - One-to-one mapping: source and destination have the same storage layout

    - Relay-out: source and destination (one or both of which can be one or more devices) have different storage layouts

- Multi-tier migration is a migration in which the data is migrated to different tiers of the hierarchy based on a best fit between data/application requirements and storage tier attributes. There are two types of multi-tier migration:

- One-time migration: data placement recommendations, based on the results of an analysis of the data and the storage tiers in the hierarchy are provided

- Continuous and policy-driven migration: this is a continuous process (requiring the installation of an archival application) that uses a set of user-defined policies to determine, in real

time, when data needs to be moved where all migrations fall into one of the above migration environments.

Understanding the overall solution is extremely important for adding value to the data migration project. It is also important that the project teams develop well-documented objectives and plans for the data migration. The same should be discussed and approved by management.

5.4.3.2 Data mapping strategy and plans review

Data mapping is the process of creating data element mappings between two distinct data models. Data mapping is used as a first step for data transformation or data mediation between a data source and a destination

The necessary foundation for maintaining the integrity of the production data during implementation is set up in this step. Information System Auditor should assess the adequacy and completeness of the planned data conversion control reporting. A review of the system data mapping for the implementation of changes to production data should be done. In addition, the historical requirements for data, if any, should be considered. For example, companies must be able to store and provide access to historical data for 8 years to meet requirements of Income Tax Act, 1961.

The data mapping plan components should include, but are not limited to:

- Migration strategy and key activities
- Data sources and destinations
- Dependencies
- Required equipment and migration tools e.g. Excel, Oracle Migration Tool etc.
- Customer expectations (customer business, technical and operational requirements)
- Test plan

- Verification procedures
- Risks and contingency plans
- Change control procedures
- Project schedule
- Post-implementation activities/responsibilities
- Migration completion criteria

During this step, Information System Auditors assess the adequacy and completeness of data mapping for implementing production data. It is done by reviewing the systems data mapping itself and the controls and reporting with regard to this activity. Special attention is also given to the impact the data conversion has on other systems that are not involved in the conversion. This is a high-risk area in all conversions, because downstream systems may be affected in unexpected ways e.g. implementation of an access control system may affect the pay-roll system in an organization.

5.4.3.3 Planned operational changes review

The migration plan, is the end deliverable of the planning step and serves as the blueprint for the migration implementation, specifying customer expectations, defining project deliverables, and identifying migration methodologies to be used.

There are four major inputs into the migration plan:

- Business and operational requirements, which provide the constraints
- Data to be migrated, with all associated attributes
- Available migration tools
- Storage and application best practices

A workable migration plan is a very important document. Different types of data require different migration tools and strategies, and

business and operational requirements like the downtime window which may require creative ways of moving the data.

Information System Auditors should have a detailed understanding of the operational changes that should be planned and facilitate an independent risk assessment of those changes. Without an ongoing risk assessment process, surprises will occur frequently, with negative consequences to schedule, cost, and quality. Ideally, the results of the audit analysis should be factored into the project team's plans and focus. The audit risk assessment should be documented in a high-level document for management's approval.

5.4.3.4 Implementation readiness review

At this stage, Information System Auditors should assess the adequacy of the testing plans, the data-conversion control reports to be used, and test scripts involved with the implementation. Auditors should ensure that appropriate project resources have been assigned to this activity, so that the level of testing efforts reflects the risks involved. Auditors should review the assignment of responsibilities and related agreements between stakeholders for completeness and appropriateness. Auditors should also review the project's outputs regarding business and IT processes required for implementation. Finally, review and feedback on the implementation plans should be provided to the project management team, and top management, where appropriate.

Internal auditors should complete a high-level readiness assessment of the organization's ability to implement the required operational and system changes. This analysis will identify whether or not additional management efforts are required to complete the preparation for the actual conversion. Auditors should review the documentation being developed to support the solution's implementation and operation — user training materials, new and refined policies and procedures, internal and external communication, and other key project outputs — as determined in the previous steps.

The data conversion readiness assessment should be documented in an audit report. An audit report should also be provided to management before the solution's implementation. Auditors should also attend key project management checkpoint

meetings and provide their views verbally as part of the audit feedback to project management.

5.4.3.5 Pre-migration Sample Test

Before any data is moved, it is important that a sample of the migration plan, with the scope depending on the specific situation and the agreement with the customer, be tested and validated. Results of the migration test determine whether modification of the migration plan for example, timeline, migration tools used, amount of data migrated per session, and so on is required. For example, if testing shows that allowable downtime would probably be exceeded, the migration methodology needs to be reviewed.

The following must also be validated in a non-production pre-migration testing-

- Network access
- File permissions
- Directory structure
- Database/applications

Once the data has been moved, all clients should also be checked by redirecting them to the destination devices.

The lessons learned during the pre-migration tests are useful in the final migration of data.

5.4.3.6 Data Conversion Verification

At implementation, management and the board expect, Information System Auditors to provide additional assurance that the implementation is executed prudently and successfully. The audit tests will focus on reviewing the results of the project team's and business unit's test results. This includes reviewing the results of the startup at the first site and monitoring the rollout at the other sites if the conversion is a multi-site implementation. A review of the testing of the initial production operations using the new solution should also be completed.

5.4.3.7 Overall audit analysis of the implementation

Information System Auditors should complete the audit analysis of the results of the implementation and the management actions that have been completed to address any issues observed during the actual implementation. For major conversions with many implementation activities, some operational issues need to be addressed during implementation that could not be considered ahead of time. For example, an obscure data conversion problem may occur for a minor data element, requiring manual corrections to be instituted to allow the implementation to go forward. Management review of this manual effort following implementation might be recommended to ensure nothing significant was missed.

Decommissioning the old system is another challenge for the management, so appropriate efforts should be taken in this area, as well. A post-implementation audit report on the adequacy and accuracy of the implementation should be prepared and presented to management.

5.4.4 Data Migration Audit Checklist Reference

Refer to the Annexure i checklist No.9 for Data Migration Audit

5.5 Business Continuity Management Audit (BCM)

5.5.1 Overview

Business Continuity Management (BCM) refers to the activities required to keep your organization running, even during a period of interruption of normal operations. BCP (Business Continuity Plan) and DRP (Disaster Recovery Plan) are the two integral parts of BCM process.

According to Business Continuity Institute's Glossary, "Business Continuity Plan" (BCP) is a collection of procedures and information which is developed, compiled and maintained in readiness for use in the event of an emergency or disaster.

"Disaster Recovery Plan" (DRP) is a document which guides an organization for the process of rebuilding an operation or infrastructure after the disaster has occurred.

Disaster and / or business interruption might occur anytime, so the organization must be prepared for the same. The organization should design a plan to minimize the impact of the same. With the emergence of e-business, many businesses are operating 24 hours per day and 7 days a week. A single downtime of few hours might be disastrous to their business. Therefore the traditional DRP / BCP, which focuses on restoring the centralized data center, might not be sufficient. A more comprehensive and rigorous BCM is needed to achieve a state of business continuity to make critical systems and networks continuously available.

The organization needs BCM to prevent the major incidents, to reduce/minimize the impact of disaster and to resume business operations at the earliest, when there is a disruption to business. BCM may prevent and/or minimize the impact of events – like the following:

- Natural disasters (like Flood, Earthquake, Hurricanes)
- Social unrest or terrorist attacks.
- Fire
- Disruption of power supply or telecommunication services
- Damage/Theft of IS asset
- Human error, sabotage or labor unrest
- Equipment failure
- Application failure or corruption of database
- Malicious Software (Viruses, Worms, Trojan horses) attack, Hacking or other Internet attacks
- Non-availability of people and services

With the shift of IT structure from centralized processing to distributed computing and client / server technology, the organization's data is now located across the enterprise. Therefore it is no longer sufficient to rely on IS department alone in Business Continuity Planning, all executives, managers and employees must participate. Business Continuity Coordinator or Disaster Recovery Coordinator will be responsible for maintaining Business Continuity Plan. However his or her job is not updating the Plan himself or herself alone. His or Her job is to carry out review periodically by distributing relevant parts of the Plan to the owner of the documents and ensure that the documents are updated.

Organization should involve employees from all levels and functions / departments in BCM at appropriate stages.

5.5.2 BCM Activities

BCM involves activities like preparation of policy and procedure document, risk assessment, business impact analysis, development, implementation and maintenance of BCP (Business Continuity Plan) / DRP (Disaster Recovery Plan).

5.5.2.1 Policy and procedure

BCM policy document provides the framework around which BCM capabilities are designed and built. BCM procedure document provides the detailed steps/activities to be carried out. Top management is primarily responsible for establishing a BCP policy and procedure in the organization. Consideration to following factors typically must be given while setting out BCM policy and procedure.

- Present business environment and business processes
- Business strategies
- Current processes and the future growth of business
- Relevant industry standards and best practices
- Legal requirements
- Health and Safety regulations

Policy and procedure documents are prepared based on the analysis of above factors. Following activities are typically included in the policy and procedure documents

- Define the scope and objective of BCM
- Identification of threats and vulnerabilities
- Evaluation of risks and business impact analysis
- Formulation of risk mitigation strategy
- Identification of teams for BCM
- Assigning tasks to teams
- Training to teams
- Test drills
- Review and Maintenance of BCM

BCM policy and procedure should be in line with business strategies. BCM policy and procedure documents must be approved by Top Management. Regular review and update to BCM policy and procedures should be conducted.

5.5.2.2 Risk assessment

Risk Assessment process involves typically the following activities

- Identification of potential threats and/or vulnerabilities to the organization
- Assessment of Probability for occurrence of such threats and/or vulnerabilities
- Assessing the critical functions necessary for organization to continue business operations
- Selection of methodology for risk evaluation
- Organisation may chose from the many computerized and non-computerized risk assessment methodologies that are

available. These methodologies range from those that classify risks as high, medium and low to those that involve complex and apparently scientific calculations to provide a numeric risk rating. While selecting the methodology to be used, the organisation should consider the level of complexity. The organisation may use subjective judgments in all risk assessment methodologies. These judgments should be validated to an appropriate level of accuracy.

While deciding the most appropriate risk assessment methodology to use, organisation typically considers the following:

- The type of information required to be collected
- The cost of software or other licenses required to use the methodology.
- The extent to which the information required is already available.
- The amount of additional information required to be collected before reliable output can be obtained, and the cost of collecting this information (including the time required to be invested in the collection exercise).
- The opinions of other users of the methodology, and their views of how well it has assisted them in improving the efficiency and/or effectiveness of their audits.

- Estimation of the impact on the organization of the threat using a numerical scoring system (Risk = Threat Impact x Probability)
- Optionally, prioritize the risks according to a formula which includes a measure of the ability to control that threat
- Review existing controls in place
- Consider appropriate measures to:
  - Transfer the risk e.g. through insurance

- Accept the risk e.g. where impact / probability is low
- Reduce the risk e.g. through the introduction of further controls
- Avoid the risk e.g. by removing the cause or source of the threat

- Ensure that planned risk measures do not increase other risks. For example, outsourcing an activity may decrease some types of risk by increase in others.
- Documentation of risk assessment
- The organisation should document the risk assessment methodology used. This should ordinarily include:
  - A description of the risk assessment methodology used.
  - The identification of significant exposures and the corresponding risks.
  - The risks and exposures the audit is intended to address.
  - The audit evidence used to support the Information System Auditor's assessment of risk.

Top Management must approve the risk assessment. Risk assessment should be conducted, at regular intervals.

5.5.2.3 Business Impact Analysis (BIA)

Business Impact Analysis means quantification of identified risks on the continuity of business operations. Management identifies a team of experts in the business operations which identifies the impact of risks on business operations. The impact of risks on business operations is measured in the form of financial loss, damage to organization’s image and loss of goodwill etc. BIA team determines the RTO (Recovery Time Objective) to control such losses.

RTO means the timescale within which the business operations need to be restored following an interruption. Determination of RTO is based on various factors like statutory and legal obligations, contractual terms, business environment and service levels agreed with customers.

RPO (Recovery Point Objective) means the amount of data lost measured in time. Example: If the last available good copy of data upon an outage was from 18 hours ago, then the RPO would be 18 hours. Management will develop recovery strategies based on accepted RTO & RPO.

Based on BIA, business operations are prioritized and management decides to implement the controls to eliminate / minimize the business impact on critical operations. BIA should be reviewed, at regular intervals.

5.5.2.4 Development and Implementation of BCP and DRP

"BCP (Business Continuity Plan) is a collection of procedures and information which is developed, compiled and maintained in readiness for use in the event of an emergency or disaster."

Management identifies a team to develop a BCP and DRP. The development team should comprise of user(s) from managerial, technical, administrative and operational levels.

Activities followed in development and implementation of BCP and DRP are typically like identification of teams, recovery priorities, recovery sites, offsite activities, back-up, restoration, training schedule and communication. Explained in details as follows:

- Identification of teams – Management will form a Plan Development Team, which will identify and establish the following teams, as appropriate for the organization:

Steering committee: - It is a high level committee comprising of members from TOP management and is primarily responsible for BCM. The Steering Committee should include representatives from typically key areas of the organization like:

- Information Systems

- Technology Support
- Systems Development
- Network and Operations Services
- Voice Communications
- Key Business Units

Typically, several teams are identified as below for BCM

- Business continuity team – A team responsible for preparation and update of BCM policies and procedures, BCP and DRP. Also carries out activities of co-ordination between other teams
- Incident response team – It is the team which is designed to receive the information about every incident that can be considered as a threat to assets/operations. This team assists and guides other teams in the event of a disaster or major interruption.
- Evacuation team – It is the team which is responsible for a evacuation of the people and critical IT assets at a safe location.
- Recovery team – It is the team primarily responsible for recovery of IS information and assets. This team is responsible for testing of various plans developed and analyzing the results.
- Media communication team - A team which communicates the information regarding a disaster to outside organizations. This team communicates information on the disaster to insurance company, news papers agencies, new channels and other media.
- Offsite operation team – A team working at offsite location. This team is responsible for security of offsite, testing of offsite, restoration of back up and supports the continuity or operations in the event of a disaster or major interruption.

- **Recovery priorities** – Based on RTO and RPO management assigns priorities to business operation. Plan development team should identify the controls to mitigate the risks in time. A procedure to recover business operation post-disruption / interruption will be documented in plan. BCP and DRP should be documented and typically should 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
    - Evacuation points
    - Escalation procedures
    - Procedure for the resumption of business activities
    - Media communication
    - Legal and statutory requirements
    - Back up and restore procedures
    - Offsite operating procedures
- **Recovery sites**- Based on criticality of business function, recovery strategy is determined. Organisation should select a type of site with due consideration to business impact, RPO, RTO and recovery costs. BCP and DRP should include appropriate type of site organisation and justification for the same. Organisation may have more than one type of site for different IS assets. Typically the sites may be Hot

Site, Split Site, Warm Site, Cold Site, Redundant Site, Mobile Site or Reciprocal Agreements.

- Hot Site – It is a site equipped with the computer, network, software, telecommunications and environmental infrastructure required for recovering critical business operations. The only additional need to start operations from hot site is the staff, program, data files and documentation. Hot sites are expensive, difficult to set up and require constant maintenance, but in the event of a disaster operations can continue with a minimum of downtime.

- Split site – Large organisation operates from multiple locations. In the event of a disaster to one site, operations would simply shift to the other. Any needed equipment could be purchased / organised as necessary in the event of a disaster. This site eliminates the need for the major up-front costs of building a disaster center; however the capacity / speed of operations may be limited till normalcy is restored.

- Warm site – It is a site equipped with some network connection, communications interfaces, electricity supply, environmental conditioning and hardware devices like disk drives, tapes, communication equipment, environmental conditioning, but without a main computer. Warm site becomes operative after additional provisioning, of software, installation of computers or customisation is performed. Warm site can takeover the operations within a day or week.

- Cold site – It is a site equipped with environmental infrastructure. It is ready to receive the required equipment to carry out operation in the event of a disaster. Cold site becomes operative only after installing computer hardware, software, telecommunications equipment, communication lines, etc. It takes several weeks to continue business operations.

- Redundant site – It is a site fully equipped with all resources necessary for recovery of operations in case there is a disaster. It can become operative within hours post disaster.

- Mobile site – It is a trailer with specific recovery needs such as computers, workstations, telephone, electrical power, office facilities, etc. Post disaster it can be transported to a business site or alternate site for recovery of operations.

- Reciprocal agreement - It is an agreement between two or more organisations with similar equipment or applications, to provide computer time to each other in the case of a disaster. Even though, this can be a least cost option, it may not work at all if the agreed organisations face the disaster at the same time.

- **Offsite activities** – One copy of BCP and DRP plans should be available at offsite facility. This facility should have appropriate physical and logical controls and should be adequately prepared for continuation of operation, such as UPS, smoke and water detectors etc. Offsite facility should be geographically different from the main operations site. Testing of this facility should be conducted at regular intervals.

Back-up and restoration – Organization should take adequate back-up of data and documents. Data should be backed up on periodic basis. Onsite and offsite back up copies should be stored in secured places. Copies of backup taken and stored offsite should have same level of security and access control. Control over offsite library facilities is important to ensure the uninterrupted operations of the business in the event of a disaster or major interruption. Rotation of media for back-up should be defined. Restoration of backup should be carried out at regular intervals. Logs for backup and restoration should be monitored by an independent person. Adequate records for data back-up stored offsite should be maintained. Organization identifies the data / information which needed to be backed up. Organization decides upon the method in which back up to be maintained. It decides on

a schedule for backing up data. Backup schedule will consist of any of the following method. **Full backups-** This is a complete set of all of the data back up. Organization wants to keep a current backup of the entire system, a full backup need not to be taken. Full back need not to be taken on daily basis, as most of data files don't change every day and full backups are time-consuming. **Differential backups-** This is the set of any files that have changed since the last full backup. These backups take less time and space than a full backup, but more than an incremental backup. **Incremental backups-** This is the set of files that have changed since the previous backup (whether it is a differential, incremental, or full backup). These backups take the least time and space, but in the event of data loss organization need to restore data from several backups (the last full backup, the last differential, and all the incremental backups since the last differential) and restore them in precisely the correct order.

Organization decides on how often to back up by considering how much data you can afford to lose. Then, using a hardware drive (tape, CD, or DVD), organization needs to decide on a rotation schedule for backups (i.e. how often you overwrite backed-up data). Organization should schedule some permanent backups (media that aren't rotated and replaced with a more recent backup). This will allow it to go back farther in time if you need to. Organization should keep the following backups updated at all times - Three daily incremental backups, a one-week-old full backup, a one-month-old full backup, a full annual backup.

A mode of taking a back up should also need to be decided based on the cost and importance of data. On-line backup storage is typically the most accessible type of data storage, which can begin to restore in milliseconds time. On-line storage is vulnerable to being deleted or overwritten, either by accident, or in the wake of a data-deleting virus payload. Near-line storage is typically less accessible and less expensive than on-line storage, but still useful for backup data storage. A good example would be a tape library which restores times ranging from seconds to a few minutes. A mechanical device is usually involved in moving media units from storage into a drive where the data can be read or written. Off-line storage is similar to near-line, except it requires human interaction to make storage media available. This can be as simple as storing

backup tapes in a file cabinet. Media access time can be anywhere from a few seconds to more than an hour.

- **Training schedule** – BCP and DRP should have an appropriate schedule for training to employees and all stakeholders.

- **Communication** – BCP and DRP documentation should be communicated to all respective employees and all stakeholders. Declaration of a disaster and communication procedure to appropriate media should be documented. The disaster should be communicated to insurance company within appropriate time-frame.

5.5.2.5 Training

The organization should ensure that all employees are provided with the relevant training. Evaluation of training provided should be carried out. Employee feedback on training should be obtained. Training should enable employees to carry out appropriate actions in the prevention, handling of and/or recovery from the disaster.

5.5.2.6 Maintenance

Maintenance of the BCM is critical to the success of an actual recovery. All changes affecting the BCM should be reflected in the revisions of BCM. Maintenance of BCM involves following two types of activities

- Testing –Organization should prepare a detailed test plan which should typically comprise of the following.
    - Scope and objective
    - Operations included and excluded
    - Users involved
    - Testing procedures
    - Maintenance of plan

BCP and DRP should be tested at regular intervals, as defined in the policy. Following kinds of testing activities should be carried out. In every Organization it is not possible to carry out full scale testing. In such cases Organization should carry out partial testing comprising of critical IS assets/operations and / or key users.The test should be scheduled during the timings which will cause the minimum impact on normal operations. Normally weekends or holidays are the good time to conduct the tests. Test results of all the activities should be documented and analyzed. Gap analysis between test results and desired results should be documented. Action plans for the corrective actions should be prepared and implemented. Iteration of testing, gap analysis, corrective actions and retesting should be conducted till desired results are achieved.

- Review – Management should review the BCM, at regular intervals, typically for changes in
    - BCM policy and procedure
    - Scope and exclusions of BCM
    - Inventory of IS assets
    - Risk assessment
    - Business impact analysis
    - Back up of system and data
    - Training to employees
    - Test drills

5.5.3 BCM Audit Scope

Information System Auditor shall express an opinion typically on the following activities in BCM audit

- Business continuity Management policy and procedure – BCM policy and procedure should be documented, approved, updated and reviewed.

- Risk assessment - Risk Assessment looks at the probability and impact of a variety of specific threats that could cause a business interruption.
- Business Impact analysis – BIA identifies quantifies and qualifies the business impacts of a loss, interruption or disruption of business processes on an organization and provides the data from which appropriate continuity strategies can be determined.
- Development and implementation of BCP & DRP
- Training – Scope, Methods and Coverage of training to employees.
- Test drills – Plan and results of testing activities of BCM
- Offsite procedure – Procedure for selection of the site, back up, restoration, security etc.
- Maintenance of BCP and DRP – Review and updates to BCP and DRP, including inputs from test drills.

5.5.4 BCM Audit Checklist Reference

Refer to the checklist No.10 Business Continuity Management .

5.5.5 BCM Audit Formats and Templates

Refer to the Annexure 2, template No.xx Business Continuity Management .

5.6 E-Commerce Audit

5.6.1 Overview

More and more organisations today are using Internet technology for running their business. It is used to gain competitive advantage and is dependent on the following factors.

- Technological maturity of the organization and its customers
- Internet usage in its geographical area

- Nature of the organisation's products/services
- Relative urgency

E-Commerce includes all commercial activities performed through various electronic sources such as the Information Technology (IT) networks, ATM machines, electronic funds transfer (EFT), and electronic data interchange (EDI). E-commerce involves the real-time processing of business transactions with full contractual liability on a business-to-business (B2B) or business-to-customer (B2C) basis.

The typical benefits of an e-commerce implementation in an organization are:

- Less transaction costs and more productivity
- Services available for 24 hours a day, 7 days a week
- Improved organizations and their supply chain communication and work with business
- Local businesses also can reach the global markets and compete with the others for products and services

Along-with the many benefits of e-commerce, it gives rise to many concern areas and risks which must be satisfactorily resolved by management. So the management expects Information System Auditors to provide an assurance on the following.

- Accomplishments of the business objectives and goals for the operations and performance
- Economical, efficient and effective usage of resources
- Safeguarding of resources
- Reliability and integrity of information
- Compliances with the appropriate laws, regulations and standards

5.6.2 Types of e-commerce

The term e-commerce is used to mean different things. However it can be broadly divided like through the Internet and through the private / dedicated networks without much use of Internet and electronic payments.

5.6.2.1 Through the Internet

ISACA defines e-commerce as the processes by which organisations conduct business electronically with their customers, suppliers and other external business partners, using the Internet as an enabling technology. It, therefore, encompasses business-to-business (B2B) and B2C e-commerce models. But other transactional forms like EDI which use their own dedicated networks are not a part of e-commerce.

B2C e-commerce refers to the processes by which organisations conduct business electronically with their customers and / or public at large using Internet as the enabling technology. The typical broad e-commerce activities are as below:

- Informational (public)—Making information regarding the organisation and its products available on the Internet for whoever wants to access the information
- Customer self-service (informational)—Making information, such as products/services and prices, available on the Internet for the customers of the organisation
- Customer self-service (transactional other than payments)—In addition to making information available on the Internet, accepting customer transactions, such as orders and cancellations, through the Internet, but payments are handled through conventional means
- Customer self-service (payments)—Accepting customer transactions including payments or fund transfers (in the case of banks) through the Internet
- Customer reporting—Providing reports, such as statement of accounts and order status to customers online

- Interactive self-service—Providing interactive responses through e-mails for requests/queries logged through the web sites
- Direct selling—Selling the products and services directly to prospective buyers through the Internet
- Auctioning—Auctioning the products online

5.6.2.2 Through Dedicated networks

This type of e-commerce method is based on dedicated private networks, such as EDI and SWIFT and is mostly outside the Internet. Internet is a publicly owned network and by staying outside the same, the security of this type of E-commerce is superior and hacking into these networks is more difficult. Electronic Data Interchange (EDI) is considered as the computer-to computer, application-to-application exchange of business data in a structured format. Effectively it replaces business forms such as invoices, purchase orders, checks, and so forth with electronic transmissions. Degrees of implementation may vary from the basic reception of a transmission on a computer and sending as an input, to a complex accounting and operational systems while effectively replacing paper audit trails with electronic signals.

EDI is not electronic mail, fax, or video text - although all of these may have a part in the overall network and to effectively function, EDI requires three primary components:

- A standard format of a common language spoken between trading partners
- Translation software performing file conversions from internal application formats to a standard format and back
- A data communications link providing information transport capabilities

Benefits of EDI include

- improved customer service
- improved control of data

- reduced clerical error
- decreased administrative costs and cost efficiency
- quick response and access to information

5.6.2.3 Electronic Payments

This type of EDI is outside the Internet and is more secure and difficult to hack and so is used for secure payments electronically. It is a major growth area which requires a mutual trust in systems between trading partners along-with a comprehensive data security policy, between the trading partners. Failure of security of one partner may lead to uncontrolled risks in others and so participation in an EDI network requires trading partners to demonstrate systems integrity on an ongoing basis.

Third-party service providers are also a new source of potential risk including risks such as:

- Disclosure of confidential information
- Loss of transactions en-route
- Loss of the network at the service provider's site
- Loss of audit trails when going intra-network

5.6.3 Risks in E-Commerce

Being connected on the network which extends beyond the physical boundaries of organizations, e-commerce applications are faced with many external threats, such as hackers, viruses and impersonation, which could affect the confidentiality, integrity and availability of the e-commerce applications. Many times the e-commerce application is directly integrated with back-end systems, without any authorizations and/or intervention and so there is a risk of even back-end systems getting affected. Whenever the organisation's e-commerce application gets affected by any means e.g. hacker attacks, the reputation and image of the organisation also gets seriously impaired.

Following are some of the typical risks of E-commerce.

5.6.3.1 Authenticity

Organizations doing business electronically have the difficulty of determining that the person or system conducting business is, indeed, the entity they claim to be. Authentication for electronic business may be partially achieved using digital signatures whereby, for every transaction; an authenticating party is enabled to check the signer's digital certificate in order to determine whether it has expired or is included in a certificate revocation list (CRL). If the certificate is still authentic and valid (confirmed with the public key), then the authenticity of the signer is accepted.

5.6.3.2 Non-Repudiation

Repudiation involves a denial of one or both parties that all or part of, the transaction took place. Use of the digital signature and digital certificate make it extremely difficult for the signer of a transaction to repudiate the transaction or deny the contents of that transaction. With a digital signature in place the sender's authenticity is confirmed and the input/processing controls ensure that the data has not been corrupted enroute.

5.6.3.3 Timing

Where the timing of a transaction is critical, for example, currency exchange, a transaction should be automatically time stamped to prove the authenticity of the exchange rates claimed.

5.6.3.4 Data Integrity

As with any business transaction, it is critical that the receiver has some degree of certainty that the transaction has not been tampered with prior to its receipt. It is common in manual systems to require original documentation rather than accept copies and, in electronic form, digital signatures can include some controls like a hash value (mathematical summarization), which is unique to the digitally signed transaction. With this defence mechanism in place, a digital signature can be seen as unique to the transaction that has just been signed. When the transaction has been received the

recipient will recalculate the hash value and compare it to determine whether the integrity of the transaction remains intact. In today's world, the software developed for e-commerce takes care of all these things.

5.6.3.5 Interception of Data

Regardless of ensuring the authenticity of the originator and the validity of the data, there may still be an organisational risk if the data is intercepted and examined or even blocked. Data may be intercepted at its origins, prior to its introduction on the system, by simple observation of the data collection process. In wireless networking this is a real threat and should be properly managed. Due to the fact that such transactions are normally transmitted electronically (as opposed to fibre-optics) for at least part of their journey, electromagnetic signals will be generated that can, in some instances, be detected using radio receiving equipment or using transducer microphones, which can detect such signals without penetrating the cables. If an unauthorized individual can gain access to the data communication network, packet sniffers, designed to enhance network security by monitoring transmissions, can be used to intercept and copy messages or possibly even introduce their own spurious messages. As such, once again, encryption comes to the fore as the major control mechanism to reduce and manage these risks.

5.6.3.6 Identity Theft

Identity threat is a major risk in today's world. In this scenario, a stranger gains access to authentication mechanisms impersonating an individual's identity in a provable fashion in order to carry out electronic transactions. Even if the individual whose identity has been "stolen" does not participate in any form of electronic transaction, they cannot deny these transactions and may have to suffer losses.

5.6.3.7 Business Interruption

Business interruption is considered a key risk; if companies cannot promptly and adequately resume business after a crisis, there may be legal liabilities because services/goods were not delivered or payments were not made. Risks within this area would include

denial of service attacks where high-volume, spurious transactions may stop the systems or slow it down to unacceptable levels.

Risk assessment will therefore be a critical tool for the internal auditor to assist in determining E-commerce audit objectives and building an audit program.

With the increased interdependence come increased vulnerabilities of computer-using companies, with a large number of partners, an upstream and downstream impact can be anticipated should anything go wrong and the domino effect makes trading partners vulnerable. From an audit point of view, the way in which we must approach our audit of these systems changes dramatically because the loss of source documents removes a large part of the auditors' evidence of:

- Authorization and execution
- Completeness
- Single processing of transactions
- Capability of batching transactions

In addition, the altered transaction audit trail to an electronic form may result in the full trail existing for only a short time. This trail in itself may be vulnerable to alteration and loss.

5.6.3.8 Corruption of Data

Corruption of data refers to issues of data integrity. The commonly held view is that risks involve activities that can be performed remotely through Web resources. The reality, however, is that almost all corruptions are conducted within the system.

Corruption may be accidental or malicious and could result in:

- Amending catalogues without authorisation (advertising, reporting, approval)
- Destruction of audit trail
- Tampering with the ordering process

- Interrupting the recording of transactions
- Disrupting online tendering.

5.6.3.9 Lack of Authentication

Lack of authentication refers to unauthorized persons/parties performing a transaction. Proper authentication is a critical component of an e-commerce transaction because, once the party has been accepted in the system, a legally binding transaction process has begun. The risk will therefore, involve creating a liability for party , for example:

- Creation of fictitious suppliers ("masquerade"); e.g. an agency believes it is dealing with its supplier when in fact it is dealing with a hacker in a foreign jurisdiction
- Unauthorized ordering or approving of a transaction
- Corruption of the list of agreed suppliers

5.6.3.10 Loss of Privacy/Confidentiality

For e-commerce to be successful, information about an organization or individual needs to be made available to other participants in the trading community. This can put information at risk such as:

- Services and prices, which are not normally provided to the general public
- Cost structures—particularly relating to tenders
- Catalogues of technical details, prices, or discounts offered
- Individuals' information such as name, address, contact details, previous purchase, services provided, and activity (such as criminal or medical).

This, in turn, may lead to inadvertent breaches of privacy legislation.

Public confidence may be adversely impacted if information is accessed without due authorization. The risks themselves may

arise as a result of malicious activity from a virus attack or hacking interception of transactions by unauthorized persons.

5.6.3.11 Frauds in e commerce

Fraud is a highly publicised risk in an e-commerce environment. Because of its global impact, fraud can be either perpetrated by a staff member within the firewalls or by anonymous parties in a foreign country using the Web as a tool and includes such activities as:

- Unauthorized movement of money such as payment to fictitious suppliers located in jurisdictions where recovery of money will be difficult
- Corruption of the electronic ordering or invoicing
- Duplication of payment
- Repudiation of a transaction at either end
- Invalid contracts
- Suppliers not being paid for goods and services delivered
- Agencies not receiving services/goods already paid for
- Denying receipt of goods

5.6.4 E-Commerce Audit Approach

In e-commerce, the business and the information system are coupled tightly. So, a review of the e-commerce also should address the business risks along with the IS risks.

As with any other audit, the audit approach in an e-commerce environment involves the standard six basic steps, namely:

1. Preliminary survey
2. Documenting the environment
3. Audit planning

4. Program development

5. Audit fieldwork

6. Audit reporting

The overall audit objective is to determine by evaluation and testing whether control objectives have been achieved, are being achieved, and will continue to be achieved. The auditor reviews the appropriate controls and their performance as expected and that standards and policies are appropriate and are being achieved. The e-commerce transactions are large and managed by the system without any human intervention. This environment normally involves the auditor in an extensive use of computer assisted audit techniques (CAATs) in determining the effectiveness of these controls. The auditor will need a mixture of skills including mainframe and micro experience as well as network and communication experience, an understanding of access and security controls, and the corporate EDI and e-commerce business cycles. Such reviews would call for technical knowledge to evaluate aspects, including the encryption technologies used, network security architecture and security technologies, such as firewalls, intrusion detection and virus protection. The Information System Auditor should have an adequate knowledge to review these aspects. Auditor may not have all these specialised skills; so, the use of multidisciplinary teams and outside experts will give the auditor access to the appropriate knowledge, skills, and disciplines. Where expert inputs are necessary, suitable external professional resources should be used. The fact that external expert resources would be used should be communicated to the organisation under audit in writing.

The preliminary survey involves a review of general background of business. This helps the auditor to understand the threats and identify controls mitigating those threats. This in turn leads to the development of overall control structures and helps the auditor to review the operations critically. All assessments of an inherent risk should be agreed with the users, IS staff, and management. Steps in reviewing the general business objectives include observing the activities of the system and evolution of the system as well as determining any known weaknesses from these evaluations. At

this stage, legal contracts may also be reviewed together with contingency plans.

In general, study of available documentation (i.e., business case, system documentation, contracts, service level agreements and logs), discussions with the stakeholders, getting actual experience of the e-commerce application and observation should be used appropriately to gather, analyse and interpret the data. Where appropriate, the Information System Auditor should test the significant processes in the test and/or production environment to verify that the processes are functioning as intended (i.e., test purchases or test ordering using the e-commerce system and test the security mechanisms using penetration testing).

Where necessary and agreed upon with the organisation, external expert inputs could be used suitably in the collection, analysis and interpretation of the data. The inferences and recommendations should be based on an objective analysis and interpretation of the data.

Appropriate audit trails should be maintained for the data gathered, analysis made, inferences arrived at, as well as corrective actions recommended. Following specific actions are recommended in the Information System Audit of E-commerce.

5.6.4.1 Evaluate the Business Aspects

- The Information System Auditor should review the e-commerce objectives, strategy and business model critically. The existing and emerging competition also should be studied in evaluating the current position of the organisation's business. This is essential for confirming the appropriateness of the objectives and strategies as well as evaluating the effectiveness and efficiency of the e-commerce strategies in fulfilling the organisational objectives and strategies.

- The Information System Auditor should ascertain whether there are appropriate mechanisms to monitor the effectiveness and efficiency of the e-commerce strategies and transactions on an ongoing basis. This should include

the processes to detect and report exceptions so as to prevent errors and frauds.

5.6.4.2 Detailed Risk Assessment

- The Information System Auditor should study the key processes. And if the same are not available, he should map the automated and manual key processes relating to the e-commerce application, for getting clarity in the application. The business as well as IS risks should be critically reviewed and their likely effect should be documented along with the controls to mitigate the risks. The criticality of the residual risk also should be assessed. The depth of the review will be dependent on the criticality of these risks.

- Review the appropriateness of the development and maintenance process followed to determine whether appropriate controls are built into the e-commerce application. The capabilities of the team developing/maintaining the B2C e-commerce application and the tools being used should be reviewed to ensure appropriate controls in the e-commerce application getting adequately addressed.

- Since the e-commerce depends largely on the availability of the application and the access on the network, the Information System Auditor should evaluate whether there are appropriate capacity planning processes, redundancies and fallback options, offsite storage, rotation of media, as well as disaster recovery procedures in place for both the system and communication link. Where relevant, the Information System Auditor also should review the fallback arrangements with reference to the automated and other related manual processes to ascertain their appropriateness in ensuring business continuity and fast recovery in the event of any disruptions.

5.6.4.3 Change Management Process

- The integrity of data and processing will be lost if the changes are not controlled. So the change management process should be reviewed critically by the Information

System Auditor. The contents of e-commerce web sites should be through a controlled content management process to ensure appropriateness of language and presentation, correctness of information, appropriate approvals for the data published (particularly, those relating to products, services, terms and conditions).

- The Information System Auditor should review the presence of adequate change logs, along-with the actual changes affected, to verify that the processes are functioning as intended. Mere availability of audit trails is not enough evidence and they should be substantiated by proper reviews and actions. There should be processes for reviewing the audit trails to provide a reasonable assurance that the actions, as reflected in the audit trails, are valid and duly authorised.

- The Information System Auditor should ensure that separate environments for development, testing, staging and production are maintained.

5.6.4.4 Identification and Authentication

Depending on the e-commerce activities permitted by the B2C e-commerce application—particularly where transactions and payments are processed—the user should be identified and authenticated uniquely to prevent non-repudiation and to preserve confidentiality. The Information System Auditor should evaluate whether the controls / mechanisms / technologies (such as User ID and passwords, digital certificates and digital signatures) deployed regarding identification and authentication are properly defined to manage the intended use of the e-commerce application.

5.6.4.5 Data Validations and Authorisations

- If the e-commerce application accepts data directly from the users by way of transactions and/or information, the Information System Auditor should verify whether adequate validations are built into the application to ensure the appropriateness of the data being entered and that such validations are being performed.

- If the e-commerce application accepts electronic payments (such as credit cards), the Information System Auditor should verify whether there are adequate validation and payment authorisation processes to ensure the authenticity as well as the actual receipt of the payments.

- In the case of e-commerce application(s) processing transactions and payments as well as accepting and/or displaying any personal details confidential in nature (such as statement of accounts), the Information System Auditor should verify whether an appropriate encryption technology/mechanism (such as secure socket layer or IPSec) is being used to encrypt the transmission between the user and the application.

- Where the e-commerce solution involves processing of transactions and payments, the Information System Auditor should evaluate the relevant controls referred to previously with reference to authentication, communication, processing, and ensuring non-repudiation.

- Where appropriate and necessary, the Information System Auditor should ascertain whether the communication across the network is made secure using a virtual private network (VPN) and related encryption.

- In the absence of paper trails, the role of automated audit trails is critical in e-commerce applications. The Information System Auditor should review the adequacy of the audit trails relating to transactions including payments, changes to critical master data (such as rates and prices and actions) and any changes carried out by the staff with system administration privilege.

5.6.4.6 Data Storage Integrity

- Every e-commerce application has at least one database at the back-end, the integrity of which is crucial. The Information System Auditor should evaluate the controls over the database to confirm that there are adequate checks and balances to prevent intentional or inadvertent damage, destruction or modification of data. In this context, the

Information System Auditor should review the database access privileges as well as the access logs.

- The Information System Auditor also should review the controls over the archived data to provide a reasonable assurance that the confidentiality and integrity are protected adequately.

5.6.4.7 Protection against External IS Threats

- The Information System Auditor should evaluate the external IS threats like denial of service, unauthorised access to data and unauthorised use of the computer equipment, etc. arising from various sources (such as casual hackers, competitors, alien governments and terrorists) to the e-commerce environment, taking into account the nature of the business of the organisation. The external threats to be addressed should typically include the characteristics of the business of the organisation (such as intensity of competition, market share, nature, timing and extent of technology usage, and innovative/strategic products and/or services) to determine the possible sources of such threats. The likely damage associated with these threats is linked closely to the dependence of the business on the e-commerce processes.

- The Information System Auditor should assess whether the protective measures in place to counter the external threats are commensurate with the level of the assessed risk. In this process, the Information System Auditor should review the following:

- Technical architecture of the application including the choice of the protocols

- Security architecture of the application

- Virus protection mechanisms

- Firewall implementation: appropriateness of the firewall solution, location of firewall, firewall policies, connections to

the firewall and any external connections bypassing the firewall

- Intrusion detection mechanisms
- Existence of relevant logs as well as their ongoing review by competent staff
- Processes in place to verify the compliance with the envisaged architectures, policies and procedures

5.6.4.8 Compliance with Privacy Regulations and Best Practices

The Information System Auditor should confirm whether the relevant privacy requirements imposed by the relevant laws as well as the best practices relating to privacy are being complied with by the organisation. The privacy policies and practices should be displayed appropriately in the web site.

5.6.4.9 Third-party Services

- Where the e-commerce solution depends on any third-party service providers, such as an Internet Service Provider (ISP), Certificate Authority (CA), Registration Authority (RA) and web-hosting agency, the Information System Auditor should ascertain whether the security procedures at their ends are appropriate and adequate.
- Where such third-party service providers are used, the Information System Auditor should review the related contracts and service level agreements (SLA) as well as the SLA reporting to assess whether the interests of the organisation are being protected adequately.
- When third parties are used for certification in B2C, the Information System Auditor should provide due diligence in reviewing how the information is collected and used for those seals of control (e.g. Better Business, Web trust).

5.6.5 Reporting

The report on the e-commerce review should address the following aspects depending on the scope of its coverage:

- The scope, objective, methodology followed and assumptions
- Overall assessment of the solution in terms of key strengths and weaknesses as well as the likely effects of the weaknesses
- Recommendations to overcome the significant weaknesses and to improve the solution
- Recommendations regarding how the experience could be used to improve similar future solutions or initiatives

5.6.6 E-commerce Audit Checklist Reference

Refer to the Checklist No. 6 for E-commerce Audit

5.7 Data Centre Audit

5.7.1 Overview

A Data Centre is a centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business. The National Climatic Data Centre (NCDC) in USA, for example, is a public Data Centre that maintains the world's largest archive of weather information. Organizations may have a private Data Centre or it may be a specialized facility servicing many organizations.

A Data Centre in simple words is a facility or room used to house mission critical computer systems and associated components for companies and organizations. It generally includes environmental controls (air conditioning, fire suppression, etc.), redundant/backup power supplies, redundant data communication connections and high security. A Data Centre is very important in any organization; without it business can cease to communicate, perceive,

remember and create. The end result is a business that ceases to function.

5.7.2 The audit process

5.7.2.1 Audit Preparation

The auditor should study the company and its critical business activities before conducting a Data Centre review. The Data Centre activities should be aligned with the goals of the business while maintaining the security and integrity of critical information and processes. To adequately determine whether the client's goal is being achieved, the auditor should perform the following before conducting the review:

- Meet with IT management to determine possible areas of concern
- Review the current IT organization chart
- Review job descriptions of Data Centre employees
- Research all operating systems, software applications and Data Centre equipment operating within the Data Centre
- Review the company's IT policies and procedures
- Evaluate the company's IT budget and systems planning documentation
- Review the Data Centre's disaster recovery plan

5.7.2.2 Establishing Audit Objectives

The next step in conducting a review of Data Centre takes place when the auditor outlines the Data Centre audit objectives. Auditors consider multiple factors that relate to Data Centre procedures and activities that potentially identify audit risks in the operating environment and assess the controls in place that mitigate those risks. After thorough testing and analysis, the auditor is able to adequately determine if the Data Centre maintains proper controls and is operating efficiently and effectively.

Information System Auditor shall express on the opinion typically on following activities in Data Centre audit

- Data Centre policy and procedure – Data Centre policy and procedure should be documented, approved, updated and reviewed
- Data Centre access controls - Data Centre should have adequate physical and logical access controls
- Data Centre Equipments – Data Centre should have appropriate facilities / equipments to carry out operations.
- Data Centre operations – Data Centre should have an appropriate change management and system development procedures in place.
- Back up and restore - Back up and restore procedure should be adequate to restore the data operations in the event of a disaster or major interruption.
- Data Centre Environment– Adequate environment measures should be implemented in Data Centre for secure, effective and efficient operations.

5.7.2.3 Performing the Review

The next step is collecting evidence to satisfy Data Centre audit objectives. This will involve actual visit to the Data Centre location and observing processes and procedures performed within the Data Centre. The following is typically reviewed to satisfy the pre-determined audit objectives – Data Centre location, policy and procedure, Data Centre personnel, Data Centre equipment, access controls, back up procedure and Data Centre environment.

1. <u>Data Centre Location</u>

Following guidelines should be taken into consideration while deciding the location of Data Centre

- Access to Data Centre location should be restricted by the use of keys, badges or other automated security devices

- Data Centre should not be at ground floor location or below ground level
- It should not have showcase window
- Adequate air conditioning should be available
- Direct access into Data Centre should not be permitted from the outside or through a public hallway
- All telecommunication line junction points (wiring and router closets, etc.) should be available and must be secured to prevent tampering
- Data Centre should be protected from a catastrophic mishap, i.e., aircraft collision, etc.

2. Data Centre Policies And Procedures

Data Centre policy and procedure should be in line with business strategies. Short and long term goals of Data Centre should be covered in Data Centre policy and procedure. These documents must be approved by Top Management and should be updated at regular interval so as to keep them in line with current Data Centre operations. Regular review of Data Centre policy and procedures should be conducted at appropriate level.

Consideration to following factors must be given while setting out Data Centre policy and procedure.

- Present business environment and business processes
- Business strategies
- Current processes and future growth of business
- Relevant industry standards and best practices
- Legal requirements

Following are the typical contents of the policy and procedure documents

- Scope and objective

- Data Centre structure
- Human resource
- Facilities
- Operations
- IS Controls
- Review and maintenance

3. Data Centre Personnel

All Data Centre personnel should be authorized access the Data Centre through a secure device like key cards, biometric devices, login IDs, secure passwords, etc. Data Centre employees are adequately educated about Data Centre equipment and properly equipped to perform their jobs. Vendor service personnel are continuously supervised when doing work in Data Centre equipment. The auditor should observe and interview Data Centre employees to satisfy the above objectives.

4. Data Centre Equipment

The auditor should verify that all Data Centre equipment is working properly and effectively. Equipment utilization reports, equipment inspection for damage and functionality, system downtime records and equipment performance measurements all help the auditor determine the state of Data Centre equipment. Additionally, the auditor should interview employees to determine if preventative maintenance policies are in place and performed.

Organization should maintain the configuration details for all critical IS assets in Data Centre. Any change in configuration of IS assets in Data Centre should be governed by change management procedure.

Typically the following facilities are a part of a Data Centre:

Servers

In Information technology, a server is an application or device that performs services for connected clients as a part of client-server architecture.

- A server application is "an application program that accepts connections in order to service requests by sending back responses."
- Server computers are devices designed to run such an application or applications, often for extended periods of time with minimal human direction and maintenance.

Monitoring of the following activities in respect of server should be carried out.

- Disk space
- Server Logs
- Server performance
- Throughput
- Power supply
- Temperature
- Proportion of downtime
- Frequency and maximum duration of outages
- Proportion, types, and causes of job failures
- Computer system peak and average utilization and trends etc.

Racks

A rack is a metal frame used to hold various hardware devices such as servers, hard disk drives, modems and other electronic equipment.

Routers

A router is a device (or in some cases software in a computer) that determines the next network point to which a data packet should be forwarded toward its destination. It is a device that can route or forward the information to connected segment of the network. Routers generally contain an operating system and memory which guides in routing / forwarding the information.

Switches

It is a device which connects two network segments.

UPS (Uninterrupted Power Supply)

It is a back-up power supply for computer systems. It is used to maintain a continuous power supply to a computer system when an electrical power fails or is interrupted.

Air conditioners

Air conditioners and air quality are essential to the reliable operation of computer equipment and must be maintained within acknowledged Data Centre standards.

Other security equipments

Data Centre should be equipped with fire detection and prevention devices such as fire extinguishers, water sprinklers, fire detectors etc. to maintain appropriate security in the Data Centre. Appropriate telecommunication devices as per the requirement of organization should be present in the Data Centre. Test drills of the safety equipment should be carried at regular interval. Employees in Data Centre should be trained on the usage of security equipment.

5. Access Controls

The auditor should assess the security of the client's Data Centre. Physical security includes bodyguards, locked cages, man traps, single entrances, bolted down equipment, and computer monitoring systems. Additionally, environmental controls should be

in place to ensure the security of Data Centre equipment. These include: Air conditioning units, raised floors, humidifiers and uninterruptible power supply.

Following are a few recommended guidelines to be followed while granting logical access.

- Suitable naming convention should be followed for user ID
- User IDs and passwords should not be same
- User IDs should have difficult-to-guess naming conventions to prevent outsiders from attempting to hack into the network
- Users should automatically be disabled after three unsuccessful logon attempts
- Users should be forced to change password on first log on
- Users should be disabled after a specified time period
- Passwords should be at least six to eight characters in length
- Passwords should have at least one special character
- Password reuse should be limited to six generations
- Users should be prohibited from logging on to concurrent terminals
- Users should be required to change their passwords periodically

Following are a few recommended guidelines to be followed while granting physical access:

- The doors to the Data Centre must always remain closed and locked at all times.
- Authorized persons should enter the Data Centre to perform only those tasks that cannot be performed remotely.

- Authorized persons entering or leaving the Data Centre should wait near the electronically controlled doors until the timeout period has expired and the door closes to insure no unauthorized persons enter the room.
- No camera or photographic equipment should be allowed within the Data Centre without the approval.
- Data Centre facilities should be restricted by the use of keys, badges or other automated security devices.
- Data Centre should not have a direct access from the outside or through a public hallway
- Access keys to cabinets, equipment rooms, and wiring closets should be held under proper custody
- No visitors should be permitted without approval.

A log for physical access should be maintained. Log should content details of the person who has accessed Data Centre, purpose of access and duration of access. In case of visitor / guest access, an employee escorting them should also sign the log register. Organization should review the physical access logs at regular intervals.

In case of logical access logs, a system generated log should be maintained. System generated reports should be run on a periodic basis to detect access violations. Some of those violations are as follows:

- User ID and passwords are the same
- Unsuccessful logon attempts
- Users who have not logged on in more than 90 days
- Users who have not changed their password in more than 30 days
- Users violated the access rights permissions granted to them

In addition to above logs, organization should review the following at regular intervals:

- List of users to Data Centre and whether they are current
- Access rights periodically to determine if the access granted is adequate.
- Employee removed from organization and his access rights are removed or not
- User access management process and updates required

Organization should prepare a report of findings of the monitoring activities. Monitoring reports should be analyzed and discussed with appropriate level of management. Actions plans should be prepared and implemented for the violation if any found in monitoring.

6. Backup Procedures

The auditor should verify that the client has backup procedures in place in the case of system failure. Clients may maintain a backup Data Centre at a separate location that allows them to instantaneously continue operations in the instance of system failure. Records for back up and restore logs should be maintained. Log consists of the details like number of files, size of data, start and end time and status of the activity either it is completed successfully or not. Online back up monitoring requires software capable of pinging the monitoring centre's servers in the case of errors. Persons responsible for the maintenance of back up and restore activity should review the back up and restore logs. Scheduled jobs for backup should be monitored at regular intervals.

7. Data Centre Environment

The environment should be evaluated as a whole and an overall determination made of its internal controls. The environmental equipment and controls should be adequate to protect the computer hardware from damage. A review of the environmental condition of the critical Data Centre facilities should be carried at

regular intervals. Following are the guidelines for good environmental controls

- Ensure that clear and adequate safety instructions are posted in strategic locations.
- Ensure that safety instructions are communicated and understood by all concerned in Data Centre.
- Fire alarm pull boxes and emergency power switches are clearly visible and unobstructed.
- Determine if the critical Data Centre facilities have automatic fire/water detection/extinguishing system and if so, perform the following procedures:
    - Review results of recent system tests performed.
    - Ensure the system is protected by a backup power supply and that it is periodically tested.
- Review the documented results of the last several fire drills for adequate frequency and evacuation timeliness.
- Ensure that the portable fire extinguishers within the critical Data Centre facilities have been inspected / recharged within the past 12 months.
- No radios or other non-computer related equipment should be plugged into any dedicated circuit or equipment without the approval.
- Review logs of preventative maintenance activities for appropriateness.
- The Data Centre should have an automatic fire extinguishing system which should be tested periodically by the manufacturer or service representative.
- The fire detection system should detect smoke, excessive heat or combustible fumes.

- The detectors should be located in the ceiling air ducts and beneath the raised flooring.
- Detectors should be tested frequently and protected by a backup power supply.
- When the fire alarm is activated, it should sound outside the Data Centre at a guard station and a local fire station or emergency control center.
- Data Centre personnel should be able to identify the sound of the fire alarm.
- Adequate precaution to save from the exposures of flooding should be taken
- The computer room should be kept clean at all times.
- Ensure that ventilation and air conditioning systems are adequate to maintain appropriate temperature and humidity levels specified by the hardware manufacturer(s).
- Ensure temperature and humidity levels are recorded, maintained and routinely monitored.
- Determine if the air conditioning and humidity control system is protected by a backup power supply. If so, ensure the backup power supply is tested periodically and review the results of the most recent test.
- Recording thermometers and humidity indicators should be located so that the readings can be obtained easily. These instruments should be monitored on a routine basis by a trained person.
- The hardware should automatically shut down to protect itself from damage if unacceptable temperature is reached.
- The computer equipment should be subject to periodic maintenance, cleaning and inspection and a record kept of such.

- The computer room ceiling should be adequately constructed to prevent water from entering the computer room.
- Overhead water steam and pipes should be avoided.
- Adequate drainage should be provided.
- Independent air conditioning system with a backup power supply should be installed.
- The organization should keep the humidity levels between 45% and 60% which are best for safe server operation as warm air can hold more water than cold air. So, if the temperature raises the relative humidity decreases. As with the recommended temperatures, this range allows a safe buffer zone in case of air conditioning or cooling failures. Conversely, if the temperature falls the relative humidity increases, ultimately to the point were condensation arises.
- Appropriate maintenance of air conditioning should be carried so as to avoid failures resulting in water leaks.
- Organization should take into account the possibility of hot spots and the layout of equipment. Most devices draw cold air in at the front and exhaust hot air at the back, so airflow needs to be sufficient to prevent warmed air being drawn in to the next equipment rack.
- Measure temperature over an extended period, 24 hours or longer. This will allow organization to check for fluctuations and to analyze trends or patterns in the data.
- Temperature measurements taken in different parts of the Data Centre can vary significantly. Concentrations of equipment can produce hot spots. Measure the temperatures between equipment racks.
- Organization should avoid temperature changes greater that 5 degrees Celsius (10 degrees F) per hour and humidity changes of + or -10% in the same period.

5.7.2.4 Data Centre Documentation

Sufficient documentation should be maintained to facilitate the timely resolution of Data Centre problems.

- Data Centre layout
- List of all IT assets in Data Centre
- Records of configuration of all critical IS assets
- All equipment should be labelled in the front panels with identification information.
- All power cables will be labelled and identified for its specific use and identified by its amperage, voltage, type connector and length of cable.
- All communication cables installed within the Data Centre will be labelled to identify their use and/or purpose. This label must be at both ends.
- When equipment is changed in the Data Centre, all pertinent documentation must be updated.
- Records for logs of back up and restores should be maintained
- The organization should put in place contingency plans and BCP plan. The plan must be communicated to all the concerned stakeholders. The plan must be reviewed and updated at regular intervals.

5.7.3 Data Centre Audit Checklist Reference

Refer to the following –

- Checklist No.1 Organization policy and procedure. Refer to the checklist No 3 and 4 physical and logical access
- Refer to the checklist No 5 and 8 for Data Centre operations
- Refer to the checklist No 5 for back up and restore
- Refer to the checklist No 3 for environmental securit

Annexure I - Audit Checklists

1. IS Policies and Procedures

IS Auditor	(Name and Signature)
Auditee	(Name and Signature)
Date(s) of Audit	

Process Objectives

- To ensure that IS long term and short term plans are in line with business plans.
- To ensure that IS policies and procedures are documented, approved and updated.
- To ensure compliance to IS policies and procedures from stakeholders.
- To ensure communication of IS policies and procedures to the concerned users.

Sr. No.	Check points	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
1.1	**Business – IS Alignment**			
1.	Whether the business strategy is documented and business objectives are defined? *(Obtain a copy of strategy document. Verify objectives / goals that are forming a part of strategy document).*			
2.	Whether the business strategy has been approved by the			

Sr. No.	Check points	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
	Management? *(Suitable form of Management approval must be evident from strategy document, signed by authorized signatory).*			
3.	Whether the IS strategy is a part of the business strategy and is in line with business objectives?			
4.	Whether periodic assessments are made by IS department (function) to ensure that IS initiatives are supporting the organizational objectives?			
5.	Whether IS issues as well as opportunities are adequately assessed and reflected in the organization's strategy, long term and short term plans?			
6.	Whether major developments in technology (hardware, software, communication etc.) are assessed for their impact on the business strategy and necessary corrective steps, wherever needed, are taken?			
1.2	**Long Term and Short Term IS Plans**			
1.	Whether short term and long term IS plans are			

Sr. No.	Check points	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
	documented?			
2.	Whether the short term and long term plans are in line with the IS strategy?			
3.	Whether the short term and long term IS plans are approved by the Management?			
4.	Whether the long term plan covers: - Existing and Proposed IS architecture for the business and its rationale - Broad strategy for procurement of IS solutions - Vendor development and management standards for IS, prescribed by the proposed architecture strategy for outsourcing, procuring off-the-shelf software, and in-house development - Information Security Architecture - IS Department's organisational structure - Desired level of IS Expertise in IS department human			

Sr. No.	Check points	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
	resources and plan to bridge the gap, if any - Strategies converted into clear IS Initiatives with a broad time frame - IS budgets and cost management - Plan for change management. - Mechanism for a periodic review of IS plans, budgets and initiatives.			
5.	Whether the IS plan integrates with other plans such as the organisational plan and the information risk management plan?			
6.	Whether IS plans are flexible enough to accommodate - Changes in business strategy - Changes in IS strategy - Changes in organisation's plan - Changes in IS environment			
7.	Whether a IS security committee, comprising of stakeholders from relevant departments like IS Department, Business Operation Group, IS			

Sr. No.	Check points	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
	Security Department and Legal Department, is formed to provide appropriate direction to formulate, implement, monitor and maintain IS security in the organization?			
8.	Whether all long-range IT plans are converted into short-range IT plans for implementation and achievability?			
9.	Whether the IT Short-range plan covers the following: - Plan for initiatives covering all elements of Long range plan - Process transition strategy. - Resources - Responsibility and schedule for achievement.			
10.	Whether adequate resources are allocated for achieving the short-range plans?			
11.	Whether short-range plans are amended and changed as necessary in response to changing business and information technology environment?			

Sr. No.	Check points	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
12.	Whether assessments are made on a periodic basis about the implementation of short range plans?			
1.3	**IS Policies and Procedures**			
1	Whether IS policies and procedures are documented?			
2	Whether concerned stakeholders are involved in the preparation and review of the IS policies? *(All the stakeholders involved / affected by policy or procedure should have appropriate representation in preparation and review of documents).*			
3.	Whether all IS operations are covered in the IS policies and procedures? *(Obtain a list of IS operations of the organization).*			
4.	Whether legal and regulatory requirements are considered in the IS policies? *(IS policies and procedures should cover all aspects of compliance with legal and regulatory requirements).*			

Sr. No.	Check points	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
5.	Whether all documents follow a standard practice? *(Organization should follow the suitable format, naming convention for identifying and tracking of documents and structure consistently).*			
6.	Whether IS policies and procedures are approved by the management?			
7.	Whether appropriate IS policies and procedures are communicated to all the concerned? *(Obtain the evidences of communication. Communication can be through an email, a training session or availability at common storage place accessible and known to all the concerned).*			
8.	Whether IS policies and procedures are - Updated based on review and changes necessitated? - Version controlled? - Appropriately secured, if confidential?			
9.	Whether the organization monitors the compliance to IS policies and			

Sr. No.	Check points	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
	procedures? If yes, is compliance level measured? *(Collect the evidences on how the organization monitors and measures the compliance).*			
10.	Whether all IS users are made aware of IS policies and procedures? *(Ensure that all IS users including vendors and customers are identified and communicated about relevant IS policies and procedures.)*			
11.	Whether users / employees feedback on IS policies is obtained? *(Feedback on IS policies, any improvements to existing policies or procedures and employee satisfaction should be taken).*			

2. IS Infrastructure and Organization

IS Auditor	(Name) and (Signature)
Auditee	(Name) and (Signature)
Date(s) of Audit	

Process Objectives

- To ensure IS organisation is defined and maintained.
- To ensure appropriate HR practices are implemented.
- To ensure IS infrastructure is maintained as per the requirements, in a secured manner.

Sr. No.	Check points	Yes/No/NA	Remarks/ Explanations	Evidences
2.1	**IS Organisation**			
1.	Whether the IS organisation is documented and approved?			
2.	Whether the IS organogram includes all the current roles and personnel assigned to them? *(Obtain the organogram and verify it for its currency).*			
3.	Whether roles and responsibilities are defined,			

Sr. No.	Check points	Yes/No/NA	Remarks/ Explanations	Evidences
	documented and communicated to the personnel?			
4.	Whether the roles assigned are appropriate? (*Verify the assigned roles that are based on the following:* - *Conflicting duties are not assigned. In case conflicting duties are assigned, review compensating controls implemented.* - *The requirement of need to do and need to know basis).*			
5.	Whether the job rotation is in place for critical roles? *(Verify that the critical roles are identified and these roles are assigned on a rotational basis*			

Sr. No.	Check points	Yes/No/NA	Remarks/ Explanations	Evidences
	to identify personnel).			
6.	Whether back up persons are identified for critical roles?			
2.2	**HR Policies – Recruitment , Training, development and Termination**			
1.	Whether Human Resource policies are documented, approved and current?			
2	Whether an adequate screening is done on new entrants? *(There should be an appropriate screening procedure including interview, technical tests, confirmation of claimed academic qualification(s), background check).*			

Sr. No.	Check points	Yes/No/NA	Remarks/ Explanations	Evidences
3.	Whether confidentiality agreement is executed with the employees? *(Check for the signed confidentiality agreements)*			
4.	Whether an appropriate training required for the roles is being provided on an ongoing basis? *(Check the training records)*			
5.	Whether a review of existing and future needs of personnel to match business requirements is carried out at regular intervals?			
6.	Whether disciplinary procedures for non-compliance to IS policies are communicated to the employees? *(Violations of*			

Sr. No.	Check points	Yes/No/NA	Remarks/ Explanations	Evidences
	security policies and remedial action taken should be reviewed).			
7.	Whether a review of the employees performance is carried out at regular intervals?			
8.	Whether procedures to be followed on termination or change in assignment are clearly assigned? *(Responsibilities typically include return of IS assets and removal of access rights).*			
2.3	**IS Assets – Acquisition, Maintenance & Disposal**			
1.	Whether the IS Asset Management procedure is documented and approved?			

Sr. No.	Check points	Yes/No/NA	Remarks/ Explanations	Evidences
2.	Whether a Technical and Financial Feasibility study is conducted in acquisition of IS assets*?*			
3.	Whether an inventory of IS Assets is maintained and reviewed by management? *(Check for the stock verification reports).*			
4.	Whether IS assets are located at secured places so that the risk of unauthorised access is avoided?			
5.	Whether IT assets are maintained in a manner to ensure availability and integrity? *(Verify scheduled maintenance activities and periodic monitoring).*			

Sr. No.	Check points	Yes/No/NA	Remarks/ Explanations	Evidences
6.	Whether adequate precautions are taken for IS assets before their disposal? *(Verify the following as:-* *- Management approval* *- Deletion / destruction of sensitive information before media disposal,* *- Compliance to internal, legal and regulatory requirements).*			

3. Physical and Environmental Security

IS Auditor	(Name) and (Signature)
Auditee	(Name) and (Signature)
Date(s) of Audit	

Process Objectives

- To ensure IS assets are maintained in a secured manner.
- To ensure the controlled environment to IS assets.

Sr. No.	Check points	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
3.1	**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			

Sr. No.	Check points	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
	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*			

Sr. No.	Check points	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
	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 visitors 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 organisation?			

Sr. No.	Check points	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
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 authorised 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 equipments are present to monitor the movements of the personnel inside the facility?			
16.	In case of an 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-			

Sr. No.	Check points	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
	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?			
3.2	**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 noncombustible / fire resistant / fire retardant).*			
3.	Whether smoking restrictions in IS facilities are in place?			
4.	Whether adequate smoke /			

Sr. No.	Check points	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
	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?			

4. Logical Access Control

IS Auditor	(Name) and (Signature)
Auditee	(Name) and (Signature)
Date(s) of Audit	

Process Objectives

- To ensure IS organisational assets are maintained in a secured manner by establishing appropriate process for authentication of users and establishing appropriate controls over user access management.

Sr. No.	Checkpoints	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
4.1	**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			

Sr. No.	Checkpoints	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
	assignment & modifications. - Emergency access Granting. - Monitoring access violations. - Review and update of document.			
4.2	**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			

Sr. No.	Checkpoints	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
	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*			

Sr. No.	Checkpoints	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
	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*			

Sr. No.	Checkpoints	Yes/ No/ NA	Remarks/ Explana-tions	Evi-dences
	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).*			

5. Operations and Incident Management

IS Auditor	(Name and Signature)
Auditee Correspondent	(Name and Signature)
Date(s) of Audit	

Process Objectives:

- To manage IS operations with required service levels.
- To safeguard information assets from unauthorized access, disclosure, and modification.
- To ensure an appropriate, effective and timely response to security incidents.

Sr. No.	Checkpoints	Yes/ No/NA	Remarks/ Explanations	Evi-dences
5.1	**Change Management**			
1.	Whether the program / data change policy and procedure documented?			
2.	Whether the change requests are initiated by documented request from users? *(Verify the changes requested and serial numbers allotted to keep a track of change requests).*			
3.	Whether the changes are reviewed and approved by the IS management before implementation? *(Review feasibility study, effects of change on existing system, rollback procedures*			

Sr. No.	Checkpoints	Yes/ No/NA	Remarks/ Explanations	Evi-dences
	carried out by IS management).			
4.	Whether development, test and production environment are separated? *(Verify whether the changes are made in development environment, tested in the test environment and the separation of development and test environment is maintained).*			
5.	Whether the transfer of changes from development to test and from test to production environment is made by employees not involved in the development and testing? *(Programmers to develop the changes, the user should test them in test environment and after adequate testing changes should be transferred to production. Employees to transfer changes should be independent of person involved in development / testing).*			
6.	Whether the appropriate back-up is taken before the transfer of change to production? *(Adequate back-up of the programs / data / set up / operating system in development / production*			

Sr. No.	Checkpoints	Yes/ No/NA	Remarks/ Explanations	Evi-dences
	environment before implementation of changes should be taken).			
7.	Whether the version controls are maintained for every change release?			
8.	Whether the change implementation guides or the user training manuals are prepared? *(Users should be given adequate training on how to operate in the changed environment).*			
9.	Whether adequate post-implementation reviews are carried out for changes implemented?			
10.	Whether the relevant records affected by the change updated? *(Program library, production library, documented policy and procedures affected by the changes should be updated).*			
11.	Whether there exists a procedure to review and monitor all the pending change requests? *(The IS management should take a timely action to resolve the pending changes).*			
12.	Whether procedure for emergency changes included			

Sr. No.	Checkpoints	Yes/ No/NA	Remarks/ Explanations	Evi-dences
	in the change management? *(Documentation should be sufficiently detailed to explain the nature of the emergency change, the immediate action taken to address the problem, and subsequent actions required / taken to correct the problem for ever).*			
5.2	**Back-up and restoration**			
1.	Whether the back-up and restoration policy is documented and approved?			
2.	Whether backup procedures are appropriate for IS information, program and IT assets? *(Back up should cover essential business information, servers, critical network components and configuration as appropriate to the policy and objectives).*			
3.	Whether back-up and restore activity are regular? *(Review the schedules maintained for back-up and restoration).*			
4.	Whether back-up is accurately logged and stored in a secure location? *(Proper records should include the media in which different data backups are stored, data*			

Sr. No.	Checkpoints	Yes/ No/NA	Remarks/ Explanations	Evi-dences
	type, location where it is stored, date of backup, due date for recycle).			
5.	Whether the practice ensures that back-up and recovery procedures will work when required? *(Review logs of restoration activities, user involvement in restoration, and generations maintained such as grandfather, father and son. One generation copy of back up should be stored offsite).*			
6.	Whether data is retained adequately to meet regulatory requirements?			
5.3	**Network Security**			
1.	Whether the network security policy is documented and approved?			
2.	Whether the security policy restricts an unauthorised access? *(Verify the security policy and procedure for access controls by organisation to restrict unauthorised access)*			
3.	Whether the policy provides for the concept of least privilege to be used in establishing access rights and privileges for users?			
4.	Whether the system			

Sr. No.	Checkpoints	Yes/ No/NA	Remarks/ Explanations	Evi-dences
	administrators' role has been segregated adequately from other roles? *(Ensure that the system administrator is not responsible for data entry, system / application programming, or database administration).*			
5.	Whether unnecessary services / access on the network are disabled? *(Every organisation needs to identify as per its operations and disable the services / access e.g. guest account, routing and remote access, and clipbook, network DDE etc.)*			
6.	Whether roles and responsibilities are documented and established for the administrator and users of the network?			
7.	Whether adequate physical and logical controls are established over access to network devices like routers and switches? *(Physical controls are like storing in secured area. Logical controls include user ID and password)*			
8.	Whether firewall and IDS protections are provided on the			

Sr. No.	Checkpoints	Yes/ No/NA	Remarks/ Explanations	Evi-dences
	network?			
9.	Whether adequate security measures are implemented for wireless and dial-up access to the network? *(Review for additional security measures for wireless and dial up access)*			
10.	Does the organization conduct penetration testing on a regular basis?			
11.	Are the results of tests properly documented and shared with the appropriate people who can respond to the identified weaknesses?			
5.4	**Mobile Computing**			
1.	Whether the policy on acceptable use of mobile devices is documented? *(Obtain the security policy on usage of mobile devices like laptops and hand-held computing devices).*			
2.	Whether the policy and procedure documents are approved by the Management?			
3.	Whether the management has analyzed the risk and business impact of mobile computing? *(Verify the risk and business impact analysis reports prepared by management).*			

Sr. No.	Checkpoints	Yes/ No/NA	Remarks/ Explanations	Evi-dences
4.	Whether the organization has an appropriate method of the user authentication? *(Verify and test the user authentication methods)*			
5.	Whether the organization has adequate controls to maintain data integrity? *(Verify the controls for prevention / detection of any change in data while transmission or storage on mobile devices.)*			
6.	Whether the organization has the process for identification of loss or theft of mobile devices and disabling such devices? Is this process implemented?			
7.	Whether respective employees are communicated with the usage of mobile device policies and procedures?			
8.	Whether the organization has reviewed and updated mobile computing policy and procedure at the regular intervals?			
5.5	**Incident Management – Antivirus protection and other incidents**			
1.	Whether antivirus / antimalware software is installed on all servers, desktops and laptops?			

Sr. No.	Checkpoints	Yes/ No/NA	Remarks/ Explanations	Evi-dences
2.	Whether antimalware software is frequently updated? *(Verify the frequency of updates and scans – to be according to the policy and procedure).*			
3.	Whether the organisation reviews logs for antivirus / antimalware update? *(Verify the logs maintained for antivirus update and corrective actions taken based on errors in the log file).*			
4.	Whether the Incident Management Policy documented? *(Incident Management policy and procedures should be established to ensure an appropriate, effective and timely response to security incidents)*			
5.	Whether the Incident Management policy and procedure documents include - Scope and objective - Definition of incident - Incident handling team - Procedure for incident handling - Escalation procedures - Reporting procedures			
6.	Whether the Management has			

Sr. No.	Checkpoints	Yes/ No/NA	Remarks/ Explanations	Evi-dences
	approved Incident Management policy and procedure documents?			
7.	Whether incident response/handling team is identified? Are responsibilities assigned to this team?			
8.	Whether owners are identified for each information asset or service?			
9.	Whether critical assets are identified and appropriate security is available?			
10.	Whether incident response team members are selected with consideration to aspects like - - Qualification and skills - Understanding of known threats, attack signatures, vulnerabilities. - Understanding of enterprise network, security infrastructure and platforms. - Understanding of security response and/or troubleshooting techniques. - Understanding of IS forensic techniques and best practices. - Understanding of regulations and laws as they pertain to privacy, disclosure and evidentiary			

Sr. No.	Checkpoints	Yes/ No/NA	Remarks/ Explanations	Evi-dences
	requirements.			
11.	Whether the incident response team has representatives from key areas like - - Information security - Corporate Communication - Legal - Human Resource - Administration - Business Unit Management and Technology - Corporate Security (incl. Physical Security).			
12.	Whether the management has carried out risk analysis for all information assets? *(Risks like loss of Intellectual property; business interruptions; legal compliances and regulatory requirements should be considered. Information assets like data, servers, workstations, software, data services, protocols etc. should be covered for risk analysis).*			
13.	Whether the IS asset prioritization process has been defined and responsibilities are assigned to prioritise incidents based on risk analysis?			
14.	Whether the incident identification, reporting and notification procedures are			

Sr. No.	Checkpoints	Yes/ No/NA	Remarks/ Explanations	Evi-dences
	clearly defined in the documents?			
15.	Whether the Incident Response and Analysis process includes aspects like – - Technical procedures and recommendations for quickly analyzing systems affected by an incident. - Technical procedures and recommendations for minimizing impact of incident. - Technical procedure for recovery of affected IS assets and services. - Procedures for post-incident analysis report.			
16.	Whether adequate IS assets are available for incident resolution? *(Verify availability of redundant and alternate IS assets for Incident Management)*.			
17.	Whether adequate training is given to the incident response team for prevention, handling and recovery from incidents?			
18.	Whether the organization conducted test drills for Incident Management activities?			

Sr. No.	Checkpoints	Yes/ No/NA	Remarks/ Explanations	Evi-dences
	(Verify the report of test drills for incidents and Corrective actions taken for gaps.)			
19.	Whether the organization review and updates Incident Response policy and procedure documents at regular intervals?			

6. E- commerce

IS Auditor	(Name and Signature)
Auditee	(Name and Signature)
Date(s) of Audit	

Process Objective
• To ensure secured transactions in e-commerce environment, consistent with business objectives.

Sr. No.	Checkpoints/Particulars	Yes/ No/ NA	Remarks/ Explanations	Evidence
1	Do business objectives clearly define E-Commerce requirements?			
2	Do IT Strategic and Tactical plans support the business objectives?			
3	Whether E-commerce policy and procedure documented and implemented?			
4	Is E-commerce policy and procedure approved by management and communicated to all stakeholders?			
5	Whether E-commerce policy and procedure document includes: - Scope and objective - Procedure for user ID creation, approval, review, suspension, and deletion			

Sr. No.	Checkpoints/Particulars	Yes/ No/ NA	Remarks/ Explanations	Evidence
	- Password Management - User access rights assignment & modifications etc. - User deletion - Monitoring access violations - Review and update of document			
6.	Whether the organization follows the principle for segregation of duties in granting access rights for doing transactions on E-commerce? *(Verify Access rights on the need to know and need to do basis.)*			
7.	Whether User IDS are in a unique format? *(Verify the naming conventions for the user IDs)*			
8.	Are invalid log in attempts for doing transactions on E-commerce monitored and User IDs are suspended on specific attempt? *(Verify the parameters set for an unsuccessful log in attempt)*			
9.	Whether the organization follows complex composition for password parameters? *(Complex composition of password parameter should be used as to make it difficult for guess and prevent unauthorized*			

Sr. No.	Checkpoints/Particulars	Yes/ No/ NA	Remarks/ Explanations	Evidence
	user from access).			
10	Is there a policy detailing business strategies and potential types or named partners for E-Commerce?			
11.	Whether the procedure for granting access to third parties for doing transactions on E-commerce is included in the user access management policy and procedure? (The organization should specify process to granting access to the third parties like contractors, auditors, consultants etc.)			
12	Whether a formally designed security framework is in place which covers - Internal security - Non-repudiation of transactions - Confidentiality of information - Positive customer authentication - Application development - End-user (browser security standards and settings.			
13	Whether the company has in place an IS infrastructure that is capable of: - Transaction volumes in line with customer expectations - Expected response times			

Sr. No.	Checkpoints/Particulars	Yes/ No/ NA	Remarks/ Explanations	Evidence
	- Availability - Scalability - Security			
14	Whether a formal process of customer activity monitoring is in place and regular management feedback is facilitated: - Measuring hits (page impressions), - Conversion of “surfers” to customers, monitoring user activities, - Identifying individuals (repeat custom), cookies, - log-in authentication, measuring sales/average volumes			
15	Whether a legal cell is available for all Compliances monitoring function?			

7. Outsourcing

IS Auditor	(Name and Signature)
Auditee	(Name and Signature)
Date(s) of Audit	

Process Objectives

- To ensure information integrity, availability and confidentiality in accordance with contractual requirements.
- To ensure security and maintenance of IS assets.
- To ensure agreed service levels.
- To ensure compliance to legal and regulatory requirements.

Sr. No.	Checkpoints	Yes/ No/NA	Remarks/ Explanations	Evi-dences
7.1	**Vendor Selection**			
1.	Whether Outsourced IS functional strategy / procedure / decisions are documented?			
2.	Whether the above is approved by the Management?			
3.	Whether the organisation has clearly defined its requirements and benefits from the outsourced process? *(Verify the justifications for outsourcing e.g. Savings are more than costs.)*			
4.	Whether the organisation has carried out a review of			

Sr. No.	Checkpoints	Yes/ No/NA	Remarks/ Explanations	Evi-dences
	resultant changes in business operation and possible impact? *(Review the pre and post outsourcing changes in organisation's environment)*			
5.	Whether the organisation has a process for evaluating and selecting a particular vendor? Has this process been complied with? *(Comparative study of vendors should be carried out. It is recommended that at least 3 vendors should be evaluated)*			
6.	Whether the organisation has reviewed proposed vendor for the aspects like – - Financial feasibility / stability - Technical feasibility - Operational feasibility - Support / continuity of services - Legal compliances			
7.2	**Service Level Agreement (SLA)**			
1.	Does the service level agreement include: - Parties to agreement - Definition of service			

Sr. No.	Checkpoints	Yes/ No/NA	Remarks/ Explanations	Evi-dences
	- Period of agreement and renewal clause - Service levels Agreed - Availability, reliability, capacity for growth - Business continuity processes - Disaster recovery / contingency planning - Escalation procedures - Security requirements - Procedure for modification of clauses of agreement - Content and frequency of performance reporting and - Agreed Performance levels - Service improvement commitment - Reporting procedures - Confidentiality - Penalty clauses for non performance or breach - Termination clause - Arbitration / dispute resolution clause - Right to access and right to audit - Security requirements - Legal compliances			
2.	Whether the organization has reviewed requirements			

Sr. No.	Checkpoints	Yes/ No/NA	Remarks/ Explanations	Evi-dences
	of transition plans with respect to - - Additional cost - Contingency plans - Training plans - Hardware and Software - Service levels - Exception / Incident handling procedures and - Legal issues.			
7.3	**Performance monitoring**			
1.	Whether the organization has reviewed performance of vendor against agreed service levels at regular intervals?			
2.	Whether the organization has taken necessary actions / escalated issues for non-performance?			
3.	Whether the organization has reviewed and updated service level agreement at regular intervals for improvements? *(Organization should review SLA at the regular intervals for improvement)*			

8. Information System Acquisition, Development and Maintenance

IS Auditor	(Name and Signature)
Auditee	(Name and Signature)
Date(s) of Audit	

Process Objectives

- To ensure an appropriate acquisition and / or development of information systems including software
- To maintain the information systems in an appropriate manner.

Sr. No.	Checkpoints	Yes/No/ NA	Remarks/ Explanations	Evidences
8.1	**Policy and Procedure**			
1.	Whether information system acquisition and / or development policy and procedure documented?			
2.	Whether system acquisition and / or development policy and procedure approved by the management?			
3.	Whether the policy and procedure cover the following: - Problems faced in the existing system and need for replacement - Functionality of new IS - Security needs - Regulatory compliance			

Sr. No.	Checkpoints	Yes/No/ NA	Remarks/ Explanations	Evidences
	- Acceptance Criteria - Proposed roles and responsibilities - Transition/ Migration to new IS - Interfaces with legacy systems - Post implementation review - Maintenance arrangements.			
4.	Whether policy and procedure documents are communicated / available to the respective users?			
5.	Whether policy and procedure documents are reviewed and updated at regular intervals?			
8.2	**IS (Including software) Acquisition / development and implementation**			
1.	Whether the organization has evaluated requirement and functionalities of proposed IS? *(Verify the* requirement analysis conducted at three levels viz. process level, application level and organization level. *Verify the site visit reports and other customer references obtained with respect to functionalities of proposed IS).*			

Sr. No.	Checkpoints	Yes/No/ NA	Remarks/ Explanations	Evidences
2.	Whether the organization carried out feasibility study in respect of the following - Financial feasibility - Operational feasibility - Technical feasibility			
3.	Whether the selection of vendor and acquisition terms considers the following: - 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.			
4.	Whether the organisation has identified and assigned roles in development activities to appropriate stakeholders? *(Verify the assigned roles should be on "need to know" and "need to basis". and duties of developers and operators are segregated).*			
5.	Whether the organization has a separate			

Sr. No.	Checkpoints	Yes/No/ NA	Remarks/ Explanations	Evidences
	development, test and production environments?			
6.	Whether the IS developed plan is prepared and approved by the management? *(Verify that IS development plan to include:* - *Input data elements,* - *Validations controls viz. Field/ Transactions/ File with appropriate error reporting* - *Process workflow* - *data classifications with security are in place, viz. Read only for users, Read/ Write for authorized persons* - *Output).*			
7.	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			

Sr. No.	Checkpoints	Yes/No/ NA	Remarks/ Explanations	Evidences
8.	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			
9.	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			
10.	If the development activities are outsourced, are the outsourcing activities evaluated based on the following practices: - What is the objective behind Outsourcing? - What are the in-house capabilities in			

Sr. No.	Checkpoints	Yes/No/ NA	Remarks/ Explanations	Evidences
	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.			
8.3	**Maintenance of IS**			
1.	Whether the organization carried out a post implementation review of new IS?			
2.	Whether a process exists for measuring vendors' performance against the agreed service levels?			
3.	Whether the post			

Sr. No.	Checkpoints	Yes/No/ NA	Remarks/ Explanations	Evidences
	implementation review results are documented?			
8.4	**Database controls**			
1.	Whether the policy and procedure documented and approved for database activities?			
2.	Whether the policy and procedure cover the following: - Appointing administrator - Conventions for database creation, storage, naming and archival - Monitoring of triggers and queries to prevent overloading of database - Configured to ensure audit trails, logging of user sessions and session auditing - Reconciliation between source and receiving system in case of interface Review of activities by admin.			
3.	Whether the policy and procedure documents are communicated / available to respective users?			
4.	Whether the policy and procedure documents are reviewed and updated at			

Sr. No.	Checkpoints	Yes/No/ NA	Remarks/ Explanations	Evidences
	regular intervals?			
5.	Whether the organization has assigned administrator and users to database?			
6.	Whether the IS Department has a laid down standards / conventions for database creation, storage, naming and archival?			
7.	Whether the vendor-supplied passwords to the default users changed? *(Verify the removal of demo user, guest users and demo databases removed)*			
8.	Whether the design or schema of tables/ files in database contains fields for recording makers, checkers and time stamp?			
9.	Whether standards are set for database control reports to ensuring accuracy and integrity of the databases? *(Verify the control total / reports like Total of transactions and balances, record counts and hash totals).*			
10.	Whether reconciliation between the source and receiving system for critical information transferred through interface system?			

Sr. No.	Checkpoints	Yes/No/ NA	Remarks/ Explanations	Evidences
8.4	**Application Controls**			
1.	Whether appropriate input controls are established by the organisation for input data? *(Verify the input verification procedures such as assigning Transaction ID, restriction on duplicate entry,* range checks, validity checks, control totals *etc.).*			
2.	Whether corrections are made to rectify differences, exceptions, duplicate transactions, missing transactions and rejected items, are they approved (e.g., maker/ checker, exception report, etc.)?			
3.	If the input of data is through batch upload, does the software have controls to ensure that all the entries in the batch have been uploaded without any omission/ commission (e.g., reconciliation of control totals, etc.)?			
4.	Whether the application prevents the same user from performing both the functions of entering a transaction and verifying the same?			

Sr. No.	Checkpoints	Yes/No/ NA	Remarks/ Explanations	Evidences
5.	Whether the application has adequate controls to ensure that all transactions input have updated the files?			
6.	Whether there are adequate procedures for investigation and correction of differences or exceptions identified by the controls over update for completeness and accuracy?			
7.	Whether controls are adequate for the programmed procedure that generates the data? *(Verify the controls implemented like recalculations (Manual), Editing, Run-to-run totals, and Limit checks etc.).*			
8.	Whether outputs viewed/ generated by users only on need to know basis. *(Check whether outputs cannot be generated by all and sundry users in the system.* Verify the procedure on the generation, distribution, authentication and preservation of outputs).			
9.	Whether appropriate controls are established on data files such as Prior and Later Image, Labeling,			

Sr. No.	Checkpoints	Yes/No/ NA	Remarks/ Explanations	Evidences
	Version and Check Digit/Parity Check.			
10	Whether appropriate controls are established on data integrity such as Domain Integrity, Relational Integrity, Entity Integrity and Referential Integrity.			

9. Data Migration

IS Auditor	(Name and Signature)
Auditee	(Name and Signature)
Date(s) of Audit	

Process Objective

- To ensure the process and actual completeness and integrity of data populated into Target database/application from legacy applications.

Sr. No.	Checkpoints/Particulars	Yes/No /NA	Remarks/ Explanations	Evidence
9.1	**DATA MANAGEMENT AND POLICY**			
1	Whether the data ownership is clearly established?			
2	Whether data users are clearly identified?			
3	Whether formal data classification policies based on data sensitivity exist and have been communicated to users?			
4	Whether a data/system owner has been appointed to make decisions about the classification and user rights?			
5	Whether policies and procedures for data storage, security, transmission, and disclosure reflect needs based upon data classification?			

Sr. No.	Checkpoints/Particulars	Yes/No /NA	Remarks/ Explanations	Evidence
9.2	**DATA QUALITY STRATEGY**			
1	Whether data quality expectations and matrices are established?			
2	Whether data quality risks are identified and assessed?			
3	Whether mitigating controls are identified and implemented?			
4	Whether results are monitored and evaluated?			
9.3	**REGULATORY REQUIREMENTS**			
1	Whether policies and procedures over data access, transmission, and storage comply with privacy, intellectual property, transborder data flow, and cryptographic regulations and requirements?			
2	Whether other relevant regulations and requirements are met?			
9.4	**IDENTIFICATION AND ASSESSMENT OF RISKS**			
1	Whether identification of situations and events that prevent the data quality from achieving the expectations?			
2	Whether assessment of the probability and severity of identified risks?			
9.5	**DATA QUALITY IMPLEMENTATION**			
1	Whether data dictionaries are			

Sr. No.	Checkpoints/Particulars	Yes/No /NA	Remarks/ Explanations	Evidence
	created based on data quality expectations?			
2	Whether the change management process ensures that data integrity is preserved during changes in data structures?			
3	Whether the impact of proposed data structure changes is assessed and reviewed by the management before implementation into production in order to minimize disruptions to operations?			
4	Whether new data structures and modifications to data structures are tested in accordance with test plans that include, as appropriate, interface testing, parallel testing, capacity testing, and user acceptance test?			
5	Whether preventive and detective controls are implemented at the point of data entry?			
6	Whether integrity of data during and after concurrent data access is ensured?			
7	Whether preventive data accuracy controls are implemented throughout data processing?			

Sr. No.	Checkpoints/Particulars	Yes/No /NA	Remarks/ Explanations	Evidence
8	Whether transactional integrity is ensured at all times?			
9	Whether data consistency is ensured among various modules and systems?			
10	Whether naming convention and other data standards are established?			
9.6	**PHYSICAL SECURITY**			
1	Whether the data hosting facility is physically secure?			
2	Whether the back-up storage is physically secure?			
3	Whether data outputs are physically secure?			
9.7	**LOGICAL DATA SECURITY**			
1	Whether the data accessed on the least privilege basis as established by the data owner?			
2	Whether clear definition of data access matrix is established?			
3	Whether access privileges are periodically reviewed by data owners?			
4	Whether authorized access to sensitive data is logged and the logs are regularly reviewed to assess whether the access and use of such data was appropriate?			

Sr. No.	Checkpoints/Particulars	Yes/No /NA	Remarks/ Explanations	Evidence
5	Whether unauthorized access attempts are detected?			
6	Whether encryption is used for sensitive and/or proprietary data?			
7	Whether authentication mechanism, such as passwords and tokens, are required for data access?			
8	Whether the security administrator is notified of employees who have changed roles and responsibilities, transferred, or been terminated and access privileges of such employees immediately changed to reflect their new status?			
9.8	**DATA BACKUPS AND RECOVERY**			
1	Whether the data is regularly backed up?			
2	Whether ongoing readability of backup and retained data is tested periodically through restoration or other methods?			
3	Whether the removable media is labeled to enable proper identification?			
4	Whether the data are destroyed in accordance with expiration dates, as directed in the data retention policy?			

Sr. No.	Checkpoints/Particulars	Yes/No /NA	Remarks/ Explanations	Evidence
9.9	**DATA TRANSFERS**			
1	Whether header/trailer records are utilized and include record counts and hash totals and the recipient system checks that the number of records received and the amounts within them match the trailer record counts?			
2	Whether all failed updates and incomplete transactions are written to an error file, reviewed, and resolved on a timely basis?			
3	Whether exception reports identify out-of-balance or missed data after all transfers?			
4	Whether detailed logs are produced documenting the transfer sessions, including parameters used?			
9.10	**TRANSACTION INTEGRITY**			
1	Whether the originator of a transaction is validated?			
2	Whether the user connects to valid destination?			
3	Whether only valid data are exchanged?			
4	Whether tracking functionality is provided to allow both parties to monitor the status of a transaction?			

Sr. No.	Checkpoints/Particulars	Yes/No /NA	Remarks/ Explanations	Evidence
5	Whether the transaction fulfillment is verified for accuracy?			
6	Whether all transactions are recorded in proper period?			
7	Whether exception reports and notices are reviewed and resolved on a timely basis?			

10. BCM (Business Continuity Management)

IS Auditor	(Name and Signature)
Auditee	(Name and Signature)
Date(s) of Audit	

Process Objectives

- To ensure the uninterrupted availability of all key business resources required to support essential (or critical) business activities.
- 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 compliance and,
- To sustain operations so that customer service and corporate image can be maintained.

Sr. No.	Checkpoints/ Particulars	Yes/No/ NA	Remarks/ Explanations	Evidences
10.1	**Policy and procedure**			
1.	Is business continuity plan documented and implemented?			
2.	Whether the scope and objectives of BCM are clearly defined in the policy document? *(Scope to cover all critical activities of business. Objectives should clearly spell out outcomes of BCM).*			
3.	Are the policy and procedure documents			

Sr. No.	Checkpoints/ Particulars	Yes/No/ NA	Remarks/ Explanations	Evidences
	approved by Top management? *(Verify sign off on policy and procedure documents and budget allocations made by management for BCM).*			
4.	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).*			
5.	Are users involved in preparation of business continuity plan? *(Managerial, operational, administrative and technical experts should be involved in the preparation of BCP and DRP).*			
6.	Does the policy and procedure documents include the following ○ List of critical information assets ○ List of vendor for service level			

Sr. No.	Checkpoints/ Particulars	Yes/No/ NA	Remarks/ Explanations	Evidences
	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 DRP plans ○ Recovery procedure to minimize losses and interruptions in business operations ○ Disaster recovery teams ○ Training and test drills Compliance with statutory and regulatory requirements			
7.	Are BCM policy and procedures circulated to all concerned? *(Verify availability and circulation of BCP & DRP to all concerned, including onsite and offsite storage).*			
8.	Is the business continuity plan updated and			

Sr. No.	Checkpoints/ Particulars	Yes/No/ NA	Remarks/ Explanations	Evidences
	reviewed regularly? *(Verify Minutes of meeting where policy and procedures are reviewed. Verify amendments made to the policy and procedure documents due to change in business environment).*			
10.2	**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 threat / vulnerability review carried out by 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*			

Sr. No.	Checkpoints/ Particulars	Yes/No/ NA	Remarks/ Explanations	Evidences
	controls mitigating the risk)			
5.	Has the organisation taken an appropriate decision on risks identified? *(Verify the decision-making on the options - accepted, reduced, avoided or transferred – for the risks identified).*			
6..	Are the risk assessment carried at regular interval? *(Verify the review frequency.)*			
10.3	**Business Impact Analysis**			
1.	Does the organization carry out business impact analysis for business operations?			
2.	Has the organization identified a BIA Team?			
3.	Are RTO and RPO defined by the management?			
4.	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.).*			
5.	Is the business impact			

Sr. No.	Checkpoints/ Particulars	Yes/No/ NA	Remarks/ Explanations	Evidences
	analysis carried at regular interval?			
10.4	**Development & Implementation of BCP & DRP**			
1.	Has the organisation prioritised recovery of interrupted business operations? *(Prioritization of activities is based on RTO and RPO).*			
2.	Has the organisation identified various BCP & 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 BCP document(s) include the following? ○ Scope and objective. ○ Roles and responsibilities of BCP and DRP Teams. ○ Incident declaration. ○ Contact list.			

Sr. No.	Checkpoints/ Particulars	Yes/No/ NA	Remarks/ Explanations	Evidences
	○ 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. ○ Back up and restore procedures. ○ Offsite operating procedures			
5.	Are the copies of up-to-date BCM 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			

Sr. No.	Checkpoints/ Particulars	Yes/No/ NA	Remarks/ Explanations	Evidences
	and document backup and restoration procedures? *(Verify the backup and restoration schedules adopted by organisation)*			
9.	Are logs for backup and restoration maintained and reviewed? *(Verify the logs maintained and review of the same by 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).*			
10.5	**Maintenance of BCP & DRP**			
1.	Whether the business continuity plan is tested at regular interval?			
2.	Has the organization reviewed gap analysis of testing results?			

Sr. No.	Checkpoints/ Particulars	Yes/No/ NA	Remarks/ Explanations	Evidences
	(Review process that includes a comparison of test results to the planned results.)			
3.	Has the organisation got a testing plan? (*Verify copy of test plan and updates)*			
4.	Are test drills conducted at appropriate intervals?			
5.	Do organisation documents and analyses have testing results? *(Verify the corrective copies of test results and analysis the report)*			
6.	Has the organization prepared action points to rectify the testing results? *(Verify the corrective action plan for all problems encountered during test drill)*.			
7.	Does the organisation carry out retesting activity for action points? *(Verify the evidences of retesting activities)*.			
8.	Does the organisation review BCP and DRP at regular intervals?			
9.	Whether a review of BCM includes following?			

Sr. No.	Checkpoints/ Particulars	Yes/No/ NA	Remarks/ Explanations	Evidences
	○ BCM policy and procedure ○ Scope and exclusion of BCM ○ 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			

11. Compliance and Legal Requirements

IS Auditor	(Name and Signature)
Auditee	(Name and Signature)
Date(s) of Audit	

Process Objective

- To ensure compliance to statutory, regulatory, contractual and internal requirements

Sr. No.	Check points	Yes/ No/NA	Remarks/ Explanations	Evidences
11.1	**Statutory and regulatory requirements**			
1	Whether the organization has identified the applicable statutory and regulatory requirements?			
2.	Whether responsibilities are identified, assigned and communicated for compliances?			
3.	Whether compliance to statutory and regulatory requirements is reviewed at regular intervals?			
4.	Whether any non-compliance is observed? If so whether corrective actions are taken up and completed?			
5.	Whether the organization monitors have any changes in statutory and			

Sr. No.	Check points	Yes/ No/NA	Remarks/ Explanations	Evidences
	regulatory requirements?			
11.2	**Contractual Requirements**			
1.	Whether the organization has listed down all contractual commitments to be honored?			
2.	Whether the organization has failed in honoring any commitment in the contract?			
3.	Whether the organization has taken and completed the corrective actions against the violation of any contractual requirements?			
4.	Whether the organization reviews compliance with contractual requirements at regular intervals?			

Annexure II – Formats and Templates

1. Engagement Letter

Purpose

Engagement letters are often used for individual assignments or for setting the scope and objectives of a relationship between external IS audit and an organisation.

Content

The engagement letter should clearly address the three aspects of responsibility, authority and accountability. Aspects to consider are set out in the following paragraphs.

(i). Responsibility

- Scope
- Objectives
- Independence
- Risk assessment
- Specific auditee requirements
- Deliverables

(ii). Authority

- Right of access to information, personnel, locations and systems relevant to the performance of the assignment
- Scope or any limitations of scope
- Evidence of agreement to the terms and conditions of the engagement

(iii). Accountability

- Intended recipients of reports

- Auditee rights
- Quality reviews
- Agreed completion dates
- Agreed budgets/fees if available

2. Audit Report

Auditee
Organization :
Location / Address :
Area/Process/Function :
Process Owner / Coordinator :
Background : - Business : - IS Environment

Audit	
Scope :	
Methodology :	
Executive Summary :	
Conclusions & Road Map :	

Audit Findings

No.	**Observations / Findings**	**Requirements**	**Recommendations**
1.			
2.			
3.			
4.			

Audit Record
List of personnel interviewed :
List of evidences verified / obtained :

Report Sign-Off

No.	Auditor	Auditee	Date(s)
1.	(Name and Signature)	(Name and Signature)	
2.			
3.			
4.			

Audit Report Distribution		
1.	(Name)	(Designation)
2.		
3.		
4.		

3. Disclaimer

This report depends upon the correctness, consistency and completeness of the information received by (IS Auditor's Organization name). Various observations / findings concluded in this report are based on the information provided to (IS Auditor's Organization name) by the Organization. Initiation of any action based on this report is the responsibility of the Organization and (IS Auditor's Organization name) is not responsible for such actions / absence of actions and resultant effects. The report is given for the internal use of the Organization and may not be given to any external agency / entity / persons nor (IS Auditor's Organization name) is responsible to them in any manner.

4. Risk Assessment

Sr. No.	Threats	Vulnerabilities	Asset category e.g. Software/ Hardware/ Infrastructure/ Networking/ People/ Data	Risk Level considering Existing Controls					Risk Level considering Proposed Controls				Risk Acceptable? Y / N	Recommended Risk treatment
				Asset Value e.g. High (3), Medium (2), Low (1)	Business Impact Value e.g. High (3), Medium (2), Low (1)	Likelihood of occurrence e.g. High (3), Medium (2), Low (1)	Risk Score = AV X BIV X LO	Risk % = Risk score /Total Risk Score value	Proposed controls	Likelihood of occurrence e.g. High (3), Medium (2), Low (1)	Risk Score = AV X BIV X LO	Risk % = Risk score /Total Risk value		
1	Theft	Lack of adequate monitoring												
2.	Fire	1. Lack of / Non-functioning of electrical safety measures 2. Inadequate / non-functioning of smoke / heat detectors 3. Inadequate / non-functioning of fire suppression systems												
3.	Legal liability	1.Inadequate knowledge of geographies / local laws 2.Contractual Obligations												
4.	Non-availability of Personnel	1. Inadequate policies / communication 2. Health condition of employees 3. Unsafe conditions / Non-availability of canteen supplies 4. Inadequate transport facilities												

5. Auditing Guidelines

I. ISACA

ISACA (*Information Systems Audit and Control Association) is* a globally recognized Information system organisation. ISACA is a global leader in information governance, control, security and audit. ISACA developed the following to assist IS auditor while carrying out an IS audit.

1. IS auditing standards: ISACA issued 16 auditing standards which defines the mandatory requirements for IS auditing and reporting.

2. IS auditing guidelines: ISACA issued 39 auditing guidelines which provide a guideline in applying IS auditing standards.

3. IS auditing procedures: ISACA issued 11 IS auditing procedures which provide examples of procedure an IS auditor need to follow while conducting IS audit for complying with IS auditing standards.

4. COBIT (Control objectives for information and related technology): is a framework containing good business practices relating to information technology.

Details regarding ISACA are available on website http://www.isaca.org

II. ISO 27001

ISO 27001 (Information Security Management-Specification with Guidance for Use) a global standard issued by ISO (The International Organization for Standardization) and IEC (The International Electro technical Commission) in October 2005. It helps to establish and maintain an effective information management system, using a continual improvement approach. It implements OECD (Organization for Economic Cooperation and Development) principles, governing security of information and network systems. ISO/ IEC 27001:2005 is designed to ensure the selection of adequate and proportionate security controls that

protect information assets and give confidence to interested parties. IT helps organizations in identification and clarification of existing information security management, formulating security requirements and objectives, managing security risks in cost effectively manner, to ensure compliance with laws and regulations, to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons and implementation of business-enabling information security.

Details regarding ISO 27001 are available on website http://www.27001-online.com

III. IIA

IIA (The Institute of Internal Auditors) is an international professional association. This association provides dynamic leadership for the global profession of internal auditing. IIA issued Global Technology Audit Guide (GTAG). GTAG provides management of organisation about information technology management, control, and security and IS auditors with guidance on different information technology associated risks and recommended practices. Following is the list of GTAG developed by IIA.

GTAG 1**:** Information Technology Controls

GTAG 2: Change and Patch Management Controls: Critical for Organizational Success

GTAG 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment

GTAG 4: Management of IT Auditing

GTAG 5: Managing and Auditing Privacy Risks

GTAG 6: Managing and Auditing IT Vulnerabilities

GTAG 7: Information Technology Outsourcing

GTAG 8: Auditing Application Controls

GTAG 9: Identity and Access Management

Details regarding IIA are available on website http://www.theiia.org

IV. ITIL

ITIL (IT Infrastructure Library) is the best practice in IT Service Management, developed by OGC and supported by publications, qualifications and an international user group. It gives a detailed description of a number of important IT practices with comprehensive checklists, tasks and procedures that can be tailored to any IT organization. ITIL provides a systematic and professional approach to the management for IT services. ITIL consists of a series of books giving guidance on the provision of quality IT services, and on the accommodation and environmental facilities needed to support IT. ITIL has been developed in recognition of organisations' growing dependency on IT and embodies the best practices for IT Service Management.

Details regarding ITIL are available on website http://www.itil-officialsite.com

ANNEXURE III - Glossary and Abbreviations

A. Glossary

1 Audit charter: The audit charter is a document which addresses the four aspects of purpose, responsibility, authority and accountability of IS audit functions.

2 Audit Evidence: Audit evidence is any information used by the IS Auditor to determine whether the entity or data being audited follows the established audit criteria or objectives.

3 Audit Methodology: Audit Methodology is the set of procedures to perform the scheduled audit and achieve the audit objectives.

4 Audit Plan: An audit plan is a detailed outline of the auditor's plans and procedures in conducting an audit.

5 audit risk: The risk of reaching an incorrect conclusion based on the audit findings.

6 Business Continuity Management: Business Continuity Management (BCM) refers to the activities required to keep your organization running, even during a period of interruption of normal operations.

7 Business Continuity Plan (BCP): Business Continuity Plan (BCP) is a collection of procedures and information which is developed, compiled and maintained in readiness for use in the event of an emergency or disaster.

8 Business continuity team: A team responsible for preparation and update of BCM policies and procedures, BCP and DRP.

9 Business Impact Analysis: Business Impact Analysis means quantification of identified risks on the continuity of business operations.

10 Cold site: It is a site equipped with environmental infrastructure. It is ready to receive the required equipment to carry out operation in the event of disaster.

11 Control Risk: Control risk is the risk that an error which could occur in an audit area, and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system.

12 Data Centre: A Data Centre is a centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business.

13 Data File Controls: Controls on the data files in the application system

14 Data Integrity Testing Controls: Controls that ensure integrity of the data in the application system.

15 Data mapping: Data mapping is the process of creating data element mappings between two distinct data models.

16 Data migration: data migration is "the transferring of data between storage types, formats or computer systems… it is required when organizations or individuals change computer systems or upgrade to new systems."

17 Data migration plan: The migration plan, is the end deliverable of the planning step and serves as the blueprint for the migration implementation, specifying customer expectations, defining project deliverables, and identifying migration methodologies to be used.

18 Detection risk: Detection risk is the risk that the IS auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors.

19. Disaster Recovery Plan (DRP): Disaster Recovery Plan (DRP) is a document which guides an organization for the process of rebuilding operation or infrastructure after the disaster has occurred.

20. e-commerce: e-commerce as the processes by which organisations conduct business electronically with their customers, suppliers and other external business partners, using the Internet as an enabling technology.

21 Evacuation team: It is the team which is responsible for evacuation of the people and critical IT assets at safe location.

22 Hot Site: It is a site equipped with the computer, network, software, telecommunications and environmental infrastructure required for recovering critical business operations.

23 Incident response team: It is the team which is designed to receive the information about every incident that can be considered as threat to assets/operations.

24 Inherent risk: Inherent risk is the susceptibility of an audit area to error which could be material, individually or in combination with other errors, assuming that there were no related internal controls.

25 Input controls: Controls that ensure all data from sources are fed into the application system.

26 IT General Controls: IT General Controls are those controls that are pervasive to all systems, processes, and data for any organization or IT environment.

27 Logical Security: Logical Security means unique user ID and password access, authentication, access rights and authority levels, which should be able to safeguard the organization's systems.

28 Media communication team: A team which communicates the information regarding disaster to outside organizations. This team communicates information on disaster to insurance company, news papers agencies, new channels and other media.

29 Mobile site: It is a trailer with specific recovery needs such as computers, workstations, telephone, electrical power, office facilities, etc.

30 Multi-tier migration: Multi-tier migration is a migration in which data is migrated to different tiers of the hierarchy based on a best fit between data/application requirements and storage tier attributes.

31 Offsite operation team: A team working at offsite location. This team is responsible for security of offsite, testing of offsite, restoration of back up and supports the continuity or operations in the event of disaster or major interruption.

32 Output Controls: Controls that ensure correct outputs from the application system.

33 Passwords: Passwords in the authentication key to login into the system.

34 Processing Controls: Controls that ensure correct processing of all data input into the application system.

35 Reciprocal agreement: It is an agreement between two or more organisations with similar equipment or applications, to provide computer time to each other in the case of disaster. Even though, this can be a least cost option, it may not work at all if the agreed organisations face the disaster at the same time.

36 Recovery Point Objective (RPO): RPO (Recovery Point Objective) means the amount of data lost measured in time.

37 Recovery team: It is the team primarily responsible for recovery of IS information and assets.

38 Recovery Time Objective (RTO): RTO means the timescale within which the business operations need to be restored following an interruption.

39 Redundant site: It is a site fully equipped with all resources necessary for recovery of operations in case there is a disaster.

40 SDLC: SDLC is a process which begins with, how new systems or modifications to the current systems are requested, prioritized, actually designed, development of the source code to perform the functions desired, testing of the system developed

and/or modified, training of employees to use the new/modified system, and the final system implementation.

41 Single-tier migration: Single-tier migration is a migration in which all source data is migrated onto one or more devices within a single tier, which is also primary storage.

42 Split site: Large organisation operates from multiple locations. In the event of a disaster to one site, operations would simply shift to the other.

43 Warm site: It is a site equipped with some network connection, communications interfaces, electricity supply, environmental conditioning and hardware devices like disk drives, tapes, communication equipment, environmental conditioning, but without a main computer.

B. Abbreviations

1	**AMC**	Annual Maintenance Contracts
2	**ATM**	Automatic Teller Machine
3	**B2B**	Business-To-Business
4	**B2C**	Business-To-Customer
5	**BCM**	Business Continuity Management
6	**BCP**	Business Continuity Plan
7	**BIA**	Business Impact Analysis
8	**CA**	Certificate Authority
9	**CAAT**	Computer Assisted Auditing Technique
10	**CCTV**	Closed Circuit Television
11	**CIS**	Continuous and Intermittent Simulation
12	**COBIT**	Control Objectives for Information Technology
13	**CRL**	Certificate Revocation List
14	**DBA**	Database Administrator
15	**DG Set**	Diesel Generator Set

16	**DRP**	Disaster Recovery Plan
17	**EAM**	Embedded Audit Modules
18	**EDI**	Electronic Data Interchange
19	**EDP**	Electronic Data Processing
20	**EFT**	Electronic Fund Transfer
21	**ERP**	Enterprise Resource Planning
22	**GTAG**	Global Technology Audit Guide
23	**ICAI**	The Institute of Chartered Accountants of India
24	**IEC**	The International Electro technical Commission
25	**IIA**	The Institute of Internal Auditors
26	**IS**	Information System
27	**ISACA**	Information Systems Audit and Control Association
28	**ISO**	The International Organization for Standardization
29	**ISP**	Internet Service Provider
30	**IT**	Information Technology
31	**ITF**	Integrated Test Facilities
32	**ITGC**	Information Technology General Controls
33	**ITGI**	The IT Governance Institute
34	**ITIL**	IT Infrastructure Library
35	**NCDC**	National Climatic Data Centre, USA
36	**NOC**	Network Operations Center
37	**OS**	Operating system
38	**PCAOB**	Public Company Accounting Oversight Board
39	**PDA**	Personal Digital Assistant
40	**RA**	Registration Authority
41	**RPO**	Recovery Point Objective

42	**RTO**	Recovery Time Objective
43	**SCARF**	Systems Control Audit Review File
44	**SDLC**	System Development Life Cycle
45	**SEC**	Securities and Exchange Commission
46	**SLAs**	Service Level Agreements
47	**SOX**	The Sarbanes-Oxley Act, 2002
48	**Sysadmin**	System Administrator
49	**UPS**	Uninterrupted Power Supply
50	**VPN**	Virtual Private Network
51	**WLAN**	Wireless local Area Networks