MODULE II

ISA

INFORMATION SYSTEMS AUDIT 2.0 COURSE

INFORMATION SYSTEMS ASSURANCE SERVICES

BACKGROUND MATERIAL

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

Background Material
On
Information Systems Audit 2.0 Course

Module 2: Information Systems Assurance Services (13%)

The Institute of Chartered Accountants of India

(Set up by an Act of Parliament)

New Delhi

Note: There are six other modules which form part of ISA Background Material

DISCLAIMER

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

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

Revised Edition	:	July 2015
Committee/Department	:	Committee of Information Technology
E-mail	:	cit@icai.org
Website	:	www.icai.org/http://cit.icai.org
Price	:	₹ 750/- (For Module - I to Module VII, Including DVD)
ISBN	:	978-81-8441-335-9
Published by	:	The Publication Department on behalf of the Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi-110 002.
Printed by	:	Finesse Graphics & Prints Pvt. Ltd. Tel.: 022-4036 4600 Fax : 022-2496 2297

Foreword

Information technology (IT) plays a vital role in supporting the activities of any organisation. The growth and change that has come about as a result of developments in technology have important implications. At the same time the increasing use of IT has also led to e-crimes like cyber warfare, hacking, data thefts, DDoS (Distributed Denial of Service) and other computer related frauds. Subsequently, there are various e-Governance, regulatory and compliance issues which are required to be looked into. These technological changes have put more focus on the role performed by Chartered Accountants, especially in the field of Information Systems Audit.

For Chartered Accountants there exist opportunities in Auditing and Assurance as well as consulting areas. Chartered Accountants with their expertise in data and indepth understanding of systems and process functions are uniquely suited for providing consulting in control implementation of IT enabled services as well as review of the same. IT by default rather than by design has become critically relevant for CA firms.

The Committee on Information Technology (CIT) of the Institute of Chartered Accountants of India (ICAI) was established to identify the emerging professional opportunities in the IT sector. It has also been conducting post qualification course on Information Systems Audit thus providing vast opportunities to Chartered Accountants. In view of the dynamism of the sector, a revised edition of the background material for the post qualification course on Information Systems Audit is being brought up by the CIT.

The background material contains various practical aspects, new technologies along with case studies related to Information Systems Audit, which will make this a great learning guide. I appreciate the efforts put in by CA. Rajkumar S. Adukia, Chairman, CA. Atul Kumar Gupta, Vice Chairman, other members and officials of CIT and faculty for bringing out the revised background material.

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

Best Wishes

CA. Manoj Fadnis
President, ICAI

Preface

Information Technology has now emerged as the Business Driver of choice by Enterprises and Government Departments to better manage their operations and offer value added services to their clients/citizens. We now find increasing deployment of IT by enterprises and governments alike in geometric progression.

While the increasing deployment of IT has given immense benefits to enterprises and government departments, there have been increasing concerns on the efficiency and effectiveness of the massive investments made in IT, apart from the safety and security of Information Systems themselves and data integrity. As enterprises are increasingly getting dependent on IT Resources to manage their core business functionality, there are also concerns of Business Continuity.

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

The updated course material has taken into consideration the latest curriculum of similar professional courses and the recent/emerging developments in the field of Information Technology and IS Auditing and has been updated taking into consideration all the suggested changes and encompasses existing modules, contents and testing methodology.

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

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

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

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

CA. Rajkumar S. Adukia
Chairman
Committee on Information Technology

Table of Contents

INFORMATION SYSTEMS ASSURANCE SERVICES SECTION 1 : OVERVIEW

CHAPTER 1: CONCEPTS OF IS AUDIT

1.1 Learning Objectives 3

1.2 Introduction 3

1.3 Definitions 3

1.4 Concepts of Audit 5

1.5 Concept of IS Audit and Auditing in a Computerised Environment 6

1.5.1 Audit in a computerised environment 6

1.5.2 IS Audit (Auditing of the computerised environment) 6

1.6 Concept of IT Risk 7

1.6.1 IT Risk in the Risk Hierarchy 7

Risk Management 8

1.7 Risk Based Auditing 8

1.8 Audit Risk and Materiality 9

1.8.1 Audit Risk 9

1.8.1 Materiality 10

1.9 Concepts of Internal Control 12

1.9.1 Types of Internal Controls 12

1.9.2 Types of IS Controls 13

1.10 Organisation of IS Audit Function 14
1.10.1 Infrastructure and Organisation 14
1.10.2 Internal and external audit control framework 14
1.10.3 Quality Assessment and Peer Reviews 15
1.10.4 Standards on Audit Performance 15
1.11 Summary 16
1.12 Questions 16
1.13 Answers and Explanations 18

CHAPTER 2: IS AUDIT IN PHASES

2.1 Learning Objectives 21
2.2 Introduction 21
2.3 Conducting an IS Audit 22
2.3.1 Setting up of audit objectives 22
2.3.2 Request for Proposal and submitting response 22
Request for proposal (RFP) 22
Response to RFP 23
2.4 Audit Charter and Terms of Engagement 24
2.4.1 IS Audit Charter 24
2.4.2 Audit Engagement Letter 25
2.4.3 Communication with Auditee 26
2.4.4 Quality Assurance Process 27
2.5 Audit Scope 27
2.6 Audit Planning 28
2.7 Objectives of IS Controls 30

2.7.1 Principles of Fiduciary 30
2.7.2 Principles of Quality 31
2.7.3 Principles of Security (CIA) 31
2.8 Understanding the Auditee Environment 32
2.8.1 Business of the Entity 32
2.8.2 Organisation Structure 32
2.8.3 IT Infrastructure 33
2.8.4 Regulations, Standards and Frameworks 33
Information Technology Act 2000 (Amended in 2008) 33
Sarbanes Oxley Act, 2002 (SOX) 34
Public Company Accounting Oversight Board (PCAOB) 34
Clause 49 – Listing Agreement on Corporate Governance 34
ISO 27000 Family 35
2.9 Standards, guidelines and best practices of IS Audit 35
2.9.1 ITAF 35
2.9.2 COBIT 5 Framework: Principles, Enablers, Processes, Assurance 36
2.10 Risk Assessment 39
2.10.1 Guidance on risk assessment by ISACA 40
2.10.2 Risk Management steps 41
Collect Data 41
Analyse Risk 41
2.10.3 Risk Assessment procedures and related activities 42
2.10.4 Use of Risk Assessment in Audit Planning 42

2.11 Governance and Management Controls 43
2.11.1 IT General Controls areas 43
Operating System controls 43
Organisational controls 43
Management Controls 46
Financial Controls 47
Data management controls 48
Organisational structure controls 48
Data Processing Controls 48
Physical Access Controls 48
Logical Access Controls 48
System development controls 49
Business Continuity Planning Controls 49
System maintenance controls 49
Computer Centre security controls 49
Internet and Intranet controls 49
Personal computers controls 49
Audit Trails 50
2.11.2 IT Application Controls types 50
1. Boundary Controls 50
2. Input Controls 51
3. Processing Controls 51
4. Data file controls 52
5. Output Controls 52

2.11.3 Scope and steps of IS Audit of Application software 52
2.12 Creation of Risk Control Matrix 54
2.13 Audit Sampling, Data Analysis and Business Intelligence 55
2.13.1 Audit Sampling 55
2.13.2 Data Analysis 56
2.13.3 Business Intelligence 56
2.13.4 Analytical Review Procedures: CAAT Tools 56
Analytical Review Procedures 56
CAATs 57
2.14 Compliance Testing 60
2.15 Substantive Testing 61
2.16 Design and Operational effectiveness 61
2.16.1 Design Effectiveness 61
2.16.2 Operational Effectiveness 62
2.17 Audit Evidence: Methods 63
2.17.1 Evaluating audit evidence 63
2.17.2 Types of evidence 64
2.17.3 Types of Audit Evidences 64
2.17.4 Evidence preservation 65
2.17.5 Standards on evidence 65
Standards by ICAI 65
Standards by ISACA 65
2.18 Audit Documentation 67
2.19 Using work of another auditor and expert 70

2.20 Evaluation of strengths and Weaknesses: Judging by materiality 72

2.20.1 Judging the materiality of findings 72

2.21 Risk Ranking 73

2.22 Audit Report Structure and contents 73

2.22.1 Audit report structure and contents 75

2.23 Management Implementation of recommendations 76

2.24 Follow up review 76

2.25 Summary 77

2.26 Questions 78

2.27 Answers and Explanations 79

CHAPTER 3: IT ENABLED SERVICES

Learning Objectives 81

3.1 Introduction 81

3.2 Classification of Audits 81

3.3 IT Enabled Services 83

3.4 Fraud 85

3.4.1 Fraud Detection 85

3.4.2 Cyber fraud Investigation 87

3.4.3 Cyber Forensics: Digital Forensics 89

3.4.4 Fraud investigation tools and techniques 90

3.4.5 Some Case Studies of frauds and lessons 90

Case Study 1: The WorldCom fraud 90

Case Study 2: The $54 million fraud 91

Case Study 3: The Satyam Fraud 91

3.4.6 Overview of lessons learned 91
3.5 Summary 92
3.6 References 92
3.7 Questions 92
3.8 Answers and Explanations 94

SECTION: 2 APPENDIX

CHECKLISTS AND OTHER RELATED MATERIALS

Reference material (available in DVD only) 97
Useful checklists (available in DVD only) 97
Useful checklists available as soft copy in DVD and in section 3: Appendixes 1 to 6 97

APPENDIX 1: RFP FROM BANK FOR IS AUDIT OF APPLICATION SOFTWARE 98

APPENDIX 2: RESPONSE TO RFP FOR LOGICAL ACCESS CONTROLS REVIEW OF SAP

Introduction 99
The Client Company (Max Infotech) 99
IS Assurance and Consulting Firm 99
Background 99
Objective of SAP Review 99
Need for SAP review 100
Need for Logical Access Controls Review of SAP 100
Understanding the need 100
Methodology for executing the Assignment 100

Primary Objective 100
Scope and Terms of Reference 101
Our Approach/Methodology 101
Audit Approach 101
Structured Methodology 101
Audit plan 102
Audit Program\Procedures 102
Assignment Team 103
Logistic arrangements 103
Infrastructure Required 103
Documentation Required 104
Estimated Timeframe, Deliverables and Fees 104
Deliverables 104
Time Frame 104
Fees 104
Out of pocket expenses 105

APPENDIX 3: SAMPLE IS AUDIT FINDING

Logical Access Controls Review of Operating System 106
1. System Users have blank user-id 106
2. PQR Computer is networked to other office computers 106

APPENDIX 4: CAAT REPORT USING SQL

Sample results of using CAAT 107

Users available with Invalid employee codes 107

Past employees having ID in user table 107

Transactions with amount as Null in FA Trans_table 107

APPENDIX 5: SAMPLE IS AUDIT REPORT

Objectives of the Assignment 109

Proposed Scope of Review/Terms of Reference 109

Our Approach/Methodology 109

Audit Environment 110

Audit Reports 110

Overall Conclusions 110

Security and Access Controls 111

Business Process Controls 111

Further Action 111

APPENDIX 6: QUESTIONNAIRE FOR PROVIDING ASSURANCE SERVICES IN E-COMMERCE 112

INTRODUCTION TO BACKGROUND MATERIAL

Need for DISA 2.0 Course

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

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

Need for updation to DISA 2.0 course

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

Objective of updated DISA Course

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

Objective of updated DISA Course Material

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

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

Use of structured approach

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

Overall Objectives

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

Course Coverage

The DISA Course will provide basic understanding of how information technology is used and deployed. It facilitates understanding of how an IS Auditor is expected to analyse, review, evaluate and provide recommendations on identified control weaknesses in different areas of technology deployment. However, it is to be noted that the DISA course is not oriented towards teaching fundamentals of technology. The DISA course is conducted through a good blend of e-learning (online and facilitated), classroom training, hands-on training with practical case studies and project work to ensure practical application of knowledge. The DISA course combines technology, information assurance and information management expertise that enables a DISA to become trusted Information Technology advisor and provider of IS Assurance services. The DISA with

the unique blend of knowledge would serve as the "bridge" between business and technology leveraging the CA's strategic and general business skills. The class room training has been supplemented with hands on training. Aspiring DISAs need to remember that the class room training is not expected to be comprehensive but as aid to facilitate understanding. Considering the extensive coverage of the course, duration and the diverse level of participants, the faculty will not be able to cover the material indepth. **Please read the background materials of the specific modules prior to attending the classes to derive maximum benefit from the class room training.**

DISA Certification

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

DISA Course : Basic competency requirements

After successful completion of the course, the DISA candidates will have conceptual clarity and will demonstrate basic competency in the following key areas:

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

Modules of the DISA Course

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

No.	Name of Module	(%) Q's
1	Primer on Information Technology, IS Infrastructure and Emerging Technologies	20
2	Information Systems Assurance Services	13
3	Governance and Management of Enterprise Information Technology, Risk Management and Compliance Reviews	13
4	Protection of Information Systems Infrastructure and Information Assets	20
5	Systems Development: Acquisition, Maintenance and Implementation.	14
6	Business Applications Software Audit	13
7	Business Continuity Management	7

Learning Objectives

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

The key learning objectives are:

1. Demonstrate understanding of functioning of key components of existing and emerging information technology and their practical deployment.
2. Provide IS assurance or IT Enabled services and perform effective audits in a computerised environment by using relevant standards, guidelines, frameworks and best practices.
3. Evaluate structures, policies, procedures, practices, accountability mechanisms and performance measures for ensuring Governance and management of Information Technology, risk management and compliance as per internal and external stakeholder requirements.
4. Provide assurance, consulting or compliance services to confirm that enterprise has appropriate security and controls to mitigate risks at different layers of technology as per risk management strategy.
5. Provide assurance or consulting services that the management practices relating to systems development: acquisition, maintenance and implementation are appropriate to meet enterprise strategy and requirements.

6. Provide assurance or consulting services to validate whether required controls have been designed, configured and implemented in the application software as per enterprise and regulatory requirements and provide recommendations for mitigating control weaknesses as required.
7. Provide assurance or consulting services to confirm whether the Business continuity management strategy, processes and practices meet enterprise requirements to ensure timely resumption of IT enabled business operations and minimise the business impact of a disaster.
8. Plan and perform IS assurance or consulting assignments by applying knowledge learnt by presenting project assignment relating to allotted case study to confirm understanding.

Skill Levels

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

Weightage and category of skills

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

Summary of revised DISA Training

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

Key highlights of DISA training

DISA Training includes e-Learning, hands on Training, project work in addition to classroom lectures.

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

DISA 2.0 Course Background Material

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

DISA 2.0 Course DVD

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

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

Feedback and updates

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

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

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

Committee of Information Technology, ICAI

Module 2:

Information Systems Assurance Services

Section 1: Overview

SECTION 1: CONTENTS
CHAPTER 1: CONCEPTS OF IS AUDIT

1.1 Learning Objectives

The objective of this chapter is to provide sufficient knowledge about the fundamental concepts of information systems audit. This chapter provides insight into all the key concepts relating to IS audit such as IS Audit methodology, enterprise risk management, risk based auditing, materiality, internal controls and the roles and responsibilities of the IS audit function. A good understanding of these concepts will enable DISAs to plan, perform and provide report on IS Assurance and consulting assignments. The concepts covered are the building blocks for execution and reporting of IS audit which are covered in Chapters 2 and 3.

1.2 Introduction

In the present age of globalisation, Information System has become a backbone for any organization whether the field of its operation is manufacturing, education, trading, technology, entertainment, etc. Nowadays, the success of any organisation thrives on information that is generated within the information system. IT is used by enterprises for providing greater satisfaction to customers, to access wider range of information, to handle business changes as real time events, and create more efficiency within the enterprise. Further, with the development of automated information systems there has been a simultaneous increase in the threats to the security of information systems which has led to financial losses to the enterprise and most importantly loss of critical information. Hence in the current competitive world, the enterprises strive not only to attain more efficiency and effectiveness of business through implementation of information systems but also secure the information which has become the most valuable asset to the enterprise.

As an IS auditor, the scope of work can vary from assisting the enterprise to select and successfully implement information systems. The engagements can go beyond just implementing some basic IT level security. It is important for organisations to take a holistic perspective and implement security from a governance perspective with involvement of board in direct and monitoring the use of IT for achieving business objectives. Regulatory requirements also demand involvement of senior management in effective decision making in all key aspects of IT security. Senior management look for assurance from IS Auditors on the availability, adequacy and appropriateness of IT controls as implemented and also seek advice on best deployment of IT for achieving business objectives. Hence, the role of the IS auditor has expanded to review not only whether IT is deployed in a safe and secure environment but also to provide advisory services on optimum use of technology to enable organisations to survive and thrive in the competitive environment while complying with regulatory requirements.

1.3 Definitions

Audit: In simple terms audit is an official inspection of an organisation's accounts, typically by an independent body. In case of financial audit, audit is an independent examination of financial information of any entity, whether profit oriented or not, and irrespective of its size or legal

form with a view to expressing an opinion thereon. In case of IS Audit, the audit encompasses independent review and evaluation of automated information systems, related manual systems and the interfaces between them.

Computer System: Refers to a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions.

Information: As per IT Act 2000, information includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche. In general data processed in a meaningful context is information. Information has value to user. Information is data that is (1) accurate and timely, (2) specific and organised for a purpose, (3) presented within a context that gives it meaning and relevance, and (4) can lead to an increase in understanding and decrease in uncertainty.

Information Systems (IS): In general it refers to the study of complementary networks of hardware and software, that people and organisations use to collect, filter, and process, create, and distribute data. Specifically in the context of IT, Information systems are the software and hardware systems that support data-intensive applications and includes the design and implementation of languages, data models, process models, algorithms, software and hardware for information systems.

Secure system: It means computer hardware, software, and procedure that:

(a) Are reasonably secure from unauthorised access and misuse;

(b) Provide a reasonable level of reliability and correct operation;

(c) Are reasonably suited to performing the intended functions; and

(d) Adhere to generally accepted security procedures;

Risk: It is the potential of uncertain event resulting in losing something of value, weighed against the potential to gain something of value. In IT parlance, it can be an uncertain event or something going wrong, which affects enterprise from achieving set objectives. Risk is the potential that a given threat will exploit the vulnerabilities of an asset or a group of assets to cause loss or damage to the assets.

Internal Control: It is a process implemented in an organisation to help in achieving specific goals. Internal control includes the policies, standards, plans and procedures, and organisational structures designed to provide reasonable assurance that enterprise objectives will be achieved and undesired events will be prevented or detected and corrected.

Business Process: A business process is a collection of related, structured activities or tasks that produce a specific service or product (serve a particular goal) for a particular customer or customers. It often can be visualised with a flowchart as a sequence of activities with interleaving decision points or with a Process Matrix as a sequence of activities with relevance rules based on data in the process.

1.4 Concepts of Audit

The general standards of auditing are applicable to IS Audit also as IS Audit is a type of internal audit or sub-set of the statutory audit. As per the general guidelines on Internal Auditing issued by ICAI, Auditing is defined as a systematic and independent examination of data, statements, records, operations and performances of an enterprise for a stated purpose. In an auditing situation, the IS Auditor perceives and recognises the propositions before him for examination, collects evidence, evaluates the same and on this basis formulates judgment which is communicated through the report.

Internal auditing is defined as an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

SA 200 describes the basic principles of audit and these principles are applicable for IS Audit also and have to be complied with. IS Audit is primarily an internal audit conducted for providing assurance after evaluation of risks and provides report on the implemented controls. Based on such evaluation, the IS Auditor would provide appropriate recommendations for mitigating control weaknesses in IT related areas. **IS Audit may also be carried out by external auditors as part of statutory audit to review internal controls in automated information systems. However, the scope would be bound by the objectives of the applicable regulatory requirements. IS Audit could also be carried out as a part of internal audit or as a specialised audit of IT environment such as: penetration testing, audit of data centre, audit of BCP or review of IT strategy, etc.**

Integrity, Objectivity and Independence: The IS Auditor should be straight forward, honest and sincere in his approach to his professional work. He must be fair and must not allow prejudice or bias to override his objectivity. He should maintain an impartial attitude and appear to be free from any interest which might be regarded whatever its actual effect as being incompatible with integrity and objectivity.

Skill and Competence: The IS audit should be performed and the report prepared with due professional care by persons who have adequate training, experience and competence. This can be acquired through a combination of general education, technical knowledge obtained through study and formal courses concluded by a qualifying examination recognised for this purpose and practical experience under proper supervision.

Confidentiality: The IS Auditor should respect the confidentiality of information acquired during the course of work and should not disclose any such information to a third party without specific authority or unless there is any legal or professional duty to disclose.

Work performed by others: When the IS Auditor delegates work to assistants or uses work performed by other IS Auditors or experts, he will continue to be responsible for forming and expressing his opinion on auditee environment as per the scope and objectives of audit. However, at the same time IS Auditors are entitled to rely on the work performed by others provided they exercise adequate skills and care and are not aware of any reason to believe that they should not have relied. The IS Auditors should carefully direct, supervise and review work delegated to assistants. They should obtain reasonable assurance that work performed by other IS Auditor or experts are adequate and in accordance with set audit objectives.

Documentation: The IS Auditor should have documentary evidence, which is important in providing evidence that the audit was carried out in accordance with IS Auditing standards, guidance and procedures and adhering to the regulatory requirements.

Information systems and internal control: The IS Auditor should gain an understanding of the information systems and related internal controls. They should study and evaluate the operation of those internal controls upon which they wish to rely to determine the nature, timing and extent of other audit procedures.

Audit conclusions and reporting: The IS Auditor should review and assess the conclusions drawn from the audit evidence obtained and from their knowledge of business of the entity as the basis for the expression of their opinion.

1.5 Concept of IS Audit and Auditing in a Computerised Environment

1.5.1 Audit in a computerised environment

Historically, all kinds of accounting and data processing job was conducted manually which involved preparation of physical records and the auditor had no choice but to conduct audit manually. With the increased use of internet and e-commerce technologies, enterprises are relying more and more on computer systems for much of accounting and all other critical business processes leading to most of the auditee information being available in electronic format rather than manual format. Hence, the audit approach, audit evidence has moved from physical to digital and it has become imperative for auditors to use computers to audit this digital information.

The overall scope and objectives of audit doesn't change in a computerised environment. However, the use of a computer changes the processing and storage of information and may affect the organisation and procedures employed by the organisation to implement adequate and appropriate internal control. Accordingly, the procedures followed by the auditor in their review and evaluation of the: information systems, related internal controls, nature, timing and extent of audit procedures are directly impacted by the computerised information systems environment.

1.5.2 IS Audit (Auditing of the computerised environment)

The IS Audit of an Information System Environment may include one or both of the following:

- Assessment of internal controls within the IS environment to assure validity, reliability, and security of information and information systems.
- Assessment of the efficiency and effectiveness of the IS environment.

The objective of IS audit process is to evaluate the adequacy of internal controls with regard to both specific computer programme and the data processing environment as a whole. ISACA defines IS Audit as: "IS audit refers to any audit that encompasses wholly or partly, review and evaluation of automated information processing systems, related non-automated processes and the interfaces between them". Although IS Audit is often mis-understood as a mere technical audit and a domain of IT professionals, it is clear that IS Audit involves evaluating the adequacy and efficiency of internal controls in business processes that are either partly or fully computerised. Hence Audit and control professionals who have expertise in understanding of business processes

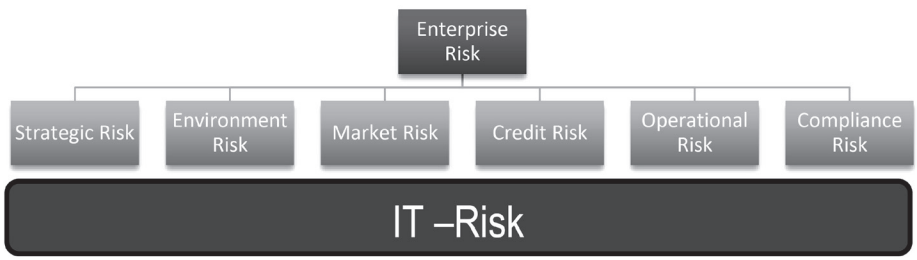
and internal controls with exposure to information technology risks and controls are considered the most appropriate professionals to conduct most of the information systems audits.

An IS Audit cannot be viewed from a narrow perspective of audit of only automated information processing systems but would include audit of non-automated control processes and interfaces. Therefore, depending on the audit environment, objectives and scope, the audit could involve audit of entire business processes, partially or fully automated, or audit of specified application, technology and related controls. IS Audit is a focused audit about auditing an information systems area whereas Audit in a Computerised Environment is a regular audit engagement performed in process area using the computer. **Please refer to the Technical guide on IS Audit (included as reference material in DVD).**

1.6 Concept of IT Risk

There are numerous changes in IT and its operating environment that emphasises the need to better manage IT related risks. This has increased the level of dependency of organisation on electronic information which are processed by IT systems. These IT systems are now essential to support critical business processes. Risk is an event which has a potential to impact organisation goal and strategy implementation in a negative manner. Another way of defining risk would be Threat exploiting Vulnerabilities.

IT risk has significant impact on the overall business risk as failure of IT could impact the business. IT risk is a component of the overall risk universe of the enterprise, as shown in below figure. Other risks that an enterprise faces include strategic risk, environmental risk, market risk, credit risk, operational risk and compliance risk. In many enterprises, IT-related risk is considered to be a component of operational risk, e.g., in the financial industry in the Basel II framework. However, even strategic risk can have an IT component to it, especially where IT is the key enabler of new business initiatives. The same applies for credit risk, where poor control on IT and IT security can lead to lower credit ratings of organisations. For that reason it is better not to depict IT risk with a hierarchic dependency on one of the other risk categories.



1.6.1 IT Risk in the Risk Hierarchy

Managing the IT risk of the enterprise starts with defining the risk universe; a risk universe describes the overall environment and provides a structure for managing IT risk. The Risk universe:

- Considers the overall business objectives, business processes and their dependencies throughout the enterprise. It describes which IT applications and infrastructure support the business objectives through the provision of IT services. It is worth highlighting that IT risk

needs to be seen from an end-to-end business activity perspective, crossing IT function silos (IT operations, project management, application development, disaster recovery, security, etc.).

- Considers the full value chain of the enterprise. This can include not only the enterprise and its subsidiaries/business units, but also clients, suppliers and service providers.
- Considers a full life-cycle of IT related business activities, including transformation programs, investments, projects and operations.
- Includes a logical and workable segmentation of the overall risk environment. This sounds relatively easy but often it is not – the hierarchical organisational of the enterprise business, business processes and supporting IT infrastructure and services often are not aligned, and it is highly probable that different views along different dimensions exist for the overall environment. It is up to the enterprise to determine which view will be the most meaningful to support the business objectives of the enterprise while considering the potential overlaps and omissions.
- Needs to be reviewed and updated on a regular basis due to the constantly changing internal and external requirements.

Risk Management

Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organisation in achieving business objectives and deciding what counter measures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organisation. Risk can be avoided, reduced, transferred or accepted. An organisation can also choose to reject risk by ignoring it, which can be dangerous and should be considered a red flag by the IS Auditor. The counter-measures for mitigating risks are also called controls and these need to be implemented as appropriate. In reviewing an IS environment, the primary focus of the IS Auditor would be to review the risk assessment done by the organisation, assess whether these risks have been mitigated by implementing appropriate controls and the residual risk is knowingly accepted and is within the risk appetite. In case the residual risks after applying the controls exceed the residual risk and have not been approved by the management, report these risks with appropriate remedial measures.

Here onwards, the word risk should be interpreted as IT Risk and Audit would be referred as IS Audit.

1.7 Risk Based Auditing

A risk based audit approach is usually adapted to develop and improve the audit process on a continuous basis so that the focus is on high risk areas and maximum value addition is derived from audit resources deployed. This approach is used to assess risk and to assist an IS Auditor to focus on high risk areas and in making the decision with regards to the sample size to perform either compliance testing and/or substantive testing. It is important to stress that the risk based audit approach efficiently assists the IS Auditor in focusing on the risk areas which are most critical and also in determining the nature and extent of testing.

Within this concept, inherent risk, control risk or detection risk are of major concern for the IS Auditor. In a risk based audit approach, IS Auditors are not just relying on risk; they also are relying on internal and operational controls as well as knowledge of the company or the business. This type of risk assessment decision can help relate the cost-benefit analysis of the control to the known risk, allowing practical choices.

Business risks include concerns about the probable effects of an uncertain event in achieving established business objectives. The nature of these risks maybe financial, regulatory or operational, and may also include risks derived from specific technology deployment. For example, an airline company is subject to extensive safety regulations and economic changes, both of which impact the continuing operations of the company. In this context, the availability of IT service and its reliability are critical.

By understanding the nature of business, IS Auditors can identify and categorise the types of risk associated with the business and identify the risks applicable to specific situations or audit environment. On the other hand, risk assessment refers to the methodology where risks have been given elaborate weights based on the nature of the business or the significance of the risk and risks are categorized as high, medium or low based on which appropriate decisions are taken by management.

SA 315, the standard for risk identification and assessment requires IS Auditors to assess risk that is part of the business environment and the internal control system. SA 330 requires IS Auditors to review whether management has designed and implemented appropriate risk remediation measures and provide recommendations on the residual risks that have been identified as critical and are not appropriately mitigated. Usually the IS Auditor would provide recommendations for risk remediation as part of the Audit Report.

1.8 Audit Risk and Materiality

1.8.1 Audit Risk

Audit risk: In general, audit risk refers to the risk that an auditor may issue unqualified report due to the auditor's failure to detect material misstatement either due to error or fraud. This risk is composed of inherent risk (IR), control risk (CR) and detection risk (DR). Audit risk can be high, moderate or low depending on the sample size selected by the Auditor. In the context of IS Audit, the meaning of audit risk is still relevant but it would vary depending on the specific scope and objectives of audit.

Inherent risk means overall risk of management which is on account of entity's business operations as a whole. Inherent risk is the susceptibility of information resources or resources controlled by the information system to material theft, destruction, disclosure, unauthorised modification, or other impairment, assuming that there are no related internal controls. Inherent risk is the risk that has natural association. The inherent risk for audit assignment can be project related risks, revenues related risks, and resource related risks. Inherent risk to business can be dependent on nature of business. If the IS Auditor concludes that there is a high likelihood and consequence of risk exposure, ignoring internal controls, the IS Auditor would conclude that the inherent risk is high.

Detection risk is the risk of the IS Auditor when he is not able to detect the inherent risk or the controllable risk. It means higher the level of non-detection by the IS Auditor, higher is the detection risk. Detection risk is the risk that the IS Auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors. For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high if the audit logs for the whole period of audit are not available at the time of the audit. Detection risk is a measure of the IS Auditor's assessment of the likelihood that the vulnerability or gaps will not be detected by the IS Auditors. IS Auditor will carry out more detailed audit to detect material vulnerabilities or gaps if the inherent risk and control risk are high. Detection risk primarily refers to the fact that there exists a control weakness that auditor fails to detect.

Control risk is the risk that an error which could occur in an audit area, and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. Control risk is a measure of the IS Auditor's assessment of the likelihood that risk exceed a tolerable level and will not be prevented or detected by the client's internal control system. This assessment includes an assessment of whether a client's internal controls are effective. For example: the enterprise has good system of segregation of duties but two employees could collaborate and still commit fraud.

Assessing inherent, control and detection risk gives the final assessment of the overall Audit Risk i.e. the risk which the IS Auditor is ready to accept in an audit assignment. Audit risk is the product of inherent risk, control risk and detection risk. The extent of audit effort is dictated by the degree of audit risk, the assessment of which is critical to the effectiveness of the audit effort. Amongst the critical factors affecting the audit risk is the appropriate assessment of the control environment. The preliminary review of audit environment enables the IS Auditor to gain understanding of the business, technology and control environment and also gain clarity on the objectives of the audit and scope of audit. Risk assessment allows the IS Auditor to determine the scope of the audit and assess the level of audit risk and error risk.

1.8.1 Materiality

The concept of materiality in the case of financial audit is based on value and volume of the transactions and the relevant error or discrepancy or control weakness detected. In case of regulatory audit, materiality is based on impact of non-compliance and in case of IS Audit, materiality is based on the effect or consequence of the risk in terms of potential loss. Hence, materiality varies based on the scope and objectives of the audit and specific auditee environment. Materiality is an important aspect of the professional judgment of the IS Auditor as he/she has to decide whether the information is material or immaterial. With regards to the materiality of the financial statements, information is regarded as material if it changes the decision of the users of the financial statement i.e. if the misstatement is of a high value and quantity. The IS Auditor should have a good understanding of these audit risks when planning an audit. An audit sample may not detect every potential error in a population. When evaluating internal controls, the IS Auditor should realise that a given system may not detect a minor error. However, that specific error, combined with others, could become material to the overall system.

The concept of materiality requires sound judgment from the IS Auditor. The IS Auditor may detect a small error that could be considered significant at an operational level, but may not be viewed as significant to upper management. Materiality considerations combined with an understanding

of audit risk are essential concepts for planning the areas to be audited and the specific test to be performed in the audit. It depends on the IS Auditor to decide whether the information is material for him which means that lower the risk than an IS Auditor is willing to undertake, lower is the level of materiality. In other words, higher the level of materiality, lower is the risk that an IS auditor is willing to take.

For systems and operations not affecting financial transactions, the following are examples of measures that should be considered to assess materiality:

- Criticality of the business processes supported by the system or operation
- Cost of the system or operation (i.e., hardware, software, staff, third-party services, overheads, and a combination of these). E.g. A virus has been detected and cleaned and there was no impact on business or operations. Apparently, this may not be a material risk. However, materiality can be correctly determined only when root cause analysis is done to ascertain the how and from where the virus entered the organisation's information system. The analysis may reveal that there is weakness in control process. Hence although the incident *per se* is not material but inherent cause of weakness is definitely material as the virus problem can recur and cause harm to the organisation information system. If auditor fails to detect this weakness it might result in detection risk
- Potential cost of errors (possibly in terms of lost sales, warranty claims, irrecoverable development costs, cost of publicity required for warnings, rectification costs, health and safety costs, unnecessarily high costs of production, high wastage, etc.)
- Number of accesses/transactions/inquiries processed per period
- Nature, timing and extent of reports prepared and files maintained
- Nature and quantities of materials handled (e.g., where inventory movements are recorded without values)
- Service level agreement (SLA) requirements and cost of potential penalties
- Penalties for failure to comply with legal and contractual requirements

SA 320 is the Auditing standard for Audit Materiality. It requires the Auditor to report those items that create an impact on the financial statements and which changes the decision that would be made by the stakeholder. The same concept is applied even when conducting an IS Audit Engagement. The ITAF, 2nd edition issued by ISACA has the following standards on "Materiality" which has to be complied by the IS Auditor.

1204.1 IS audit and assurance professionals shall consider potential weaknesses or absences of controls while planning an engagement, and whether such weaknesses or absences of controls could result in a significant deficiency or a material weakness.

1204.2 IS audit and assurance professionals shall consider audit materiality and its relationship to audit risk while determining the nature, timing and extent of audit procedures.

1204.3 IS audit and assurance professionals shall consider the cumulative effect of minor control deficiencies or weaknesses and whether the absence of controls translates into a significant deficiency or a material weakness.

1204.4 IS audit and assurance professionals shall disclose the following in the report:

- Absence of controls or ineffective controls
- Significance of the control deficiency
- Likelihood of these weaknesses resulting in a significant deficiency or material weakness

1.9 Concepts of Internal Control

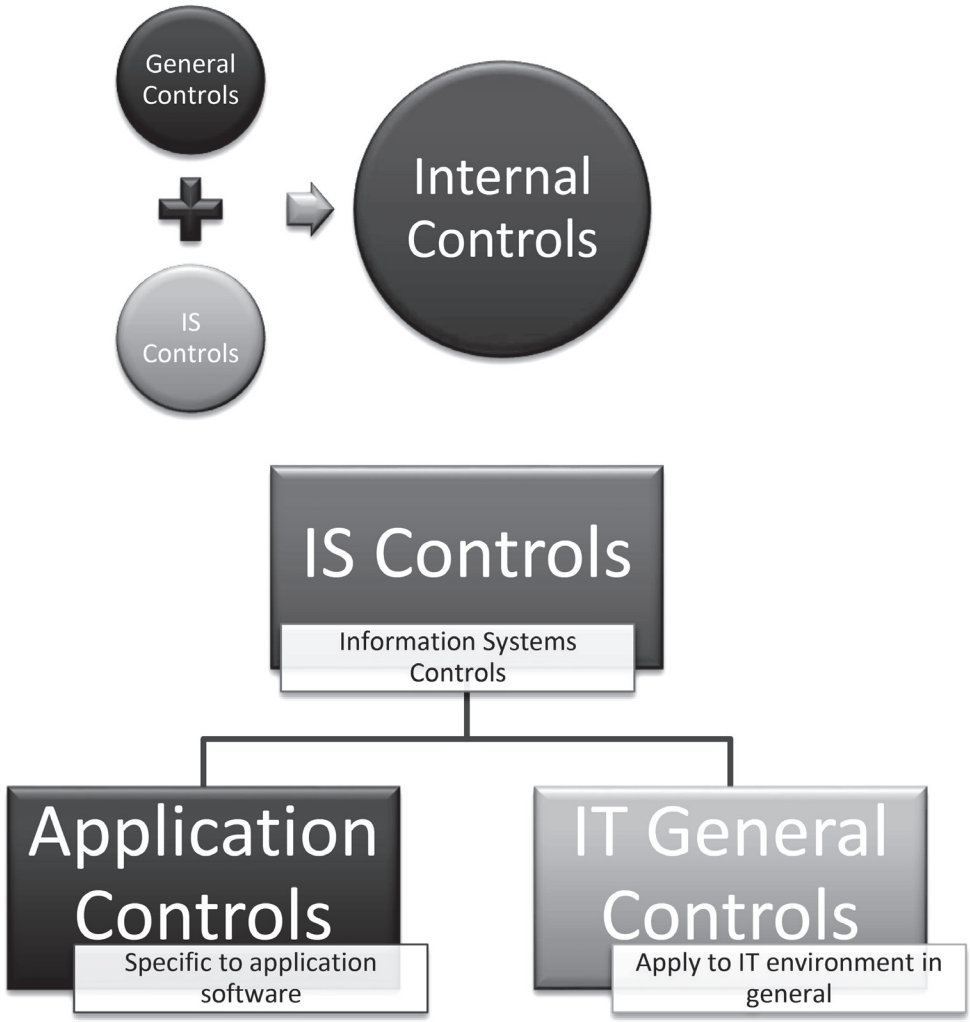
The increasing use of IT in organisations has made it imperative that appropriate information systems are implemented in an organization. IT should cover all key aspects of business process of an enterprise which have an impact on its strategic and competitive advantage for its success. Control is defined by ISACA as: "Control refers to the policies, procedures, practices and organisation structure that are designed to provide reasonable assurance that the business objectives will be achieved and undesired events are prevented or detected and corrected". This definition of control is applied for all IS Audits. Internal Controls are normally composed of policies, procedures, practices and organisational structures which are implemented to reduce risks in the organisation to an acceptable level. Internal controls are developed to provide reasonable assurance to management that the organisation's business objectives will be achieved and risk events will be prevented or detected and corrected.

Internal control activities and supporting processes are either manual or driven by automated computer information resources. Thus, IS audit includes reviewing the implemented systems or providing consultation and evaluating the reliability of operational effectiveness of controls. The objective of controls is to reduce or if possible eliminate the causes of the exposure to potential loss.

1.9.1 Types of Internal Controls

1. **Preventive:** Designed to prevent errors or irregularities from occurring.
2. **Detective:** Designed to detect errors or irregularities that may have occurred.
3. **Corrective:** Designed to correct errors or irregularities that have been detected and report them.

Internal Controls is said to be a mechanism that is established by organisations which is a sum of General Controls and IS Controls. IS controls is said to be a sum of IT Application Controls and IT General Controls. General Controls refers to internal controls that encompass all administrative areas in general including IT implementation whereas application controls are implemented in specific application software. In general, it can be said that IS Controls are controls that are present on the enterprise's IT Infrastructure. IT Infrastructure includes hardware and software.



1.9.2 Types of IS Controls

IS Controls can also be classified in the following manner:

Preventive Controls: Controls that prevents problems before they arise. They monitor both operation and inputs. They attempt to predict potential problems before they occur and make adjustments. They also help in preventing an error, omission or malicious act from occurring.

Detective Controls: Controls that detect and report the occurrence of an error, omission or malicious act.

Corrective Controls: Controls that minimise the impact of a threat. They remedy problems that are discovered by Detective controls. They help in identification of the cause of the problem. They correct errors arising from the problem. They modify the processing systems to minimise future occurrences of the problem.

1.10 Organisation of IS Audit Function

The IS audit function should be placed in the organisation so as to ensure its objectivity and independence. The appointment of external auditor should also be governed by stipulations for independence and objectivity, which is the foundation for an effective audit function. The composition and constitution of the IS audit function should ideally be decided by the audit committee and should be the prime reporting pointer for the IS Audit function. The role of the IS Audit function is defined by the audit charter which defines the authority, scope and responsibility. The audit charter provides mandate for performing the audit function. Based on the overall guidelines defined in the audit charter, the audit function is created with specific roles and responsibilities.

1.10.1 Infrastructure and Organisation

IS audit function should be equipped with sufficient resources to discharge its duties efficiently and effectively. An important determinant in the quality of the IS audit function is the quality of human resource that staff the audit function. The skills and competence requirements should be clearly established and as an IS Audit function should collectively possess the skills and knowledge necessary for performing an effective and professional audit. Even in cases where external agencies are engaged, the professional competence and skills of such agencies should be ensured. Continuing Professional Education should be included as part of the IS audit management plan.

Assurance function perspective: It describes what is needed in an enterprise to build and provide assurance function(s). The assurance function perspective describes how each factor contributes to the overall provisioning of assurance, for example:

- Which organizational structures are required to provide assurance (board/audit committee, audit function, etc.)
- Which information items are required to provide assurance (audit universe, audit plan, audit reports, etc.)

The function might require special infrastructure for using CAATs. If so, availability of appropriate tools and infrastructure should be ensured.

ITAF, 2nd edition issued by ISACA provides the following standard regarding independence of IS Auditor.

1002 Organisational Independence

1002.1 The IS audit and assurance function shall be independent of the area or activity being reviewed to permit objective completion of the audit and assurance engagement.

1003 Professional Independence

1003.1 IS audit and assurance professionals shall be independent and objective in both attitude and appearance in all matters related to audit and assurance engagements.

1.10.2 Internal and external audit control framework

The internal and external audit control framework ensures the minimum quality of audits. This forms the basis for the organisation to implement the appropriate audit control framework.

Accordingly, policies and procedures for risk assessment, planning, implementation and reporting are to be established. The audit control framework assures the effectiveness and efficiency of operations, reliability of reporting and compliances with laws and regulations. The standards and professional pronouncements should be strictly adhered to, and this should be reflected in the organisation and operations of the audit function. Specific guidelines have to be issued to ensure the qualitative work under control environment.

1.10.3 Quality Assessment and Peer Reviews

Quality Assessment ensures that the IS audit function is delivering in line with the best auditing practices and following the professional standards and pronouncements, It also ensures that the IS Audit function is subject to both internal and external quality assessments, peer reviews, certification and accreditation. Though the objective of the internal and external IS audit remains same, the scope and approach might vary. In case of an internal IS audit, the IS Auditor reviews the internal control environment in detail whereas an external IS Auditor takes an overall view of internal control environment and focuses on substantive testing as per the specific scope and objective of the assignment. In case of external audit, the audit engagement letter defines the scope and objectives of individual audit assignment.

1.10.4 Standards on Audit Performance

IS auditors have to comply with the following standards of ITAF, 2nd Edition issued by ISACA.

1004 Reasonable Expectation

1004.1 IS audit and assurance professionals shall have reasonable expectation that the engagement can be completed in accordance with the IS audit and assurance standards and, where required, other appropriate professional or industry standards or applicable regulations and result in a professional opinion or conclusion.

1004.2 IS audit and assurance professionals shall have reasonable expectation that the scope of the engagement enables conclusion on the subject matter and addresses any restrictions.

1004.3 IS audit and assurance professionals shall have reasonable expectation that management understands its obligations and responsibilities with respect to the provision of appropriate, relevant and timely information required to perform the engagement.

1005 Due Professional Care

1005.1 IS audit and assurance professionals shall exercise due professional care, including observance of applicable professional audit standards, in planning, performing and reporting on the results of engagements.

1006 Proficiency

1006.1 IS audit and assurance professionals, collectively with others assisting with the assignment, shall possess adequate skills and proficiency in conducting IS audit and assurance engagements and be professionally competent to perform the work required.

1006.2 IS audit and assurance professionals, collectively with others assisting with the assignment, shall possess adequate knowledge of the subject matter.

1006.3 IS audit and assurance professionals shall maintain professional competence through appropriate continuing professional education and training.

1007 Assertions

1007.1 IS audit and assurance professionals shall review the assertions against which the subject matter will be assessed to determine that such assertions are capable of being audited and that the assertions are sufficient, valid and relevant.

1008 Criteria

1008.1 IS audit and assurance professionals shall select criteria, against which the subject matter will be assessed, that are objective, complete, relevant, measureable, understandable, widely recognised, authoritative and understood by, or available to, all readers and users of the report.

1008.2 IS audit and assurance professionals shall consider the source of the criteria and focus on those issued by relevant authoritative bodies before accepting lesser-known criteria.

1.11 Summary

This chapter has provided brief overview of the fundamental concepts of Audit, IS audit, risks, controls and internal controls. We have also provided the distinction between audit in an IS environment and audit of a computerised environment. Further, the conceptual understanding of IT risk and risk based auditing has been provided with an overview of types of audit risks and their categorisation as: Inherent Risk, Controllable Risk and Detection Risk. The concept of materiality and internal controls with overview of types of internal controls has been provided. Controls can be classified as: IS Controls and general Controls and IT controls are bifurcated as IT Application Controls which are specific to application software and IT General Controls which pertain to the IT environment in general. The classification of controls as preventive, detective and corrective has been explained. The overall objective of this chapter is to provide an understanding of the key concepts of information systems, audit function, materiality and the attached risk.

1.12 Questions

1. Who among the following is responsible for establishing IS Audit function in the organisation?
   - A. Audit Charter
   - B. Audit Governance
   - C. Audit Objectives
   - D. Audit Project Plan
2. Which of the following control classifications identify the cause of a problem and minimize the impact of threat?
   - A. Administrative Controls
   - B. Detective Controls
   - C. Preventive Controls
   - D. Corrective Controls

3. Which of the following is NOT generally considered a category of Audit Risk?
   A. Detection Risk
   B. Scoping Risk
   C. Inherent Risk
   D. Control Risk
4. Which of the following are most commonly used to mitigate risks discovered by organizations?
   A. Controls
   B. Personnel
   C. Resources
   D. Threats
5. Which of the following is not a type of internal controls?
   A. Detective
   B. Corrective
   C. Preventive
   D. Administrative
6. What means the rate at which opinion of the IS Auditor would change if he selects a larger sample size?
   A. Audit Risk
   B. Materiality
   C. Risk Based Audit
   D. Controls
7. Which of the following cannot be classified as Audit Risk?
   A. Inherent Risk
   B. Detection Risk
   C. Controllable Risk
   D. Administrative Risk
8. After you enter a purchase order in an on-line system, you get the message, "The request could not be processed due to lack of funds in your budget". This is an example of error?
   A. Detection
   B. Correction
   C. Prevention
   D. Recovery

9. When developing a risk-based audit strategy, an IS auditor should conduct a risk assessment to ensure that:
   A. Controls needed to mitigate risks are in place.
   B. Vulnerabilities and threats are identified.
   C. Audit risks are considered.
   D. A gap analysis is appropriate
10. Reviewing management's long-term strategic plans helps the IS auditor:
   A. Gains an understanding of an organization's goals and objectives.
   B. Tests the enterprise's internal controls.
   C. Assess the organization's reliance on information systems.
   D. Determine the number of audit resources needed.

1.13 Answers and Explanations

1. An audit charter establishes the role of the internal audit function. These are established by the senior management.
2. Corrective Controls classifications identify the cause of a problem and minimise the impact of threat. The Goal of these controls is to identify the root cause of an issue whenever possible and eliminate the potential for that occurring again. The other controls are useful but perform other functions instead.
3. Scoping risk is not generally considered as category of audit risk. The other risk categories are also possible types of risk; however they are not the one that question demand.
4. Controls are most commonly used to mitigate risks discovered by organisations. This is what organisations implement as a result of the risks an organization discovers. Resources and personnel are often expended to implement controls.
5. Administrative is not a type of internal controls. Detective is designed to detect errors or irregularities that may have occurred. Corrective is designed to correct errors or irregularities that have been detected. Preventive is designed to keep errors or irregularities from occurring.
6. Audit risk means the rate at which opinion of the IS Auditor would change if he selects a larger sample size. Audit risk can be high, moderate or low depending on the sample size selected by the IS Auditor. A risk based audit approach is usually adapted to develop and improve the continuous audit process. Materiality means importance of information to the users. It is totally the matter of the professional judgment of the IS Auditor to decide whether the information is material or immaterial.
7. Inherent risk means overall risk of management which is on account of entity's business operations as a whole. Controllable risk is the risk present in the internal control system and the enterprise can control this risk completely and eliminate it from the system. Detection risk is the risk of the IS Auditor when he is not able to detect the inherent risk or the controllable risk.

8. To stop or prevent a wrong entry is a function of error prevention. All other options work after an error. Prevention works before an occurring of error.

9. In developing a risk-based audit strategy, risks and vulnerabilities are to be understood. This determines areas to be audited and the extent of coverage. Understanding whether appropriate controls required to mitigate risks are in place is a resultant effect of an audit. Audit risks are inherent aspects of auditing, are directly related to the audit process and are not relevant to the risk analysis of the environment to be audited. Gap analysis would normally be done to compare the actual state to an expected or desirable state.

10. Strategic planning sets corporate or departmental objectives into motion. It is time and project-oriented, but must also address and help determine priorities to meet business needs. Reviewing long-term strategic plans will not achieve objectives by other choices.

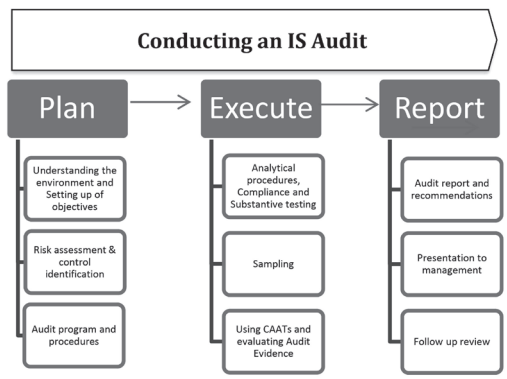
CHAPTER 2: IS AUDIT IN PHASES

2.1 Learning Objectives

This chapter provides detailed insights into the various phases of IS audit. The fundamental concepts which were discussed in earlier chapter are connected to their practical aspects in terms of how to define the audit scope and objectives, gain knowledge of the organisation's business, assessment of risk, IT application controls and IT general controls of the enterprise. Sampling and testing methodologies using CAAT as used by the IS auditor are also discussed. How to develop audit programmes and approach and design appropriate tests for compliance and substantive testing for reviewing the design effectiveness and operational effectiveness of the IS systems are explained. The need for IS auditor to obtain sufficient evidence as a part of the audit process which forms critical part of the assurance services as well as use of global best practices as benchmarks for performing and reporting IS audit findings are discussed in this chapter. Please note that organisation and enterprise are used inter-changeably.

2.2 Introduction

Information systems have become an integral part assurance process. The growth of technology has made IT, an indispensable part of our day to day functioning. Organisations value information as the most critical asset and hence has become more vulnerable to theft causing loss for the enterprise. There is a risk that the information shall be stolen in fraudulent manner and it can be used by the fraudster for financial gains. Dependency on information and information technology has helped organizations in improving efficiency in customer delivery and also opened up new delivery channels. In order to adapt to these technological advancements organisations have reengineered their processes result of which has introduced vulnerabilities. There is critical requirement of enhancing value of information by making it available online but this has to be coupled with right level of security. In the networked world, the fraudster can intrude into the system anytime and from anywhere. It is important that management has systems and processes in place not only to ensure that adequate controls exist and are working effectively but by having an independent evaluation of information systems from IS Audit professionals. The IS auditor has to plan the audit keeping in mind the scope and objectives of the audit including the auditee environment, regulatory requirements and technology deployment. The IS Audit phases are summarised in the following diagram.



2.3 Conducting an IS Audit

2.3.1 Setting up of audit objectives

Audit objectives refer to the specific goals that must be met by the audit. In contrast, a control objective refers to how an internal control should function. An audit may, and generally does, incorporate several audit objectives. Audit objectives often focus on substantiating that internal controls exist to mitigate business risks, and that they function as expected. These audit objectives include assuring compliance with legal and regulatory requirements as well as the confidentiality, integrity, reliability and availability of information and IT Resources. Audit management may give the IS Auditor a general control objective to review and evaluate when performing an audit.

One of the basic purposes of any IS audit is to identify control objectives and the related controls that address these objectives. The objective of an information systems audit (design and operating effectiveness of the internal control system) is to enable the IS Auditor to express an opinion on whether the internal control system set up and operated by the organisation for the purpose of managing risks to the achievement of the objectives was suitably designed and operated effectively in the period. If there are control weaknesses, report these with appropriate recommendations for mitigating these risks by improving controls and thus provide value addition.

2.3.2 Request for Proposal and submitting response

Request for proposal (RFP)

A RFP is a standard solicitation document used by various organisations to compete for contract opportunities. A RFP is most often used to acquire services, although it may be used in some circumstances to acquire goods. A successful RFP process will support the principles of fair, open, and transparent procurement; it will satisfy the business requirements. This guide has been developed to help organisations successfully navigate the RFP process. Well-prepared RFPs can go a long way to creating effective solutions and programmes for business development and associations. With an RFP, proposals are evaluated against multiple criteria such as price, qualifications and experience, and the proposed solution or approach. The best proposal will be awarded the contract and the best proposal may, or may not, have the lowest price. **Please refer to section-3 for format of request for proposal.**

The stages in developing an effective RFP are as follows:

Introduction: This is the first stage in the RFP process where the background of the proposed activity is provided. The potential bidders are provided the need and rationale for publishing the RFP. It may also contain a key summary of the key contents which form the other sections of the document.

Requirements: This is the most important part of the document as it specifies the requirement of the organisation. The requirements have to be specified in detail and if the need be the same can be broken down into various subsections depending upon the number of requirements and specifications for e.g.

1. **Size and quality of the service deliverables.**
2. **Technical specification needed for the product.**
3. **Quantity and specific expectations.**

Selection Criteria: In this section the selection criteria of the proposed bidders/vendors should be specified. The selection would be based on the predefined criteria of deliverables and would be decided by a committee.

Timelines: This section should define of the timelines for submission of bids and the manner in which the same shall be accepted by the organisation. This would ensure that not only potential vendors would comply with the timelines but also defines the structure of the bidding document; the vendors who fail to comply with the specifications would get eliminated immediately.

Process: In this section there is a need to explain how the whole process will work from sending the RFP to awarding the contract and starting the work. The commercial terms and conditions shall be mentioned along with the clauses on default and applicable damages for failure to deliver on the requirements as specified in the above section. The specific requirements of skills and competencies of the personnel deployed for the assignment would have to be provided. Further, the approach or methodology to be followed with standard templates of reporting will be requested from the bidders. This will help organisation in evaluating the technical competence of the vendor in executing the assignment by following a standard approach and using best practices framework and practices as applicable.

Request for References: This is an optional content which the organisation can insert where the potential bidders/vendors need to furnish one or more references of their clients. The objective is to evaluate experience of performing similar work and obtain confidence on the capacities of the bidder/vendor for performance.

Point of contact: This forms the concluding section of the RFP, where the organisation mentions of a point of contact within the company to not only ensure that one person is assigned to the process but also that the vendors/bidders can connect regarding any queries/clarities on the RFP.

Response to RFP

The response to the RFP should be complete in all respects and assist the evaluators from the organisation to come to a conclusion on technical competencies for executing the services as required. The details provided should lead to a potential awarding of the contract. The stages for responding to an RFP are as follows:

Introduction: In this section the organisation introduces itself in brief, the areas of work and specialisation to make the client understand the business offerings and areas of specialisation that are on offer.

Submission of Technical Bid: The organisation has to highlight the detailed response to each requirement of the proposer. The information on the product in the offering, the technical specifications, design specifications and other important details has to be inserted in this section. Here, it can be reflected as to how the product meets the requirements of the proposer.

Price Offering: In this section the price being offered is mentioned. If there exist any discounts, other offers the same has to be mentioned. If there exists, any time frame for the offer the same needs to be provided.

Commercial Terms: All the commercial terms and conditions of the product, deliveries, warranties, replacements, etc. should be mentioned. If there are any special clauses, these have to be highlighted.

Point of contact: This forms the concluding section of the RFP response, where the organisation mentions of a point of contact within the company to connect regarding any queries/clarities on the service offerings.

Request for References: This is an optional content which the organisation can insert, if requested by the proposer.

Please refer to section-3 for sample proposal in response to request for proposal.

2.4 Audit Charter and Terms of Engagement

2.4.1 IS Audit Charter

The IS Audit charter is like the constitution for the IS Audit function as it mandates the authority, scope and responsibility of IS Audit in the organisation. The IS Auditor should have a clear mandate to perform the IS audit function as authorised through the audit charter. This mandate is generally documented in an audit charter that should be formally accepted and approved by senior management. Where an audit charter exists for the audit function as a whole, the IS audit mandate should be included in the same.

The IT Auditing Assurance framework has the following standards for audit charter:

1001.1: The IS audit and assurance function shall document the audit function appropriately in an audit charter, indicating purpose, responsibility, authority and accountability.

1001.2: The IS audit and assurance function shall have the audit charter agreed upon and approved at an appropriate level within the enterprise.

Contents of the Audit Charter

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

Purpose

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

Responsibility

- Operating principles
- Independence
- Relationship with external audit
- Auditee requirements

- Critical success factors
- Key performance indicators
- Risk assessment
- Other measures of performance

Authority

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

Accountability

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

2.4.2 Audit Engagement Letter

Purpose: Engagement letters are often used for individual assignments or for setting the scope and objectives of a relationship between external IS audit and an 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.

Responsibility

- Scope
- Objectives
- Independence
- Risk assessment

- Specific Auditee requirements
- Deliverables

Authority

- Right of access to information, personnel, locations and systems relevant to the performance of the assignment
- Scope or any limitations of scope
- Evidence of agreement to the terms and conditions of the engagement

Accountability

- Intended recipients of reports
- Auditee rights
- Quality reviews
- Agreed completion dates
- Agreed budgets/fees if available

The standards of auditing (SA) 210 Agreeing the terms of Audit Engagements requires the auditor and the client to agree on the terms of engagement and document them in the audit engagement letter. It requires that the engagement letter be renewed if necessary before the commencement of the consecutive audit that follows.

The IS Audit is performed internally as per audit charter or it may be outsourced to an external IS Auditor. In case it is outsourced, an audit engagement letter is issued as per details discussed earlier. It is critical to note that external IS audits would have specific scope, objectives, timelines and deliverables whereas in case of internal IS Audit, these may be flexible and could vary depending on the needs of the enterprise. The audit assignment requires extensive involvement of the required personnel including management of the auditee environment, before, during and after completion of the assignment. Hence, continuing communication with the auditee is critical.

2.4.3 Communication with Auditee

Effective communication with Auditee involves:

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

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

- Availability for unplanned work
- Delivery of reports
- Costs
- Response to Auditee complaints

- Quality of service
- Review of performance
- Communication with Auditee
- Needs assessment
- Control risk self-assessment
- Agreement of terms of reference for audits
- Reporting process
- Agreement of findings

2.4.4 Quality Assurance Process

The IS Auditor should consider establishing a quality assurance process (e.g., interviews, customer satisfaction surveys, assignment performance surveys) to understand Auditee' needs and expectations relevant to the IS audit function. These needs should be evaluated against the charter with a view to improving the service or changing the service delivery or audit charter, as necessary. The IS Audit standards require IS Auditor to deploy and monitor completion of the assurance assignments with the staff having required competencies and skill-sets. If required, external experts may be used in the assignment as required. However, the responsibility of the assignment would still remain with the IS Auditor. IS auditor should develop standard approach, documentation and methodology with appropriate templates for various types of assignments. Best practices and frameworks along the required standards, guidelines and procedures should be used in developing quality assurance process and all the staff should be trained in the process to be followed in all stages of planning to execution and reporting of various types of assignments.

2.5 Audit Scope

A determination of the range of the activities and the period (of records that are to be subjected to an audit examination) is the scope of audit. The scope and objectives for every audit are determined through discussion with the auditee management and a specific risk assessment. The scope of audit would be specifically determined by the management in case of internal audit and is set by statute if it is as per regulatory requirement.

While each audit is unique, there are some general or common objectives applied to most audits. Once planning work begins, clearly defining the audit scope is important in determining the budget, human resources, and time required for audit and in determining what will have to be specifically reported and in which format. Scoping the audit involves narrowing the audit to relatively few matters of significance that pertain to the audit objective and that can be audited with resources available to the audit team. In a multi-entity audit, the scope includes identifying the specific departments or applications that will be included in the audit.

To identify matters of significance, the IS auditor has to conduct research on competitive environment, nature of business, technology used and the regulatory requirements to understand the auditee environment so as to plan and execute the assignment as per scope and objectives of the assignment:

- Are there areas that have an important impact on the organisation's results?

- Will the audit of the issue make a difference; that is, will it result in improved performance, accountability, or value for money?
- Are there issues with high visibility or of current concern?
- Are there areas that have undergone a significant degree of change? Examples of changes within an entity are new technology deployed, increased staff turnover, and reorganization; examples of changes to an entity's environment are new regulatory requirements, change in senior management, reporting of fraud amendments to enabling legislation, and budget cuts.
- Is the timing appropriate for auditing the issue?
- Are there any regulatory requirements which are critical? Are there any examples of past of non-compliance?
- What is the management style and the risk appetite and approach to risk management?
- Are there any cases of fraud or material errors of the past or reported which need review?

Carefully scoping the audit early in the process helps increase the efficiency and effectiveness of the audit. The statement of scope should be clear about any related areas that are not included.

2.6 Audit Planning

One of the primary and important phases in an IS Audit is planning which ensures that the audit is performed in an effective way and completed in a timely manner. Planning takes on more significance in case of IS Audit since audit risk in case of IS audits are significantly impacted by inherent risks. Hence, for the audit effort to be successful, a good audit plan is a critical success factor. In case of IS audit done by the internal IS Audit function, annual audit plan is developed based on the audit schedule, materiality, risk rating, business and regulatory requirements and previous audits done. Based on this and resource availability, specific teams and individuals are assigned for specific assurance reviews as per time plan. The audit planning process has to consider budgets of time and costs, and management priorities as per organisational goals and policies. The objective of audit planning is to optimise the use of audit resources. In case of independent assurance assignments, audit planning is done by external firm as per scope of audit engagement letter and considering available resource requirements and auditee availability schedule and schedule for reporting to regulatory authorities, if required.

As per SA 300 on "Planning" issued by ICAI

- Adequate planning of the audit work helps to ensure that appropriate attention is devoted to important areas of the audit, those potential problems are identified and that the work is completed expeditiously. Planning also assists in proper assignment of work to assistants and in co-ordination of work done by other Auditors and experts.
- The extent of planning will vary according to the size of the entity, the complexity of the audit and the IS Auditor's experience with the entity and knowledge of the business.
- Obtaining knowledge of the business is an important part of planning the work. The IS Auditor's knowledge of the business assists in the identification of events, transactions and practices which may have a material effect on the financial statements.
- The IS Auditor may wish to discuss elements of the overall audit plan and certain audit

procedures with the entity's audit committee, management and staff to improve the effectiveness and efficiency of the audit and to co-ordinate audit procedures with work of the entity's personnel. The overall audit plan and the audit programme; however, remain the IS Auditor's responsibility.

The IS Auditor should develop and document an overall audit plan describing the expected scope and conduct of the audit. While the record of the overall audit plan will need to be sufficiently detailed to guide the development of the audit program, its precise form and content will vary depending on the size of the entity, the complexity of the audit and the specific methodology and technology used by the IS Auditor.

The audit should be guided by an overall audit plan and underlying audit programme and methodology. Audit planning is often mistaken as a one-time activity to be taken and completed in the beginning of the audit. While for all practical purposes, planning is a continuous activity which goes on throughout the entire audit cycle. Many times changes in conditions or circumstances or unexpected findings during the course of audit require changes in the audit procedures and methodology initially planned. Hence IS Auditor is expected to modify the audit plan as warranted by the circumstances. The documentation of the audit plan is also a critical requirement. All changes to the audit plan should follow a change management procedure with every change being recorded with reason for change. Information Technology Assurance Framework (ITAF), 2nd edition issued by ISACA provides the following standards to be followed by IS Auditor: **(ITAF is included as reference material in the DVD).**

1201.1 IS audit and assurance professionals shall plan each IS audit and assurance engagement to address:

- Objective(s), scope, timeline and deliverables
- Compliance with applicable laws and professional auditing standards
- Use of a risk-based approach, where appropriate
- Engagement-specific issues
- Documentation and reporting requirements

1201.2 IS audit and assurance professionals shall develop and document an IS audit or assurance engagement project plan, describing the:

- Engagement nature, objectives, timeline and resource requirements
- Timing and extent of audit procedures to complete the engagement

Risk Assessment in Planning

1202.1 The IS audit and assurance function shall use an appropriate risk assessment approach and supporting methodology to develop the overall IS audit plan and determine priorities for the effective allocation of IS audit resources.

1202.2 IS audit and assurance professionals shall identify and assess risk relevant to the area under review, when planning individual engagements.

1202.3 IS audit and assurance professionals shall consider subject matter risk, audit risk and related exposure to the enterprise.

2.7 Objectives of IS Controls

IS audit requires primarily review of Controls in the IS environment and provide recommendations on areas of control weaknesses. The objective of IS controls is to ensure that risk management is implemented as per the risk management strategy which involves risk: avoid, eliminate, reduce or transfer and finally accept. Hence, controls should result in risk remediation as decided. Controls can be classified into 3 broad categories: Fiduciary which focuses on regulatory requirements, quality which focuses on efficiency and effectiveness and security which covers confidentiality, integrity and availability of information. These are the seven information criteria for implementing controls as per COBIT 4.1. It is important for IS Auditors to understand controls and control objectives as these form the most important criteria used for evaluation. Each of the controls are illustrated and explained above. Every IS Audit would have a combination of these controls which are used at time of scoping the assignment.

2.7.1 Principles of Fiduciary

Reliability: It relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities. The objective behind the rationale being that information should be reliable at any given point of time and the same is accessible as and when needed.

Compliance: It deals with complying laws, regulations and contractual regulations to which the business project is subject i.e. externally imposed business criteria as well as internal policies. For any business to succeed there is a need for compliance with regulations, hence one of the principles embedded in the framework deals with compliance parameters for all regulations at any given point of time.

2.7.2 Principles of Quality

Efficiency: A measure of whether the right amount of resources have been used to deliver a Process, Service or Activity. An Efficient Process achieves its Objectives with the minimum amount of time, money, people or other resources. Efficiency is one of the measures needed to determine value for money. It concerns the ratio of inputs (economy) to outputs (effectiveness) and is sometimes referred to as 'bangs per buck'. Typical measures will include money, time, people and quality.

Effectiveness: A measure of whether the Objectives of a Process, Service or Activity have been achieved. An Effective Process or Activity is one that achieves it agreed Objectives. Effectiveness, or Cost Effectiveness, is one of the measures needed to determine value for money. It concerns the cost of the outputs from an activity and the conformance of those outputs to a specification or need. Typical measures will include money, time, people and quality. Any investment that increases the cost of providing IT services should result in an enhancement to service quality or quantity. If this is not so, then the business case must be quite clear about why the Change is necessary.

2.7.3 Principles of Security (CIA)

Confidentiality: It refers to preventing the disclosure of information to unauthorised individuals or systems. Privacy or the ability to control or restrict access so that only authorised individuals can view sensitive information. One of the underlying principles of confidentiality is "need-to-know" or "least privilege". In effect, access to vital information should be limited only to those individuals who have a specific need to see or use that information. Confidentiality is necessary for maintaining the privacy of the people whose personal information a system holds.

For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorised party obtains the card number in any way, a breach of confidentiality has occurred.

Integrity: Information is accurate and reliable and has not been subtly changed or tampered with by an unauthorized party. Integrity includes:

- Authenticity: The ability to verify content has not changed in an unauthorised manner.
- Non-repudiation & Accountability: The origin of any action on the system can be verified and associated with a user.

The term Integrity is used frequently when considering Information Security as it is represents one of the primary indicators of security (or lack of it). The integrity of data is not only whether the data is 'correct', but whether it can be trusted and relied upon. Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people.

Availability: For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to

access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks. Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

It is important to note that confidentiality, integrity and availability are not the exclusive concern of information security. Business continuity planning places a significant emphasis on protecting the availability of information as part of the overall objective of business recovery. Common back office procedures, such as maker/checker, quality assurance, change control, etc. along with such regulatory areas as SOX 404 (Clause 49 is Indian version of Sarbanes Oxley Act i.e. SOX 2002) focus on ensuring the integrity of information.

The CIA Triad is entirely concerned with information. While this is the core factor of most IT security, it promotes a limited view of security that tends to ignore some additional, important factors. For instance, while Availability might serve to ensure that one does not lose access to resources, one need to provide information when it is needed, thinking about information security in and of itself in no way guarantees that someone else isn't making unauthorised use of your hardware resources.

2.8 Understanding the Auditee Environment

IS Auditors will have to understand the business processes of the enterprise and organisation structure to be able to perform an effective audit. This understanding of the business process has to be coupled with understanding of the enterprise's policies, procedures and practices as implemented. Any enterprise executes its business operations through its staff. These staff need to have defined job responsibilities, which are provided in the organisation structure. The organization structure needs to have internal control structure. IT implementation in the enterprise makes it imperative that the internal control structure is built into the IT as deployed. Further, IT impacts the way business operations could be performed and internal controls are implemented. Hence, it is critical for auditors to understand the organisation structure of the enterprise being audited as relevant to the objectives and scope of the assignment. The four key areas which have to be specifically understood by the IS Auditors are explained here.

2.8.1 Business of the Entity

The IS Auditor should obtain a preliminary knowledge of the entity and of the nature of ownership, management, regulatory environment and operations of the entity. Industry factors and indicators affecting the entity, for e.g. market and competitive forces, technology or service delivery mechanism, key business risk, legislation and regulatory framework should be understood.

Entity specific information of management, ownership, board composition with key personnel, corporate ethics and policies, details on information systems of financial package and Enterprise Resource Planning (ERP) system and IT controls are few areas, not exclusive, which the IS Auditors should acclimatise himself with, which shall enable them to plan and perform the audit.

2.8.2 Organisation Structure

Some of the organisational structure activities are task allocation, co-ordination and supervision,

which are directed towards the achievement of organisational aims. It can also be considered as the viewing glass or perspective through which individuals see their organisation and its environment. Organisations are a variant of clustered organisations. It can be structured in many different ways, depending on the objectives of the entity. Organisational structure allows the expressed allocation of responsibilities for different functions and processes to different organisations such as the branch, department, workgroup and individual. The IS Auditor has to factor the manner in which the organisation is set up to understand definitions of roles and responsibilities, policy framework, etc. to ensure efficiency and effectiveness of audit.

2.8.3 IT Infrastructure

The IS Auditor has to obtain understanding on the present IT infrastructure of the entity. As a part of developing the audit plan the IS Auditor has to keep in mind the present IT infrastructure capacities, the age of hardware and software, licensing agreements, third party vendor agreements etc. which is essential during the development of the IS audit plan. This ensures that the plan is effective and efficient. IS Auditors can accordingly plan their assessment testing on various areas like architecture testing, vulnerability testing, and other control testing.

2.8.4 Regulations, Standards and Frameworks

The IS auditor should ensure that specific regulatory requirements as applicable for the assignment are included as one of the primary criteria for evaluation. The specific steps for understanding this would include:

- Identify various regulations that are applicable to the organisation, depending on the nature of the organisation
- Compliance under all the regulations as identified above for the organisation.
- SA 250 “Considerations of laws and regulations in conducting an Audit” mentions that the auditor has to obtain just a general understanding of the laws and regulations applicable to the organisation and he should alert the management of the material non-compliances and the applicable penalties thereof, found during the engagement.

The auditor can exclusively perform engagements under any of the regulatory enactments to ensure its compliance depending on the nature of business organisation.

Information Technology Act 2000 (Amended in 2008)

Section 7A Audit of documents i.e. in Electronic Form: Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form. **(IT Act 2008 and rules are included in DVD).**

Under Section 43A of the (Indian) Information Technology Act, 2000, a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected. It is important to note that there is no upper limit specified for the compensation that can be claimed by the affected party in such circumstances.

The IT Act 2008 recognises and punishes offences by companies and individual (employee) actions. For example: Section 66 to 66F and 67 deal with the following crimes:

- Sending offensive messages using electronic medium or using body corporate's IT for unacceptable purposes
- Dishonestly stolen computer resource
- Unauthorised Access to computer resources
- Identity theft/Cheating by personating using computer
- Violation of privacy
- Cyber terrorism/Offences using computer
- Publishing or transmitting obscene material

Under Section 72A of the (Indian) Information Technology Act, 2000, disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years and fine extending to INR 5,00,000.

Sarbanes Oxley Act, 2002 (SOX)

As per section 404 of Sarbanes Oxley Act, 2002 (SOX), the independent Auditor of the organisation is required to opine on the effectiveness of internal control over financial reporting in addition to the Auditor's opinion on the fair presentation of the organisation's financial statements.

Section 404 draws attention to the significant processes that feed and comprise the financial reporting process for an organisation. In order for management to make its annual assessment on the effectiveness of its internal control, management is required to document and evaluate all controls that are deemed significant to the financial reporting processes.

Public Company Accounting Oversight Board (PCAOB)

PCAOB released Auditing Standard 5 "An audit of Internal Control over Financial Reporting that is integrated with an Audit of Financial Statements". This standard establishes requirements and provides direction that applies when an Auditor is engaged to perform an audit of management's assessment of the effectiveness of internal control over financial reporting ("the audit of internal control over financial reporting") that is integrated with an audit of the financial statements. Effective internal control over financial reporting provides reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes. If one or more material weaknesses exist, the company's internal control over financial reporting cannot be considered effective.

Clause 49 – Listing Agreement on Corporate Governance

Audit Committee

Role of the Committee sharpened with specific responsibilities including recommending appointment of Auditors and monitoring their independence and performance, approval of related party transactions, scrutiny of inter-corporate loans and investments, valuation of undertaking/ assets etc. Audit committee is contemplated as a major vehicle for ensuring controls, sound

financial reporting and overall good corporate governance.

Some of the reviews done by the Audit committee are as follows:

- Internal audit reports relating to internal control weaknesses; and
- The appointment, removal and terms of remuneration of the Chief internal Auditor shall be subject to review by the Audit Committee

ISO 27000 Family

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, which form the subject of the ISMS family of standards, and defines related terms and definitions.

ISO/IEC 27001 formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information security risks. The ISMS is an overarching management framework through which the organisation identifies, analysis and addresses its information security risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts – an important aspect in such a dynamic field, and a key advantage of ISO27k's flexible risk-driven approach.

ISO/IEC 27001 is a formalised specification for an Information System Management System (ISMS) with two distinct purposes:

1. It lays out, at a high level, what an organisation can do in order to implement an ISMS
2. It can (optionally) be used as the basis for formal compliance assessment by accredited certification IS Auditors in order to certify an organisation.

ISO/IEC 27002 is a code of practice – a generic, advisory document, not a formal specification such as ISO/IEC 27001. It recommends information security controls addressing information security control objectives arising from risks to the confidentiality, integrity and availability of information.

The standard is structured logically around groups of related security controls. Many controls could have been put in several sections but, to avoid duplication and conflict, they were arbitrarily assigned to one and, in some cases, cross-referenced from elsewhere. For example, a card-access-control system for, say, a computer room or archive/vault is both an access control and a physical control that involves technology plus the associated management/administration and usage procedures and policies.

2.9 Standards, guidelines and best practices of IS Audit

2.9.1 ITAF

ISACA has issued Information Technology Assurance Framework (ITAF) which is a comprehensive and good-practice-setting reference model that:

- Establishes standards that address audit and assurance professional roles and responsibilities; knowledge and skills; and diligence, conduct and reporting requirements
- Defines terms and concepts specific to IS assurance

- Provides guidance and tools and techniques on the planning, design, conduct and reporting of IS audit and assurance assignments

ITAF audit and assurance standards are divided into three categories:

- **General standards (1000 series)**—Are the guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments, and deal with the IS audit and assurance professional's ethics, independence, objectivity and due care as well as knowledge, competency and skill.
- **Performance standards (1200 series)**—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilisation, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgment and due care.
- **Reporting standards (1400 series)**—Address the types of reports, means of communication and the information communicated.

ITAF audit and assurance guidelines provide the auditor with information and direction about an IS audit or assurance area. In line with the three categories of standards outlined above, guidelines focus on the various audit approaches, methodologies and related material to assist in planning, executing, assessing, testing and reporting on IS processes, controls and related IS audit or assurance initiatives. Guidelines also help clarify the relationship between organisation activities and initiatives, and those undertaken by IT.

2.9.2 COBIT 5 Framework: Principles, Enablers, Processes, Assurance

As per COBIT 5, Information is the currency for organisations of the 21st century. Information, and the technology that supports it, can drive success, but it also raises challenging governance and management issues. This section explains the need for using the approach and latest thinking provided by globally recognised framework COBIT 5 as a benchmark for reviewing and implementing governance and management of enterprise IT. It explains the principles and enablers of COBIT 5 and how it can be as an effective tool to help organisations to simplify complex issues, deliver trust and value, manage risk, reduce potential public embarrassment, protect intellectual property and maximize opportunities. **You can download COBIT 5 from www.isaca.org/cobit.**

COBIT 5 helps organisations to manage IT related risk and ensures compliance, continuity, security and privacy. COBIT 5 enables clear policy development and good practice for IT management including increased business user satisfaction. The key advantage in using a generic framework such as COBIT 5 is that it is useful for organisations of all sizes, whether commercial, not-for-profit or in the public sector.

Five Principles of COBIT 5

COBIT 5 simplifies governance challenges with just 5 principles. The five key principles for governance and management of enterprise IT in COBTI 5 taken together enable the organisation to build an effective governance and management framework that optimises information and technology investment and use for the benefit of stakeholders.

Principle 1: Meeting stakeholders Needs: Enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimisation of risk and use of resources. COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT. Because every enterprise has different objectives, and enterprise can customise COBIT 5 to suit its own context through the goals cascade, translating high level enterprise goals into manageable specific, IT related goals and mapping these to specific processed and practices.

The COBIT 5 goals cascade is the mechanism to translate stakeholder needs to specific, actionable and customised enterprise goals; IT related goals and enabler goals.

Principle 2: Covering the enterprise End to End: COBIT 5 integrates governance of enterprise IT into enterprise governance. It covers all functions and processes within the enterprise; COBIT 5 does not focus only on the IT function, but treats information and related technologies as assets that needs to be dealt with just like any other asset by everyone in the enterprise. It considers all IT related governance and management enablers to be enterprise wide and end to end i.e. inclusive of everything and everyone internal and external that is relevant to governance and management of enterprise information and related IT.

Principle 3: Applying a Single Integrated Framework: There are many IT related standards and best practices, each providing guidance on a subset of IT activities. COBIT 5 is a single and integrated framework as it aligns with other latest relevant standards and frameworks; this allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator. It is complete in enterprise coverage, providing a basis to integrate effectively other frameworks, standards and practices used.

Principle 4: Enabling a Holistic Approach: Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several integrating components. COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as anything that can help to achieve objectives of the enterprise.

Principle 5: Separating Governance from Management: The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities require different organisational structures and serve different purposes.

- **Governance:** It ensures that stakeholders needs, conditions and options are evaluated to determine balanced, agreed on enterprise objectives to be achieved; setting direction through prioritisation and decision making, and monitoring performance and compliance against agreed on direction and objectives. In most organisations the governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities many be delegated to special organisational structures at an appropriate level, especially in larger, complex organisations.
- **Management:** It plans, builds, runs and monitors activities in alignment with the direction set by the governing body to achieve the objectives. In most of the enterprises management is the responsibility of the executive management under the leadership of the Chief Executive Officer (CEO).

From the definition of governance and management it is clear that they comprise different types of activities, with different responsibilities; however, given the role of governance to evaluate, direct and monitor a set of interactions is required between governance and management to result in an efficient and effective governance system.

Seven enablers of COBIT 5

Enablers are factors that, individually and collectively, influence whether something will work, in this case, governance and management over enterprise IT. Enablers are driven by the goals cascade, i.e. higher level IT related goals defining what the different enablers should achieve.

The seven categories of enablers are:

- Principles, Policies and Frameworks
- Processes
- Organisational structures
- Culture, Ethics and Behaviour
- Information
- Services, Infrastructure and Applications
- People, Skills and Competence

(These are discussed in more detail in Module 3)

Using COBIT 5 for IS Assurance

COBIT 5 has been engineered to meet expectation of multiple stakeholders, It is designed to deliver benefits to both an enterprise's internal stakeholders, such as the board, management, employees, etc. as well as external stakeholders – customers, business partners, external IS Auditors, shareholders, consultants, regulators, etc. It is written in a non-technical language and is therefore, usable not only by IT professionals and consultants but also by senior management personnel, assurance providers; regulators for understanding and addressing IT related issues as relevant to them. Globally from the GRC perspective, COBIT has been widely used with COSO by management, IT professionals, and regulators and Auditors (internal/external) for implementing or evaluating governance and management practices from an end to end perspective.

In the rapidly changing digital world, enterprises are inundated with new demands, stringent regulations and risk scenarios emerging daily, making it critical to effectively govern and manage information and related technologies. This has resulted in enterprise leaders being under constant pressure to deliver value to enterprise stakeholders by achieving business objectives. This has made it imperative for management to ensure effective use of information and technology investments and related IT for not only supporting enterprise goals but also to maintain compliance with internally directed and externally imposed regulations. This dynamic changing environment provides a challenge for Chartered Accountants (as assurance providers) to provide assurance with the required level of confidence. However, with the right type of skills and toolsets, this provides an excellent opportunity for Chartered Accountants to act as consultants, who provide relevant IT enabled services. A key component of this knowledge base is usage of globally accepted good practices and frameworks and developing a holistic approach, which meets the needs of stakeholders.

Evaluating the system of internal controls

COBIT 5 has specific process: "MEA 02 monitor, Evaluate and Assess the system of Internal Control", who provides guidance on evaluating and assessing internal controls implemented in an enterprise. Providing such review would provide assurance on the transparency for key stakeholders on the adequacy of the system of internal controls and this provide trust in

operations, confidence in the achievement of enterprise objectives and understanding of residual risks. The key management practices for assessing and evaluating the system of internal controls in an enterprise are as follows:

- Monitor internal controls
- Review business process controls effectiveness
- Perform control self-assessment
- Identify and report control deficiencies
- Ensure that assurance providers are independent and qualified
- Plan, scope and execute the assurance initiatives

2.10 Risk Assessment

As soon as the audit engagement begins, the IS Auditor should identify all the risks that are present in the IT Environment. IS Auditors have to perform a risk assessment to provide reasonable assurance that all material items will be adequately covered during the assignment. Based on this the required audit strategies, materiality levels and resource requirements can then be developed. The IS Auditor should perform this step bearing in mind that the said risks identified in this stage would be evaluated for the controls that have been incorporated to treat the risk. Thus the IS Auditor can focus on the High Risk areas and decide the sampling that would be performed on the identified areas. The risks can be identified by reviewing the factors implemented by the enterprise:

1. Reviewing IT principles, policies and frameworks.
2. Reviewing Processes, including risk-function-specific details and activities.
3. Reviewing organisational structures.
4. Observing culture, ethics and behaviour, factors of the employees.
5. Risk-specific information types for enabling risk governance and management within the enterprise.
6. With regard to services, infrastructure and applications, review service capabilities required to provide risk and related functions to an enterprise.
7. For the people, skills and competencies enabler, review the skills and competencies specific for risk.

The key business applications in use at a client are identified and addressed at a high level, in order to incorporate them into the future planning process. The controls within the client business application systems residing on the various platforms are evaluated during the course of the review. The management of the enterprise is expected to “Continually examine and make judgment on the effect of risk on the current and future use of IT in the enterprise. Consider whether the enterprise risk appetite is appropriate and that risk to enterprise value related to the use of IT is identified and managed.

2.10.1 Guidance on risk assessment by ISACA

The guidance provided by ISACA on risk assessment to be performed by IS Auditor is outlined here. When planning ongoing activities, the IS audit and assurance function should:

- Conduct and document, at least annually, a risk assessment to facilitate the development of the IS audit plan.
- Include, as part of the risk assessment, the organisational strategic plans and objectives and the enterprise risk management framework and initiatives.
- For each IS audit and assurance engagement, quantify and justify the amount of IS audit resources needed to meet the engagement requirements.
- Use risk assessments in the selection of areas and items of audit interest and the decisions to design and conduct particular IS audit and assurance engagements.
- Seek approval of the risk assessment from the audit stakeholders and other appropriate parties.
- Prioritise and schedule IS audit and assurance work based on assessments of risk.
- Based on the risk assessment, develop a plan that:
  - Acts as a framework for IS audit and assurance activities
  - Considers non-IS audit and assurance requirements and activities
  - Is updated at least annually and approved by those charged with governance
  - Addresses responsibilities set by the audit charter

When planning an individual engagement, IS audit and assurance professionals should:

- Identify and assess risk relevant to the area under review.
- Conduct a preliminary assessment of the risk relevant to the area under review for each engagement.

Objectives for each specific engagement should reflect the results of the preliminary risk assessment. :

- In considering risk areas and planning a specific engagement, consider prior audits, reviews and findings, including any remedial activities. Also consider the board's overarching risk assessment process.
- Attempt to reduce audit risk to an acceptable level, and meet the audit objectives by an appropriate assessment of the IS subject matter and related controls, while planning and performing the IS audit.
- When planning a specific IS audit procedure, recognise that the lower the materiality threshold, the more precise the audit expectations and the greater the audit risk.
- To reduce risk for higher materiality, compensate by either extending the test of controls (reduce control risk) and/or extending the substantive testing procedures (reduce detection risk) to gain additional assurance.

2.10.2 Risk Management steps

Risk management process practices, input/output and activities describe the following steps to be undertaken to assess risk:

Collect Data

1. Identify and collect relevant data to enable effective IT related risk identification, analysis and reporting.
2. Establish and maintain a method for the collection, classification and analysis of IT risk-related data, accommodating multiple types of events, multiple categories of IT risk and multiple risk factors.
3. Record relevant data on the enterprise's internal and external operating environment that could play a significant role in the management of IT risk.
4. Survey and analyse the historical IT risk data and loss experience from externally available data and trends, industry peers through industry-based event logs, databases, and industry agreements for common event disclosure.
5. Record data on risk events that have caused or may cause impacts to IT benefit/value enablement, IT programmer and project delivery, and/or IT operations and service delivery. Capture relevant data from related issues, incidents, problems and investigations.
6. For similar classes of events, organise the collected data and highlight contributing factors. Determine common contributing factors across multiple events.
7. Determine the specific conditions that existed or were absent when risk events occurred and the way the conditions affected event frequency and loss magnitude.
8. Perform periodic event and risk factor analysis to identify new or emerging risk issues and to gain an understanding of the associated internal and external risk factors.

Analyse Risk

1. Develop useful information to support risk decisions that take into account the business relevance of risk factors.
2. Define the appropriate breadth and depth of risk analysis efforts, considering all risk factors and the business criticality of assets. Set the risk analysis scope after performing a cost-benefit analysis.
3. Build and regularly update IT risk scenarios, including compound scenarios of cascading and/or coincidental threat types, and develop expectations for specific control activities, capabilities to detect and other response measures.
4. Estimate the frequency and magnitude of loss or gain associated with IT risk scenarios. Take into account all applicable risk factors, evaluate known operational controls and estimate residual risk levels.
5. Compare residual risk to acceptable risk tolerance and identify exposures that may require a risk response.
6. Analyse cost-benefit of potential risk response options such as avoid, reduce/mitigate, transfer/share, and accept and exploit/seize. Propose the optimal risk response.

7. Specify high-level requirements for projects or programmers that will implement the selected risk responses. Identify requirements and expectations for appropriate key controls for risk mitigation responses.
8. Validate the risk analysis results before using them in decision making, confirming that the analysis aligns with enterprise requirements and verifying that estimations were properly calibrated and scrutinised for bias.

SA 315 – Standard on Risk Assessment procedures issued by ICAI is also applicable for risk assessment pertaining to IS Audit assignment. This requires that the IS Auditor perform Risk Assessment Activities.

2.10.3 Risk Assessment procedures and related activities

The IS Auditor shall perform risk assessment procedures to provide a basis for the identification and assessment of risks and assertion levels. Risk assessment procedures by themselves, however, do not provide sufficient appropriate audit evidence on which to base the audit opinion. The risk assessment procedures shall include:

(a) Inquiries of management and of others within the entity who in the IS Auditor's judgment may have information that is likely to assist in identifying risks.

(b) Analytical procedures.

(c) Observation and inspection.

When the IS Auditor intends to use information obtained from the IS Auditor's previous experience with the entity and from audit procedures performed in previous audits, the IS Auditor shall determine whether changes have occurred since the previous audit that may affect its relevance to the current audit. The IS Auditor shall then assess the risk which is present in the business environment and in the internal control system that have the influence of the information systems and determine the nature and extent of the audit engagements on the relevant subjects.

2.10.4 Use of Risk Assessment in Audit Planning

When determining the functional areas to be audited, the IS Auditor could face a large variety of audit subjects. Each of these subjects may represent different types of risk. The IS Auditor should evaluate these various risk candidates to determine the high-risk areas that should be audited.

There are many risk assessment methodologies, computerised and non-computerised from which the IS Auditor may choose. These range from simple classifications of high, medium and low, based on the IS Auditor's judgment, to complex scientific calculations that provide a numeric risk rating.

One such risk assessment approach is a scoring system that is useful in prioritising audits based on an evaluation of risk factors. The system considers variables such as technical complexity, level of control procedures in place and level of financial loss. These variables may or may not be weighted. The risk values are then compared to each other and audits are scheduled accordingly. Another form of risk assessment is judgmental, where an independent decision is made based on business knowledge, executive management directives, historical perspectives, business goals and environmental factors. A combination of techniques may be used as well. Risk assessment methods may change and develop over time to best serve the needs of the organisation. The IS

Auditor should consider the level of complexity and detail appropriate for the organisation being audited.

2.11 Governance and Management Controls

2.11.1 IT General Controls areas

A general controls review attempts to gain an overall impression of the controls that are present in the environment surrounding the information systems. These include the organisational and administrative structure of the IS function, the existence of policies and procedures for the day-to-day operations, availability of staff and their skills and the overall control environment. It is important for the IS auditor to obtain an understanding of these as they are the foundation on which other controls reside.

A general controls review would also include the infrastructure and environmental controls. A review of the data centre or information processing facility should cover the adequacy of air conditioning (temperature, humidity), power supply (uninterruptible power supplies, generators) and smoke detectors/fire suppression systems, a conducive clean and dust free environment, protection from floods and water seepage as well as neat and identifiable electrical and network cabling.

Physical access control is another important area for review. Today in a highly networked world, logical access to computer systems is literally universal, yet there is a necessity to control physical access too. There are certain commands and settings that can be executed only from the console of the server and hence it is important to enclose all servers in a secure location protected by suitable mechanisms like locked doors, access swipe cards, biometric access devices or a combination of these. Further the IS auditors also should review the overall access control measures to the entire facility for controls like security guards at the entry gates, displaying of identification badges and logging visitor access.

IT General controls are controls that are not specific to any application, but exist in an IT environment. The general controls are designed for the environment as a whole. Some of the IT General Controls are as follows:

Operating System controls

Operating system is the computer control programme. It allows users and their applications to share and access common resources, such as processor, main memory, database and printers. It performs the main tasks of scheduling jobs, managing hardware and software resources, maintaining system security, enabling multi user resource sharing, handling interrupts and maintaining usage records.

Organisational controls

These controls are concerned with the decision-making processes that lead to management authorisation of transactions. Companies with large data processing facilities separate data processing from business units to provide control over its costly hardware, software, and human resources. Combining data processing into the business units would be too much responsibility for one manager. Organisational control techniques include documentation of:

- Reporting responsibility and authority of each function,
- Definition of responsibilities and objectives of each function,
- Policies and procedures,
- Job descriptions, and
- Segregation of duties.

(i) **Responsibilities and objectives:** Each IS function must be clearly defined and documented, including systems software, application programming and systems development, database administration, and operations. The senior manager, of all these groups, and managers of the individual groups make up the IS management team responsible for the effective and efficient utilisation of IS resources. Their responsibilities include:

- Providing information to senior management on the IS resources, to enable senior management to meet strategic objectives;
- Planning for expansion of IS resources;
- Controlling the use of IS resources; and
- Implementing activities and functions that support accomplishment of company's strategic plan.

(ii) Policies, standards, procedures and practices: Policies establish the rules or boundaries of authority delegated to individuals in the enterprise. These are the standards and instructions that all IS personnel must follow when completing their assigned duties. Procedures establish the instructions that individuals must follow to compete their daily assigned tasks. Mandating all requests for changes to existing programmes must be approved by user and IS management before programmers and analyst can work on them is an example of a policy. Documented instructions for filling out a standard change request form, how to justify the costs of the change, how to specify the changes needed, how to obtain approvals, and from whom obtain the approvals are examples of procedures. Documented policies should exist in IS for:

- Use of IS resources,
- Physical security,
- Data security
- On-Line security,
- Use of Information systems,
- Reviewing, evaluating, and purchasing hardware and software,
- System development methodology, and
- Application programme changes.
- Documented procedures should exist for all data processing activities.

(iii) Job descriptions

These communicate management's specific expectations for job performance. Job procedures establish instructions on how to do the job and policies define the authority of

the employee. All jobs must have a current documented job description readily available to the employee. Job descriptions establish responsibility and the accountability of the employee's actions.

(iv) Segregation of duties

Segregation of duties refers to the concept of distribution of work responsibilities such that individual employees are performing only the duties stipulated for their respective jobs and positions. The main purpose is to prevent or detect errors or irregularities by applying suitable controls. It reduces the likelihood of errors and wrongful acts organisation structure and allied controls should be structured in a manner that ensures the highest level of separation of duties. Critical factors to be considered in segregation of duties in a computerized information system are:

- Nature of business operations;
- Managerial policy;
- Organisation structure with job description; and
- IT resources deployed such as: Operating system, Networking, Database, Application software, technical staff available, IT services provided in-house or outsourced, centralised or decentralised IT operations.

Segregation of duties is the most common control technique aimed at separating conflicting job duties, primarily to discourage fraud, because separating duties makes collusion necessary to commit a fraud. Such separation can also force an accuracy check of one-person work by another, so that employees to some extent police each other. Examples of segregation of duties are:

- Systems software programming group from the application programming group;
- Database administration group from other data processing activities;
- Computer hardware operations from the other groups;
- Systems analyst functions from the programming function;
- Physical, data, and online security group(s) from the other IS functions; and
- IS Audit from business operations groups.

It is the responsibility of the senior management to implement a division of roles and responsibilities, which should exclude the possibility for a single individual to subvert a critical process. Management should also make sure that personnel are performing only those duties stipulated for their respective jobs and positions. From a functional perspective, segregation of duties should be maintained between the following functions:

- Information systems use,
- Data entry,
- Computer operation,
- Network management,
- System administration,
- Systems development and maintenance,

- Change management,
- Security administration, and
- Security audit.

Guidelines on segregation of duties

There are various general guidelines, with reference to 'Segregation of Duties', which may be followed in addition with concepts like, the maker should not be the checker:

- Separate those, who can run live programmes e.g. operations department, from those who can change programmes e.g. programmers. This is required in order to ensure that unauthorised programs are prevented from running.
- Separate those, who can access the data e.g. data entry and the DBA, from those who can run programs e.g. computer operators. This is required in order to ensure that unauthorized data entry cannot take place.
- Separate those, who can input data e.g. data entry, from those, who can reconcile or approve data e.g. data authorisation persons. This is required in order to ensure that unauthorised data entry cannot take place.
- Separate those, who can test programmes e.g. users, quality assurance and security, from those, who can develop programmes e.g. application programmers. This is required in order to ensure that unauthorised programmes cannot be allowed to run.
- Separate those, who can enter errors in a log e.g. data entry operator, who transfer the data to an error log, from those who can correct the errors like the end user departments. This is required in order to ensure that unauthorised data entry cannot take place.
- Separate those, who can enter data e.g. data entry personnel, from those who can access the database e.g. the DBA. This is required in order to ensure that unauthorised data entry or data modification cannot take place.

Management Controls

The controls adapted by the management of an enterprise are to ensure that the information systems function correctly and they meet the strategic business objectives. The management has the responsibility to determine whether the controls that the enterprise system has put in place are sufficient to ensure that the IT activities are adequately controlled. The scope of control here includes framing high level IT policies, procedures and standards on a holistic view and in establishing a sound internal controls framework within the organisation. The high level policies establish a framework on which the controls for lower hierarchy of the enterprise. The controls flow from the top of an organisation to down; the responsibility still lies with the senior management. The controls considerations while reviewing management controls in an IS system shall include:

- **Responsibility:** The strategy to have a senior management personnel responsible for the IS within the overall organizational structure.
- **An IT Organisation Structure:** There should be a prescribed IT organisational structure with documented roles and responsibilities and agreed job descriptions.

- **An IT Steering Committee:** The steering committee shall comprise representatives from all areas of the business, and IT personnel. The committee would be responsible for the overall direction of IT. Here the responsibility lies beyond just the accounting and financial systems; for example, the telecommunications system (phone lines, videoconferencing) office automation, and manufacturing processing systems.

Financial Controls

These controls are generally defined as the procedures exercised by the system user personnel over source, or transactions origination, documents before system input. These areas exercise control over transactions processing using reports generated by the computer applications to reflect un-posted items, non-monetary changes, item counts and amounts of transactions for settlement of transactions processed and reconciliation of the applications (sub. system) to general ledger. The financial control techniques are numerous. A few examples are highlighted here:

- **Authorisation:** This entails obtaining the authority to perform some act typically accessing to such assets as accounting or application entries.
- **Budgets:** These estimates of the amount of time or money expected to be spent during a particular period, project, or event. The budget alone is not an effective control. Budgets must be compared with the actual performance, including isolating differences and researching them for a cause and possible resolution.
- **Cancellation of documents:** This marks a document in such a way to prevent its reuse. This is a typical control over invoices marking them with a “paid” or “processed” stamp or punching a hole in the document.
- **Documentation:** This includes written or typed explanations of actions taken on specific transactions; it also refers to written or typed instructions, which explain the performance of tasks.
- **Dual control:** This entails having two people simultaneously access an asset. For example, the depositories of banks’ 24-hour teller machines should be accessed and emptied with two people present, many people confuse dual control with dual access, but these are distinct and different. Dual access divides the access function between two people: once access is achieved, only one person handles the asset. With teller machines, for example, two tellers would open the depository vault door together, but only one would retrieve the deposit envelopes.
- **Input/ output verification:** This entails comparing the information provided by a computer system to the input documents. This is an expensive control that tends to be over-recommended by auditors. It is usually aimed at such non-monetary by dollar totals and item counts.
- **Safekeeping:** This entails physically securing assets, such as computer disks, under lock and key, in a desk drawer, file cabinet storeroom, or vault.
- **Sequentially numbered documents:** These are working documents with preprinted sequential numbers, which enables the detection of missing documents.
- **Supervisory review:** This refers to review of specific work by a supervisor but this control requires a sign-off on the documents by the supervisor, in order to provide evidence that the supervisor at least handled them. This is an extremely difficult control to test after the

fact because the auditor cannot judge the quality of the review unless he or she witnesses it, and, even then, the auditor cannot attest to what the supervisor did when the auditor was not watching.

Note: Topic 2.11 is covered in more detail in module 4: Protection of Information assets.

Data management controls

Data management controls fall in 2 categories being:

- **Access controls:** Access controls are designed to prevent unauthorised individual from viewing, retrieving, computing or destroying the entity's data.
- **Back up control:** It ensures the availability of system in the event of data loss due to unauthorised access, equipment failure or physical disaster, the organisation can restore its files and database.

Organisational structure controls

In a computerized environment, transaction initiation is a critical activity. It requires segregation of duties at authorisation, processing and recording all aspects of a transaction. Segregation is done at many levels like segregation of maker and checker, asset record keeper and physical asset keeper, regular checking of effectiveness of internal controls.

Data Processing Controls

These controls are related to hardware and software and include procedures exercised in the IS environment. This includes on-Line transaction systems, database administration, media library, application programme change control, the data center.

Physical Access Controls

These controls are personnel; hardware and software related and include procedures exercised on access to IT resources by employees/outsiders. The controls relate to establishing appropriate physical security and access control measures for IT facilities, including off-site use of information devices in conformance with the general security policy. These Physical security and access controls should address supporting services (such as electric power), backup media and any other elements required for the system's operation. Access should be restricted to authorized individuals Where IT resources are located in public areas; they should be appropriately protected to prevent or deter loss or damage from theft or vandalism. Further, IT management should ensure zero visibility.

Logical Access Controls

Logical access controls are implemented to ensure that access to systems, data and programmes is restricted to authorised users so as to safeguard information against unauthorised use, disclosure or modification, damage or loss. The key factors considered in designing logical access controls include confidentiality and privacy requirements, authorisation, authentication and incident handling, reporting and follow-up, virus prevention and detection, firewalls, centralised security administration, user training and tools for monitoring compliance, intrusion testing and reporting.

System development controls

Such controls are targeted to ensure that proper documentation and authorisations are available for each phase of the system development process. It includes controls at controlling new system development activities and includes six activities of System authorisation activities, user specification activities, technical design activities, internal IS Auditor's participation, program testing and user test and acceptance procedures as a part of the system development controls. **These are covered in detail in module-5.**

Business Continuity Planning Controls

These controls are related to having an operational and tested IT continuity plan, which is in line with the overall business continuity plan, and its related business requirements so as to make sure IT services are available as required and to ensure a minimum impact on business in the event of a major disruption. The controls include criticality classification, alternative procedures, back-up and recovery, systematic and regular testing and training, monitoring and escalation processes, internal and external organizational responsibilities, business continuity activation, fall-back and resumption plans, risk management activities, assessment of single points of failure and problem management. **These are covered in detail in module-6.**

System maintenance controls

Management activities do include changes to programme logic, additional controls insertion and regular system maintenance activity. It is needed for efficient functioning of present systems.

Computer Centre security controls

Computer security can be of the following types: Physical security, software & data security and data communication security. Physical security attempts to restrict breach of computers and unauthorised access to records. Software and data security ensures that there is use of passwords, authorisations, screening and logs of all activity of the entity. Data communication security is implemented by terminal locks, encryption of data, network administration, sign on user identifiers, etc.

Internet and Intranet controls

There are two major exposures in the communication sub-system of component failure and subversive threats. Component failure can cause failure of transmission between sender and receiver. Subversive threats are invasion attempts to violate the integrity of some components in the system. It can provide intruders with important information about messages being transmitted and the intruder can manipulate these messages.

Personal computers controls

Some of the risks related to personal computer controls are that being small in size and portable the same can be carried within and outside the organisation resulting in loss of information, weak access controls and access to pen drives and external drives makes personal computers vulnerable for information loss.

Audit Trails

Audit trails are logs that can be designed to record activity at the system, application, and user level.

2.11.2 IT Application Controls types

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

Most users interact with the computer systems only through the application software. The application software enables and also limits the actions that a user can do. It is very important to subject application software to a thorough audit because the business processes and transactions involving money, material and services flow through the application software package.

The first question to ask in an application software review is, "What does the application software do; what business function or activity does it perform?" In this context it is very necessary for the IS auditor to know the business. For application reviews, the IS auditor's knowledge of the intricacies of the business is as important, if not more so, as the technical knowledge. Hence the first step in an application review is to understand the business function/activity that the software serves. This can be done through the study of the operating/work procedures of the organisation or other reference material. The other alternative is by interviewing the personnel.

Once this is done, it is necessary to identify the potential risks associated with the business activity/function served by the application (what can go wrong?) and to see how these risks are handled by the software (what controls it?).

Note: Application controls are covered in more detail in module-7: Business application software audit.

IT Applications controls are the controls that are in-built in the application itself. As the controls are built within the applications the same can be monitored, edited, re-structured and configured without the need for making changes to the whole environment. The objectives of application controls are:

- Input data is accurate, complete, authorised and correct.
- Data is processed in an acceptable time period.
- Data stored is accurate and complete
- Output is accurate and compete

A record is maintained to track the data from input to storage and to the eventual output.

Some of the categories of application control are as follows:

1. Boundary Controls

Controls to ensure that access to the application is restricted only to authorised users and that it protects systems from unauthorised access.

The objective of boundary controls is to prevent unauthorised access to applications and their data. Such data may be in any stage, in input, processing, transit or output. The controls restrict user access in accordance with the business policy of an organization and its structure; and protect other associated applications, systems software, database and utilities from unauthorised access.

Access controls may be implemented by using any of the logical security techniques embedded in the application software. Besides access security implemented at the operating system and/or database management systems level, a separate access control mechanism is required for controlling access to application. The application is to have boundary controls to ensure adequate access security to prevent any unauthorised access to:

- Applications themselves
- Application data during communication or transit
- Stored application data
- Resources shared with other processes

2. Input Controls

Controls to ensure that only complete, accurate and valid data and instructions form an input to the application.

Input controls address the following:

a. Source Document Design

b. Data entry screen design

c. Data code controls

d. Batch Controls

e. Data Input Validation Controls

f. Data Input Error Handling and Reporting

g. Instruction Input Controls

3. Processing Controls

Controls to ensure that there is only authorised processing and integrity of processes and data is ensured. Data processing controls perform validation checks to identify errors during the processing of data. They are required to ensure both the completeness and accuracy of the data being processed. Normally the processing controls are enforced through the database management system. However, adequate controls should be enforced through the front end application system also to ensure consistency in the control. Some of the data processing controls are as follows:

- Run to run totals
- Reasonableness verification
- Edit checks
- Exception reports

4. Data file controls

Controls to ensure that data resident in the files are maintained consistently with the assurance of integrity and confidentiality of the stored data.

Some of the data file controls are as follows:

- Version usage
- Internal and external labelling
- Data file security
- Before and after image and logging
- File updating and maintenance authorisation
- Parity checking

5. Output Controls

Controls to ensure that outputs delivered to the users in a consistent and timely manner in the format prescribed/required by the user. Output controls ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secured manner. Output can be in any form: either printed data report or a database file in a removable media such as a floppy disk, CD-ROM or removable hard disk. Whatever the type of output, confidentiality, integrity, and consistency of the output is to be maintained. The following form a part of output controls:

- Storage and logging of sensitive, critical forms
- Logging of output programme executions
- Spooling/queuing
- Controls over printing
- Report distribution and collection controls
- Retention controls

Existence controls ensure the continued availability of the application system and data in a consistent manner to the users. These form an integral part of the input, processing and output controls. Recovery of the application system from failures and restoration of both standing data as well as transaction data is very critical. Therefore, existence controls should include backup and recovery procedures of data. This requires secure storage of data files. Existence controls over processing of data should include adequate checkpoint/restart controls that recover the process from a failure without having to repeat the entire process from the beginning. Existence controls should also be exercised over output to prevent loss of output in any form.

2.11.3 Scope and steps of IS Audit of Application software

The information systems audit of application software should mainly cover the following areas:

- Adherence to business rules in the flow and accuracy in processing
- Validations of various data inputs
- Logical access control and authorisation

- Exception handling and logging

The steps to be performed in carrying out an application software review are as follows:

- Study and review of documentation relating to the application. However, the IS auditor may find situations in real life where documentation is not available or is not updated. In such cases, the auditor should obtain technical information about the design and architecture of the system through interviews.
- Study key functions of the software at work by observing and interacting with operating personnel during work. This gives an opportunity to see how processes actually flow and also observe associated manual activities that could act as complementary controls.
- Run through the various menus, features and options to identify processes and options for conformance to business rules and practices. (Studying the documentation before this can significantly hasten the activity.) To illustrate with an example, it is a well-accepted rule in financial accounting that once an accounting transaction has been keyed in and confirmed on the system to update the ledgers it should not be edited or modified. The correct method would be to pass a fresh reversal transaction to correct errors, if any. However, if the IS auditor observes that there is an option in the software to "edit/modify transactions," this would be noted as a control deficiency for correction. This kind of run-through can be done more effectively if a development/test system is made available to the IS auditor. In the absence of such a facility, the auditor only can watch the system run by the system administrator and make notes. The auditor is advised not to do any testing on a production system as this could affect adversely a "live" system.
- Validate every input to the system against the applicable criteria. Such validations go a long way in eliminating errors and ensuring data integrity. Apart from simple validations for numeric, character and date fields, all inputs should be validated with range checks, permissible values, etc. Validation checks that are built on application-specific logic can act as powerful controls not only for ensuring data accuracy but also to prevent undesirable data manipulations. The IS auditor can check validations by actually testing them out in the development/test system. Alternatively, looking at the database definitions, the associated triggers and stored procedures would be the way for a technically savvy IS auditor to review the validations.
- Verify access control in application software. This consists of two aspects-the inherent design of the access control module and the nature of access granted to various users and its maintenance. Every application software has a number of modules/options/menus that cater to the different functionality provided by the software. Different users will need access to various features based on their responsibilities and job descriptions. All access should be strictly based on the need to know and do. The design of the access control module may be of varied types. Most software would check a combination of user id and passwords before allowing access. Access may be controlled for each module, menu option, each screen or controlled through objects. Often the matrix of users versus the options/actions becomes too large and complex to maintain hence it is normal to define certain roles for different classes of employees and group them together and assign them similar access. The IS auditor should review the design of the access control module keeping in mind the criticality of the functions/actions possible in the software and evaluate whether the design provides the level of control and granularity to selectively and strictly allows access as per the job requirements of all the users.

Having done this, the auditor should proceed to verify whether all existing users have appropriate access as evidenced by their job descriptions and whether access to certain critical activities are allowed only to select personnel duly authorised. It also is necessary to verify who has administrator/SuperUser rights and how such rights are used/controlled. Ideally no one in the IT/ development group should have any access to the production data. All actions on the data by the SuperUser should be logged and verified by the data owners regularly.

- Verify how errors and exceptions are handled. In many activities software provides options and ways to reverse transactions, correct errors, allow transactions under special circumstances, etc. Each one of these is special to the business and based on the rules and procedures defined by the organisation for these. The IS auditor needs to see how the software handles these. Are these circumstances properly authorised in the software? Does it capture the user id and time stamp for all transactions to provide suitable trails? Are the exceptions and critical activities like updates to global parameters logged for independent review later?
- Correct any weaknesses found at the end of an applications review in the software that could lead to errors or compromises in security. These would need to be corrected by either changes in design and/or some recoding. While this would be addressed by the IT department, the user or owner of the application from the functional area would want to know if any of these weaknesses have been exploited by anyone and whether there have been any losses. To provide an answer to this question the IS auditor should download all the data for the period in question and run a series of comprehensive tests using an audit software and determine if any error or fraud really occurred or not.
- Evaluate the environment under which the application runs. The audit of the application software alone is not enough. Generally, it is prudent to conduct a security review of the operating system and the database in which the application runs while doing an application review.

All critical applications used in an organisation need to be subjected to detailed review by an IS auditor. This is one of the most important aspects of IS audit for a business. The job of application review becomes more complex as the application becomes larger and integrated. While auditing complex applications, it is always good to start with a generic industry-based template of an audit work programme and slowly customise the work program to the specific situation as the audit progresses.

2.12 Creation of Risk Control Matrix

An IS Audit is performed using the Risk Based approach. An IS Auditor charts a Risk and Control Matrix and uses the same for the audit engagement. The risk and control matrix is a matrix of the risks that have been identified in the Risk assessment phase. A typical RCM would consist the following –

- A series of spreadsheets marking a single process (Purchase Process), application (Custom Business Application), area (Information security, Logical Security, Physical security) etc.
- Each Spread sheet would contain generally the following columns –
  - Risk No, Risk in depth

- Control Objective – This column would contain the control(s) that is ideal to counter the identified risk.
- Control no
- Control in present – The present control that is implemented by the enterprise to counter the risk.

In addition to the above columns, the RCM may also be used as an Audit Notebook which contains the details of the control owner, process owner, testing plans and results, audit observations, evidences, Risk Ranking, Recommendations etc.

By using the RCM Methodology, an IS Auditor would be able to effectively identify evaluate the controls that are in place. The adequacy of the controls would be evaluated better and thus would be able to provide better assurance with regards to the controls that are in place and is sufficient.

2.13 Audit Sampling, Data Analysis and Business Intelligence

2.13.1 Audit Sampling

Audit sampling is defined as the application of audit procedures to less than 100 per cent of the population to enable the IS auditor to evaluate audit evidence about some characteristic of the items selected to form or assist in forming a conclusion concerning the population.

ISACA has issued guideline on audit sampling which may be referred and used for sampling in case of IS Audits. It states that the IS auditor should consider selection techniques that result in a statistically based representative sample for performing compliance or substantive testing. Examples of compliance testing of controls, where sampling could be considered, include user access rights, programme change control procedures, procedures documentation, programme documentation, follow-up on exceptions, review of logs and software licences audits. Examples of substantive tests, where sampling could be considered, include re-performance of a complex calculation (e.g., interest) on a sample of accounts, sample of transactions to vouch to supporting documentation, etc.

SA 530 – Audit Sampling: This Standard on Auditing (SA) applies when the auditor has decided to use audit sampling in performing audit procedures. It deals with the auditor's use of statistical and non-statistical sampling when designing and selecting the audit sample, performing tests of controls and tests of details, and evaluating the results from the sample.

The IS auditor can use the following methods for sampling:

1. Statistical Sampling which includes methods of Random Sampling & Systematic Sampling
2. Non Statistical Sampling which includes haphazard sampling, judgmental sampling.

While designing the sample the auditor should consider the objectives of the test and attributes of the population from which the sample would be drawn. Also the IS auditor has to keep in mind the conditions that constitute errors in reference to the objectives of the test. When using either statistical or non-statistical sampling methods, the IS auditor should design and select an audit sample, perform audit procedures, and evaluate sample results to obtain sufficient, reliable, relevant and useful audit evidence. The IS auditor can use the sampling technique while assessing the controls designed in the environment. On the basis of the initial assessment the sample size can be increased or decreased to achieve the objective of assessing the tests of existence of control for the IT environment.

2.13.2 Data Analysis

In the digital decade, the need for IT governance and IS assurance services is gaining increasing prominence. Rapid deployment of Information technology is making it imperative that Auditors have practical knowledge of using IT as a tool for drawing inferences and gathering relevant and reliable evidence as per requirements of the assignment. Data analysis through use of Computer Assisted Audit Techniques (CAATs) provide the tools for Auditors to directly access digital information and facilitate in conducting an effective and efficient audit. The need for understanding and auditing IT is not only relevant for specialist IS auditors but is imperative even for any audit. Understanding of data analysis tool and techniques will help auditors not only to perform their existing audits more efficiently and effectively but also facilitate the auditor in knowing how to create and execute new type of IT related audit assignments.

CAATs are a significant tool for auditors to gather information independently. CAATs can be used in various types of Audits including IS Audits. CAATs provide a means to gain access and to analyse data for a predetermined audit objective and to report the audit findings with emphasis on the reliability of the records produced and maintained in the system. The reliability of the source of the information used provides reassurance on findings generated. Auditors and more particularly IS Auditors should have a thorough understanding of CAATs and know where and when to apply them. Auditors to be effective in auditing IT environments need to gain practical experience in using CAATs for various audit and assurance assignments.

The use of Data analytics tools and techniques helps the IS auditor to improve audit approaches, unlike in the traditional approach which is based on a cyclical process involving manually identifying controls, performing tests and sampling a small population to measure the effectiveness. Data analytics also accommodates the growing risk focus on fraud detection.

The IS auditor can use data analytics by which insights are extracted from financial, operational and other forms of electronic data internal or external to the organisation. These insights can be historical, real time or predictive and can also be risk focused enabling the IS auditor to cover the audit from all dimensions and ensure effectiveness of audit.

2.13.3 Business Intelligence

Business intelligence (BI) is a set of theories, methodologies, architectures, and technologies that transform raw data into meaningful and useful information for business purposes. BI encompasses the collection and analysis of information to assist decision making and assess organisational performance. BI can handle enormous amount of unstructured data to help identify, develop and otherwise create new opportunities.

2.13.4 Analytical Review Procedures: CAAT Tools

Analytical Review Procedures

Analytical review procedures may be defined as substantive tests for a study of comparisons and relationship among data. An accounting system, whether it is manual or computer-based, is subject to mismanagement, error, fraud, and general abuse. The most direct way to combat these potential problems is to implement and maintain a strong system of internal controls for preventing and for detecting errors and irregularities.

CAATs

CAAT refer to the computer-based tools and techniques that give auditors ability to maximise their efficiency and effectiveness in performing audit function. CAATs are considered to be essential part of Toolkit for Auditors. CAATS can greatly enhance effectiveness and efficiency in the audit process during the planning, fieldwork, and reporting phases. IS auditors can use CAATs to perform tests that would normally be impossible or time-consuming to perform manually. For example: sorting, calculations, matching, and extracting of information as required. CAATs can allow an auditor to interrogate and analyse data more interactively, by removing the boundaries that can be imposed by a fixed audit program. For example, an auditor can analyse data and react immediately to the results of the analysis by simply modifying the parameters

The underlying reasons strongly call for controls and auditing in a computerised setup.

- **Absence of input documents:** Data may be entered directly into the computer system without supporting documents. In some on-Line transaction systems written evidence of data entry authorisation (for example, approval for order entry) may be replaced by other procedures, such as authorisation controls contained in computer programmes (for example, credit limit approval).
- **Lack of visible transaction trail:** Certain data may be maintained on computer files only. In a manual environment, it is normally possible to follow a transaction through the system by examining source documents, books of account and reports. In a computerized environment, however, the transaction trail may be partly in machine -readable form, or it may exist only for a limited period of time.

Functional Capabilities of CAATs

1. **File access:** Enables the reading of different record formats and file structures. All common formats of data such as database, text formats, excel files are accessible through the import function.
2. **File reorganisation:** Enables the indexing, sorting, merging and linking with another file. These functions facilitate the auditor to get an instant view of the data from different perspectives.
3. **Data selection:** Enables global filtration conditions and selection criteria. These functions enable selection of data based on defined criteria.
4. **Statistical functions:** Enables sampling, stratification and frequency analysis. These functions facilitate analysis of data.
5. **Arithmetical functions:** Enables arithmetic operators and functions. These functions facilitate re-computations and re-performance of results.

How to use CAATs?

IS Auditors need to have adequate computer knowledge, expertise and experience in using CAATs. They need to formulate appropriate methodology for using CAATs. This includes having a walk-through of the system to identify areas of weakness. Based on the results, Auditors will perform compliance tests, evaluate the results and if required, design substantive tests. CAATs can also be used to carry out detailed testing and collect evidences. Based on the results of these tests, Auditors would recommend suitable control measures as relevant. The step-by-step approach for using CAATs is given below:

1. Set the objective of the CAAT application
2. Determine the content and accessibility of the entity's files
3. Define the transaction types to be tested
4. Define the procedures to be performed on the data
5. Define the output requirements
6. Identify audit and IT personnel to be involved in design and use of tests for CAATs.

General Uses and Applications of CAATs

CAATs can be used for various types of tests. Some examples of tests are given below:

1. Exception identification: Identifying exceptional transactions based on set criteria
2. Control analysis: Identify whether controls as set have been working as prescribed.
3. Error identification: Identify data, which is inconsistent or erroneous.
4. Statistical sampling: Perform various types of statistical analysis.
5. Fraud detection: Identify potential areas of fraud
6. Verification of calculations: Perform various computations to confirm the data stored.
7. Existence of records: Identify fields, which have null values.
8. Completeness of data: Identify whether all fields have valid data.
9. Consistency of data: Identify data, which are inconsistent. For example: identify data, which is not in a particular sequence.
10. Duplicate payments: Establish relationship between two or more tables as required and identify duplicate transactions.
11. Undeserved discounts for rapid payment: Identify this based on analysis of set criteria.
12. Obsolescence of inventory: Identify obsolescence of inventory based on stratification, classification or aging.
13. Accounts exceeding authorised limit: Identify data beyond specified limit.
14. Overdue invoices: Identify data based on aging of invoices.

Strategies for using CAATs

CAATs are important tools for Auditors. They need to work out effective strategies to ensure their effective use.

The key strategies for using CAATs are:

1. Identify the goals and objectives of the investigation or audit. This may not always mean that CAATs will be used for a particular audit The point is to keep in mind all relevant techniques and technologies and to avoid traditional attitudes and thinking
2. Identify what information will be required, to address the goals and objectives of the investigation or audit.
3. Determine what the sources of the information are (Accounts payable system, payroll master file system, contracts system)

4. Identify who is responsible for the information (supervisors, department leaders, IT personnel)
5. Review documentation that describes the type of data in the system
6. Review documentation that describes how the information flows. Take time to understand the data. Know what each field in the data set represents and how it might be relevant to performing the audit. Review the record layout for the file Verify that the data is complete (Compare it to a hard copy).
7. Understand the system generating the data. The best defence against misunderstanding how the system processes data:
8. Review documentation on the system For example, user manuals, flowcharts, output reports
9. Develop a plan for analysing the data (What, When, Where, Why, and How)
    - **What:** Specific objectives that should be addressed by the analysis
    - **When:** Define the period of time that will be audited, and arrange with IT personnel to secure the data for that period
    - **Where:** Define the sources of the data to be analysed (Accounts payable, payroll)
    - **Why:** Reason for performing the tests and analysis (general review, fraud audit, VFM: Value for Money)
    - **How:** The types of analysis planned to be carried out by the audit (Note - Because of the nature of CAATs, the analysis plan should be viewed as a framework and not set in stone For example, additional *ad-hoc* test might be performed, based on preliminary findings)

Please refer to Module 6: Business application software audit which detailed coverage of CAATs with some case studies.

A sample listing of tools with brief outline of their category and key functions they perform are given here. These tools provide specific functionalities and need to be used as per the requirements of audit. Most of these tools are specialised in nature and perform specialised functions.

Tool Category	Example Tools	Tool Function
Data Reverse Engineering – Metadata based and relationships.	Bachman Logic Works ERWIN/ERX Embarcadero ER/1 Kismet	Process metadata to document systems and abstract business rules and relationships (High-end tools also derive some logical and conceptual schema information)
Data reverse Engineering – Data Content Based	Vanity Integrity QDB Analyse Data Star Wiz Rule	Process data content in conjunction with metadata to abstract business rules and relationships, automatically.

Tool Category	Example Tools	Tool Function
Batch Export/Transport – Parameter based extraction code generators	Carleton Passport ETI Extract Prism Warehouse Manager	Extraction is centrally controlled by parameters, code programmes are automatically generated. The tool accommodates data conversion and abstraction, as well as transport.
Data Content Quality – Filter based	Apercus Trillium	Positioned between export and import, it supports parameter based data filtering, they are used with different keys to keep data in alignment.
Special purpose data quality	Vality DB star IDI WizRule	Data quality is evaluated based on data content. Data patterns, rules and relationships discovered assist analysts determine data quality problem areas.

2.14 Compliance Testing

Compliance testing is evidence gathering for the purpose of testing an organisations' compliance with control procedures. A compliance test determines if controls are being applied in a manner that complies with management policies and procedures. For example, if the IS Auditor is concerned about whether production programme library controls are working properly, the IS Auditor might select a sample of programmes to determine if the source and object versions are the same. The broad objective of any compliance test is to provide IS Auditors with reasonable assurance that the particular control on which the IS Auditor plans to rely is operating as the IS Auditor perceived in the preliminary evaluation. Compliance Procedures are tests designed to obtain reasonable assurance that those internal controls on which audit reliance is to be placed are in effect.

It is important that the IS Auditor understands the specific objective of a compliance test and of the control being tested. Compliance tests can be used to test the existence and effectiveness of a defined process, which may include a trail of documentary and/or automated evidence for example, to provide assurance that only authorised modifications are made to production programmes.

The IS Auditor needs to ensure that internal control exist and that the internal control is operating effectively and being operating continuously throughout the period under audit to ensure that they can be relied upon. By performing Compliance Tests, the IS Auditor is able to ascertain the existence, effectiveness and continuity of the internal control system. Examples of compliance testing of controls where sampling could be considered include user access rights, programme change control procedures, documentation procedures, programme documentation; follow up of exceptions, review of logs, software licence audits, etc.

2.15 Substantive Testing

Substantive testing is testing where evidence is gathered to evaluate the integrity of individual transactions, data or other information. Substantive Procedures are tests designed to obtain evidence to ensure the completeness, accuracy and validity of the data. A substantive test substantiates the integrity of actual processing. It provides evidence of the validity and integrity of financial statements, and the transactions that support these balances. IS Auditors could use substantive tests to test for monetary errors directly affecting financial statement balances, or other relevant data.

Substantive testing is that which validates the details of financial transactions and balances, whereas compliance testing concentrates on validating the internal control procedures exercised over those financial transactions. Substantive testing validates the amounts of the transactions themselves. Substantive Testing are those which are performed in every audit and are sometimes known as default procedures. These procedures relate to the checking the completeness, accuracy and validity of the data produced by the enterprise. Examples of substantive tests where sampling could be considered include performance of a complex calculation on a sample of accounts or a sample of transactions to vouch for supporting documentation, etc.

2.16 Design and Operational effectiveness

2.16.1 Design Effectiveness

Testing of Design Effectiveness and testing of operating effectiveness would be performed by the IS Auditor on every identified control. Testing and operational effectiveness would be performed using CAAT, substantive testing and compliance testing as applicable. Testing of Design Effectiveness refers to the working design of the control as documented. It is a blue print of the control. The IS Auditor evaluates in general that the documented control is effective to remove the risk. It can be evaluated by reviewing the policies, procedure documents, brainstorming sessions etc.

A walkthrough of a business process and the risk controls within it can help evaluate its design effectiveness for compliance. Performing a walkthrough of the relevant functions or transactions and tracing them all the way through the complete process, from instigation, through authorisation, recording, processing and reporting will assist with the identification or existence of control activities to establish whether control activities are being performed (i.e. are in place), appraisal of the design of the risk controls, as well as substantiating the accuracy of process documentation.

A walkthrough is an end to end evaluation, step-by-step of a process and its controls to verify and validate understanding on the operation of the process and its associated controls and to evaluate whether the actual controls, if operated as designed can effectively mitigate risk to an acceptable level. In conducting the walkthrough it would be ensured sufficient evidence exists that reconciliations are being prepared by the nominated personnel (i.e. a reconciliation statement together with documentary evidence of the balance, and documentation intended to explain/justify/ evidence clearance of 'reconciling items') and that these are being reviewed (i.e. supervisor's signature). Where there is such evidence it can be concluded that the control has been placed in operation and (assuming that it is properly mitigating the related risk) considered 'design effective'.

Evaluation of design effectiveness is critical because only properly designed controls are capable of operating effectively. A control deficiency exists when the design or operation of a control, or group of controls, does not allow management or employees, in the normal course of performing their assigned roles and responsibilities, to prevent or detect failures on a timely basis.

2.16.2 Operational Effectiveness

Testing of Operating Effectiveness refers to actual performance of the Control in the IT Environment. The IS Auditor should evaluate the controls that have been documented. The purpose of operational self-testing is to gather sufficient documented evidence to enable a conclusion and testimony whether or not the controls as documented are operating in practice.

The IS Auditor will evaluate the effectiveness and efficiency of the control and would gain reasonable assurance whether the said control is sufficient to counter the identified risk. The IS Auditor would primarily check that the control is working to its expectations in accordance with its documented design.

Sample based self-testing. This involves the selection of samples (for each control tested) from the entire population of the particular control being tested, and the performance of specific test procedures on the selected sample. Testing requires accurately documented controls that are tested to ensure conformance to a requirement and, therefore, compliance.

The test will either start from the initiating documents within a process such as purchase order/ requisitions, for the Purchasing process or the test starts from the end of the process, i.e. the records in the accounting system. This flow of the test is determined by the assertions that need to be addressed. Once the sample has been selected from the complete population, evidence must be obtained that the control has been performed. For example, for a manual authorisation control this evidence will be the signature of the person who performs that control.

Documented evidence must be obtained to ascertain that the control has been performed as it has been designed. For manual controls; the evidence that the control has been performed should be available through physical records created when these controls have operated.

For system controls, the evidence of the control will be obtained through obtaining appropriate reports and screen shots to prove that the system configuration, system access, and system reports are as documented within the design. System controls, once established either work, or they do not. Evidence gathered to prove that a system control operated also proves that the control operated consistently and effectively.

Manual controls however, are subject to human error, and therefore we should test the quality of the control to gain assurance that the control has operated consistently and effectively. For example a signature on a User Access request does not necessarily mean that the person has carefully reviewed it. The signature itself does not provide sufficient evidence that the control has operated as intended; therefore we also need to test that the control has been performed correctly.

This would involve selecting a sample of the user access request process that is being tested and inspecting that the details on user access requests followed the process, so as to provide after the fact evidence that the individual carefully reviewed the user access request before approving it and was authorised to do so.

2.17 Audit Evidence: Methods

Evidence is any information used by the IS Auditor to determine whether the entity or data being audited follows the established criteria or objectives, and supports audit conclusions. It is a requirement that the IS Auditor's conclusions be based on sufficient, relevant, competent and appropriate audit evidence. When planning the IS audit, the IS Auditor should take into account the type of audit evidence to be gathered, its use as audit evidence to meet audit objective and its varying levels of reliability.

Audit evidence may include the IS Auditor's observations, notes taken from interviews, results of independent confirmations obtained by the IS Auditor from different stakeholders, material extracted from correspondence and internal documentation or contracts with external partners, or the results of audit test procedures. While all evidence will assist the IS Auditor in developing audit conclusions, some evidence is more reliable than others. The rules of evidence and sufficiency as well as the competency of evidence must be taken into account as required by audit standards.

2.17.1 Evaluating audit evidence

Determinants for evaluating the reliability of audit evidence include:

- **Independence of the provider of the audit evidence:** Evidence obtained from outside sources is more reliable than from within the organisation. This is why confirmation letters are used for verification of accounts receivable balances.
- **Qualifications of the individual providing the information/evidence:** Whether there providers of the information/evidence are inside or outside of the organisation, the IS Auditor should always consider the qualifications and functional responsibilities of the persons providing the information. This can also be true of the IS Auditor. If an IS Auditor doesn't have a good understanding of the technical area under review, the information gathered from testing that area may not be reliable, especially if the IS Auditor doesn't fully understand the test.
- **Objectivity of evidence:** Objectivity evidence is more reliable than evidence that requires considerable judgment or interpretation. An IS Auditor's review of media inventory is direct, objective evidence. An IS Auditor's analysis of the efficiency of an application, based on discussions with certain personnel, may not be objective audit evidence.
- **Timing of the evidence:** The IS Auditor should consider the time during which information exists or is available in determining the nature, timing and extent of compliance testing and, if applicable, substantive testing.

The IS Auditor gathers a variety of evidence during the audit. Some evidence may be relevant to the objectives of the audit, while other evidence may be considered as peripheral. The IS Auditor should focus on the overall objectives of the review and not the nature of the evidence gathered.

The quality and quantity of evidence must be assessed by the IS Auditor. These two characteristics are referred to be competent and sufficient. Evidence is competent when it is both valid and relevant. Audit judgment is used to determine when sufficiency is achieved in the same manner that is used to determine the competency of evidence.

2.17.2 Types of evidence

Physical examination: Is the inspection or count by the IS Auditor of a tangible asset. Most often associated with inventory and cash, but it is also applicable to the verification of securities, notes receivable and tangible fixed assets.

Confirmation: Is the receipt of a direct written response from a third party verifying the accuracy of information that was requested by the IS Auditor. The request is made to the client, and the client asks the third party to respond directly to the IS Auditor.

Documentation: Is the IS Auditor's inspection of the client's documents and records to substantiate the information that is, or should be, included in the Financial Statements. Documents can be INTERNAL (has been prepared or used within the client's organisation and is retained without going to an outside party) or EXTERNAL (has been handled by someone outside the client's organisation who is a party to the transaction being documented, which are either currently held by the client or readily accessible).

Analytical procedures: Uses comparisons and relationships to assess whether account balances or other data appear reasonable compared to the IS Auditor's expectations. An IS Auditor may compare the gross margin in the current year with the preceding years.

Inquiries of the Client: Is the obtaining of written or oral information from the client in response to questions from the IS Auditor. This type of evidence is usually not conclusive because it is not from an independent source. The IS Auditor must obtain additional evidence through other procedures.

Recalculation: Involves rechecking a sample of calculations made by the client. Rechecking client calculations consists of testing the client's arithmetical accuracy and includes such procedures as extending sales invoices and inventory, adding journals and subsidiary records, and checking the calculation of the depreciation expense and prepaid expenses.

Performance: Is the IS Auditor's independent tests of client accounting procedures or controls that were originally done as part of the entity's accounting and internal control system. Recalculation is rechecking a calculation, where performance involves checking other procedures.

Observation: Is the use of the senses to assess client activities. Observation is rarely sufficient by itself because of the risk of an IS Auditor changing their behaviour because of the IS Auditor's presence.

2.17.3 Types of Audit Evidences

The following are the different types of audit evidences that is usually generated.

- Documentation: Policy Documents, Procedure Documents
- Screenshots
- Photographs
- E-mail Correspondence with time stamps
- Memory Dump, Log Dump generated from the applications under consideration
- Surveys
- Audit work papers

- External Confirmations
- Written Representations – Refer SA 580

2.17.4 Evidence preservation

The evidence of a computer crime exists in the form of log files, file time stamps, contents of memory, etc. rebooting the system or accessing files could result in such evidence being lost, corrupted or overwritten. Therefore, one of the first steps taken should be copying one or more images of the attacked system. Memory content should also be dumped to a file before rebooting the system. Any further analysis must be performed on an image of the system and on copies of the memory dumped – not on the original.

In addition to protect the evidence, it is also important to preserve the chain of custody. Chain of custody is a term that refers to documenting, in detail, how evidence is handled and maintained, including its ownership, transfer and modification. This is necessary to satisfy legal requirements that mandate a high level of confidence regarding the integrity of evidence.

2.17.5 Standards on evidence

Standards by ICAI

Standard on Auditing (SA) 230, "Audit documentation" deals with the Auditor's responsibility to prepare audit documentation for financial statements. As a good practice the Auditor must document work in all stages which helps in maintaining the same not only as a progress report but later it can be used as evidence in courts of law.

Standard on Auditing (SA) 500, "Audit Evidence" explains what constitutes audit evidence in an audit of financial statements, and deals with the Auditor's responsibility to design and perform audit procedures to obtain sufficient appropriate audit evidence to be able to draw reasonable conclusions on which to base the Auditor's conclusions. Hence, the Auditor should clearly understand the importance of what constitutes as audit evidence and then the same should be preserved as a part of audit procedure.

Standard on Auditing (SA) 580 "Written Representations" deals with the Auditor's responsibility to obtain written representations from the management and, where appropriate, those charged with governance. The Auditor should document all the written representations as obtained from the management as a part of working papers and the same can be produced in the court of law, if the need arises.

Standards by ISACA

The standards by ISACA on evidence require the following compliance by IS Auditors>

1205 Evidence

1205.1 IS audit and assurance professionals shall obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the engagement results.

1205.2 IS audit and assurance professionals shall evaluate the sufficiency of evidence obtained to support conclusions and achieve engagement objectives.

Guidance by ISACA on evidence covers following key aspects

In performing an engagement, IS audit and assurance professionals should:

- Obtain sufficient and appropriate evidence, including:
  - The procedures as performed
  - The results of procedures performed
  - Source documents (in either electronic or paper format), records and corroborating information used to support the engagement
  - Findings and results of the engagement
  - Documentation that the work was performed and complies with applicable laws, regulations and policies
- Prepare documentation, which should be:
  - Retained and available for a time period and in a format that complies with the audit or assurance organisation's policies and relevant professional standards, laws and regulations.
  - Protected from unauthorised disclosure or modification throughout its preparation and retention.
  - Properly disposed of at the end of the retention period.
- Consider the sufficiency of the evidence to support the assessed level of control risk when obtaining evidence from a test of controls.
- Appropriately identify, cross-reference and catalogue evidence.
- Consider properties such as the source, nature (e.g., written, oral, visual, electronic) and authenticity (e.g., digital and manual signatures, stamps) of the evidence when evaluating its reliability.
- Consider the most cost-effective and timely means of gathering the necessary evidence to satisfy the objectives and risk of the engagement. However, difficulty or cost is not a valid basis for omitting a necessary procedure.
- Select the most appropriate procedure to gather evidence depending on the subject matter being audited (i.e., its nature, timing of the audit, professional judgement). Procedures used to obtain the evidence include:
  - Inquiry and confirmation
  - Re-performance
  - Recalculation
  - Computation
  - Analytical procedures
  - Inspection
  - Observation
  - Other generally accepted methods

- Consider the source and nature of any information obtained to evaluate its reliability and further verification requirements. In general terms, evidence reliability is greater when it is:
- In written form, rather than oral expressions
- Obtained from independent sources
- Obtained by the professional rather than by the entity being audited
- Certified by an independent party
- Kept by an independent party
- The result of inspection
- The result of observation

- Obtain objective evidence that is sufficient to enable a qualified independent party to re-perform the tests and obtain the same results and conclusions.
- Obtain evidence commensurate with the materiality of the item and the risk involved.
- Place due emphasis on the accuracy and completeness of the information when information obtained from the enterprise is used by the IS audit or assurance professional to perform audit procedures.
- Disclose any situation where sufficient evidence cannot be obtained in a manner consistent with the communication of the IS audit or assurance engagement results.
- Secure evidence against unauthorised access and modification.
- Retain evidence after completion of the IS audit or assurance work as long as necessary to comply with all applicable laws, regulations and policies.

2.18 Audit Documentation

As in any other audits, documentation of audit work forms a critical task which the IS Auditor should retain in support of his audit work. Significant amount of information may be generated during the course of the IS Auditor's work. The IS Auditor is required to ensure the evidence obtained by him on whom he bases his audit opinion is sufficient, reliable, relevant and useful and enables effective achievement of audit objectives. The audit documentation generally includes:

- Basic documents relating to the business, technology and control environment
- Documents relating to laws, regulations and standards applicable
- Preliminary review and how the audit objectives and scope were evaluated and agreed upon.
- Documents relating to Risk analysis
- Audit plan and progress against plan, Audit programmes
- Audit procedures as applied to the audit
- Audit findings, observations, inspection reports, management representations, logs, audit trails and other related evidence
- Interpretation of audit evidence
- Audit Report issued

- Auditee's observations and response to findings and recommendations.
- Reports by third party experts
- Peer Reviews

The audit working papers:

- Aid in the planning and performance of the audit
- Aid in the supervision and review of the audit work
- Provide evidence of the audit work performed to support the IS Auditor's opinion

The IS Auditor's work must be documented and organised in a standardised fashion for easy reference in future audits and reference by other IS Auditors. For purposes of easy reference, the documents may be organised as follows:

- Test work papers
- Permanent work papers
- Pending files
- Report files

Test working papers

The testing work papers, either electronic or otherwise are those prepared or obtained as a result of the compliance and substantive testing procedures performed by the IS Auditor, relevant to the audit engagement. Each working paper should follow a naming convention and numbering convention for naming and numbering of the work papers. The files should also contain a brief description of the content.

The compliance test files should contain documentation of:

- Review of the existing internal controls
- A summary of the tests conducted
- Documentation of procedures performed and tools, if any used
- Supporting documentation of detailed tests

Substantive test files require the same elements as compliance test files except for the review of existing internal controls.

Organisation of audit working papers:

Each document must describe the following:

- Objective – Why the work was done?
- Work done – What was actually done?
- Finding – What issues arose?
- Risk – What are the risks associated with the finding, expressed in terms of impact on business?
- Recommended action – What is being recommended?
- Action – What action was agreed with management?
- Each working paper should be supported by evidence of the weaknesses observed

Documentation Controls

Information systems audit documentation is the record of the audit work performed and the audit evidence supporting the IS Auditor's findings and conclusions.

- Each working paper (or work paper) should be:
- Dated and manually or digitally signed by the person completing the work
- Referenced with a unique number

In case of work papers and evidence in electronic format, special care must be taken to ensure their recoverability at any subsequent date with sufficient controls to prove the date of creation and ensure protection against any modifications to the content or the state of such documents. This would require the IS Auditor to use necessary technology such as use of appropriate media for storage of electronic evidence and their assured recoverability, use of digital signatures for protecting authenticity of documents, use of encryption techniques to safeguard the confidentiality of such documents. The IS Auditor should also take care to ensure retention of such audit documentation to be retained for sufficient length of period such that it complies with legal, regulatory, professional and organisational requirements.

Audit documentation should include, at a minimum a record of the

- Planning and preparation of the audit scope and objectives
- Description and/or walkthroughs on the scoped audit areas
- Audit program
- Audit steps performed and audit evidence gathered
- Use of services of other IS Auditors and experts
- Audit findings, conclusions and recommendations
- Audit documentation relation with document identification and dates
- A copy of the report issued as a result of the audit work.
- Evidence of audit supervisory review

Documents should include audit information that is required by laws and regulations, contractual stipulations and professional standards. Audit documentation is the necessary evidence supporting the conclusions reached, and hence should be clear, complete, easily retrievable and sufficiently comprehensible. Audit documentation is generally the property of the auditing entity and should be accessible only to authorised personnel under specific or general permission. Where access to audit documentation is requested by eternal parties, the IS Auditor should obtain appropriate prior approval of senior management and legal counsel.

The IS Auditor/IS audit department should also develop policies regarding custody, retention requirements and release of audit documentation. The documentation format and media are optional, but due diligence and best practices require that work papers are dated, initiated, page-numbered, relevant, complete, clear, self-contained and properly labelled, filed and kept in custody. Work papers may be automated. IS Auditors should particularly consider how to maintain integrity and protection of audit test evidence to preserve their proof value in support of audit results.

Audit documentation or work papers can be considered the bridge or interface between the audit objectives and the final report. They should provide a seamless transition with traceability and

accountability from objectives to report and from report to objectives. The audit report, in this contact, cab is viewed as a sort of particular work papers. Audit documentation should support the finding and conclusions/opinion. Time of evidence sometimes will be crucial to supporting audit findings and conclusions. The IS Auditor should take enough care to ensure that the evidence gathered and documented will be able to support audit findings and conclusions. An IS Auditor should be able to prepare adequate working papers, narratives, questionnaires and understandable system flowcharts.

IS Auditors are a scarce and expensive resource. Any technology capable of increasing the audit productivity is welcome. Automating work papers affects productivity directly and indirectly. The quest for integrating work papers in the IS Auditor's environment has resulted in all major audit and project management packages, CAATs and expert systems offering a complete array of automated documentation and import-export features.

2.19 Using work of another auditor and expert

Due to the scarcity of IS Auditors and the need for IT security specialists and other subject matter experts to conduct audits of highly specialized areas, the audit department or IS Auditors entrusted with providing assurance may be require the services of other IS Auditors or experts. Outsourcing of IS assurance and security services is increasingly becoming a common practice. External experts could include experts in specific technologies such as networking, automated teller machine, wireless, systems integration and digital forensics, or subject matter experts such as specialists in a particular industry or area of specialisation such as banking, securities trading, insurance, legal experts etc.

When a part or all IS audit services are proposed to be outsourced to another audit or external service provider, the following should be considered with regard to using the services of other IS Auditors and experts:

- Restrictions on outsourcing of audit/security services provided by laws and regulations
- Audit charter or contractual stipulations
- Impact on overall and specific IS audit objectives
- Impact on IS audit risk and professional liability
- Independence and objectivity of other auditors and experts
- Professional competence, qualifications and experience
- Scope of work proposed to be outsourced and approach
- Supervisory and audit management controls
- Method and modalities of communication of results of audit work
- Compliance with legal and regulatory stipulations
- Compliance with applicable professional standards

Based on the nature of assignment, the following may also require special consideration:

- Testimonials/references and background checks
- Access to systems, premises and records
- Confidentiality restrictions to protect customer related information

- Use of CAATs and other tools to be used by the external audit service provider
- Standards and methodologies for performance of work and documentation
- Non-disclosure agreements

The IS Auditor or entity outsourcing the services should monitor the relationship to ensure the objectivity and independence throughout the duration of the engagement. It is important to understand that often, even though a part of or whole of the audit work may be delegated to an external service provider, the related professional liability is not necessarily delegated. Therefore, it is the responsibility of the IS Auditor or entity employing the services providers to:

- Clearly communicate the audit objectives, scope and methodology through a formal engagement letter.
- Put in place a monitoring process for regular review of the work of the external service provider with regard to planning, supervision, review and documentation.
- Assess the usefulness and appropriateness of reports of such external providers, and assess the impact of significant findings on the overall audit objectives.

ISACA standards require the following to be complied by IS Auditor in using services of external experts.

1206 Using the Work of Other Experts

- 1206.1 IS audit and assurance professionals shall consider using the work of other experts for the engagement, where appropriate.
- 1206.2 IS audit and assurance professionals shall assess and approve the adequacy of the other experts' professional qualifications, competencies, relevant experience, resources, independence and quality-control processes prior to the engagement.
- 1206.3 IS audit and assurance professionals shall assess, review and evaluate the work of other experts as part of the engagement, and document the conclusion on the extent of use and reliance on their work.
- 1206.4 IS audit and assurance professionals shall determine whether the work of other experts, who are not part of the engagement team, is adequate and complete to conclude on the current engagement objectives, and clearly document the conclusion.
- 1206.5 IS audit and assurance professionals shall determine whether the work of other experts will be relied upon and incorporated directly or referred to separately in the report.
- 1206.6 IS audit and assurance professionals shall apply additional test procedures to gain sufficient and appropriate evidence in circumstances where the work of other experts does not provide sufficient and appropriate evidence.
- 1206.7 IS audit and assurance professionals shall provide an appropriate audit opinion or conclusion, and include any scope limitation where required evidence is not obtained through additional test procedures.

2.20 Evaluation of strengths and Weaknesses: Judging by materiality

The IS Auditor will review evidence gathered during the audit to determine if the operations reviewed are all well controlled and effective. This is also an area that requires the IS Auditor's judgment and experience. The IS Auditor should assess the strengths and weaknesses of the controls evaluated and determine if they are effective in meeting the control objectives established as part of the audit planning process.

A control matrix is often utilised in assessing the proper level of controls. Known types of errors that can occur in the area under review are placed on the top axis and known controls to detect or correct errors are placed on the side axis and known controls to detect or correct errors are placed on the side axis. Then, using a ranking method the matrix is filled with the appropriate measurements. When completed the matrix will substrate areas where controls are weak or lacking.

In some instances, one strong control may compensate for a weak control in another area. For example, if the IS Auditor finds weaknesses in a system's transaction error report, the IS Auditor may find that a detailed manual balancing process over all transactions compensates for the weaknesses in the error report. The IS Auditor should be aware of compensating controls in areas where controls have been identified as weak.

While a compensating control situation occurs when one stronger controls supports a weaker one, overlapping controls are two strong controls. Normally a control objective will not be achieved by considering one control adequate. Rather the IS Auditor will perform a variety of testing procedures and evaluate how these relate to one another. Generally a group of controls when aggregated together may act as compensating control and thereby minimise the risk. An IS Auditor should always review for compensating controls prior to reporting a control weakness. The IS Auditor may not find each control procedure to be in place but should evaluate the comprehensiveness of controls by considering the strengths and weaknesses of control procedures.

2.20.1 Judging the materiality of findings

The concept of materiality is a key issue when deciding which findings to bring forward in an audit report. Key to determining the materiality of audit findings is the assessment of what would be significant to different levels of management. Assessment requires judging the potential effect of the finding if corrective action is not taken. A weakness in computer security physical access controls at a remote distributed computer site may be significant to management at the site, but will not necessarily material to senior management at headquarters. However, there may be other matter at the remote site that would be material to upper management.

The IS Auditor must use judgment when deciding which findings to present to various levels of management. For example the IS Auditor may find that the transmittal form for delivering tapes to the offsite storage location is not properly initialed or authorisation evidenced by management as required by procedures. If the IS Auditor finds that management otherwise pays attention to this process and that there have been no problems in this area, the IS Auditor may decide that the failure to initial transmittal documents is not material enough to bring to the attention of upper management. The IS Auditor might decide to discuss this only with local operations management.

However, there may be other control problems that will cause the IS Auditor to conclude that this is a material error because it may lead to a larger control problem in other areas. The IS Auditor should always judge which findings are material to various levels of management and report them accordingly.

2.21 Risk Ranking

Risks are typically measured in terms of impact and likelihood of occurrence. Impact scales of risk should mirror the units of measure used for organisational objectives, which may reflect different types of impact such as financial, people, and/or reputation. Similarly, the time horizon used to assess the likelihood of risks should be consistent with the time horizons related to objectives.

Risk rating scales may be defined in quantitative and/or qualitative terms. Quantitative rating scales bring a greater degree of precision and measurability to the risk assessment process. However, qualitative terms need to be used when risks do not lend themselves to quantification, when credible data is not available, or when obtaining and analysing data is not cost-effective.

Organisations typically use ordinal, internal, and/or ratio scales. Ordinal scales define a rank order of importance (e.g., low, medium, or high), interval scales have numerically equal distance (e.g., 1 equals lowest and 3 equals highest, but the highest is not 3 times greater than the lowest), and ratio scales have a "true zero" allowing for greater measurability (e.g., a ranking of 10 is 5 times greater than a ranking of 2). Risk rating scales are not one-size-fits-all and should be defined as appropriate to enable a meaningful evaluation and prioritisation of the risks identified and facilitate dialogue to determine how to allocate resources within the organisation.

An example of a Risk Rating Model is given below –

Green Areas: These are areas that have been identified as being low risk, from a business as well as an audit perspective. It is not critical that the controls over these areas are reviewed in detail on an annual or a rotational basis. However, the decision not to rotate is a management decision.

Orange Areas: These are areas that have been identified as medium risk (i.e., an important risk exists, but it is not so material that it is likely to result in significant loss or embarrassment should the required controls not operate effectively). The controls over these areas should be reviewed at least once every two to three years on a rotational basis.

Red Areas: These are areas considered to be inherently high risk from either a business or audit perspective and therefore capable of resulting in significant financial loss or embarrassment. The controls over these systems should be reviewed on an annual basis to confirm that the controls are in place and continue to be adequate to mitigate the inherent risks.

2.22 Audit Report Structure and contents

ISACA standards require IS audit and assurance professionals shall provide a report to communicate the results upon completion of the engagement including:

- Identification of the enterprise, the intended recipients and any restrictions on content and circulation
- The scope, engagement objectives, period of coverage and the nature, timing and extent of the work performed

- The findings, conclusions, and recommendations
- Any qualifications or limitations in scope that the IS audit and assurance professional has with respect to the engagement
- Signature, date and distribution according to the terms of the audit charter or engagement letter

Further, it requires IS audit and assurance professionals shall ensure findings in the audit report are supported by sufficient and appropriate audit evidence.

The exit interview, conducted at the end of the audit, provides that the IS Auditor with the opportunity to discuss findings and recommendations with management. During the exit interview the IS Auditor should:

- Ensure that the facts represented in the report are correct
- Ensure that the recommendations are realistic and cost effective, and if not, seek alternatives through negotiation with Auditee management.
- Recommend implementation dates for agreed on recommendations.

The IS Auditor will frequently be asked to present the results of audit work to various levels of management. The IS Auditor should have a thorough understanding of the presentation techniques necessary to communicate the results. Presentation techniques could include the following:

- **Executive summary:** An easy to read concise report that presents findings to management in an understandable manner. Findings and recommendations should be communicated from a business perspective. Detailed attachments can be more technical in nature since operations management will require the details to correct the reported situations.
- **Visual presentation:** May include slides or computer graphics

IS Auditors should be aware that ultimately they are responsible to senior management and the audit committee of the board of directors. IS Auditors should feel free to communicate issues or concerns to such management. An attempt to deny access by levels lower than senior management would limit the independence of the audit function.

Before communicating the results of an audit to senior management, the IS Auditor should discuss the findings with the management staff of the audited entity. The goal off such a discussion would be to gain agreement on the findings and develop a course of corrective action. In cases where there is disagreement, the IS Auditor should elaborate on the significance of the findings, risks and effects of not correcting the control weakness. Sometimes the auditor's management may request assistance from the IS Auditor in implementing the recommended control enhancements. The IS auditor's role and that of a consultant, and give careful consideration to how assisting the Auditee may adversely affect the IS Auditor's independence.

Once agreement has be reached with the audited, IS audit management should brief senior management of the audited organisation. A summary of audit activities will be presented periodically to the Audit Committee. Audit Committees typically are composed of individuals who do not work directly for the organization and thus provide the IS Auditors with an independent route to report sensitive findings.

2.22.1 Audit report structure and contents

Audit reports are the end product of the IS audit work. They are used by the IS Auditor to report findings and recommendations to management. The exact of are audit report will vary by organization, however the skilled IS Auditor should understand the basic components of an audit report and how it communicates audit findings to the management.

There is no specific format for an IS audit report; the organisation's audit policies and procedures will dictate the general format. Audit reports will usually have the following structure and content:

- An introduction to the report, including a statement of audit objectives, limitations to the audit and scope, the period of audit coverage, and a general statement on the nature and extent of audit procedures conduct and processes examined during the audit, followed by a statement on the IS audit methodology and guidelines.
- A good practice is to include audit findings in separate sections. These findings can be grouped in sections by materiality and/or intended recipient.
- The IS Auditor's overall conclusion and opinion on the adequacy of controls and procedures examined during the audit, and the actual potential risks identified as a consequence of detected deficiencies.
- The IS Auditor's reservations or qualifications with respect to the audit. This may state that the controls or procedures examined were found to be adequate or inadequate. The balance of the audit report should support that conclusion and the overall evidence gathered during the audit should provide an even greater level of support for the audit conclusions.
- Detailed audit findings and recommendations – the IS Auditor would decide whether to include specific findings in an audit report. This should be based on the materiality of the findings and the intended recipient of the audit report
- A variety of findings some of which may be quite material while others are minor in nature. The IS Auditor may choose to present minor findings to management in an alternative format such as by memorandum.

The IS Auditor however should make the final decision about what to include or exclude from the audit report. Generally, the IS Auditor should be concerned with providing a balanced report, describing not only negative issues in terms of findings but positive constructive comments regarding improving process and controls or effective controls already in place. Overall, the IS Auditor should exercise independence in the reporting process.

Auditee management evaluates the findings, stating corrective actions to be taken and timing for implementing these anticipated corrective actions. Management may not be able to implement all audit recommendations immediately. For example, the IS Auditor may recommend changes to an information system that is also undergoing other changes or enhancements. Rather, all may be implemented at once.

The IS Auditor should discuss the recommendations and any planned implementation dates while in the process of releasing the audit report. The IS Auditor must realise that various constraints, such as staff limitations, budgets or other projects may limit immediate implementation. Management should develop a firm programme for corrective actions. It is important to obtain a commitment from the Auditee/management on the date by which the action plan will be

implemented and the manner in which it will be performed since the corrective action may bring certain risks that may be avoided if identified while discussing and finalising the audit report. If appropriate, the IS Auditor may want to report to upper management on the progress of implementing recommendations. **Sample format of IS Audit finding, audit report and executive summary of audit report are given in Section - 3.**

2.23 Management Implementation of recommendations

IS Auditors should realise that auditing is an ongoing process. The IS Auditor is not effective if audits are performed and reports issued. But no follow up is conducted to determine whether management has taken appropriate corrective actions. IS Auditors should have a follow up programme to determine if agreed on corrective actions have been implemented. Although IS Auditors who work for external audit firms may not necessarily follow this process, they may achieve these tasks if agreed to by the audited entity.

The timing of the follow-up will depend on the criticality of the findings and would be subject to the IS Auditor's judgment. The results of the follow up should be communicated to appropriate levels of management. The level of the IS Auditor's follow up review will depend on several factors. In some instances, the IS Auditor may merely need to inquiries to the current status. In other instances, the IS Auditor who works in an internal audit function may have to perform certain audit steps to determine whether the corrective actions agreed on by management have been implemented.

2.24 Follow up review

ISACA standards require IS audit and assurance professionals shall monitor relevant information to conclude whether management has planned/taken appropriate, timely action to address reported audit findings and recommendations. The effectiveness of an IS Audit is realised only if the action points and recommendations committed and agreed to by the Auditee management are implemented. Hence an important task of the IS Auditor is to review the previous audit reports and follow up on the corrective actions and recommendations implemented within the time schedules committed by the Auditee management. It is a limited scope review and do not entail going beyond the examination of actions agreed upon by the client to correct deficiencies. Normally, the status of follow up activities is included in a separate Compliance Audit Report which is issued after the completion of follow-up review. IT audit is not effective if audits are performed and reports issued, but no follow-up is conducted to determine if Auditee organisation has taken appropriate corrective action.

The IS Auditor should have a follow-up programme to determine if agreed corrective actions have been implemented. The level of the IS Auditor's follow-up review will depend upon several factors. In some instances, the IS Auditor may merely need to inquire as to the current status. In other instances, the IS Auditor may have to perform certain audit steps to determine if the corrective action agreed to by the Auditee organisation have been implemented

The Institute of Internal IS Auditors definition of a follow-up: "A follow-up is defined as a process by which the internal IS Auditors determine the adequacy, effectiveness and timeliness of actions taken by management on reported audit findings." Where agreed action plans are not completely implemented the IS Auditor asks the following questions:

- What remains to be done?
- By whom and when?
- Have alternatives been implemented that may be more appropriate?
- Has the agreed action plan ceased to be of value?
- If no action was taken, why not?
- What is the issue or concern causing inaction?

The end result should be a brief summary of the status of every action plan agreed upon. The final summary is reviewed with the person responsible for clearing the audit report before the follow-up report is issued.

2.25 Summary

This chapter has provided detailed explanation of how an IS Audit is executed in all its phases from planning to execution to reports. IS auditors to be able to perform IS Audit assignments need to have good understanding of concepts of auditing, IT and management. This chapter has covered in the following concepts along with extracts from relevant standards and guidelines as applicable.

- How to conduct various types of IS audit as per scope and objective of assignment after understanding the auditee environment including the nature of business, organisation structure, technology environment, applicable regulations using relevant standards and best practices framework?
- How to review and evaluate various types of risk and its assessment which form the basis on which the audit conclusions can be made?
- How to use analytical procedures, compliance and substantive testing method for performing the audit.
- How to review the design effectiveness and control effectiveness?
- How to collect and evaluate evidence and maintain relevant documentation during the course of IS audit?
- How to perform risk ranking and prepare the final audit report with recommendations and follow up procedures?

The primary objective of this chapter was to provide understanding of both the concepts and practice of IS audit and the various phases involved covering the planning of audit process, understanding of the risks involved, conducting the audit by, obtaining and evaluating evidence using CAATs and issuing the final audit report containing recommendations.

2.26 Questions

1. The IS Auditor should use which of the following when developing the overall IS Audit Plan and determining priorities for the effective allocation of IS Audit Resources?
   A. Audit Materiality
   B. The work of outside experts
   C. Risk Assessment
   D. IT Governance
2. Which of the following sampling types is used to estimate the rate of occurrence of a specific quality in population?
   A. Discovery Sampling
   B. Statistical Sampling
   C. Attribute Sampling
   D. Stop-or-go Sampling
3. Which of the following criteria for selecting the applications to be audited is LEAST likely to be used?
   A. Materiality of audit risk
   B. Sensitivity of transactions
   C. Technological complexity
   D. Regulatory agency involvement
4. The first step IS Auditor should take when preparing the annual IS audit plan is to:
   A. Meet with the audit committee members to discuss the IS audit plan for the upcoming year
   B. Ensure that the IS audit staff is competent in areas that are likely to appear on the plan and provide training as necessary
   C. Perform a risk ranking of the current and proposed application systems to prioritise the IS audits to be conducted
   D. Begin with the prior year's IS audit plan and carry over any IS audits that had not been accomplished
5. The purpose of compliance tests is to provide reasonable assurance that:
   A. Controls are working as prescribed
   B. Documentation is accurate and current
   C. The duties of users and data processing personnel are segregated
   D. Exposures are defined and quantified

6. While reviewing internal controls in a microcomputer environment, an IS auditor recommends that duties should be regularly rotated. The effect of implementing this recommendation would ensure which of the following controls?
   A. Detective
   B. Compensating
   C. Corrective
   D. Preventive
7. Which of the following is the least important factor in determining the need for an IS Auditor to be involved in a new system development project?
   A. The cost of the system
   B. The value of the system to the organization
   C. The potential benefits of the system
   D. The number of lines of code to be written
8. Each of the following is a general control concern EXCEPT
   A. Organisation of the IS Department
   B. Documentation procedures within the IS Department
   C. Balancing of daily control totals
   D. Physical access controls and security measures
9. Which of the following types of audits requires the highest degree of data processing expertise?
   A. Systems software audits
   B. General controls reviews
   C. Microcomputer application audits
   D. Mainframe application audits

2.27 Answers and Explanations

1. C. The IS Auditor should use Risk Assessment while developing an overall IS Audit Plan. The other examples are examples of audit standards.
2. C. Attribute sampling is used to estimate the rate of occurrence of a specific quality in population. The other sampling methods described are legitimate sampling methods often employed by auditors during audit.
3. C. Because technical complexity of an application is not as important as the materiality of the audit risk associated with an application or sensitivity of the transactions. Regulatory agency requirements also play an important role in determining what to audit. Answer "b" is NOT the best choice because sensitivity of transactions would be an exposure to a company and should be considered in determining which applications should be audited.

Answer "a" is NOT the best choice because the measurement of audit risk is an important component when determining the scope of an audit plan. The materiality of the audit risk associated with specific application would have an impact on whether the application is included in the audit scope. Answer "d" is NOT the best choice because applications may relate to operational areas of the Company where regulatory agencies have required audits.

4. C Because IS audit services should be expended only if the risk warrants it. Answers a, b, and d occur after c has been completed. Answer "b" is NOT correct because the IS Audit Manager does not know what areas are to appear on the IS audit plan until a risk analysis is completed and discussions are held with the Audit Committee members. Answer "a" is NOT correct because the IS Audit Manager would not meet with the Audit Committee until a risk analysis of areas of exposure has been completed. Answer "d" is NOT correct because a risk analysis would be the first step before any IS audit services are expended.

5. A. The compliance tests determine whether prescribed controls are working. Answer "b" is NOT the best choice. Current and accurate documentation may be a good procedure but it is only one type of control procedure, therefore, answer *'A'* is a better choice as more control procedures are evaluated. Answer "c" is NOT the best choice because segregation of duties is only one type of control procedure; therefore, answer *'A'* is a better choice as more control procedures are evaluated. Answer "d" is NOT the correct choice. Exposures are defined and quantified to determine audit scope. Compliance tests provide reasonable assurance that controls are working as prescribed.

6. B. A small institution may find that separation of duties (which is a preventative control) may not be practical since there are too few employees. In such a circumstance, it may be possible to establish an acceptable control environment by instituting compensating measures such as rotation of job duties.

7. D. The size of the system is the least important of the factors listed. All other factors have specific financial implications and an IS Auditor can be used to help mitigate the risk to the corporation with the development of a new system.

8. C. Balancing of daily control totals relates to specific applications and is not considered an overall general control concern. Answer "b" is NOT the best answer since documentation procedures within the IS Department is an important general control concern. Answer "a" is NOT the best answer since organisation of the IS Department is an important general control concern. Answer "d" is NOT the best answer since physical access controls and security measures are important general control concerns.

9. A. The IS Auditor needs specialised education in hardware and operating systems software. Answers b, c, and d can be performed when an IS Auditor has a basic level of data processing technical knowledge and usually requires no special training. Answer "b" is NOT correct because general controls reviews typically do not require as technical a level of knowledge as an audit of systems software. Answer "c" is NOT correct because microcomputer application reviews generally do not require as technical a background as an audit of systems software. Answer "d" is NOT correct because mainframe application audits typically do not require special training or as technical level of knowledge as system software reviews.

CHAPTER 3: IT ENABLED SERVICES

Learning Objectives

This chapter provides an overview of different types of audit engagements that can be undertaken by the IS auditor. Further, there is an insight into the world of frauds and cyber-crimes which have grown as a part of the technological advances. The IS auditor may also undertake role of an investigator on behalf of the enterprise to investigate various modes of data leakage and theft and use digital forensics to retrieve data from damaged hard disks, and other mediums of data storage. This requires advance technical skills but a brief overview is provided so that DISAs who are interested can venture into new area.

3.1 Introduction

As information systems' presence has become indispensable part of our day-to-day living and as enterprise processes have become inseparable from IT, it has becoming increasingly critical to ensure safe and secure access to information from a computing environment and make it available to anyone at any point of time. This heavy reliance on information from information systems maintained on computers has become the very edifice of enterprises today. Information has to be available but with security as the information when accessed and mis used by unauthorised people can lead to loss of revenue, reputation and non-compliance with regulations thereby impacting the very survival of enterprises. There are new types of computer fraudster who are tech-savvy who using their technical expertise can exploit information for wrong purposes. Hence, ensuring security of any IS environment is of utmost importance within the organisation as the loss of which can not only lead to huge financial losses but the enterprise can incur damages for loss of private data of customers, loss of goodwill and market share. Due to the increase in sophistication of technology there has been an unprecedented growth in frauds and cyber-crimes. On the positive side, using technology effectively can help enterprises to reach out to customers anytime, anywhere leading to growth in geometric progression. Enterprise management look for assurance on security and consulting on value addition using IT. This provides a great opportunity for IS auditors who are equipped with the right competencies and skill-sets to provide assurance and value added services.

3.2 Classification of Audits

An information technology audit, or information systems audit, is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organisation's goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement. IT audits are also called IS Audits and computer audits or IT or IS assurance services.

The wide range or spectrum of IT audits cover the whole gamut of IT right from conception to post-implementation review as also consulting on effective deployment. Some examples of these services areas:

- **Systems and Applications:** An audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.
- **Information Processing Facilities:** An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.
- **Systems Development:** An audit to verify that the systems under development meet the objectives of the organisation and to ensure that the systems are developed in accordance with generally accepted standards for systems development.
- **Management of IT and Enterprise Architecture:** An audit to verify that IT management has developed an organisational structure and procedures to ensure a controlled and efficient environment for information processing.
- **Client/Server, Telecommunications, Intranets, and Extranets:** An audit to verify that telecommunications controls are in place on the client (computer receiving services), server, and on the network connecting the clients and servers.
- **Compliance Audits:** Compliance audits include specific tests of controls to demonstrate adherence to specific regulatory or industry standards. These audits focus on particular systems or data. Examples include Payment card industry Data security standard audits, Health Insurance Portability and accountability Act Audit (HIPAA) etc.
- **Operational Audit:** An operational audit is designed to evaluate the internal control structure in a given process or area. Audits of application controls or logical security systems are some examples of operational audits.
- **Financial Audit:** The purpose of a financial audit is to assess the accuracy of financial reporting. A financial audit will often involve detailed, substantive testing, although increasingly, IS Auditors are placing more emphasis on a risk and control based audit approach. This kind of audit relates to financial information integrity and reliability.
- **Integrated audits:** An integrated audit combines financial and operational audit steps. An integrated audit is also performed to assess the overall objectives within an organisation, related to financial information and assets' safeguarding, efficiency and compliance.
- **Administrative Audits:** These are oriented to assess issues related to the efficiency of operational productivity within an organisation.
- **IS audits:** This process collects and evaluates evidence to determine whether the information systems and related resources adequately safeguard assets, maintain data and sys integrity and availability, provide relevant and reliable information, achieve organisational goals effectively, consume resources efficiently, and have, in effect, internal controls that provide reasonable assurance that business, operational and control objectives will be met and that undesired events will be prevented or detected or corrected, in a timely manner.
- **Specialised Audit:** Within the category of IS audits, there are a number of specialised reviews that examine areas such as serviced performed by third parties. Because businesses are becoming increasingly reliant on third party service providers, it is important that internal controls be evaluated in these environments.

- **Forensic Audit:** Forensic Auditing has been defined as the auditing specialised in discovering, disclosing and following up on frauds and crimes. The primary purpose of such a review is the development of evidence for review by law enforcement and judicial authorities.
- **Control Self-assessments:** This is conducted by the business process owners but facilitated by the auditors. The main difference between this and the other engagement types is that the auditors as control experts identify with those responsible for implementing controls the required controls and assist them in self-assessment. Therefore, setting the evaluation criteria and executing the evaluation are carried out by the business owners themselves. It is clear that proper guidance and follow-up are required to optimise the added value of this type of engagement within the enterprise. Especially with regard to approach, tools and reporting, the auditors should clearly lead the way and verify whether assessors are using the existing guidelines.
- **Internal audit/compliance review:** Performed by a third party who is not involved in the functioning of the enabler, but who is employed by the same enterprise as the business owners of the enablers. Commonly, in a (medium- to large-sized) enterprise, the evaluation criteria are set and the review is performed by the internal audit or compliance department. This type of review is more independent than a self-assessment because the auditor is not involved in the functioning of the enabler and therefore contributes to the reliability/credibility of the evaluation outcome. Good practices and consistent guidance are required to optimise the added value of this type of engagement.

A number of IT Audit professionals from the Information Assurance realm consider there to be three fundamental types of controls regardless of the type of audit to be performed, especially in the IT realm. Many frameworks and standards try to break controls into different disciplines or arenas, terming them “Security Controls”, “Access Controls“, “IA Controls” in an effort to define the types of controls involved. At a more fundamental level, these controls can be shown to consist of three types of fundamental controls: Protective/Preventative Controls, Detective Controls and Reactive/Corrective Controls. IS auditing considers all the potential risks and controls in information systems. It focuses on issues such as: operations, data, integrity, software applications, security, privacy, budgets and expenditures, cost control, and productivity.

In an IS system, there are two types of IS Auditors and audits: internal and external. IS auditing is usually a part of internal auditing, and is frequently performed by corporate internal IS Auditors. An external IS Auditor reviews the findings of the internal audit as well as the inputs, processing and outputs of information systems. **The external audit of information systems is frequently a part of the overall external auditing performed by an assurance professional.**

3.3 IT Enabled Services

There is a wide variety of services that can be offered by the IS Auditor. There are innumerable opportunities in every area of IT implementation depending on area of technical expertise. Hence, IS Auditors can provide assurance or consulting services at various stages of technology deployment right from conception to post-implementation. Given below is a sample problem statement with proposed solution and listing of service opportunities for the IS Auditor. This is only an illustrative list for one problem statement. Please refer to Module 1: Facilitated eLearning for more details and examples of IT Enabled services.

Problem: There are no proper IT management practices in the enterprise.

Solution	Opportunity for an IS Auditor
Policies should be drafted and enforced around the environment	• Create the appropriate policies that the enterprise needs in terms of scope and enforcement of the policy • Provide services of performing the review of the policies
Procedures should arise from the policies	• Assist in development of the procedures that the employees of the enterprise should follow. Review designed procedures and provide recommendations for a better solution in order to reduce costs
Correct software should be installed and enforced	• Assist in application implementation • Participate as an PMO in terms of development and procurement of the applications • Assist as scope Manager in the SDLC process in terms of requirement gathering
Business workflows should be designed and enforced in the applications	• Apart from procedures design, develop necessary workflows that are to be enforced through the information system • Perform a BPR on information system requirements of the enterprise and provide recommendations or assist in implementation
Perform risk assessment and rank the risk	• Perform the risk assessment exercise on the existing workflows and processes and identify those areas of high risk that need a higher level of attention
Ensure appropriate segregation of duties by ensuring right Access is given to the right employees	• Provide in designing the roles and responsibilities of the employees • Review the existing roles and responsibilities of the employees and can identify conflicts in segregation of duties

Solution	Opportunity for an IS Auditor
Training is to be provided	• Provide necessary training to the employees regarding the new workflows, procedures, applications etc.

3.4 Fraud

"Fraud is the wrongful or criminal description intended to result in financial or personal gain"

Fraud is a deception deliberately practiced in order to secure unfair or unlawful gain. Defrauding people or organisations of money or valuables is the usual purpose of fraud, but it sometimes instead involves obtaining benefits without actually depriving anyone of money or valuables, such as obtaining a driver's licence by way of false statements made in an application for the same. The establishment of a strong internal control environment where written policies and procedures are enforced, internal controls are appropriately implemented and employees are educated about fraud and its consequences is one of the best deterrents and methods of curtailing fraud. For internal controls to be effective, they must be constantly evaluated for effectiveness and changed as business processes are changed or altered.

3.4.1 Fraud Detection

The use of information technology for business has immensely benefited enterprises in terms of significantly increased quality of delivery of information. However, the widespread use of information technology and the Internet leads to risks that enable the perpetration of errors and frauds. Fraud is any act involving the use of deception to obtain illegal advantage. Detecting fraud in IT environment poses its own challenges as the data is in digital format and can be easily erased by the fraudster.

Management is primarily responsible for establishing, implementing and maintaining a framework and design of IT controls to meet the internal control objectives. A well-designed internal control system provides good opportunities for deterrence and/or timely detection of fraud, internal controls may fail where such controls are circumvented by exploring vulnerabilities or through management perpetrated weakness in controls or collusion among people. Legislation and regulations relating to corporate governance cast significant responsibilities on management, IS Auditors and the audit committee regarding detection and disclosure of any frauds, whether material or not. Understanding the auditee´s business and the risks it faces is a critical step to developing an effective audit plan focused on the areas most sensitive to fraudulent or inaccurate practices. IS Auditors should observe and exercise due professional care in all aspects of their work. IS Auditors entrusted with assurance functions should ensure reasonable care while performing their work and be alert to the possible opportunities that allow fraud to materialise.

The presence of internal controls does not altogether eliminate fraud. IS Auditors should be aware of the possibility and means of perpetrating fraud, especially by exploiting the vulnerabilities and overriding controls in the IT enabled environment. IS Auditors should have knowledge of fraud and fraud indicators, and be alert to the possibility of fraud and errors while performing an audit. During the course of regular assurance work, the IS Auditor may come across instances or indicators of fraud. The IS Auditor may, after careful evaluations, communicate the need for

a detailed investigation to appropriate authorities. In the case of the IS Auditor identifying major fraud, or if the risk associated with the detection is high, audit management should also consider communicating in a timely manner to the Audit Committee.

Regarding fraud prevention, the IS Auditor should be aware of potential legal requirements concerning the implementation of specific fraud detection procedure and reporting fraud to appropriate authorities. Where the IS auditor is aware that management is required to report fraudulent activities to an outside organisation, the IS auditor should formally advise management of this responsibility.

Let us look at the regulatory requirements of fraud as per Indian legislations.

1. **Information Technology (Amendment) Act, 2008:** Casts responsibility on body corporates to protect sensitive personal information by implementing reasonable security practices and procedures. It also recognises and punishes offences committed by companies and individuals through the misuse of IT.
2. **Clause 49 of the Listing Agreement:** Makes the top management accountable for weaknesses in the internal control systems. It requires CEOs and CFOs to certify on the effectiveness of the Internal Controls.
3. **CARO 2003:** Requires verifying the adequacy of internal control procedures and determining whether there were any continuing failures to correct major weaknesses in internal controls. It also requires to report whether any frauds on or by the company had been noticed or reported during the year.

The Government of India last year released the National Cyber Security Policy. This policy aims at protecting information and information infrastructure in cyberspace and building capabilities to prevent and respond to cyber threats. It aims to reduce vulnerabilities and minimise damage from cyber incidents through a combination of institutional structures, people, processes, technology and co-operation

The **Standard on Internal Audit (SIA) 11 defines Fraud** as: *"an intentional act… involving the use of deception to obtain unjust or illegal advantage".* A fraud that involves use of Computers and Computer Networks is called a Cyber fraud. Frauds don't occur randomly, but result from opportunities available to commit them. Thus the goal should be to eliminate the factors that cause fraud rather than looking for temporary solutions. Strengthening the system of internal controls is by and large the best deterrence to frauds and IS auditors have an important role to play here. By evaluating the adequacy of internal controls and identifying high risk areas in the system they can provide valuable guidance on dealing with the risk of frauds. They need to have appropriate knowledge of relevant standards and regulations as well as the various data analysis tools and techniques available.

Standard on Auditing (SA) 505 "External Confirmations" deals with the Auditors' use of external confirmation procedures to obtain audit evidence in accordance with the requirements of SA 330 and SA 500. The reliability of audit evidence is influenced by its source and nature and dependent on the circumstances on which it was obtained. Audit evidence is more reliable when it is obtained from independent sources outside the entity. Further, evidence obtained directly by the IS Auditor is more reliable than obtaining indirectly. Hence the IS Auditor can use these guidelines while conducting the investigation and design the audit programme to obtain evidence from external sources.

Standard on Auditing (SA) 580 "Written Representations" deals with the Auditor's responsibility to obtain written representations from the management and, where appropriate, those charged with governance. The IS Auditor during the course of audit should try and obtain written representations from the management as and when needed. However, it should also be noted that it does not absolve the IS Auditor from performing his duties while conducting the audit.

Standards on Internal Audit: SIA 2 requires internal auditors to use their knowledge and skills to reasonably enable them to identify fraud indicators. SIA 11 defines fraud and lays the responsibility for prevention and detection of frauds on the management and those charged with governance.

Standards on Auditing: SA 240 requires an auditor to evaluate whether the information obtained from risk assessment procedures and related activities indicate presence of fraud risk factors. SA 315 requires an auditor to identify risks of material misstatement arising due to fraud.

3.4.2 Cyber fraud Investigation

In case of cyber fraud, the fraud is carried out using a mouse of computer rather than traditional methods of paper and pen. The computer is simply the mechanism for perpetrating the fraud. Cyber fraud investigations procedures are similar to a fraud investigation where the procedure is divided into many phases such as:

1. Collecting and analysing documentation
2. Conducting interviews
3. Data mining & digital forensics

Fraud risk assessment is a tool that helps in identifying areas of fraud vulnerabilities and assessing the effectiveness of internal controls. IS Auditors need to validate that the risk assessment is regular and complete and that the controls designed are appropriate and effective. The assessment essentially involves:

- Identifying significant risk areas where an organisation is vulnerable to cyber frauds,
- Assessing their likelihood and impact,
- Determining where, how & by whom they may be committed, and
- Assessing whether the existing controls would be able to prevent their occurrences.

A Sample Cyber fraud risk assessment list is given below:

Cyber Fraud	Likeli hood	Impact	Internal Controls
<u>Physical theft</u> – Unauthorised access to computer Hardware. (e.g. Data centres, Server rooms, etc.)	Low	High	1. Key Cards 2. Security Guards 3. Visitor Logs 4. Circuit Cameras 5. Back up & Recovery Plans

Cyber Fraud	Likeli hood	Impact	Internal Controls
<u>Identity theft</u> – Unauthorised access to personal information of Customers and Employees. (e.g. Credit card information of customers, Login IDs & Passwords of employees, etc.)	Medium	High	1. Unique user IDs 2. Strict password policy 3. IDS & Firewalls 4. Incident response policy 5. Delete terminated employee access
<u>Information theft</u> - Unauthorised access to confidential information of Company. (e.g. Strategic Plans, Unpublished financial reports, etc.)	Medium	High	1. Segregation of Duties 2. Access Logs 3. Transaction Logs 4. Security violation logs 5. Encryption
<u>Copyright Infringement</u> – Unauthorised access to Software and Database. (e.g. Software piracy, Peer-to-peer file sharing, e¬tc.)	Medium	High	1. Block peer-to-peer sharing 2. Internet Surveillance 3. Software Licensing 4. Information sharing policy 5. Protection of Software code

A holistic approach to *fraud deterrence and fraud prevention* would be strengthening the Governance and Management framework. IS auditor could assist in evaluating control framework for fraud prevention and detection by assessing the adequacy of the internal control framework and related policies by reviewing following enablers. Sample questions for review for each of seven enablers adapted from COBIT 5 are given below:

1. **Principles, Policies and Frameworks:** Whether the organisation has a documented Cyber Fraud Governance and management Program which is approved by board.
2. **Processes & Internal Controls:** Does the board approve the security policy and direct that senior management conduct cyber fraud risk assessment regularly and evaluate whether remedial measures are implemented controls to address cyber fraud risks and these are formalised and performed?
3. **Organisation Structures:** Whether the organisation has clearly defined roles and responsibilities in relation to cyber fraud management which meets both regulatory and stakeholder requirement?
4. **Culture, Ethics and Behaviour:** Does management conduct periodic employee awareness programmes and training in relation to corporate governance, compliance and cyber fraud?
5. **Information:** Whether the organisation has a proper reporting mechanism for notifying fraud concerns to the top management and these are escalated to the board and reviewed by Audit Committee.

6. **Services, Infrastructure and Applications:** Has the organisation made appropriate use of technology in preventing and detecting Cyber Fraud?
7. **People, Skills and Competencies:** Has the organisation formed expert teams or arranged for services of experts to conduct periodic fraud investigations?

3.4.3 Cyber Forensics: Digital Forensics

By definition, computer forensics is the "process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings (i.e. court of law). An IS Auditor may be required or asked to be involved in a forensic analysis in progress to provide expert opinion or to ensure the correct interpretation of information gathered. Computer forensics includes activities that involve the exploration and application of methods to gather, process, interpret and use digital evidence that help to substantiate whether an incident happened such as:

- Providing validation that an attack actually occurred
- Gathering digital evidence that can later be used in judicial proceedings

Any electronic document or data can be used as digital evidence, provided there is sufficient annual or electronic proof that the contents of digital evidence are in their original state and have not been tampered with or modified during the process of collection and analysis. It is very important to preserve evidence in any situation. Most organizations are not well equipped to deal with intrusions and electronic crimes from an operational and procedural perspective, and they respond to it only when the intrusion has occurred and the risk is realized. The evidence loses its integrity and value in legal proceedings if it has not been preserved and subject to a documented chain of custody. This happens when the incident is inappropriately managed and responded to in an ad hoc manner. For evidence to be admissible in a court of law, the chain of custody needs to be maintained professionally. The chain of evidence essentially contains information regarding:

- Who had access to the evidence (chronological manner)
- The procedures followed in working with the evidence (such as disk duplication, virtual memory dump)
- Providing that the analysis is based on copies that are identical to the original evidence (could be documentation, checksums, timestamps)

It is important to demonstrate integrity and reliability of evidence for it to be acceptable to law enforcement authorities.

Identify: Refers to identification of information that is available and might form the evidence of an incident

Preserve: Refers to practice of retrieving identified information and preserving it as evidence. The practice generally includes the imaging of original media in presence of an independent third party. The process also requires being able to document chain of custody so that it can be established in a court of law.

Analyze: Involves extracting, processing and interpreting the evidence. Extracted data could be unintelligible binary data after it has been processed and converted into human readable format. Interpreting the data requires an in depth knowledge of how different pieces of evidence may fit together. The analysis should be performed using an image of media and not the original.

Present: Involves a presentation to the various audiences such as management, attorneys, court, etc. acceptance of the evidence depends upon the manner of presentation, qualifications of the presenter, and credibility of the process used to preserve and analyze the evidence.

3.4.4 Fraud investigation tools and techniques

Data analysis technologies using Computer Assisted Audit Techniques (CAAT) are the most effective tools and techniques to combat fraud. CAATs provide powerful software capable of running through large volumes of data and drawing inferences from them quickly. This makes it possible to analyse the entire population instead of adopting the sampling approach. CAATs are extensively used in the process of fraud detection. Some useful functions available in CAAT are:

1. Stratification: To identify abnormal strata.
2. Classification: To identify abnormal patterns.
3. Summarisation: To compute control totals and identify analyse variances.
4. Outliers: To identify outlying transactions which are outside normal range.
5. Benford Law: To identify possible fraud areas.
6. Trend Analysis: To analyse trends by reviewing patterns which vary from normal.
7. Gap Test: To identify gaps in a sequence.
8. Duplicate Test: To identify duplicate records.
9. Relation – to relate records from different tables.
10. Compare – to compare records and identify differences.

3.4.5 Some Case Studies of frauds and lessons

Case Study 1: The WorldCom fraud

This is a popular example of using technology for fraud detection. The Internal Auditors had found a round $500 million debit in the Property, Plant and Equipment (PP&E) account for which they could not find any invoices or documentation to back up. As the Company would not provide full access to the financial system, the Auditors had to apply data mining techniques to search the data by using a small script and MS Access. Thereby they were able to search the entire populations of data for anomalies in the trends & patterns. As they followed through the accounts they discovered misallocated expenses of several billion dollars and bogus accounting entries that inflated the revenues.

Lessons and Tips:

While sampling techniques may be good for identifying weaknesses in internal controls, they are not recommended in fraud detection. Frauds involve human intelligence and may affect only a few transactions which may not be represented in a sample. Hence fraud detection methodologies require analysis of the entire population, which needs the aid of computer technology and data analytics techniques.

Case Study 2: The $54 million fraud

This is a typical example of how lack of segregation of duties could lead to a phenomenal fraud. The treasurer of an Illinois town, with an annual budget of $6 million to $8 million, was able to embezzle nearly $54 million over two decades. The fraud remained undetected in annual audits by two independent accounting firms and in annual audit reviews by state regulators. She launched the fraud scheme on Dec. 18, 1990, when she opened a secret bank account in the name of the City of Dixon. Crundwell was the only signatory on the account, which was called the RSCDA - Reserve Fund. She began transferring funds from city accounts into the RSCDA account in 1991. The city, which does not have a city manager, gave Crundwell wide rein over its finances and set the stage for her massive fraud. The failure to segregate duties allowed Crundwell to set up and operate a fairly simple fraud scheme.

Lessons and Tips

Roles and responsibilities must be clearly defined and proper segregation of duties must be done to ensure that no single person can be maker as well as the checker of a particular transaction flow. Ensure the existence of internal control with systems designed to prevent or deter these types of fraud. Conduct regular fraud risk assessment to Identify areas of risk where theft or manipulation are likely to occur.

Case Study 3: The Satyam Fraud

This is a case of manipulation of the books of account by inflating revenues through fake invoices. The Company's standard billing systems were subverted to generate false invoices to show inflated sales. 7,561 invoices worth Rs.51 billion (US$1.01 billion) were found hidden in the invoice management system using a Super User ID. The value of these fake invoices were shown as receivables in the books of account thereby inflating the revenues of the company. The charge framed against the Auditors was that they did not bring the internal control deficiencies to the notice of audit committee and thereby, facilitated the continuance of the fraudulent practices unabated.

Lessons and Tips

Auditors must remember that anyone of any stature could act with monumental recklessness, selfishness and self-destructiveness as Ramalinga Raju did. They must also be conscious of the fact that anything can be faked in this modern technology oriented world and that they need to continuously update their skills and knowledge in order to keep up with the new challenges.

3.4.6 Overview of lessons learned

More often than not, it is poor governance and mismanagement that makes an organisation vulnerable to the risk of Cyber Fraud. Management must ensure that their responsibility of protecting the organisation from these risks is ensured by implementing that adequate and appropriate internal control systems and framework. IS Auditors can assist organisations not only in investigating and detecting fraud but also play a proactive role in helping organisations to maintain effective fraud management program that would include fraud deterrence, fraud prevention, fraud detection, fraud investigation and effective and prompt response to frauds.

3.5 Summary

In this chapter, we have learnt the various types of assurance and advisory services which can be provided IS Auditors. Further, an insight into fraud related activity which results in loss of critical information of the enterprise and how to conduct investigation into fraud related activity by using data analysis and forensic tools was discussed.

3.6 References

www.icai.org

www.isaca.org

www.csoonline.com

www.businessdictionary.com

www.sans.org

3.7 Questions

1. Which of the following factors should not be considered in establishing the priority of audits included in an annual audit plan?
   - A. Prior audit findings
   - B. The time period since the last audit
   - C. Auditee procedural changes
   - D. Use of audit software
2. Which of the following is LEAST likely to be included in a review to assess the risk of fraud in application systems?
   - A. Volume of transactions
   - B. Likelihood of error
   - C. Value of transactions
   - D. Extent of existing controls
3. An IS auditor discovers evidence of fraud perpetrated with a manager's user id. The manager had written the password, inside his/her desk drawer. The IS auditor should conclude that the:
   - A. Manager’s assistant perpetrated the fraud.
   - B. Perpetrator cannot be established beyond doubt.
   - C. Fraud must have been perpetrated by the manager.
   - D. System administrator perpetrated the fraud.

4. Which of the following situations would increase the likelihood of fraud?
   A. Application programmers are implementing changes to production programs.
   B. Application programmers are implementing changes to test programs.
   C. Operations support staff are implementing changes to batch schedules.
   D. Database administrators are implementing changes to data structures.
5. Neural networks are effective in detecting fraud, because they can:
   A. Discover new trends since they are inherently linear.
   B. Solve problems where large and general sets of training data are not obtainable.
   C. Attack problems that require consideration of a large number of input variables.
   D. Make assumptions about shape of any curve relating variables of output.
6. The FIRST step in managing the risk of a cyber-attack is to:
   A. Assess the vulnerability impact.
   B. Evaluate the likelihood of threats.
   C. Identify critical information assets.
   D. Estimate potential damage.
7. Which of the following refers to imaging of original media in presence of an independent third party?
   A. Identify
   B. Preserve
   C. Analyze
   D. Present
8. What involves extracting, processing and interpreting the evidence?
   A. Identify
   B. Preserve
   C. Analyze
   D. Present
9. What is also performed to assess the overall objectives within an organization, related to financial information and assets' safeguarding, efficiency and compliance?
   A. Operational Audit
   B. Financial Audit
   C. Integrated Audit
   D. IS Audits

10. What is designed to evaluate the internal control structure in a given process or area?
    A. Operational Audit
    B. Financial Audit
    C. Integrated Audit
    D. IS Audits
11. After initial investigation, IS auditor has reasons to believe that there is possibility of fraud, the IS auditor has to:
    A. Expand activities to determine whether an investigation is warranted.
    B. Report the matter to the audit committee.
    C. Report the possibility of fraud to top management and ask how they would like to proceed.
    D. Consult with external legal counsel to determine the course of action to be taken.

3.8 Answers and Explanations

1. D. Use of audit software merely refers to a technique that can be used in performing an audit. It has no relevance to the development of the annual audit plan.
2. B. An error is the least likely element to contribute to the potential for fraud. Answer A and C are incorrect since volume times value of transactions gives an indication of the maximum potential loss through fraud. Answer D is incorrect since gross risk less existing control gives net risk.
3. B. The password control weaknesses means that any of the other three options could be true. Password security would normally identify the perpetrator. In this case, it does not establish guilt beyond doubt.
4. A. Production programs are used for processing an enterprise's data. It is imperative that controls on changes to production programs are stringent. Lack of control in this area could result in application programs being modified to manipulate the data. Application programmers are required to implement changes to test programs. These are used only in development and do not directly impact the live processing of data. The implementation of changes to batch schedules by operations support staff will affect the scheduling of the batches only; it does not impact the live data. Database administrators are required to implement changes to data structures. This is required for reorganization of the database to allow for additions, modifications or deletions of fields or tables in the database.
5. C. Neural networks can be used to attack problems that require consideration of numerous input variables. They are capable of capturing relationships and patterns often missed by other statistical methods, and they will not discover new trends. Neural networks are inherently nonlinear and make no assumption about the shape of any curve relating variables to the output. Neural networks will not work well at solving problems for which sufficiently large and general sets of training data are not obtainable.
6. C. The first step in managing risk is the identification and classification of critical information resources (assets). Once the assets have been identified, the process moves onto the identification of threats, vulnerabilities and calculation of potential damages.

7. B. Preserve refers to practice of retrieving identified information and preserving it as evidence. This practice generally includes the imaging of original media in presence of an independent third party.

8. C. Analyse involves extracting, processing and interpreting the evidence. Extracted data could be unintelligible binary data after it has been processed and converted into human readable format. The analysis should be performed using an image of media and not the original.

9. C. An integrated audit combines financial and operational audit steps. An integrated audit is also performed to assess the overall objectives within an organization, related to financial information and assets' safeguarding, efficiency and compliance.

10. A. An operational audit is designed to evaluate the internal control structure in a given process or area. Audits of application controls or logical security systems are some examples of operational audits.

11. A. An IS auditor's responsibilities for detecting fraud include evaluating fraud indicators and deciding whether any additional action is necessary or whether an investigation should be recommended. The IS auditor should notify the appropriate authorities within the organization only if it has determined that the indicators of fraud are sufficient to recommend an investigation. Normally, the IS auditor does not have authority to consult with external legal counsel.

SECTION: 2 APPENDIX
CHECKLISTS AND OTHER RELATED MATERIALS

Reference material (available in DVD only)

Following publications are available in DVD as reference material:

1. Compendium of Standards on Internal Audit
2. Data Analysis For Auditors
3. Data Analytics and Continuous Control Monitoring
4. Guide on Risk Based Internal Audit
5. Guide to Internal Controls Over Financial Reporting
6. Information Technology Amendment Act, 2008
7. ITAF 2nd Edition
8. National Cyber Security Policy 2013
9. Notifications of Rules under Sections 6A to 43A
10. Technical guide to IT Migration Audit
11. Technical guide to IS Audit

Useful checklists (available in DVD only)

1. IS General Control Review – Audit Report Sample
2. IS Application Control Review – Audit Report Sample
3. Risk Control Matrix Sample for Physical access controls
4. Risk Control Matrix Sample for Logical access controls
5. Risk Control Matrix Sample for Data Centre and Server

Useful checklists available as soft copy in DVD and in section 3: Appendixes 1 to 6

1. Request for proposal from bank for IS Audit of application software
2. Sample proposal in response to request for Logical access controls review of SAP
3. Sample IS Audit Finding of OS review
4. Sample report using CAAT for auditing Database
5. Sample IS Audit report (Executive Summary)
6. Self-assessment questionnaire for providing assurance services on eCommerce

APPENDIX 1: RFP FROM BANK FOR IS AUDIT OF APPLICATION SOFTWARE

Below is the request received from a Public Sector Bank for submitting a proposal for IS Audit.

Extract from this simple RFP are:

Software Packages to be audited are:

Category A: Developed In-house (Standalone)

1. Bills
2. Remittance
3. Vostro Accounts
4. Preventive Monitoring System

Category B: (Outsourced)

1. Cash Management Services
2. Centralised Banking Solution

The Scope of Audit is as under:

- Evaluation of Effectiveness & Effectiveness of the package vis-à-vis business process and requirements
- Application Security & Controls review
- Database Security and Integrity review
- Review of Interface Controls with other applications
- Review of Network & Communications controls with relation to the application package

Inter-alia, the above scope shall include the following:

1. Whether the design of the software conforms to the Requirements Specification.
2. Objectives of the application – whether these have been fulfilled/ likely to be fulfilled by implementation.
3. Whether bank's systems & procedures are being followed in the application.
4. What are the controls built in the application? Whether these take care of bank's systems and procedures.
5. What are the security features available/built into the application package and whether these are sufficient to take care of the risks in a financial transaction.
6. What is the relative efficiency of the application in conduct of transactions vis-à-vis the performance in similar packages?
7. Testing robustness of the application package by running a specified number of transactions on int.
8. Assessment of the Risk component in the package.
9. To test and verify for any bugs in the application package.
10. To specify clearly methodology to be adopted in carrying out each of the above steps.

APPENDIX 2: RESPONSE TO RFP FOR LOGICAL ACCESS CONTROLS REVIEW OF SAP

Introduction

The Client Company (Max Infotech)

Max Infotech began its business operations in 1959 with the roll out of India's first tractor. Today the Max Infotech Group is a significant player in the Indian software industry with a gross sales turnover of ₹ 10.20 Billion in 2013-14. The Max Infotech Group offers a range of IT enabled services. The services of the Group are divided into the specific business units covering specific business interests. Max Infotech has over 5,000 employees located in 10 ITPs and 20 marketing offices in India and abroad. Max Infotech has implemented SAP Ver. X and has been using it successfully since more than 3 years. It has more than 500 SAP users in the group. Max Infotech is also considered as one of the SAP Competency Centres in India. The primary SAP modules used are SD, FD, PD, HR, QM and PM. It intends to provide information access to its dealers. Max Infotech intends to have an IS Audit of SAP implementation covering Logical Access Security encompassing security at Network, OS, Database and functionality layers.

IS Assurance and Consulting Firm

IS Assurance and Consulting Company (ISACC) is a 20-year-old firm of Chartered Accountants specializing in Information Systems Assurance, Training and Consulting including Management consultancy services. ISACC provides services in the areas of Information Systems Audit, Training, Implementation and Consultancy. ISACC is led by Mr. Abraham who is a Chartered Accountant and has a diploma in Information Systems Audit of ICAI. The firm has qualified and trained IS audit personnel. We are enclosing brief profile of the firm. The firm also has on its panel Technology/Domain experts available, as required. ISACC have been involved in providing Information Systems Assurances for both the public and private sector in India and abroad. ISACC's clients include IT Companies, Banks and public sector companies.

Background

Objective of SAP Review

Max Infotech Group has been using Information Technology as a key enabler for facilitating business process Owners and enhancing services to its customers. The senior management of Max Infotech has very proactive in directing the management and deployment of Information Technology. Most of the mission critical applications in the company have been computerised and networked. The IT department of Max Infotech has issued Information Systems Controls (Policies, Procedures, practices and organisation structure) as envisaged by the management for ensuring uniformity and standardisation in implementation of IT Solutions across the company. The internal audit team of the company has been well trained in IT and has gained extensive experience in auditing all IT applications and they have also specific competency in all the key functionality of SAP.

Need for SAP review

Max Infotech has successfully implemented SAP covering all its critical operations and has been using it since more than 2.5 years. The implementation has stabilised and standardised across all the operational locations\functions. A functionality assessment was performed by SAP to confirm the effective usage of SAP about one year ago. The internal audit team now intends to have a security assessment of SAP implementation, primarily to assess the logical access security framework. The objective is to identify areas of control weaknesses by benchmarking against global best practices. The risks identified are expected to be mitigated by implementing controls as deemed relevant to ensure that SAP implementation is secure and safe and provide assurance to the senior management of Max Infotech.

Need for Logical Access Controls Review of SAP

Max Infotech has formulated and implemented documented policies and procedures covering all key areas of SAP implementation. The internal audit team have been involved in conducting audits using SAP Functionalities and features for all business related aspects. However, being proactive, Max Infotech has envisaged the need to have an Information Systems Audit covering review of Logical Access Security for SAP users across the company. They intend to benchmark the prevailing Policies, Procedures and practices with the global best practices as relevant to SAP implementation in the company. The objective of this IS Audit is to have an independent assessment of the prevailing procedures, practices and procedures relating to Logical Access Security and identify areas of improvement. Further, they expect that all mission critical operational practices be identified and benchmarked with global best practices. To achieve this, Max Infotech proposes to engage external consultants who have expertise in IS Assurance and Information Technology. ARA having expertise in these areas have been asked to provide their techno-commercial offer for the assignment.

Understanding the need

Based on the discussion held with the internal audit team headed by Mr. B.S.Sinha at the Max Infotech premises at Ghaziabad on 6th March, 2014, the scope has been proposed and defined. This proposal outlines the overall strategy and methodology for this assignment.

Methodology for executing the Assignment

Primary Objective

The primary objective of the assignment is to conduct Logical Access Controls Review of SAP by using the Latest and globally recognised standard COBIT 5 issued by the Information Systems Audit and Control Association, USA. The review of SAP would be with the objective of providing comfort on the adequacy and appropriateness of controls so as to mitigate the following system operational risks and ensure that the information systems are implemented so as to provide a safe and secure computing environment.

Scope and Terms of Reference

Based on our understanding of Max Infotech's needs for conducting systems audit of SAP, it was decided to primarily focus on Review of Logical Access Controls in SAP. We propose the scope of review and the terms of reference as laid down in the following paragraphs. The envisaged terms of reference are based on the personal discussions key members of assignment team had with the internal audit team of Max Infotech on 7th March, 2014 at Bengaluru. The detailed scope of review and methodology followed are given in the annexure. The methodology would be further enhanced and refined as the audit progresses based on specific needs of the audit environment. Broadly the scope of review primarily from security\controls and would involve:

A. Review of IT Resources as relevant
   a. Operating Software – Access controls
   b. Telecommunications Software – Access Controls
   c. RDBMS - Access Controls
   d. SAP - Major focus area – Configuration of Parameters and Access Controls
   e. Application controls at various stages such as Input, Processing, Output, Storage, Retrieval and transmission so as to ensure Confidentiality, Integrity and Availability of data.

B. Organisation structure policies, procedures and practices as mapped in the information systems - efficiency\controls.

Our Approach/Methodology

Audit Approach

A. Our approach to the assignment would be as follows:

(i) We propose to deploy a core team of 4 to 6 IS audit personnel for this assignment in batches of 2 to 3 as per the skill sets required, under the personal direction and liaison of the Principal, Mr. Abraham.

(ii) Max Infotech should designate a person at a senior level to co-ordinate between us. Max Infotech should also depute one personnel each from systems and audit group to form part of the audit team.

(iii) Detailed systematic audit procedures would be finalised after completing review of the documentation and discussion with the systems staff and the users.

In tune with terms and scope of reference of the assignment, we will adapt the methodology from COBIT®. Specific Control Objectives/Management Guidelines of the relevant IT process of Logical Access Controls shall be selected for this assignment after obtaining understanding of the organisation structure, Information Technology deployment and available documented policies and procedures.

Structured Methodology

The above-mentioned objectives shall be achieved through the following structured methodology

- Obtain understanding of IT Resources deployment at Max Infotech
- Obtain understanding of the IT Strategy and internal control system at Max Infotech
- Identification and documentation of IT related Circulars issued by Max Infotech.
- Identification and documentation of Organisation Structure and Information Architecture
- Identification and documentation of existing policies, procedures and practices
- Application of COBIT® for formulating IT best practices for the Policy and procedures of Max Infotech
- Formulation of draft report on our findings covering our review and benchmarking.
- Presentation of final report with agreed action plan based on feedback of IT management of Internal Audit team of Max Infotech

Max Infotech shall make available all the required resources on time and provide one coordinator for interaction and clarifications as required.

Audit plan

The audit plan would cover the following activities:

Discussions with the

- Internal Audit Team
- Systems\Implementation Team
- Users and user management
- Review of Operating Systems (OS) documentation
- Examination of OS access rights
- Review of Oracle\SAP Manuals
- Examination of selected Modules access profiles
- Observation of the Users and the systems in operation
- Review of access controls over Computers as relevant
- Examination of computerised processing controls incorporated within the selected modules.

Audit Program\Procedures

Our audit team would perform the following tasks based on the audit methodologies given in Annexure 'A' to 'B' and include the following programmes/procedures:

1. Undertake an in-depth study and analysis of all aspects of SAP as implemented at Max Infotech. We will take steps to identify the way in which the system currently operates. In doing so, the following objectives would be kept in mind while setting the overall goals:
    - Accurate and complete processing of data
    - Error messages in case of incomplete/aborting of processing of data
    - Optimise data handling and storage
    - Better management of information

2. Review the software in operation; understand how the various modules interact within the overall system.
3. Review how each module in the system has been tested including the documentation prepared in respect of each.
4. Review the methods employed for implementation of the system, including post-implementation review procedures undertaken to ensure that the objectives set out were actually achieved.
5. Understand the business processes and review how these have been mapped in the information systems by tracing the modules with a top down approach.
6. Review the modules by performing detailed documented tests of all the menu options and their related effects.
7. Review the controls established over the continuity of stored data, necessary to ensure that once data is updated to a file, the data remains correct and current on the file.
8. Review the in-built controls for stored data so as to ensure that only authorised persons have access to data on computer files.
9. Review the controls established which ensure that all transactions are input and accepted for further processing and that transactions are not processed twice.
10. Review the controls established so as to ensure that only valid transactions are processed.
11. Review the procedures established for back-up and recovery of files in the package.
12. Review controls established for the development, documentation and amendment of programs so as to ensure that they go live as intended.

Assignment Team

Our approach to selecting the right people for a project is to bring together the necessary skills and experience for a particular assignment from the rich mix of skills and experience available. The assignment would be executed under the personal supervision and lead by Mr. Abraham. The team would be a blend of professionals with extensive experience in management, Information Technology and Auditing. The team includes Chartered Accountants, IT Professionals, Management Consultants and Certified Information System Auditors. The senior members of the team are:

- Abraham
- Ramprakash
- Ravindra Jain
- Hariram

Logistic arrangements

Infrastructure Required

It will be necessary for Max Infotech to appoint one co-ordinator who will be part of the discussion on the work plan initially and continue to work with the ARA team till the assignment is complete.

Max Infotech will make available the necessary computer time, software resources and support facilities necessary for completing the assignment within the agreed timeframe. The conduct of the assignment should be adequately communicated to the required personnel so as to facilitate extensive co-operation from the respective personnel. During the course of the assignment, we will require the following infrastructure.

- Three Nodes with Read only access to SAP
- One Laptop with windows 8/Microsoft office 2013.
- Access to a laser printer for printing reports as required.
- Adequate seating and storage space for audit team
- Facilities for discussions amongst our team and your designated staff.

Documentation Required

- User Manuals and Technical Manuals relating to System Software and SAP.
- Organisation chart outlining the organisation hierarchy and job responsibilities
- Access to circulars\guidelines issued to employees.
- Access to user manuals and documentation relating to SAP Implementation by Max Infotech.
- Any other documentation as identified by us as required for the assignment

Estimated Timeframe, Deliverables and Fees

Deliverables

1. Draft Report including executive summary of the result of the review along with the recommendations of findings and recommendations with risk analysis of findings.
2. Final Report incorporating Management Comment and agreed priority plan of action based on exposure analysis.
3. Soft or hard copy of Checklist used for the audit.
4. Soft or hard copy of Audit Methodology and documentation

Time Frame

The elapsed time for the assignment is approximately 4 weeks (three man months). We would require lead-time of two weeks for commencing the assignment. The availability of coordinating team, user involvement, availability of resources and information by the auditee would also impact the audit duration and time schedule, which we would be communicating to you in advance.

Fees

The Fees for this assignment is ₹ x.xx Lakhs (₹ xxx Only) to be paid as follows:

- 50% Advance with Order
- 50% on presentation of Final Report

Out of pocket expenses

Travelling, Boarding, Lodging and conveyance expenses to be reimbursed on actuals in case of outstation travel. As our HO is in Bangalore, the assignment may involve one/two trips of Mr. Abraham from Bangalore to Delhi for the assignment.

Authorised Signatory

Encl: Profile of ISACC

APPENDIX 3: SAMPLE IS AUDIT FINDING

Logical Access Controls Review of Operating System

We have reviewed procedure of granting access to the Operating system and Toll Operations Package. Our specific findings and recommendations with agreed action plan are given below:

The overall control objective in implementing OS Access controls:

"The creation of users and their access need to be controlled through appropriate Authorization levels. Controls have to be laid down and adhered to while granting authorization. Access logs are to be generated whenever the O/S is accessed and Access logs should show details as to the users accessing the O/S, the period of access and the resources accessed. System must enforce a systematic procedure for logins and logouts. All access points to the system are to be monitored by way of access logs and these access points are available only on the administrators console and terminals".

1. System Users have blank user-id

Issue: Presently, system manager has the system administration rights and toll manager is also created as a user who can modify the ini settings in PQR. These users have a blank user-id and passwords have not been changed since installation.

Implication: High

User accountability may not be established on account of lack of documentation. The operations of PQR may be affected in case of breakdown and non-availability of the relevant personnel.

Recommendations

- The users of Operating System and Toll Operations Package in PQR Computer need to be authorized in writing by senior management. Creation of their user id and password should be documented and accepted by the user and kept by senior management in sealed cover in safe custody to be available in case of need.
- Password policy has to be formulated and passwords should be changed at least once in 90 days without being reused.

Management comment: Agree. System manager will create user ids for all authorized users.

2. PQR Computer is networked to other office computers

Issue: The PQR Computer is linked to other Computers in the Network. These computers are only being used by the Toll Manager and his Staff for performing administration jobs such as preparing Toll Reports. Networking of these office computers with PQR computer makes it vulnerable to unauthorized access.

Implication: High

PQR System could be accessed by any of the users of the office computers.

Recommendations:

A review of security and operations settings needs to be done and all access to PQR Computer from any of the office computers has to be removed or restricted.

Management comment: Agree. Will be reviewed and modified as required.

APPENDIX 4: CAAT REPORT USING SQL

Sample results of using CAAT

As a part of our audit procedure, we have used SQL to directly access and analyze the data stored in the tables. Our observations and the related analysis are given below. As these observations relate to the data stored which could impact financial accounts, we have submitted this information to Statutory Auditors and user department of ABC with a request to verify these SQL results and confirm the impact on the financial statements. The detail tables of SQL Statements can be obtained from ABC, IT Department. We have given a copy of this draft report to ABC with a request to confirm the facts to us. Our observations with implications, comments and our Risk assessment are given below.

Users available with Invalid employee codes

Rating: High

There are two user ids within user id 15, which is still being used. These transactions used by live users will result in user accountability not being established.

Implications

As the employer code is invalid, it will be difficult to establish accountability for transactions entered using this ID in case of errors or frauds.

IT Department's feedback and Agreed Action

This user-id has been created during the time of data conversion. This user-id has been disabled so that transactions can be entered using this.

Past employees having ID in user table

Rating: High

There are 19 Users who have user ID. Their employee ID and name is given so that a final list may be prepared with actual users who are expected to have access in the system.

Implications

The number of users in the system is much more than the actual users. This is on account of the fact that past and temporary users have not been disabled.

IT Department's feedback and Agreed Action

The number of users will correspond with actual users. All other users will be disabled.

Transactions with amount as Null in FA Trans_table

Rating: Medium

Transactions with Amount as Null are listed day-wise. There are 181 transactions, which need to be analysed.

Implications

These results in dummy transactions, which may not have any value, or genuine transactions might have been stored without values.

IT Department's feedback and Agreed Action

This has occurred on account of transactions where DD charges are deducted from loan amount for obtaining DD whereas the loan account is debited with the total amount including DD Charges. This does not have any financial impact.

APPENDIX 5: SAMPLE IS AUDIT REPORT

Objectives of the Assignment

The primary objective of this Information Systems Audit assignment was to provide assurance to the management of ABC Limited (ABC) on the availability, appropriateness and adequacy of controls in the Financial Accounting and Loan Processing System (FALPS) through review of the control framework of their in-house package - Financial Accounting and Loan Processing System (FALPS), review of Logical access controls of FALPS and conduct Implementation audit of General Controls at 2 select branches with specific emphasis on implementation of FALPS.

Proposed Scope of Review/Terms of Reference

Based on understanding of ABC's needs for conducting systems audit of FALPS Package, it was decided to primarily focus on Review of data integrity in FALPS Package. The review of FALPS Package was with the objective of providing comfort on the adequacy and appropriateness of controls and data so as to mitigate the following system operational risks and ensure that the information systems are implemented so as to provide a safe and secure computing environment. The detailed scope of review/methodology were also agreed to. Broadly the overall scope of review primarily from security/controls involved the following: Application controls at various stages such as Input, Processing, Output, Storage, Retrieval and Transmission so as to ensure Confidentiality, Integrity and Availability of data. Further, organization structure policies, procedures and practices as mapped in the information systems focusing on efficiency\ controls were also reviewed.

Broadly, the areas reviewed covering the following:

1. Logical Access Controls Review as implemented through:

a. Operating System Software (Unix) - Access controls

b. Telecommunications Software - Access Controls

c. RDBMS (Oracle)- Access Controls

d. FALPS Package - Major focus area – Access, security and effectiveness

2. Review of General controls at 2 select branches covering Environmental and Physical Access Controls Review, Logical access Controls review as implemented, Application Controls as implemented and review of policies, procedures and practices relating to IT Implementation.

Our Approach/Methodology

The Audit was carried out as pre-planned Audit Plan and programme, which was discussed with the statutory auditors and ABC's senior management. We have used the international accepted standard for IS Audit – COBIT (Control Objectives for Information and Related Technology, issued by the Information Systems Audit and Control Association, USA for this review. The Key tasks of our Audit plan are highlighted below:

- Discussions with the IT department and user management.

- Review of Circulars issued by ABC Ltd. relating to IT operations
- Review of Environmental Access and Physical Access controls
- Review of Operating Systems (Unix) and RDBMS (Oracle) Manuals
- Examination of OS and RDBMS access rights
- Review of FALPS Package Technical and User Manuals
- Examination of access profiles and parameter settings in FALPS package
- Review of Application Controls in FALPS package
- Observation of the Users and the system in operation
- Examination of processing controls in FALPS using test data.
- Review of Reports and Audit Logs in System Software and FALPS package

Audit Environment

We have conducted IS Audit at the IT department of ABC in a simulated environment using a Windows 7 Computer connected to Server with SCO UNIX as Operating System and RDBMS as Oracle using latest version of FALPS with copy of data of Bengaluru Branch (upto 31st March, 2012). We have also visited reviewed two branch operations at Mangaluru and Hassan.

Audit Reports

We issued a draft report outlining our issues and recommendations and obtained feedback from the IT Department. Further, a meeting was held with IT department represented by Mr. Sam, AGM (IT) and Mr. Ram, AGM (Finance and Accounts) where the issues and recommendations were discussed in detail. The IT Department has been very proactive in incorporating our suggestions. The issues rectified so far are given in separately in Annexure-3 for the purpose of record. The report incorporates all the issues, which have been agreed and confirmed. This IS Audit report includes the following annexure and has to be read in its totality:

1. Summary of Findings: Outlines all key issues with exposures
2. Specific Issues and recommendations: Issues which need to be implemented
3. Issues identified which have been rectified by It dept. Issues rectified as on date
4. Logical access Control Review of Unix: Access Controls issues of Unix
5. Logical Access Control Review of Oracle: Access Controls issue of Oracle
6. Review of Financial data using SQL: Highlights data integrity issues in existing data

Overall Conclusions

Based on our review our overall conclusions on specific areas are:

Security and Access Controls

Our review of security and access controls at the IT Environment as reviewed by us and as implemented in ABC using Unix, Oracle and FALPS confirms that appropriate security and access controls have been implemented by using related functions and features of the packages. Our test checks have revealed that systems of security and controls are reliable. However, there are some areas where controls need to be strengthened and these are given in annexure.

Business Process Controls

Our review of business process validations and data integrity controls covering all the core functions of ABC as facilitated by FALPS such as interest computation, allocation and aging, confirms that all related data have been duly captured, processed and stored correctly and completely subject to some transaction data not available pertaining to previous years. However, there are also missing data in master tables which impact the MIS and statements of accounts. The issues, which have come to our notice during the process of our review, are highlighted in annexure.

Further Action

We consider that the recommendations given in annexure to this report would be very useful for facilitating business process controls of ABC and will aid in improving the effectiveness of FALPS package and computer operations. We would like to affirm that the matters included in this report are those which came to our notice during our review by following normal Information System audit procedures by complying with globally applicable Information Systems Auditing Standards, Guidelines and procedures that apply specifically to Information Systems Auditing issued by Information Systems Audit and Control Association, USA and Security and Control Practices as outlined in COBIT 5 issued by ISACA as adapted to ABC operations for review of Application software and implementation audit. Further, on account of limitations of scope and time, we have used sample test and test check approach. Hence, certain areas, which are outside the scope of this review such as source code, review, implementation controls and general controls specific to branches are not covered.

APPENDIX 6: QUESTIONNAIRE FOR PROVIDING ASSURANCE SERVICES IN e-COMMERCE

1. How many (approximately) of the businesses you audit will be electronic in that there is no paper, or other non-electronic forms of audit trail available?
2. In general, as an auditor, what special steps or approach would you take when auditing a business that is engaged in e-Commerce compared with a comparable business not engaged in electronic commerce?
3. Which national or international standards or pronouncements would you use or are using in undertaking an audit of a business engaged in electronic commerce?
4. To what extent would you want that records and audit trails of e-Commerce transactions be maintained and in what form?
5. How would you assure the management that records and audit trails are being properly created?
6. To what extent would you recommend that records and audit trails of e-Commerce transactions be maintained over time?
7. To what extent do you foresee that records and audit trails of e-Commerce transactions will be combined with other transactions or otherwise consolidated, so that the transactional trail is lost?
8. How do you satisfy yourself that records and audit trails of e-Commerce transactions have not been altered?
9. How would you test the above – through review of system controls or substantive testing?
10. To what extent do you perceive the risks that records and audit trails of e-Commerce transactions could be incorrectly transferred through into accounting systems? How would perceive such a risk?
11. If you find that that records and audit trails of e-Commerce transactions are inaccessible either through being stored remotely, or through the effects of data security mechanisms, or otherwise, how would you, as auditors, audit the same?
12. What are the minimum types of records that must be archived, by the business entity, which will allow both external financial or statutory auditors to perform their functions? On what basis do you expect these records to be maintained? In what form do you want these records – Digital or manual?
13. How would you face the following issues and problems you could be facing in practice when carrying out audits of businesses engaged in e-Commerce?
    - ✓ Accessing initial transaction data
    - ✓ Processing of the transaction by accounting systems
    - ✓ Identifying suitable sources of confirmation
    - ✓ Determining the system processing “rules”
    - ✓ Storage and retrieval of the e-Commerce records, and
    - ✓ Forming an opinion as to the timeliness, completeness and accuracy of the Transaction data.

14. What issues and problems do you anticipate arising in the future when carrying out audits of businesses engaged in electronic commerce? These could be from perspectives of:
    - Accessing initial transaction data
    - Processing of the transaction by accounting systems
    - Identifying suitable sources of confirmation
    - Determining the system processing "rules"
    - Storage and retrieval of the e-Commerce records, and
    - Forming an opinion as to the timeliness, completeness and accuracy of the Transaction data.
15. How many of your present clients do you perceive could be engaged in electronic commerce?
16. What specific approaches, solutions, methods, procedures or techniques do you need to develop to assist in the auditing of businesses engaged in electronic commerce?
17. What approaches, solutions, etc. do you anticipate might help you in the future when auditing businesses engaged in electronic commerce?
18. In what way would the solutions, methods, etc. you devised for auditing non-e-Commerce clients differ from auditing the e-Commerce Clients?
19. Do you think there are differences in business-to-business e-Commerce compared with business-to-consumer e-Commerce that would warrant different audit considerations and if so, what are the considerations?

ISBN: 978-81-8441-335-9

₹ 750/- (For Modules I to VII) with DVD

http://cit.icai.org

www.icai.org

July/2015/P3000(Revised)