ISA

(Modules 1 to 6)

Background Material

INFORMATION SYSTEMS AUDIT 3.0 COURSE

Module - 1
Information Systems Audit Process

Digital Accounting and Assurance Board
The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

Background Material
on
Information Systems Audit 3.0 Course

Module-1:
Information Systems Audit Process

Digital Accounting and Assurance Board

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

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 PQC 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	:	August, 2020
Committee/Department	:	Digital Accounting and Assurance Board
Email :		gdaab@icai.in
Website :		www.icai.org/ https://pqc.icai.org
Price	:	₹ 750/- (For Complete Set)
ISBN	:	978-81-8441-995-5
Published by	:	The Publication Directorate on behalf of The Institute of Chartered Accountants of India ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi - 110002
Printed by	:	Sahitya Bhawan Publications, Hospital Road, Agra – 282 003 August | 2020 | P2724 (Revised)

Foreword

The digital revolution is transforming the traditional ways of doing business, necessitating realignment of profession to leverage the multipliers of digital technology - enhanced efficiency, scale and speed, effectiveness, agility and giving access to newer markets. In view of the rapid technological changes, it is imperative for Information System Auditors to adapt, be innovative in aiding organizations to improve its control environment and strengthen governance of IT risks. Adoption of emerging technologies will help them to assimilate vast amount of data and provide value added analysis in the form of data analysis and business intelligence. Chartered Accountants possess unique blend of systems and process understanding and expertise in controls and governance, thereby best suited to be the perfect Information Systems Auditor.

The Institute of Chartered Accountants of India (ICAI), through its Digital Accounting and Assurance Board (DAAB), is continuously monitoring technological developments and taking initiatives to disseminate updated knowledge amongst our members and other stakeholders. In this direction, it is heartening to note that the DAAB is bringing out next version of "Educational Material" for Post Qualification Course on Information Systems Audit. This updated and revised Material combines technology, information assurance and information management expertise that enable Chartered Accountants to be an advisor and handling assurance assignments.

In this updated course curriculum various aspects of emerging technologies like, Blockchain, Robotics Process Automation, etc., have also been introduced to keep members fully abreast. With focus on increased practical aspects, case studies and lab manuals at appropriate places this material is a great learning guide for members aspiring to be Information Systems Auditor.

I compliment CA. Manu Agrawal, Chairman, CA. Dayaniwas Sharma, Vice-Chairman and other members of the Digital Accounting and Assurance Board for generation next material in digital era by taking up this timely initiative.

I am confident that our members would take benefit of these updated modules of post qualification course on Information Systems Audit, so as to render their professional responsibility as Information System Auditor more efficiently and highest standards to achieve global recognition.

CA. Atul Kumar Gupta
President, ICAI

Place: New Delhi

Date: April 12, 2020

Preface

Evolution of digital economy and ever-changing dynamic ecosystem presents significant challenges, including new competition, new business and service delivery models, unprecedented transparency, privacy concerns and cyber threats. With a goal to keep members abreast of impact of emerging technologies, Digital Accounting and Assurance Board has come out with the updated Post Qualification Course on Information Systems Audit Modules to equip members with specialised body of knowledge and skill sets so that they become Information Systems Auditors (ISAs) who are technologically adept and are able to utilize and leverage technology to provide reasonable assurance that an organization safeguards it data processing assets, maintains data integrity and achieves system effectiveness and efficiency. This updated syllabus facilitates high level understanding about the role and competence of an IS Auditor to analyse, review, evaluate and provide recommendations on identified control weaknesses in diverse areas of information systems deployment.

Revised Modules of Post Qualification Course on Information Systems Audit has specific objective, i.e., "To provide relevant practical knowledge and develop skills for planning and performing various types of assurance or consulting assignments in the areas of Governance, Risk management, Security, Controls and Compliance of Information Systems." The core of DISA 3.0 lies in inculcating competence to add to service delivery of the members. The updated course would help the members to apply appropriate strategy, approach, methodology and techniques for auditing information system and perform IS Assurance and consulting assignments by using relevant best practices, IS Audit standards, frameworks, guidelines and procedures.

The updated ISA Course 3.0 has a blend of training and includes e-learning, live case studies and lab manuals, project work in addition to class room lectures. This updated background material also includes a DVD which has e-Learning lectures, PPTs, case studies, DEMO CAAT software, useful checklists and sample audit reports. New Module on "Emerging Technology and Audit" has been added which covers Information System Assurance and Data Analytics, Assurance in Block chain Ecosystem, and Embracing Robotic Process Automation in Assurance Services. In addition to this Artificial Intelligence and Internet of Things (IoT) has also been inducted in the new modules.

We would like to take this opportunity to place on record our deep appreciation for the efforts put in by Convener, Dr. Onkar Nath as well as authors and reviewers of the various modules, viz., CA Anand Prakash Jangid, Mr. N.D. Kundu, Mr. Inder Pal Singh, Mr. Avinash Gokhale, CA Pranay Kochar, CA Naresh Gandhi, Dr Manish Kumar Srivastava, Dr. Saurabh Maheshwari, CA Narasimhan Elangovan and CA Atul Kumar Gupta. It would be also appropriate to express our thanks to all the ISA faculties for giving their inputs/ suggestions for the implementation of DISA 3.0.

We would like to express gratitude to CA. Atul Kumar Gupta, President, ICAI, and CA. Nihar Niranjan Jambusaria, Vice President, ICAI, for their thought leadership and encouragement to the initiatives of the Board. We would also like to place on record our gratitude for all the Board members, co-opted members and special invitees for providing their valuable guidance and support in this initiative of the Board. We also wish to express my sincere appreciation for CA. Amit Gupta, Secretary, DAAB, Ms. Nishi Saraf, Section Officer for their untiring efforts in finalization of the updated Modules.

We are sure that these updated Modules on Post Qualification Course on Information Systems Audit would be of immense help to the members and enable them to enhance service delivery not only in compliance, consulting and assurance of IT services, but also provide new professional avenues in the areas of IT Governance, Cyber Security, Information System Control and assurance services.

CA. Manu Agrawal	CA. Dayaniwas Sharma
Chairman	Vice-Chairman
Digital Accounting and Assurance Board	Digital Accounting and Assurance Board

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 auditors 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.

1.2 Introduction

In the present age of globalization, Information Systems have become the backbone for any organization whether the field of its operations is manufacturing, education, trading, technology or entertainment, etc. Nowadays, the success of any organization thrives on information that is generated within the information systems. 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 in selection and implementation of information systems to providing assurance services. The engagements can go beyond just implementing some basic IT level security. It is important for organisations to take a holistic approach and implement security from a governance perspective with involvement of board in directing 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 IS auditor has expanded to review not only whether IT is deployed in a safe and secure environment but also to provide advisory services on optimum use of technology to enable organizations to survive and thrive in the competitive environment while complying with regulatory requirements.

1.3 Definitions

Audit: In simple terms, audit is an inspection of an organization's accounts, typically by an independent body. In case of financial audit, audit is an independent examination of financial information of any entity, whether profit oriented or not, and irrespective of its size or legal form with a view to expressing an opinion thereon. In case of IS Audit, the audit encompasses independent review and evaluation of automated information systems, related manual systems and the interfaces between them.

Computer System: A computer is an electronic device that processes data by following a set of instructions. It has the ability to receive input, process data, and with the processed data, create information for storage and/or output. A computer system is a complete and functional computer that includes required hardware and software.

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

Information Systems (IS): Information systems are formal, sociotechnical, organizational systems designed to collect, process, store, and distribute information. In a sociotechnical perspective, information systems are composed by four components: task, people, structure, and technology. In general, Information Systems refer to hardware and software, that people and organizations use to collect, filter and process, create, and distribute data. Specifically in the context of IT, Information systems support data-intensive applications and include the design and implementation of languages, data models, process models, algorithms, networks etc.

Secure system: It means computer hardware, software and procedures that are reasonably:

(a) Secure from unauthorized access and misuse;

(b) Provide assurance for correct information processing;

(c) Suited to perform 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 its 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 organization to help in achieving specific goals. Internal controls include the policies, standards, practices & procedures, and organisational structures designed to provide reasonable assurance that enterprise objectives will be achieved and undesired events will be prevented, detected and corrected.

Business Process: A business process is a collection of related, structured activities or tasks that produce a specific service or product (serve a particular goal) for a particular customer or customers. It often can be visualized with a flowchart as a sequence of activities, decision points or with a Process Matrix showing interrelated activities based on data flow 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 a requirement of the statutory audit. As per the general guidelines on Internal Auditing issued by ICAI, Auditing is defined as a systematic and independent examination of data, statements, records, operations and performances of an enterprise for a stated purpose. In an auditing situation, the IS Auditor perceives and recognizes the propositions before him for examination, collects evidence, evaluates the same and on this basis formulates judgment which is communicated through the report.

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

Standard on Auditing (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 can be carried out by external auditors as part of statutory audit to review internal controls in automated information systems. However, the scope would be bound by the objectives of the applicable regulatory requirements. IS Audit could also be carried out as a part of internal audit or as a specialized audit of IT environment such as penetration testing, audit of data centre, audit of Business Continuity Plan or review of IT strategy etc.

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

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

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

Work performed by others: When the IS Auditor delegates work to assistants or uses work performed by other IS Auditors or experts, he continues 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 latter have adequate skills and exercise due care and the former are not aware of any reasons to believe that they should not have relied upon the work of the latter. The IS Auditors should carefully direct, supervise and review work delegated to assistants. They should obtain reasonable assurance that work performed by other IS Auditors or experts are adequate and in accordance with set audit objectives.

Documentation: The IS Auditor should maintain documentary evidence that the audit was carried out in accordance with IS Auditing standards, guidelines and procedures and is 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 Computerized Environment

1.5.1 Audit in a Computerized Environment

Historically, all kinds of accounting and data processing jobs were 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, data analytics 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.

However, the overall scope and objectives of audit do not change in a computerised environment. The use of computers changes the methodology of processing and storage of information that may affect the organization and the procedures employed by it to implement adequate and appropriate internal controls. Accordingly, the procedures followed by the auditors 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. Hence, the audit approach and the audit evidence have moved from physical to digital and it may become necessary for auditors to use computers to audit this digital information.

1.5.2 IS Audit and Audit of Computerised Environment

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

- Assessment of internal controls within the IS environment to ascertain the degree of confidentiality, integrity and availability of information and information systems.
- Assessment of the efficiency and effectiveness of the IS environment to evaluate whether it achieves the organization's goals and objectives

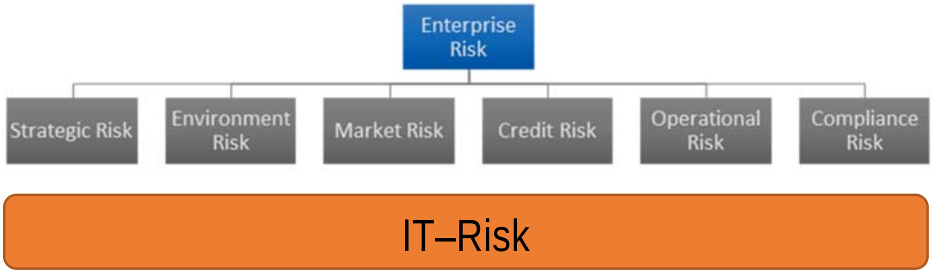
The objective of IS audit process is to evaluate the adequacy of internal controls with regard to both specific computer program and the data processing environment as a whole. ISACA defines IS Audit as: "any audit that encompasses wholly or partly, review and evaluation of automated information processing systems, related non-automated processes and the interfaces between them". Although IS Audit is often misunderstood as a mere technical audit and a domain of IT professionals, it is clear that IS Audit involves evaluating the adequacy and efficiency of internal controls in business processes that are either partly or fully computerized. Hence, Audit and Control professionals who have expertise in understanding of business processes and internal controls and knowledge of information systems' risks and associated 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 automated information processing systems only but would include audit of non-automated processes and their interfaces to the automated processes. 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 applications, technology and related controls. IS Audit being a focused audit about auditing an information systems area whereas Audit in a Computerized Environment is a regular audit engagement performed in process area that uses computers.

1.6 Concept of IT Risk

There are numerous changes in IT and its operating environment that emphasizes the need to better manage IT related risks. This has increased the level of dependency of organizations on electronic information which are processed by IT systems. These IT systems are now essential to support critical business processes. Risk is an event which has a potential to impact organization's goals 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 the figure given below. 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 controls on IT and IT security can lead to lower credit ratings of organizations. For this 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 risk in the overall environment and provides a structure for managing IT risk. The Risk universe:

- considers the overall business objectives, business processes and their dependencies throughout the enterprise. It describes which IT applications and infrastructure support the business objectives through the provision of IT services. It is worth highlighting that IT risk needs to be seen from an end-to-end business activity perspective, crossing IT function silos (IT operations, project management, application development, disaster recovery, security, etc.).
- considers the full value chain of the enterprise. This can include not only the enterprise and its subsidiaries/business units, but also clients, suppliers and service providers.

- considers a full life-cycle of IT related business activities, including transformation programs, investments, projects and operations.
- includes a logical and workable segmentation of the overall risk environment. This sounds relatively easy but often it is not – the hierarchical organizational of the enterprise business, business processes and supporting IT infrastructure and services often are not aligned, and it is highly probable that different views along different dimensions exist for the overall environment. It is up to the enterprise to determine which view will be the most meaningful to support the business objectives of the enterprise while considering the potential overlaps and omissions.
- needs to be reviewed and updated on a regular basis due to the constantly changing internal and external requirements.

1.6.2 Risk Management

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

Here onwards, the word Risk should be interpreted as IT Risk and Audit would be referred to 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 risks 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 note 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 business of the company. This type of risk assessment decision can help relate the cost-benefit analysis of the controls to the known risks, 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 services and their reliability are critical.

By understanding the nature of business, IS Auditors can identify and categorize the types of risks associated with the business and identify the risks applicable to specific situations. 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 the 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 Universe

Audit universe consists of all risk areas that could be subject to audit, resulting in a list of possible audit engagement that could be performed. The audit universe includes projects and initiatives related to the organisation's strategic plan, and it may be organised by business units, product or service lines, processes, programs, systems or controls or by risk category/ prioritisation.

Organisation should identify and keep up to date all the possible audits that can be done.

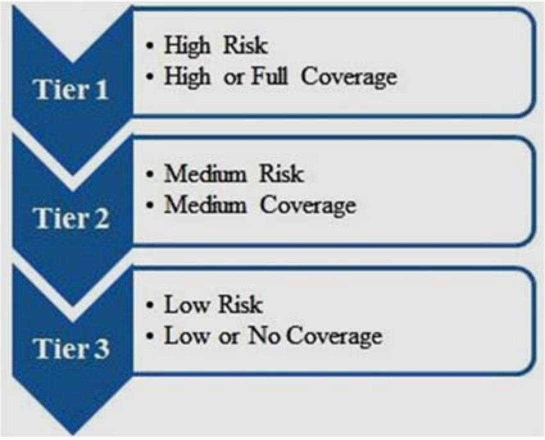
1.8.1 Benefits of having an Audit Universe

One of the advantages of having an audit universe is that it enables the audit activity to be clear about the extent of coverage of key risks and other risk areas each year. It can also provide a degree of rigour around areas not being audited. This means that for those audit committees and senior managers who value a degree of cyclical assurance, the audit universe could be used to inform this. The benefits of an audit universe could also be extended to organisations with a network of retail outlets, depots, branches, regional operations, subsidiaries where managers are mitigating risks on a day to day basis at the front line of service provision.

In these situations, individual engagements in the audit plan, drawn from the audit universe, can be organised to address the top risks to the organisation focused on those aspects managed at the location. The important issue here is making sure regular or cyclical audit reviews result in auditing the management of significant risks rather than risks that have little or no significance.

Thus, entities or areas within the audit universe with a lower risk ranking would be audited at a different frequency than those with a higher risk rating. Indeed it is possible that some areas within the audit universe will never be audited, highlighting the importance of other assurance providers for those areas.

An audit universe can be a useful aid to help communicate the amount of coverage of the organisation by internal audit, which can be invaluable during resourcing discussions. The table below shows an example of planned coverage by audit against the total audit universe (in this case, ranked into tiers 1, 2 and 3, as per their risk impacts).



In practice, other considerations may override the simplified tier classification. Those include, but are not limited to:

1. Board/senior management requested review(s)
2. Regulator requested review(s)

In these circumstances, those considerations would be incorporated into the risk assessment and therefore form part of the risk rating to facilitate tier classification.

The audit universe can be valuable to assist the head of internal audit consider all of the relevant areas in forming an "overall audit opinion".

1.9 Audit Risk and Materiality

1.9.1 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 systems to material theft, destruction, disclosure, unauthorized modification, or other impairment, assuming that there are no related internal controls. Inherent risk is the risk that has natural association. The inherent risk for audit assignment can be project related risks, revenues related risks, and resource related risks. Inherent risk to business can be dependent on nature of business. If the IS Auditor concludes that there is a high likelihood and consequence of risk exposure, ignoring internal controls, the IS Auditor would conclude that the inherent risk is high.
>
> 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 exceeds 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.
>
> 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 risks and control risks are high. Detection risk primarily refers to the fact that there exists a control weakness that auditor fails to detect.

Assessing inherent, control and detection risks 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.

1.9.2 Materiality

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

The concept of materiality requires sound judgment from the IS Auditor. The IS Auditor may detect a small error that could be considered significant at an operational level, but may not be viewed as significant to upper management. Materiality considerations combined with an understanding of audit risk are essential concepts for planning the areas to be audited and the specific tests to be performed in the audit. Higher the level of materiality, lower is the risk that an IS auditor is, usually, willing to take.

For systems and operations not affecting financial transactions, following are the 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). As for example 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 as to how and from where the virus entered the organisation’s information systems. The analysis may reveal that there is a 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's information systems. 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 (Information Technology Assurance Framework) 3rd edition issued by ISACA has the following standards on "Materiality" which have 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:

a. Absence of controls or ineffective controls

b. Significance of the control deficiency

c. Likelihood of these weaknesses resulting in a significant deficiency or material weakness.

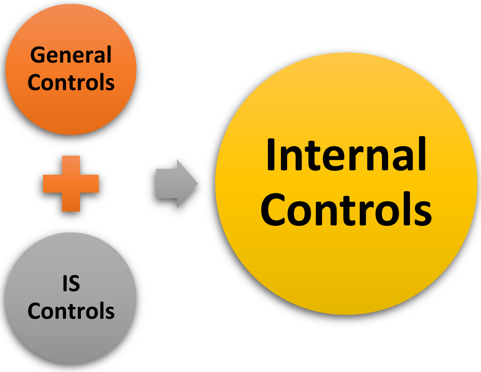
1.10 Concepts of Internal Controls

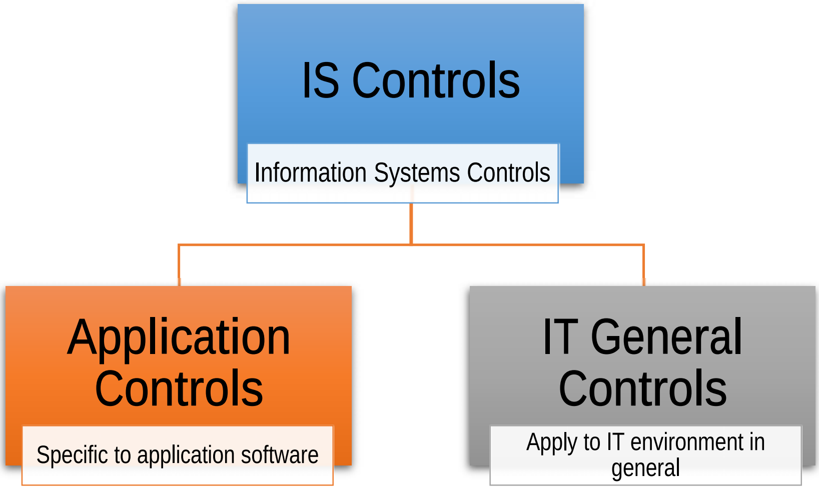
The increasing use of IT in organizations has made it imperative that appropriate information systems are implemented in an organization. IT should cover all key aspects of business process of an enterprise which have an impact on its strategic and competitive advantage for its success. Control is defined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

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

1.10.1 Types of Internal Controls

Internal Controls is said to be a mechanism that is established by organizations which is a sum of General Controls and IS Controls. IS controls is said to be a sum of IT Application Controls and IT General Controls. General Controls refers to internal controls that encompass all administrative areas in general including IT implementation whereas application controls are implemented in specific application softwares. 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.




IS Controls
Information Systems Controls
Application Controls
Specific to application software
IT General Controls
Apply to IT environment in general

1.10.2 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 operations 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; e.g. Firewalls.

Detective Controls: Controls that detect and report the occurrence of an error, omission or malicious act; e.g. Audit Trails.

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

1.11 Organization of IS Audit Function

The IS audit function should be placed in the organization so as to ensure its objectivity and independence. The composition and constitution of the IS audit function should ideally be decided by the Audit Committee which should be the prime reporting authority 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. The appointment of external auditors should also be governed by stipulations for independence and objectivity, which is the foundation for an effective audit function.

1.11.1 Infrastructure and Organization

IS audit function should be equipped with sufficient resources to discharge its duties efficiently and effectively. An important determinant in the quality of the IS audit function is the quality of human resources that staff the audit function. The skills and competence requirements should be clearly established and the 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 competences 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:

d. Which organizational structures are required to provide assurance (board/audit committee, audit function, etc.)?

e. 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 3rd 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.

1.11.2 Internal and External Audit Control Framework

The internal and external audit control framework ensures the minimum quality of audits. This forms the basis for the organization to implement 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 organization and operations of the audit function. Specific guidelines have to be issued to ensure the qualitative work under control environment.

1.11.3 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.

1.11.4 Standards on Audit Performance

IS auditors are expected to comply with the following standards of ITAF 3rd 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, measurable, 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.

1.12 Summary

This chapter has provided brief overview of the fundamental concepts of Audit, IS audit, risks, controls and internal controls. We have also provided the distinction between audit in an IS environment and audit of a computerized environment. Further, the conceptual understanding of IT risk and risk-based auditing has been provided with an overview of types of audit risks and their categorization as: Inherent Risk, Control 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 IS controls are bifurcated as IT Application Controls which are specific to application softwares 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 risks.

1.13 Case Study

Case Background:

M/s InfoTech Solutions have been assigned to review effectiveness of existing controls of Online Portal of a large Retail Chain. One of the clauses of service level agreement is stated below:

“InfoTech Solutions to submit final audit report within 1 month from date of agreement. In case of deviation following penalty to be impacted:

Turn Around Time	Penalty
Within 30 days	Nil
31-40 days	10% of total fees payable
41-50 days	20% of total fees payable

51-60 days	30% of total fees payable
Above 60 days	50% of total fees payable

To adhere to SLA, M/s InfoTech Solutions detailed out following audit program:

(i) Detailed Risk Assessment will not be carried out. Audit will be assigned to a Senior IS Auditor and he will decide audit area and sampling techniques as per his prior experiences.

(ii) Initially, 2 associates will be allotted for the assignment. More resources will be provided as and when required.

(iii) Senior Auditor will have to submit his draft report to Partner by 25th day and final report to be issued to client by 30th day.

(iv) To preserve time, working papers and evidence gathering will be structured once the final report is submitted.

Questions:

(1) While planning an audit M/s InfoTech Solutions should have FIRST identified:

(a) Areas of High risk.

(b) Skill sets of the audit staff.

(c) Test steps in the audit.

(d) Time allotted for the audit.

Correct Answer: A, areas of high risk

Explanation:

(a) When designing an audit plan, it is important to identify the areas of highest risk to determine the areas to be audited.

(b) Skill sets of audit staff is an important consideration. However, unless risks are identified it will not be known how and where to utilize the skills.

(c) Compliance test and substantial test can be effectively carried out only once auditor is aware about areas of high risk.

(d) Allotment of time is important but not the first & primary step like identification of high-risk areas.

(2) M/s InfoTech Solutions has decided to Skip Risk Assessment Process. What is the Primary Risk involved here?

(a) Resources may not be allocated to the areas of highest concern.

(b) Budgets are more likely to be met by the IS audit staff.

(c) May not able to complete assignment as per timelines defined in SLA.

(d) Senior Auditor may not take responsibility of Audit Observations.

Correct Answer: A, Resources may not be allocated to areas of highest concern

Explanation: Primary Risk involved here is critical risks are not identified and may remain unnoticed. Other areas are not of that concern.

(3) The decisions and actions of Senior Auditor of M/s InfoTech Solutions are MOST likely to affect which of the following risks?

(a) Detection

(b) Inherent

(c) Control

(d) Business

Correct Answer: A, Detection Risk

Explanation:

(a) Detection risks are directly affected by the auditor's selection of audit procedures and techniques.

(b) Inherent risks usually are not affected by the IS auditor.

(c) Control risks are controlled by the actions of the company's management.

(d) Business risks are not affected by the IS auditor.

1.14 Questions

1 **The primary purpose and existence of an audit charter is to**:

A. Document the audit process used by the enterprise

B. Formally document the audit department's plan of action

C. Document a code of professional conduct for the auditor

D. Describe the authority and responsibilities of the audit department

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. To conduct a system audit, the IS auditor should

A. Be technically at par with client's technical staff

B. Be able to understand the system that is being audited

C. Possess knowledge in the area of current technology

D. Only possess a knowledge of auditing.

4 Which of the following are most commonly used to mitigate risks discovered by organizations?

A. Controls

B. Personnel

C. Resources

D. Threats

5 The rate of change in technology increases the importance of:

A. Outsourcing the IS function

B. Implementing and enforcing good processes

C. Hiring personnel willing to make a career within the organisation

D. Meeting user requirements

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. 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.

1.15 Answers and Explanations

1 An audit charter describes the authority, responsibility of the audit department. These are established by the senior management. Correct answer is D.

2 Corrective Controls classification identify the cause of a problem and minimize the impact of threat. The goal of these controls is to identify the root cause of an issue whenever possible and eliminate the potential for that occurring again. The other controls are useful but perform other functions instead. Correct answer is D.

3 To conduct IS Audit by the IS Auditor, the primary requirement is that he should be able to understand the system and technology being audited. He is not required to be the expert in all subjects. There is no comparison of his knowledge with that of

auditee's staff. He should have the knowledge of audit along with the technology in the related subject of audit. Correct answer is B.

4 Controls are most commonly used to mitigate risks discovered by organizations. This is what organizations implement as a result of the risks an organization discovers. Resources and personnel are often expended to implement controls. Correct answer is A.

5 Rate of change of technology increases the importance of implementing and enforcing good practices. Correct answer is B.

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. Correct answer is A.

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. Correct answer D

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

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. Correct answer B.

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 choice. Correct answer is A.

Chapter 2

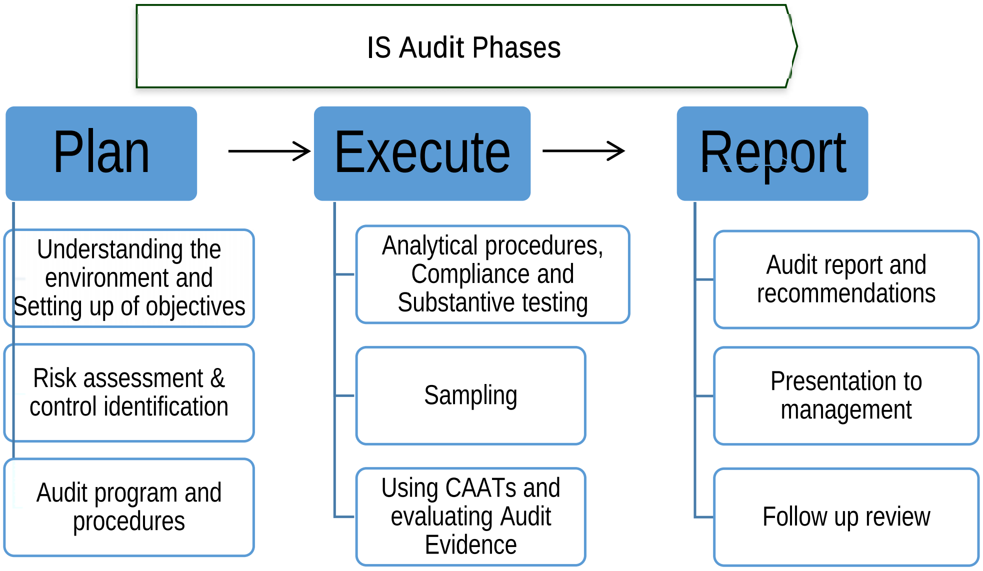
IS Audit in Phases

2.1 Learning Objectives

This chapter provides detailed insights into various phases of IS audit. The fundamental concepts which were discussed in earlier chapter are connected to their practical aspects in terms of how to define the audit scope and objectives, gain knowledge of the organisation's business, assessment of risk, IT application controls and IT general controls of the enterprise. Sampling and testing methodologies using CAAT as used by the IS auditor are also discussed. How to develop audit programs and approach and design appropriate tests for compliance and substantive testing for reviewing the design effectiveness and operational effectiveness of the Information 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' words are used inter-changeably.

2.2 Introduction

Information systems have become an integral part of business processes. The growth of technology has made IT an indispensable part of our day to day functioning. Organizations value information as the most critical asset and hence it has become more vulnerable to theft causing loss to the enterprise. There is a risk that the information may be stolen fraudulently and fraudsters can use it for financial gains. Information systems are helping organizations in improving efficiency in customer delivery and also opening up new delivery channels. In order to adapt to these technological advancements organizations have reengineered their processes which has potential of introducing new vulnerabilities. There is critical requirement of enhancing value of information by making it available online but this should be coupled with right level of security. In the networked world, the fraudsters can intrude the systems anytime and from anywhere. It is important that the management not only has systems and processes in place to ensure that adequate controls exist and are working effectively but also having an independent evaluation by 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 summarized in the following diagram.


IS Audit Phases
Plan
Execute
Report
Understanding the environment and Setting up of objectives
Risk assessment & control identification
Audit program and procedures
Analytical procedures, Compliance and Substantive testing
Sampling
Using CAATs and evaluating Audit Evidence
Audit report and recommendations
Presentation to management
Follow up review

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. Auditee 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, these should be reported with appropriate recommendations for mitigating these risks by improving controls and thus add value.

2.3.2. Request for proposal (RFP)

Many a times, organizations may need to engage outside agencies i.e. external auditors for some audit assignments. An RFP is a standard solicitation document used by various organisations to compete for contract opportunities. An RFP is most often used to acquire services, although it may be used in some circumstances to acquire goods. A successful RFP process will support the principles of fair, open, and transparent procurement and will satisfy the business requirements. Well-prepared RFPs can go a long way in creating effective solutions and programs for business development and associations. With an RFP, proposals are evaluated against multiple criteria such as price, qualifications and experience, and the proposed solution or approach. The best proposal is awarded the contract though it may, or may not, quote the lowest price. **IS Auditor can play an important role in preparation and evaluation of responses to** RFP.

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 authorized through the audit charter. This mandate 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 therein.

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
- Organizational structure, including reporting lines to board and senior management
- Grading of IS audit staff

Accountability

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

2.4.2 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 organization.

Content: The engagement letter should clearly address the three aspects of responsibility, authority and accountability. Aspects to consider are set out in the following paragraphs.

Responsibility

- Scope
- Objectives
- Independence
- Risk assessment
- Specific Auditee requirements
- Deliverables

Authority

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

Accountability

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

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

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 continuing involvement of client personnel. Hence, on-going communication with the auditee is critical.

2.4.3 Communication with Auditee

Effective communication with Auditee involves:

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

The audit charter forms a sound basis for communication with Auditee and should include references to service level agreements for things such 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's 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 IS Auditor continues to remain responsible for the assignment. IS auditor should develop standard approach, documentation and methodology with appropriate templates for various types of assignments. Best practices and frameworks along with 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.

According to SA 220 of ICAI, Quality Control Systems, policies and procedures are the responsibility of the audit firm. Under SQC 1, the firm has an obligation to establish and maintain a system of quality control to provide it with reasonable assurance that: (a) The firm and its personnel comply with professional standards and regulatory and legal requirements; and (b) The reports issued by the firm or engagement partners are appropriate in the circumstances. This SA 220 is premised on the basis that the firm is subject to SQC 1. Within the context of the firm's system of quality control, engagement teams have a responsibility to implement quality control procedures that are applicable to the audit engagement and provide the firm with relevant information to enable the functioning of that part of the firm's system of quality control relating to independence. Engagement teams are entitled to rely on the firm's system of quality control, unless information provided by the firm or other parties suggests otherwise.

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 should 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 including:

- 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 and budget cuts etc.
- Is the timing appropriate for auditing the issue?
- Are there any examples of past non-compliances?
- What is the management style and the risk appetite and approach to risk management?
- Are there any cases of past fraud or material errors?

Carefully scoping the audit early in the process helps increase efficiency and effectiveness of the audit. The statement of scope should be clear about any areas excluded from audit.

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 risks 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, teams and individuals with specific skills are assigned to specific assurance reviews as per time plan. The audit planning process has to consider budgets of time and costs, and management priorities as per organizational goals and policies. The objective of audit planning is to optimize the use of audit resources. In case of independent assurance assignments, audit planning is done by external firm as per scope of audit engagement letter considering available resource requirements, auditee availability and reporting timings to regulatory authorities.

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

effectiveness and efficiency of the audit and to coordinate audit procedures with work of the entity's personnel. The overall audit plan and the audit program; however, remain the IS Auditor's responsibility.

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

Audit should be guided by an overall audit plan and underlying audit program and methodology. Audit planning is often mistaken as a one-time activity to be taken and completed in the beginning of the audit. While for all practical purposes, planning is a continuous activity which goes on throughout the entire audit cycle. Many a 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 circumstances may require. 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 the reason for the change. Information Technology Assurance Framework (ITAF) 3rd edition issued by ISACA provides the following standards to be followed by IS Auditors:

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's 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.

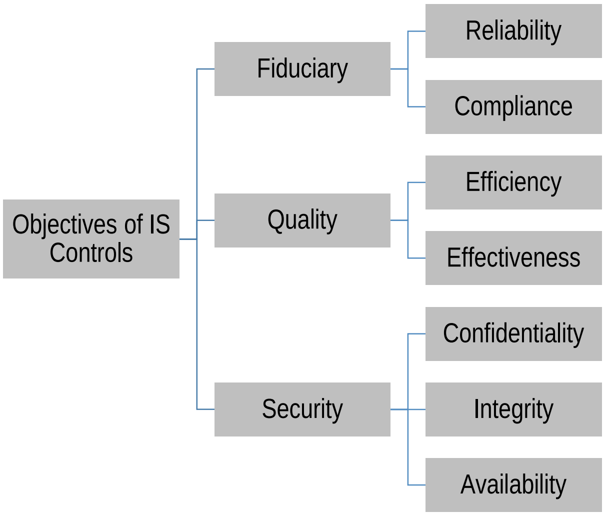
1202.3 IS audit and assurance professionals shall consider subject matter risk, audit risk and related exposure to the enterprise.

Steps for Audit Planning

- Gain an understanding of the business's mission, objectives, purpose and processes, which include information and processing requirements such as availability, integrity, security and business technology and information confidentiality.
- Understand changes in business environment of the auditee
- Review prior work papers
- Identify stated contents such as policies, standards and required guidelines, procedures and organisation structure
- Perform a risk analysis to help in designing the audit plan
- Set the audit scope and audit objectives
- Develop the audit approach or audit strategy
- Assign personnel resources to the audit
- Address engagement logistics.

2.7 Objectives of IS Controls

IS audit requiring primarily review of Controls in the IS environment and provide recommendations on areas of weaknesses. The objective of IS controls is to ensure risk management processes are implemented as per the risk management strategy which involves risk avoidance, risk elimination where possible, risk reduction or risk transfer and finally risk acceptance. Hence, controls should result in risk remediation. IS 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 2019. It is important for IS Auditors to understand controls and control objectives as these forms the most important criteria used for evaluation. Every IS Audit would have a combination of these controls which are used at the 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 and the information processes should be reliable at any given point of time and the same are accessible as and when needed.

Compliance: It deals with complying with laws, regulations and contractual regulations to which the business is subjected to e.g. 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: It is 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: It is a measure of whether the objectives of a process, service or activity have been achieved. An Effective Process or Activity is one that achieves its agreed Objectives. Effectiveness, or Cost Effectiveness, is one of the measures needed to determine value for money. It concerns the cost of the outputs from an activity and the conformance of those outputs to a specification or need. 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 unauthorized individuals or systems and maintain Privacy i.e. the ability to control or restrict access so that only authorized individuals can view information. One of the underlying principles of confidentiality is "need-to-know" or "least privilege". In effect, access to vital information should be limited only to those individuals who have a specific need to see or use that information. Confidentiality is necessary for maintaining the privacy of the people whose personal information a system holds.

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

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

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

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

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. It is the assurance that the systems are available 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(LODR of SEBI - the 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 that are needed to provide information when it is needed but thinking in terms of information security, Availability in itself in no way guarantees that someone else isn't making unauthorized use of your hardware resources.

2.8 Understanding the IT Environment of Auditee

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

Auditor may follow the guidelines mentioned in SA 315 of ICAI to understand the entity and its environment.

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, 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) systems (wherever implemented) and IT controls are few areas, not exclusive, which the IS Auditors should acclimatize with, which shall enable them to plan and perform the audit.

2.8.2 Organization Structure

Some of the organizational structure activities are task allocation, coordination and supervision, which are directed towards the achievement of organizational aims. It can also be considered as the viewing glass or perspective through which individuals see their organization and its environment. Organizational structure allows the allocation of responsibilities for different functions and processes to different sub sets of organisation such as the branch, department, workgroup and individual. The IS Auditor has to factor in the manner in which the organization is setup to understand roles and responsibilities, policy frameworks, etc. to ensure efficiency and effectiveness of audit.

2.8.3 IT Infrastructure

The IS Auditor has to obtain understanding of the 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 all information 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 tastings etc.

2.8.4 Regulations, Standards, Policy, Procedures, Guidelines & Practices

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
- Identify compliance requirements 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 compliance depending on the nature of business organisation.

Information Technology Act 2000 (Amended in 2008)

Section 7A Audit of Documents etc. maintained in Electronic Form states that 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 processed and maintained in electronic form.

Section 43A of the (Indian) Information Technology Act, 2000 provides that a body corporate possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates and is negligent in implementing and maintaining reasonable security practices and procedures resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages by way of compensation 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 Amendment Act 2008 recognizes and punishes offences by companies and individual (employee) actions. For example: Section 66 to 66F and 67 deal with the following crimes:

- Sending offensive messages using electronic medium or using body corporate's IT for unacceptable purposes
- Dishonestly stolen computer resources
- Unauthorized Access to computer resources
- Identity theft/Cheating by impersonating 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 or fine extending to INR 5,00,000 or with both.

Sarbanes Oxley Act, 2002 (SOX)

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

Section 404 draws attention to the significant processes that feed and comprise the financial reporting process for an organization. In order for management to make its annual assessment on the effectiveness of its internal controls, the 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.

LODR – Listing Obligations & Disclosure Requirements of SEBI on Corporate Governance

Audit Committee

As per the above regulation of SEBI, the role of the Audit Committee has 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/IEC 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 27001:2013 formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information security risks. The ISMS is an overarching management framework through which the organization identifies, analyses and addresses its information security risks. The ISMS ensure 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 ISO/IEC 27001:2013 flexible risk-driven approach.

ISO/IEC 27001:2013 is a formalized specification for an Information System Management System (ISMS) with two distinct purposes:

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

ISO/IEC 27002:2013 is a code of practice - a generic, advisory document, not a formal specification such as ISO/IEC 27001:2013. 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.

Regulators' guidelines

Financial regulators Reserve Bank of India & SEBI have issued various guidelines over the last few years and all of them bear various control procedures and directives for implementing security and best practices in the financial organisations. Some of the important guidelines are mentioned below:

- Working Committee Guidelines on Cyber Security, IS Audit, IT Security, BCP etc. (Gopalakrishna Committee report) issued on 29.04.2011
- Cyber Security Guidelines and Framework (02/06/2016)
- IT and Cyber Risk Management (10/10/2016)
- Fraud Risk Management – do's and don'ts (01/02/2017)
- Report on working group of FinTech and Digital Banking (08/02/2018)
- SEBI circular on Cyber Security Framework
- Section 143 of Companies ACT- requirement of IFC's.

2.9 Frameworks and Best Practices of IS Audit

2.9.1 ITAF (3rd edition)

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 professionals' roles and responsibilities; knowledge and skills; and diligence, conduct and reporting requirements
- Defines terms and concepts specific to IS assurance
- Provides guidance and tools and techniques on the planning, design, conduct and reporting of IS audit and assurance assignments

ITAF audit and assurance standards are divided into three categories:

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

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

2.9.2 COBIT 2019 Framework: Principles, Components and Core Models

COBIT 2019 is a globally accepted framework and caters for the governance and management of enterprise information and technology, aimed at the whole enterprise. COBIT defines the components and design factors to build and sustain a best-fit governance system.

COBIT 2019 framework helps ensure effective enterprise governance and management of Information and Technology, facilitating easier, tailored implementation and also plays an important role as a driver of innovation and business transformation.

COBIT 2019 helps organisations to manage IT related risk and ensures compliance, continuity, security and privacy. It 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 2019 is that it is useful for organisations of all sizes, whether commercial, not-for-profit or in the public sector.

Governance System Principles of COBIT 2019

COBIT 2019 simplifies governance challenges with just 6 principles. The six key principles for governance and management of enterprise Information and Technology in COBIT taken together enable the organisation to build an effective governance and management framework that optimizes information and technology investments and use for the benefit of stakeholders.

Principles 1: Provide Stakeholder Value: Enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources. COBIT 2019 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, the enterprise can customize COBIT 2019 to suit its own context through the goals cascade, translating high level enterprise goals into manageable specific IT related goals and mapping these to specific processes and practices.

The COBIT 2019 goals cascade is the mechanism to translate stakeholder drivers and needs to specific, actionable and customised enterprise goals and aligning the Goals; Governance and Management objectives.

Principle 2: Holistic Approach: Efficient and effective governance and management of enterprise I & T require a holistic approach, taking into account several integrating components. COBIT 2019 defines a set of seven components of Governance system to support the implementation of a comprehensive governance and management system for enterprise I & T. Enablers are broadly defined as anything that can help to achieve objectives of the enterprise.

Principle 3: Dynamic Governance System: A Governance system should be dynamic. This means that each time one or more of the design factors changes (e.g., a change in strategy or technology), the impact of these changes on the Enterprise Governance of Information and Technology (EGIT) system must be considered. A dynamic view of EGIT will lead towards a viable and future proof EGIT system.

Principle 4: Governance distinct from Management: The COBIT 2019 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities that require different organizational structures and serve different purposes.

- **Governance:** It ensures that stakeholders needs, conditions and options are evaluated to determine balanced, agreed on enterprise objectives to be achieved; setting direction through prioritization and decision making, and monitoring performance and compliance against agreed on direction and objectives. In most organizations the governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities many be delegated to special organizational structures at an appropriate level, especially in larger, complex organizations.
- **Management:** It plans, builds, runs and monitors activities in alignment with the directions 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.

Principle 5: Tailored to Enterprise Needs: A Governance system should be customized to the enterprise needs, using a set of design factors as parameters to customise and prioritise the Governance system components.

Principle 6: End to End Governance System: A governance system should cover the enterprise from end to end, focussing on not only the IT function but on all technology and information processing the enterprise puts in place to achieve its goals, regardless of its location in the enterprise.

Governance Framework Principles

COBIT-2019 talks about three governance framework principles in addition to the above six Governance Systems principles. They are:

1. Based on conceptual model
2. Open and flexible
3. Aligned to major standard

Components of Governance System

Components are enablers and 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 components of Governance system are:

- Processes
- Organizational structures
- Information flows and items
- People, skills and competence
- Policies and procedures
- Culture, ethics and behaviour
- Services, infrastructure and applications

Core Governance and Management Objectives in COBIT 2019

The Governance and Management objectives are grouped into 5 domains. There are 40 core objectives.

Governance objectives are grouped in the Evaluate, Direct and Monitor domain. Basic five objectives are Ensured Governance Framework Setting and Maintenance, Ensured Benefit Delivery, Ensured Risk Optimisation, Ensured Resource Optimisation and Ensured Stakeholder Engagement.

Management Objectives are grouped into 4 domains.

1. Align, Plan and Organise (APO)

This domain addresses the overall organization, strategy and supporting activities for I&T. The objectives are Managed IT & Management framework, strategy, enterprise architecture, innovation, portfolio, budget & costs, human resources, relationships, service agreements, vendors, quality, risk, security and finally data.

2. Build, Acquire and Implement (BAI)

This domain treats the definition, acquisition and implementation of I&T solutions and their integration in business processes. The objectives are managed programs, requirement definition, solution identification & build, availability & capacity, organisational change, IT changes, IT change acceptance & transitioning, Knowledge, Assets, configuration and projects.

3. Deliver, Service and Support (DSS)

This domain addresses the operational delivery and support of I&T services, including security. The objectives are managed operations, service requests & incidents, problems, continuity, security services and business process controls.

4. Monitor, Evaluate and Assess (MEA)

This domain addresses performance monitoring and conformance of I&T with internal performance targets, internal control objectives and external requirements. The objectives are managed performance & conformance monitoring, system of internal controls, compliance with external requirements and assurance.

Using COBIT 2019 for IS Assurance

COBIT 2019 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, 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 2019 has specific process: “MEA 02 Managed System of Internal Control”, which provides guidance on evaluating and assessing internal controls implemented in an enterprise. Such review would provide assurance on the transparency for key stakeholders on the adequacy of the system of internal controls and this provides 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

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 risks identified in this stage would be evaluated for the controls that have been incorporated to treat the risk. Thus, the IS Auditor can focus on the high-risk areas and decide the sampling that would be performed on the identified areas. The risks can be identified by reviewing the factors implemented by the enterprise:

1. Reviewing IT principles, policies and frameworks.
2. Reviewing processes, including risk, function-specific details and activities.
3. Reviewing organizational structures.
4. Observing culture, ethics and behavioural 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 risks relevant to the area under review.

- Conduct a preliminary assessment of the risks 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 program and project delivery, and/or IT operations and service delivery. Capture relevant data from related issues, incidents, problems and investigations.
6. For similar classes of events, organize the collected data and highlight contributing factors. Determine common contributing factors across multiple events.

7. Determine the specific conditions that existed or were absent when risk events occurred and the way the conditions affected event frequency and loss magnitude.
8. Perform periodic event and risk factor analysis to identify new or emerging risk issues and to gain an understanding of the associated internal and external risk factors.

Analyze Risk

1. Develop useful information to support risk decisions that consider 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. Consider all applicable risk factors, evaluate known operational controls and estimate residual risk levels.
5. Compare residual risk to acceptable risk tolerance and identify exposures that may require a risk response.
6. Analyze cost-benefit of potential risk response options such as avoid, reduce/mitigate, transfer/share or accept and exploit/seize. Propose the optimal risk response.
7. Specify high-level requirements for projects or programmers that will implement the selected risk responses. Identify requirements and expectations for appropriate key controls for risk mitigation responses.
8. Validate the risk analysis results before using them in decision making, confirming that the analysis aligns with enterprise requirements and verifying that estimations were properly calibrated and scrutinized for bias.

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

2.10.3 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 within 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 risks which are present in the business environment and in the internal control system that influence 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 to audit.

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

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

2.11 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 organizational and administrative structure of the IS function, the existence of policies and procedures for the day-to-day operations, availability of staff and their skills and the overall control environment. It is important for the IS auditor to obtain an understanding of these as they are the foundation on which other controls are built.

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 should also 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 visitors' access.

IT General controls are controls that are around the applications. These controls support the healthy maintenance and general security of the applications and the IT processes present. These processes include Change Management, Logical and Physical Access Management, Backup and Recovery procedures, Incident Management, Job and Batch Scheduling, procedures for review of security within Operating systems and databases etc.

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 and are all pervasive. If the IT General controls are not effective it may not be possible to rely on other controls within the IT environment i.e. the application controls. Some of the IT General Controls are as follows:

Operating System Controls

Operating System (OS) is the computer control program. It allows users and their applications to share and access common resources, such as processor, main memory, database and printers. It performs the main tasks of scheduling jobs, managing hardware and software resources, maintaining system security, enabling multiuser resource sharing, handling interrupts and maintaining usage records. To enhance usability, the Operating System must manage these resources so that these are available to each authorized user. Moreover, each user must be able to execute a job without regard to the other users.

Auditors often pay little attention to Operating System controls. Breaches of operating systems controls could have catastrophic effect. The OS must be protected from user processes and should be robust. Among various controls of OS, limiting administrator account access, safeguarding domain controller, implementing adequate password policy and access control mechanism for OS, deactivating default accounts, regular patch management, implementing updated anti-virus solution, hardening of OS etc. would help the system to remain secure.

Organisational Controls

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

- 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 utilization of IS resources. Their responsibilities include:

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

(ii) Policies, standards, procedures and practices: Policies establish the rules or boundaries of authority delegated to individuals in the enterprise. Procedures establish the instructions that must be followed for completing the assigned tasks. Mandating all requests for changes to existing programs must be approved by user and IS management before programmers and analysts 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 (Acceptable use policy),
- Reviewing, evaluating, and purchasing hardware and software,
- System development methodology, and
- Application program changes.

Documented procedures should exist for all data processing activities.

(iii) Job Descriptions

These communicate management's specific expectations for job performance. Job procedures establish instructions on how to do the job and policies define the authority and responsibility of the employee. All jobs must have a current documented job description readily available to the employee. Job descriptions establish responsibility and the accountability of the employee's actions.

(iv) Segregation of Duties

Segregation of duties refers to the concept of distribution of work responsibilities such that individual employees are performing only the duties stipulated for their respective jobs and positions. The main purpose is to prevent or detect errors or irregularities by applying suitable controls. It reduces the likelihood of errors and wrongful acts. Organization structure and allied controls should be structured in a manner that ensure 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;
- Organization structure with job description; and
- IT resources deployed such as: Operating system, Networking, Database, Application software, technical staff available, IT services provided in-house or outsourced, centralized or decentralized IT operations etc.

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's work by another, so that employees to some extent police each other. Examples of segregation of duties are, separating:

- Systems software programming group from the application programming group;
- Database administration group from other data processing activities;
- Computer hardware operations from other groups;

- Systems analyst functions from the programming function;
- Application programming group from operations and data preparation group.
- 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 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 operations,
- Network management,
- System administration,
- Data Base administration
- Systems development and maintenance,
- Change management,
- Security administration, and
- Security audit.

Guidelines on Segregation of Duties

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

- Separate those, who can run live programs e.g. operations department, from those who can change programs e.g. programmers. This is required in order to ensure that unauthorized programs are prevented from running.
- Separate those, who can access the data e.g. data entry and the DBA, from those who can run programs e.g. computer operators. This is required in order to ensure that unauthorized data entry cannot take place.
- Separate those, who can input data e.g. data entry, from those, who can reconcile or approve data e.g. data authorization persons. This is required in order to ensure that unauthorized data entry cannot take place.
- Separate those, who can test programs e.g. users, quality assurance and security, from those, who can develop programs e.g. application programmers. This is required in order

to ensure that unauthorized programs cannot be allowed to run.

- Separate those, who can enter errors in a log e.g. data entry operator, who transfer the data to an error log, from those who can correct the errors like the end user departments. This is required in order to ensure that unauthorized data entry cannot take place.
- Separate those, who can enter data e.g. data entry personnel, from those who can access the database e.g. the DBA. This is required in order to ensure that unauthorized data entry or data modification cannot take place.

Management Controls

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

- **Responsibility:** The strategy to have a senior management personnel responsible for the IS within the overall organizational structure.
- **An IT Organization Structure***:* There should be a prescribed IT organizational structure with documented roles and responsibilities and agreed job descriptions.
- **An IT Steering Committee***:* The steering committee shall comprise of representatives from all areas of the business, and IT personnel. The committee would be responsible for the overall direction of IT. Here the responsibility lies beyond 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 and control over transactions processing using reports generated by the computer applications to reflect un-posted items, non-monetary changes, item counts and amounts of transactions for settlement of transactions processed and reconciliation of the applications (subsystem) to general ledger. The financial control techniques are numerous. A few examples are highlighted here:

- **Authorization**: This entails obtaining the authority to perform some act typically accessing assets such as accounting or application entries.

- **Budgets:** These are 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. It can be monetary (dollar value) or non-monetary fields like item counts/item sequence number.
- **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 pre-printed 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.

Data Management Controls

Data management controls fall in two categories – Access Controls and Back up Controls.

- Access controls are designed to prevent unauthorized individuals from viewing, retrieving, computing or destroying the entity's data.
- Back up controls are designed to ensure the availability of data in the event of its loss due to unauthorized access, equipment failure or physical disaster. The organization can

restore its files and databases from backups.

Data Processing Controls

These controls are related to hardware and software and include procedures exercised in the IS environment. These controls are applicable to on-line transaction processing systems, database administration, media library, application program change procedures, data centre operations etc.

Physical Access Controls

These controls are procedures exercised to control 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 also cover supporting services (such as electric power), backup media and any other elements required for the system's operations. Access should be restricted to authorized individuals only. Where IT resources are located in public areas; they should be appropriately protected to prevent or deter loss or damage from theft or vandalism.

Logical Access Controls

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

System Development Controls

These controls are targeted to ensure that proper documentation and authorizations are available for each phase of the system development process. It includes controlling new system development activities and includes six activities of System authorization activities, user specification activities, technical design activities, internal IS Auditor's participation, program testing and user test & acceptance procedures as a part of the system development controls. These are covered in detail in module-3.

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 subsequent module.

System Maintenance Controls

System maintenance controls include controls on changes to program logic, additional controls insertions and regular data base maintenance activities. These are needed for efficient functioning of present systems/ correction/ upgradation of software solutions.

Computer Centre Security Controls

Computer centre security aims at restricting access to computer systems, infrastructure, data and network components and also protection from natural and environmental threats housing the above in a computer centre. The controls can be: Physical security controls, software & data security controls, data communication security controls and environmental security controls. Physical security attempts to restrict breach of access to computers and unauthorized access to records. Software and data security ensures that there is use of passwords, authorizations, screening and logs of all activity of the entity. Data communication security is implemented by terminal locks, encryption of data, network administration, sign on user identifiers etc.

Internet and Intranet Controls

There are two major exposures in the communication sub-system - 1. Component failure and 2. 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/data in the system. These can provide intruders with important information about messages being transmitted and the intruder can manipulate these messages. The controls against component failures include building component level redundancy, avoiding single point of failures, using tested and robust systems. Controls against subversive threats include hardening of systems, patch management, use of updated anti -virus solutions, firewalls, IDS, encryption etc.

Personal Computers Controls

The major risks related to personal computers are the physical theft/damage as logical controls are very weak or missing. The controls refer to safeguard mechanisms for personal computers, pen drives and external drives etc. against the risk of theft of hardware, data/information.

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

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 in 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. Application Controls are controls within the application. These controls can be effective only if the aggregate evaluation on the ITGC (Information Technology General Controls) processes are concluded as effective and support the applications adequately. This is so, as IT General controls are pervasive in nature and if they are not effective, effective operation of application controls cannot be ensured.

There are two types of application controls - i.e. Automated Controls (Fully automated, no human judgement or requirement), the other being Manual controls (these are semi-automated controls requiring an input or action from a human in addition to the execution by IT systems). 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.

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

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

IT Applications controls are the controls over input, processing and output functions. The objectives of application controls are:

- Input data is accurate, complete, authorized and correct.
- Data is processed in an acceptable time period.
- Ensure that the internal processing produces the expected results.
- Processing accomplishes the desired tasks
- Data stored is accurate and complete
- Output is accurate and compete and protected from unauthorized disclosure

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 authorized users and that it protects systems from unauthorized access.

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

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

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

2. Input Controls

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

Input controls address the following:

(a) Source Document Design

(b) Data entry screen design

(c) Data code controls

(d) Batch Controls

(e) Data Input Validation Controls

(f) Data Input Error Handling and Reporting controls

(g) Instruction Input Controls

3. Processing Controls

Controls to ensure that there is only authorized processing and integrity of processes and data is ensured. Data processing controls perform validation checks to identify errors during the processing of data. They are required to ensure both the completeness and accuracy of the data being processed. 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 authorization
- Parity checking

5. Output Controls

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

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

6. Existence 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.

As noted earlier, If IT General Controls are not effective, we cannot proceed to rely on the Application controls and the auditor is required to execute substantive procedures i.e. detailed procedures to obtain the necessary comfort required to provide assurance.

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 authorization
- 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 editable. The correct method would be to pass a 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 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 several modules/options/menus that cater to different functionalities provided by the software. Different users will need access to various features based on their responsibilities and job descriptions. All access should be strictly based on the need to know and do. The design of the access control module may be of varied types. Most software would check a combination of user id and passwords before allowing access. Access may be controlled for each module, menu option, each screen or controlled through objects. Often the matrix of users versus the options/actions becomes too large and complex to maintain hence it is normal to define certain roles for different classes of employees and group them together and assign them similar access. The IS auditor should review the design of the access control module keeping in mind the criticality of the functions/actions possible in the software and evaluate whether the design provides the level of control and granularity to selectively and strictly allows access as per the job requirements of all the users.

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

- Verify how errors and exceptions are handled. At times, software provides options and ways to reverse transactions, correct errors, allow transactions under special circumstances, etc. Each one of these is special to the business and based on the rules and procedures defined by the organization. The IS auditor needs to see how the software handles these. Are these circumstances properly authorized in the software? Does it capture the user id and time stamp for all transactions to provide suitable trails? Are the exceptions and critical activities like updates to global parameters logged for independent review at a later stage.

- Identify all 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 upon which the application runs and the databases it uses/updates while doing an application review.

All critical applications used in an organization need to be subjected to detailed review by an IS auditor. This is one of the most important aspect of IS audit for a business. The job of application review becomes more complex as the application becomes larger and integrated. While auditing complex applications, it is always good to start with a generic industry-based template of an audit work program and slowly customize the work program to the specific situation as the audit progresses. Such audit programs and templates can be obtained from various resources including ISACA.

2.12 Creation of Risk Control Matrix (RCM)

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 matrix details the risks that have been identified in the Risk Assessment phase. A typical RCM would consist of 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 number
    - Control Implemented – The 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 and evaluate the controls that are in place. This way adequacy of the controls would be evaluated better and thus the IS Auditor would be able to provide better assurance with regards to the controls that are in place and their sufficiency.

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 percent of the population to enable the IS auditor to evaluate audit evidence about some characteristic of the items selected to form or assist in forming a conclusion concerning the population.

ISACA has issued guideline on audit sampling which may be referred and used for sampling. It states that the IS auditor should consider selection techniques that result in a statistically based representative sample for performing compliance or substantive testing. Examples of compliance testing of controls, where sampling could be considered, include user access rights, program change control procedures, procedures for documentation, program documentation, follow-up on exceptions, review of logs and software licenses audits. Examples of substantive tests, where sampling could be considered, include re-performance of a complex calculation (e.g., interest) on a sample of accounts or sample of transactions, 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. Based on the initial assessment, the sample size can be increased or decreased to achieve the objective of assessing the tests of existence and adequacy 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 systems 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. 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 non-IS Auditors. Understanding of data analysis tools and techniques will help auditors to not only perform their existing audits more efficiently and effectively but also facilitate the auditors in knowing how to create and execute new types of IT related audit assignments.

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

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

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

An IS auditor can use data analytics for the following purposes:

- Determination of the operational effectiveness of current control environment
- Determination of the effectiveness of anti-fraud procedures and controls
- Identification of business process improvements and efficiencies in the control environment and errors, if any
- Identification of exceptions or unusual business results
- Identification of frauds
- Identification of areas where poor data quality exists
- Performance of risk assessment at the planning phase of an audit

Data Analytics can be effective for an IS Auditor in both planning and fieldwork phases of the audit. Data analytics can be used to accomplish the following:

- Comparing logical access files with the human resources employee master files for authorised users
- Comparing file library settings with data from change management systems and dates of the file changes that can be matched to date of authorised events
- Reviewing table or system configuration settings
- Reviewing system logs for unauthorised access or unusual activities
- Testing system conversion/ migration.

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 organizational performance. BI can handle enormous amount of structured as well 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.

The underlying attributes of computer based transactional systems make the task of auditing more complex and therefore, the auditors may be required to rely upon use of CAAT tools.

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

- Dispersed and different sources of input and distributed processing.

2.14 Compliance Testing

Compliance testing is the process of evidence gathering for the purpose of testing an organization's compliance with control procedures. Compliance review determines if controls are being applied in accordance with organizational policies. For example, if the IS Auditor is concerned about whether production program library controls are working properly, the IS Auditor might select a sample of programs to determine if the source and object versions are the same. The broad objective of any compliance test is to provide IS Auditors with reasonable assurance that the control on which the IS Auditor plans to rely is operating as perceived in the preliminary evaluation. Compliance Procedures help obtain reasonable assurance that those internal controls on which audit reliance is to be placed are operating effectively.

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

The IS Auditor needs to ensure that internal controls exist, are 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 Auditors can ascertain the existence, effectiveness and continuity of the internal control system. Examples of compliance testing of controls where sampling could be considered include user access rights, program change control procedures, documentation procedures, program documentation, follow up of exceptions, review of logs, software license audits, etc.

Test of controls are audit procedures executed to ascertain the design effectiveness and operating effectiveness of the controls and the attributes. This is evaluation at a process level and not at a transactional level (which is more granular level as transaction is a result of execution of a process). If the IS Auditor conclude a control as ineffective, then the auditor has no option but to exercise substantive audit procedures on the application/process.

2.15 Substantive Testing

In substantive testing, 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 verifies 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 validates the details of financial transactions and balances. In contrast, compliance testing concentrates on validating the internal control procedures in place over those financial transactions. Substantive testing validates the amounts of the transactions themselves. Substantive Testing are performed in every audit and are sometimes known as default procedures. These procedures relate to checking the completeness, accuracy and validity of the data produced by the enterprise. Further, if auditor concludes that a compliance test is ineffective then the auditor has no option but to exercise substantive audit procedures on the application/process.

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 and Operational Effectiveness would be performed by the IS Auditor on every identified control. Testing of Design Effectiveness refers to the working design of the control as documented. It is a blueprint of the control. The IS Auditor evaluates in general that the documented control is effective to mitigate the risk. It can be evaluated by reviewing the policies, procedure documents, brainstorming sessions etc.

A walkthrough of a business process and the risks and 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 whole process, from initiation, through authorization, recording, processing and reporting will assist with the identification or existence of control activities to establish whether control activities are being performed (i.e. are in place), and appraisal of the design of the 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 operations of the process and its associated controls and to evaluate whether the controls, if operated as designed can effectively mitigate risk to an acceptable level. In conducting the walkthrough, it would be ensured that sufficient evidence exists, and that reconciliations are being prepared and reviewed. Where there is such an evidence, it can be concluded that the control is operatively effective and that its design is 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, does not 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 key controls that he intends to rely on for the purpose of audit. The purpose of operational self-testing is to gather sufficient documented evidence to enable a conclusion and testimony whether or not the controls 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 begin either from initiating documents in a process such as purchase order / requisitions, for the Purchasing Process or from the end of the process, i.e. the records in the accounting system. This flow of the test is determined by the assertions that need to be addressed. Once the sample has been selected from the complete population, evidence must be obtained that the control has been performed. For example, for a manual authorization control, the evidence will be the signature of the person who executes that control.

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

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 they 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 auditor 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 that has been implemented performs 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 authorized 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 consider the type of audit evidence to be gathered, its use as audit evidence to meet audit objectives 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 considered 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 organization. This is why confirmation letters are used for verification of accounts receivable balances.
- **Qualifications of the individual providing the information/evidence:** Whether the providers of the information/evidence are inside or outside of the organization, the IS Auditor should always consider the qualifications and functional responsibilities of the persons providing the information. This can also be true of the IS Auditor. If an IS Auditor doesn't have a good understanding of the technical area under review, the information gathered from testing that area may not be reliable, especially if the IS Auditor doesn't fully understand the test.
- **Objectivity of evidence:** Objective 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 (have been prepared or used within the client's organization and are retained without going to an outside party) or EXTERNAL (have been handled by someone outside the client's organization who is a party to the transaction being documented, which are either currently held by the client or readily accessible).

Analytical procedures: Use 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 etc.

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 systems.

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

SA 580 talk details about the written documentation as audit evidences.

2.17.3 Evidence Preservation

The evidence of a computer fraud/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 dump and 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.

2.17.4 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 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 modifications 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-references 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 results of inspection
  - The results 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 professionals 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 modifications.
- 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 that the evidence obtained by him on which he bases his audit opinion is sufficient, reliable, relevant and useful and enables effective achievement of audit objectives. The audit documentation generally includes:

- Basic documents relating to the business, technology and control environment

- Documents relating to laws, regulations and standards applicable
- Preliminary review and how the audit objectives and scope were evaluated and agreed upon.
- Documents relating to Risk analysis
- Audit plan and progress against plan, Audit programs
- Audit procedures as applied to the audit
- Audit findings, observations, inspection reports, management representations, logs, audit trails and other related evidence
- Interpretation of audit evidence
- Audit Report issued
- Auditee observations and response to findings and recommendations.
- Reports by third party experts
- Peer Reviews

The audit working papers:

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

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

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

Test working papers

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

The compliance test files should contain documentation of:

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

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

Organization of audit working papers

Each document must describe the following:

- Objective – why the work was done?
- Work done – what was 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, and
- Referenced with a unique number

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

Audit documentation should include, at a minimum a record of

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

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

The IS Auditor/IS Audit Department should also develop policies regarding custody, retention requirements and release of audit documentation. The documentation format and media are optional, but due diligence and best practices require that work papers are dated, initialled, 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. Audit documentation should support the findings 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 system flowcharts.

IS Auditors being 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 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, ATM switch services, VAPT, wireless technologies, systems integration and digital forensics, or subject matter experts such as specialists in a particular industry or area of specialization such as banking, securities trading, insurance, legal experts etc.

When a part or all IS of audit services are proposed to be outsourced to another audit or external service provider, the following should be considered about 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 competences, 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 expert/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 with 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.

SA 600, 610, 620 may also be referred for covering the reports of other experts.

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

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

Where a compensating control situation occurs when one stronger control supports a weaker one, overlapping controls may exit. 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 controls and thereby minimize the risk. An IS Auditor should always review for compensating controls prior to reporting a control weakness. The IS Auditor may not find each control procedure to be in place but should evaluate the comprehensiveness of controls by considering the strengths and weaknesses of control procedures.

Judging the Materiality of Findings

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

The IS Auditor must use judgment when deciding which findings to present to various levels of management. For example, the IS Auditor may find that the transmittal form for delivering tapes to the offsite storage location is not properly initialled or authorization evidenced by management as required by procedures. If the IS Auditor finds that management otherwise pays attention to this process and that there have been no problems in this area, the IS Auditor may decide that the failure to initial transmittal documents is not material enough to bring to the attention of upper management. The IS Auditor might decide to discuss this only with local operations management. However, there may be other control problems that will cause the IS Auditor to conclude that this is a material error because it may lead to a larger control problem in other areas. The IS Auditor should always judge which findings are material to various levels of management and report them accordingly.

2.21 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 organizational objectives, which may reflect different types of impact such as financial, people, and/or reputation. Similarly, the time horizon used to assess the likelihood of risks should be consistent with the time horizons related to objectives.

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

Organizations 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 prioritization of the risks identified and facilitate dialog to determine how to allocate resources within the organization.

An example of a Risk Rating Model is given below -

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

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

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

2.22 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 is required that IS audit and assurance professionals shall ensure that findings in the audit report are supported by sufficient and appropriate audit evidence.

The exit interview, conducted at the end of the audit, provides 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 auditee's management may request assistance form the IS Auditor in implementing the recommended control enhancements. Here the IS auditor's role is that of a consultant, and, therefore, he should give careful consideration to how assisting the Auditee may adversely affect the IS Auditor's independence.

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

2.22.1 Audit Deliverables & Communicating Audit Results

Main deliverable of audit is the audit report. These are used by the IS Auditors to report findings and recommendations to the management. The contents of audit report will vary by organization. However, the skilled IS Auditor should understand the basic components of an audit report and how the report communicates audit findings to the management.

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

- An introduction to the report, including a statement of audit objectives, limitations to the audit and scope, the period of audit coverage, and a general statement on the nature and extent of audit procedures conducted 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 recipients of the audit report.
- There would be a variety of findings some of which may be quite material while others 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 improved processes 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. In such a case, all recommendations may be implemented at the time of implementing changes.

The IS Auditor should discuss the recommendations and any planned implementation dates while in the process of releasing the audit report. The IS Auditor must realize that various constraints, such as staff limitations, budget or other projects may limit immediate implementation. Management should develop a firm program for corrective actions. It is important to obtain a commitment from the Auditee/management on the date by which the action plan will be implemented and the manner in which it will be performed since the corrective action may result in certain risks being avoided, if identified while discussing and finalizing the audit report. If appropriate, the IS Auditor may want to report to senior management on the progress of implementing recommendations. Sample format of IS Audit finding, audit report and executive summary of audit report are given in Appendix-7.

2.23 Management Implementation of Recommendations

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

2.24 Follow up Review

ISACA standards require that 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. An IS Audit will be effective 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 does 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.

The Institute of Internal Auditors defines a follow-up as: "a process by which the internal 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 issuing reports. IS auditors, to be able to perform IS Audit assignments need to have a good understanding of concepts of auditing, IT and management. This chapter has covered, in detail, 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 objectives 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 risks and their assessment which forms the basis on which the audit conclusions can be made.

- How to use analytical procedures, compliance and substantive testing methods 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 practices of IS audit and the various phases involved covering the planning of audit process, understanding of the risks involved, conducting the audit, obtaining and evaluating evidence and issuing the final audit report containing recommendations.

2.26 Case Study

Case Study Scenario

Client company, AIA Aircrafts Ltd., a Company engaged in the manufacturing of private jets and aviation accessories has implemented a newly conceptualized Firewall System over its legacy ERP Suite. The company has appointed an IS Auditor to audit the effectiveness of the Firewall system along with its interfaces with the ERP System.

The IS Auditor, while carrying out the IS Audit, was verifying a sample of Firewall Operation Logs and found that 2 users were constantly trying to access a particular external source which was denied by the Firewall system as per the security policy of the company. The Auditor immediately issued an audit finding and went to seek explanations from the management.

Moreover, while verifying the Firewall Operations Logs further, he observed that a particular site was not prevented by the Firewall which, ideally should be prevented as per the company's security policy. When, it came to the notice of IT Management, they immediately fixed the Firewall. Yet, the IS Auditor included the same in his IS Audit Report.

As an IS auditor performing the IS audit, respond to the following:

1. What should an IS Auditor do FIRST, when he observed that two users are constantly trying to access some external sources?

   A) Inform the management and expand the sample to get further evidences.

   B) Issue an Audit Finding

   C) Seek Explanations from Management

   D) Ask for clarification from the Firewall Vendor

   Correct Answer is A.

Explanation

A) IS Audit and Assurance Standards suggest that an IS Auditor should gather sufficient and appropriate audit evidence on which his opinion is based. Here the IS Auditor needs to determine whether this is an isolated incident or a systematic failure. It would be a good practice to make management informed about the incident.

B) Directly issuing an Audit Finding, without gathering sufficient and appropriate audit evidence is not the proper practice as per the Standards.

C) Directly seeking explanations from management, without gathering sufficient and appropriate audit evidence is not the proper practice as per the Standards.

D) Directly asking clarifications from Firewall Vendor without investigating the matter further is not the proper practice on the part of IS Auditor. (Note: As per information detailed in question, Vendor is not managing the firewall configuration files. Rushing to Vendor means the auditor is overstepping the premise and is not in line with auditor's responsibilities).

2. An IS Auditor found one security loophole in the System. However, when the IT Management got to know about it, immediately corrected it. The IS Auditor should:

A) Report the same in his Audit Report if the finding is material.

B) Don't include in the Audit Report as the same is corrected.

C) Don't include in the Audit Report but discuss the same in Exit Interview for recommendation.

D) Don't include in the Audit Report and send a letter of appreciation to IT Management.

Correct Answer is A.

Explanation

A) As per the IS Audit and Assurance Standards, any finding, whether subsequently corrected or not should be included in the IS Audit Report if it is material.

B) Not including the finding as it is corrected is not the proper treatment as per IS Audit and Assurance Standards.

C) Not including the finding and discussing the same only at Exit Interview is not the proper treatment as per IS Audit and Assurance Standards.

D) Not including the material audit finding is not the proper treatment as per IS Audit and Assurance Standards. A Letter of appreciation has nothing to do with Auditor's Responsibilities of including material finding in IS Audit Report.

3. IS Auditor rightly found one weakness in the Firewall implementation and he recommended the name of sister concern to address the weakness. The IS Auditor has failed to maintain:

   A) Professional Independence

   B) Professional Competence

   C) Organizational Independence

   D) Personal Competence

   Correct Answer is A.

   Explanation

   A) Professional Independence carries the highest weight in Assurance Services field. If due to any action of the IS Auditor, his capacity to carry out audit independently is hindered then the same amounts to failure to maintain Professional Independence.

   B) Professional Competence is nowhere failed as the diagnosis of the Auditor is correct.

   C) Organizational Independence has no role to play here as in the given question only one matter is involved which is related to only one of the area of organization.

   D) Personal Competence has no role to play here.

2.27 Questions

1. Which of the following forms of evidence would be considered to be the most reliable when assisting an IS Auditor develop audit conclusion?

   A. A confirmation letter received from a third party for the verification of an account balance.

   B. Assurance via a control self-assessment received from the management that an application is working as designed.

   C. Trend data obtained from World Wide Web (Internet) sources.

   D. Ratio analysis developed by an IS Auditor from reports supplied by line management

2. During a review of the controls over the process of defining IT service levels, an IS auditor would most likely interview the:

   A. Systems programmer

   B. Legal staff

C. Business Unit Manager

D. Programmer

3. Which of the following procedures would an IS Auditor not perform during pre-audit planning to gain an understanding of the overall environment under review?

A. Tour key organisation activities

B. Interview key members of management to understand business risks

C. Perform compliance tests to determine if regulatory requirements are met.

D. Review prior audit reports.

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 prioritize the IS audits to be conducted.

D. Begin with the prior year's IS audit plan and carry over any IS audits that had not been accomplished.

5. The purpose of compliance tests is to provide reasonable assurance that:

A. Controls are working as prescribed.

B. Documentation is accurate and current.

C. The duties of users and data processing personnel are segregated.

D. Exposures are defined and quantified.

6. IS Auditors being most likely to perform tests of internal controls if, after their evaluation of such controls, they conclude that:

A. A substantive approach to the audit is cost-effective

B. The control environment is poor.

C. Inherent risk is low.

D. Control risks are within the acceptable limits.

7. Which of the following is the least important factor in determining the need for an IS Auditor to be involved in a new system development project?

A. The cost of the system

B. The value of the system to the organization.

C. The potential benefits of the system.

D. The number of lines of code to be written.

8. Each of the following is a general control concern EXCEPT:

A. Organization of the IS Department.

B. Documentation procedures within the IS Department.

C. Balancing of daily control totals.

D. Physical access controls and security measures

9. Which of the following types of audits requires the highest degree of data processing expertise?

A. Systems software audits

B. General controls reviews

C. Microcomputer application audits

D. Mainframe application audits

10. A manufacturing company has implemented a new client/server system enterprise resource planning (ERP) system. Local branches transmit customer orders to a central manufacturing facility. Which of the following controls would BEST ensure that the orders are accurately entered and the corresponding products produced?

A. Verifying production to customer orders

B. Logging all customer orders in the ERP system

C. Using hash totals in the order transmitting process

D. Approving (production supervisor) orders prior to production

2.28 Answers and Explanations

1. Correct answer is: A. The IS Auditor requires documented evidence to be submitted during audit procedures. Control self-assessment though is a good control but it cannot work as an evidence. Trend and ratio analysis can be used to justify some conclusion but cannot be considered as a conclusive evidence whereas a confirmation letter is.

2. Correct answer is: C. Business unit manager is the owner of that business unit and he is the right authority to provide the required information in this context. First point of interview should be with the person related to business not the programmer or legal staff

3. Correct answer is: C. During pre-audit planning there is no question of doing any compliance test. Compliance test starts during the process of audit. All other options are the process of collecting information during pre-audit process

4. Correct answer is: C. 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. Correct answer is: A. The compliance tests determine whether prescribed controls are working as intended. 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. Correct answer is: B. IS auditor will most probably perform the test of internal control when control environment is poor. When inherent risks are low and control risks are within acceptable limit, likelihood of testing internal controls get reduced. Concluding the cost-effectiveness of substantive approach is not the outcome of testing internal controls.

7. Correct answer is: 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. Correct answer is: C. Balancing of daily control totals relates to specific applications and is not considered an overall general control concern. Answer "B" is NOT the correct answer since documentation procedures within the IS Department are an important general control concern. Answer "A" is NOT the correct answer since organization of the IS Department is an important general control concern. Answer "D" is NOT the correct answer since physical access controls and security measures are important general control concerns.

9. Correct answer is: A. The IS Auditor needs specialized type of education in hardware and operating system software. Options at 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.

10. Correct answer is: A. Verification will ensure that production orders match customer orders. Logging can be used to detect inaccuracies, but does not in itself guarantee accurate processing. Hash totals will ensure accurate order transmission, but not accurate processing centrally. Production supervisory approval is a time-consuming

manual process that does not guarantee proper control.

Chapter 3

IS Audit Tools & Techniques

3.1 Learning Objectives

Computer Assisted Audit Tools and Techniques are important tools for collecting and evaluating evidences during the Audit Process. Selection of right tools and characteristics, category and uses of various available tools are discussed in this chapter.

3.2 Computer Assisted Audit Techniques

CAAT is a significant tool for auditors to gather evidences independently. It provides means to gain access and to analyse data for predetermined audit objectives, and report the audit findings with evidences. It helps the auditor to obtain evidence directly on the quality of records produced and maintained in the system. The quality of the evidence collected gives reassurance on the quality of the system processing such transactional evidences.

3.2.1 Needs for CAAT

During the course of the audit, an IS auditor should obtain sufficient, relevant and useful evidence to effectively achieve the audit objectives. The audit findings and conclusions have to be supported by appropriate analysis and interpretation of this evidence. Computerised information processing environments pose challenges to the IS auditor to collect sufficient, relevant and useful evidence, since the evidence exists on magnetic media and it may not be possible to analyze data without the help of some software tool(s). With systems having different hardware and software environments, different data structures, record formats, processing functions etc., it is almost impossible for the auditors to collect evidence and analyse the records without a software tool. Owing to resource constraints it becomes very difficult, if not impossible, to quickly develop audit capabilities, without using audit software like CAATs.

The ICAI Guidance note on CAAT describes CAATs as important tools for the auditor in performing audits. CAATs may be used in performing various auditing procedures including the following:

(a) Tests of details of transactions and balances, for example, the use of audit software for recalculation of interest or the extraction of invoices over a certain value from the computer records.

(b) Analytical procedures, for example, identifying inconsistencies or significant fluctuations.

(c) Tests of general controls, for example testing the setup or configurations of the operating system or access procedures to the program libraries or by using code comparison software to check that the version of the program in use is the version approved by management.

(d) Sampling programs to extract data for audit testing

(e) Tests of application controls, for example, testing the functionality of a programmed control

(f) Re-performing calculations performed by the organisation's accounting system.

Purpose of CAATs

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

Functional Capabilities of CAATs

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

How to use CAATs

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

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

General Uses and Applications of CAATs

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

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

Strategies for using CAATs

CAATs are important tools for Auditors. Auditors 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, which is the best defense against misunderstanding how the system processes data.
8. Review documentation on the system, for example, user manuals, flowcharts, output reports.
9. Develop a plan for analyzing the data (What, When, Where, Why, and How)
    - What: Specific objectives that should be addressed by the analysis
    - When: Define the period that will be audited, and arrange with IT personnel to secure the data for that period
    - Where: Define the sources of the data to be analyzed (Accounts payable, payroll)
    - Why: Reason for performing the tests and analysis (general review, fraud audit, VFM: Value for Money)
    - How: The types of analysis planned to be carried out by the auditor (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)

3.2.2 Types of CAATs

While selecting the CAAT, IS Auditor is faced with certain critical decisions that he / she may be required to make, while balancing on the quality and cost of audit:

a. Use the audit software developed by the client.

b. Design and develop his /her own audit software.

c. Use a standard off the shelf Generalised Audit Software

The first two options require the auditor to be technically competent in programming and its methodology, which may not be his area of expertise. Computer audit software also known as Generalised Audit Programs (GAS) is readily available off-the-shelf with specific features useful for data interrogation and analysis. The auditors do not require much expertise and knowledge to be able to use these for auditing purpose

Different types of CAATs can be categorized as follows:

1. Generalised Audit Software
2. Specialised Audit Software
3. Utility Software

A brief description of the types of software is given below:

3.2.2.1 Generalised Audit Software (GAS)

Computer audit software may be defined as: “The processing of a client’s live files by the auditor’s computer programs”. Computer audit software may be used either in compliance or substantive tests. Generalised Audit software refers to generalized computer programs designed to perform data processing functions such as reading data, selecting and analyzing information, performing calculations, creating data files and reporting in a format specified by the auditor. The use of Generalised Audit Software is perhaps the most widely known computer assisted audit technique.

GAS has standard packages developed by software companies exclusively for auditing data stored on computers. These are economical and extensively used by auditors the world over. Available off the shelf, GAS can be used for a wide range of hardware, operating systems, operating environments and databases.

Typical operations using GAS include:

a. Sampling Items are selected following a value based or random sampling plan.

b. Extraction Items that meet the selection criteria are reported individually.

c. Totalling the total value and number of items meeting selection criteria are reported.

d. Ageing Data is aged by reference to a base date.

e. Calculation Input data is manipulated prior to applying selection criteria,

3.2.2.2 Specialised Audit Software (SAS)

Specialised Audit software, unlike GAS, is written for special audit purposes or targeting specialized IT environments. The objective of these softwares is to achieve special audit procedures which may be specific to the type of business, transaction or IT environment e.g. testing for NPAs, testing for UNIX controls, testing for overnight deals in a Forex Application software etc. Such software may be either developed by the auditee or embedded as part of the client's mission critical application software. Such software may also be developed by the auditor independently. Before using the organisation's specialized audit software, the auditor should take care to get an assurance on the integrity and security of the software developed by the client.

3.2.2.3 Utility Software

Utility software or utilities though not developed or sold specifically for audit are often extremely useful and handy for conducting audits. These utilities usually come as part of office automation software, operating systems, and database management systems or may even come separately. Utilities are useful in performing specific system command sequences and are also useful in performing common data analysis functions such as searching, sorting, appending, joining, analysis etc. Utilities are extensively used in design, development, testing and auditing of application software, operating systems parameters, security software parameters, security testing, debugging etc. Some examples are

a. File comparison: A current version of a file for example, is compared with the previous year's version, or an input file is compared with a processed file.

b. Production of circularisation letters.

3.2.3 Typical Steps in using GAS

i. Define the audit objectives.

ii. Identify the tests that the package can undertake to meet the objectives.

iii. Make out the package input forms for the tests identified.

iv. Compile the package on the computer, clearing reported edit errors.

v. If a programmer has been adding coded routines to the package to fill out the input forms or to advice, the programmer's work must be tested.

vi. Obtain copies of the application files to be tested.

vii. Attend the execution of the package against these copy files.

viii. Maintain security of the copy files and output until the tests have been fully checked out.

ix. Check the test results and draw audit conclusions.

x. Interface the test results with whatever subsequent manual audit work is to be done.

3.2.4 Selecting, implementing and using CAATs

Computer Assisted Audit Techniques (CAATs) are significant tools for auditors to gather evidence independently. CAATs provide a means to gain access and analyse data for a predetermined audit objective and to report audit findings with evidence. They help the auditor to obtain evidence directly on the quality of the records produced and maintained in the system. The quality of the evidence collected confirms the quality of the system processing. Following are some examples of CAATs, which can be used to collect evidence:

- ACL, IDEA, Knime etc.
- Utility Software such as Find, Search, Flowcharting utilities
- Spreadsheets such as Excel
- SQL Commands, OS commands
- Third party access control software
- Embedded routines in Application software systems
- Options and reports built in as part of the application/systems software
- Performance monitoring tools
- Network management tools, OS utilities
- High end CAATs
- RSAREF, DES, PGP
- TCP Wrapper, SOCKS, TIS Toolkit
- COPS, Tripwire, Tiger
- ISS, SATAN, etc.

3.3 Continuous Auditing Approach

Continuous auditing is a process through which an auditor evaluates the particular system(s) and thereby generates audit reports on real time basis. Continuous auditing approach may be required to be used in various environments. Such environments usually involve systems that are 24*7 mission critical.

3.3.1 Techniques for Continuous Auditing

3.3.1.1 Snapshot

Most applications follow a standard procedure whereby, after taking in the user input they process it to generate the corresponding output. The snapshot technique uses a series of sequential data captures referred to as snapshots. These are taken in a logical sequence that a transaction follows. Snapshot, thus, produces an audit trail for review by the auditor. Typically, snapshots are implemented for tracing steps executed by an application software.

Let us consider, for example, a banking transaction. Numerous transactions are performed and processed by various application systems in a banking environment. Snapshot software installed as part of the production environment would continuously record transactions passing a particular control point e.g. instruction set executed in the memory of the ATM machine. Hence the error in code/ instruction can be identified by analyzing the steps recorded by the snapshot software.

Snapshots are typically employed for:

- analysing and tracking down the flow of data in an application program, so as to know the underlying logic of the data processing software.
- documenting the logic, input/output controls (or conditions) of the application program and the sequence of processing.

Snapshots are also deployed for tracking down the reasons for any disruption in the functioning of application or system software like operating system or database system.

3.3.1.2 Integrated Test Facility (ITF)

Integrated Test Facility (ITF) is a system in which a test pack is pushed through the production system affecting "dummy" entities. For example, the auditor would introduce certain test transactions affecting targeting dummy customer accounts and dummy items created earlier for testing purpose. The approach could also involve setting a separate dummy organisation using the application software in the live environment. ITF is useful in identifying errors and problems that occur in the live environment and that cannot be traced in the test environment. However, the disadvantage in using ITF is that the dummy transactions also append to the live database and hence will impact the results and reports drawn from the live database. It will, therefore, be necessary to delete the test transactions from the system once the tests have been performed. As with all test packs, the output produced is compared with predicted results. This helps to determine whether the programmed procedures being tested are operating correctly.

3.3.1.3 System Activity File Interrogation

Most computer operating systems provide the capability of producing a log of every event occurring in the system, both user and computer initiated. This information is usually written to a file and can be printed out periodically. As part of audit testing of general controls, it may be useful for the auditor to review the computer logs generated at various points to build an audit trail. Wherever possible, unauthorised or anomalous activity would need to be identified for further investigation. Where a suitable system activity file is retained on magnetic media, one can select and report exceptional items of possible audit interest such as unauthorised access attempts, unsuccessful login attempts, changes to master records and the like.

3.3.1.4 Embedded Audit Facilities

Embedded audit facilities consist of program audit procedures, which are inserted into the client's application programs and executed simultaneously. The technique helps review transactions as they are processed and select items according to audit criteria specified in the resident code, and automatically write details of these items to an output file for subsequent audit examination.

This technique generally uses one or more specially designed modules embedded in the computer application system to select and record data for subsequent analysis and evaluation. The data collection modules are inserted in the application system or program at points predetermined by the auditor. The auditor also determines the criteria for selection and recording. Automated or manual methods may be used to analyse the data later.

3.3.1.5 Continuous and Intermittent Simulation Audit

With significant advancements in technologies, business systems are increasingly driven by client-server systems with distributed computing and databases. The components of such systems are networked generally over geographically disparate locations. This has resulted in the need for auditing systems that not only enable continuous auditing of transactions but also have a low overhead on the IT resources of the auditee but without compromising on the independence of such systems. When a transaction meets a pre-defined criterion, the audit software runs an audit of the transaction (intermittent test). Then the computer waits for the next transaction that meets the criteria. This provides continuous testing.

3.3.1.6 Systems Control Audit Review File (SCARF)

The use of this technique involves embedding specially written audit software in the organisation's host application systems so that the application systems are monitored on a continuous basis. The technique involves collecting and storing data related to application system errors, policy and procedural variances and application exceptions etc. for further examination.

3.3.1.7 Audit Hook

This technique involves embedding audit modules in application systems to function as red flags as real time notification of suspicious transactions to induce IS security and auditors to act before an error or irregularity gets out of hand.

3.4 Summary

This chapter describes CAATS, types of CAATs, their uses, their functionalities and how and when to select them and the benefits of using CAATs.

3.5 Questions

1. What is one of the key tests which can be ideally carried out using Computer Assisted Audit Tools (CAATs)?

   A. Identification of exceptional transactions based upon set criteria

B. Projections on future trends for specific parameters

C. Carrying out employees' reference checks

D. Carry out employee appraisals Key

2. Find out the best process carried out using Computer Assisted Audit Tools (CAATs)?

A. Identify potential areas of fraud

B. Carry out employee appraisals of Information Systems Assurances Services

C. Projections on future trends for specific parameters

D. Carrying out employees' reference checks Key

3. What can be ideally carried out using Computer Assisted Audit Tools (CAATs)?

A. Identify data which is inconsistent or erroneous

B. Carry out employee appraisals

C. Projections on future trends for specific parameters

D. Carrying out employees' reference checks Key.

4. What is one of the key tests which can be ideally carried out using Computer Assisted Audit Tools (CAATs)?

A. Perform various types of statistical analysis

B. Carry out employee appraisals

C. Projections on future trends for specific parameters

D. Carrying out employees' reference checks Key

5. What is one of the key tests which can be ideally carried out using Computer Assisted Audit Tools (CAATs)?

A. Establishing whether the set controls are working as prescribed

B. Carry out employee appraisals

C. Projections on future trends for specific parameters

D. Estimation of competitor activity Key.

6. What is one of the key tests which can be ideally carried out using Computer Assisted Audit Tools (CAATs)?

A. Establishing relationship between two or more areas & identify duplicate transactions

B. Carry out market surveys for a new product launch

C. Projections on future trends for specific parameters

D. Estimation of competitor activity Key

7. Which is one of the most effective tools and techniques to combat fraud?

A. Computer Assisted Audit Techniques (CAAT)

B. Threats of severe punishment

C. Validation by the I.T. dept. of the police

D. Use of authenticated hard copies Key

8. An IS Auditor, concerned that application controls are not adequate to prevent duplicate payment of invoices, decided to review the data processing files for possible duplicate payments. Which of the following techniques/tools would be useful to the IS Auditor?

A. An integrated test facility.

B. Statistical sampling.

C. Generalized audit software.

D. The Audit Review File.

9. Many automated tools are designed for testing and evaluating computer systems. Which one of the following such tools impact the systems performance with a greater load and stress on the system?

A. Test data generators

B. Statistical software packages

C. Test drivers

D. Network traffic analyzers

10. The most appropriate type of CAAT tool the auditor should use to test security configuration settings for the entire application systems of any organization is:

A. Generalised Audit Software

B. Test Data

C. Utility Software

D. Expert System

3.6 Answers and Explanations

1 One of the many key tests that can be carried out by CAATs is identification of exceptional transactions based upon set criteria. The IS auditor can set the criteria based upon the sort of transactions which are not expected to occur on the basis of the controls which presumably have been incorporated in the organization’s systems. CAATs are more in the nature of audit tools & would not be ideal for the other purposes listed in Options B to D above. Hence, answer at Option A alone is correct.

2 One of the many key tests that can be carried out by CAATs is identification of potential areas of fraud. The IS auditor can set the criteria based upon the sort of transactions which are not expected to occur on the basis of presumably have been incorporated in the organization’s systems. CAATs are more in the nature of audit tools & would not be ideal for the other purposes listed in Options B to D above. Correct answer is A.

3 One of the many key tests that can be carried out by CAATs is identification of data which is inconsistent or erroneous. The IS auditor can set the criteria based upon the sort of data which are not expected to occur on the basis of the controls which presumably have been incorporated in the organization’s systems. CAATs are more in the nature of audit tools & would not be ideal for the other purposes listed in Options B to D above. Hence, answer at Option A alone is correct.

4 One of the many key tests that can be carried out by CAATs is the carrying out of various types of statistical analysis which could throw up areas of inconsistencies, defaults, etc. CAATs are more in the nature of audit tools & would not be ideal for the other purposes listed in Options B to D above. Hence, answer at Option A alone is correct.

5 One of the many key tests that can be carried out by CAATs is establishing whether the set controls are working as intended. CAATs are more in the nature of audit tools & would not be ideal for the other purposes listed in Options B to D above. Hence, answer at Option A alone is correct.

6 One of the many key tests that can be carried out by CAATs is establishing relationship between two or more areas & identify duplicate transactions. CAATs are more in the nature of audit tools & would not be ideal for the other purposes listed in Options B to D above. Hence, answer at Option A alone is correct.

7 CAAT is one of the tools useful for carrying out the detection of suspicious transactions as a pre-emptive or post fraud activity. Hence, answer at Option A is correct.

8 Generalised Audit software is mainly used to find duplicate data. Options A and D are on line application audit tools and statistical sampling may not be able to find duplicates. Correct answer is C.

9 Statistical software packages use all data resources impacting the processing time and response time. Network traffic analyzers also use the system resources but not putting stress on production data. Test data generator is not resource intensive and

test drivers are for specific use without impacting much resources. Correct answer is B.

10 When testing the security of the entire application system including operating system, database and application security, the auditor will most likely use a utility software that assists in reviewing the configuration settings. In contrast, the Auditor may use GAS to perform a substantive testing of data and configuration files of the application. Test data are normally used to check the integrity of the data and expert systems are used to inquire on specific topics. Hence correct answer is C.

Chapter 4

Application Controls Review of Business Applications

4.1 Learning Objectives

To understand the business application controls implemented in an organisation

4.2 Introduction

Business applications are the tools to achieve management goals and objectives. Each organisation selects the software as per its business goals and needs. The selection of appropriate software is an important decision for top management to make as it contributes to success of business.

An application or application system is a software that enables users to perform tasks employing systems' capabilities. These applications are the interface between the user and business functions. For example, a counter clerk at a bank is required to perform various business activities as part of his job and assigned responsibilities. From the point of view of users, it is the application that drives the business logic. Application controls relate to individual business processes including data edits, separation of business functions, balancing, transaction logging, and error reporting. From an organizational perspective, it is important that application controls help to:

- Safeguard assets
- Maintain data integrity
- Achieve organisational goals effectively and efficiently

4.3 Business Application Software: Selection Parameters

Organisations need to document the business requirements and business goals. This helps them to conclude which type and nature of business application(s) to use.

Key parameters of selection of business application software may be:

The business goal: Organisation may have varied business objectives, say for example many organisations are customer driven, few may be driven by social causes, others may emphasise capitalist mind-set.

The nature of business: One of the key determinants of the business application software is the nature of organisation's business. A few businesses may generate daily cash e.g. petrol pumps and departmental stores etc. while some others may require daily update of sales like milk suppliers, newspaper agents etc. while still some others may generate lots of credit sales.

The geographical spread: As globalisation has spread, many Indian companies have been able to reap the benefits by becoming Indian MNCs. Few Indian companies are trying to foray in export markets or increase their global footprint. The more the geographical spread of an organisation, more robust business application software is needed. Robustness here is intended to denote the capability of the business application system to work 24/7 as this may become a critical business need, and it may also denote whether the business application system has capability to handle **multiple currency accounting.**

The volume of transactions: As the transaction volumes increase, it is important for organisation to go for business application softwares that can support business for the next few years.

The regulatory structure at place of operation: As the number and nature of compliances increase across the world, organisation shall prefer that software which is capable to cater to the compliance requirements. A software company selling a product that is **SOX compliant** is likely to find more buyers than others.

4.4 Types of Business Applications

Business applications can be classified based on their processing type (batch, online or real-time) or the source (in-house, brought-in) or based on the functions covered. Following are a few business application types based on functions they perform.

a. **Accounting Applications**:

Applications like TALLY, TATA EX, UDYOG used by business entities for purpose of accounting for day to day transactions, generation of financial information like balance sheet, profit and loss account, cash flow statements, are classified as accounting applications.

b. **Banking Applications:**

Today all public sector banks, private sector banks including regional rural banks have shifted to core banking business applications (referred to as CBS). CBS used by Indian banks include FINACLE (by Infosys Technologies Ltd.), FLEXCUBE (by Oracle Financial Services Software Limited, formerly called i-flex Solutions Limited), TCS BaNCS (by TCS Limited), and many more such solutions.

c. **ERP Applications**:

The need for optimising resource utilization while deriving maximum benefit of the technology deployed has created a separate category of business application systems called ERP (Enterprise Resource Planning). These application solutions are used by entities to manage resources optimally and to maximize E^3 i.e. economy, efficiency and effectiveness of business operations.

d. Payroll Applications:

Many companies across the world are using application softwares that process payrolls for their employees. In India also many CA firms are doing good job on payroll outsourcing. TALLY has a payroll application built into it.

Other Business Applications

i. Office Management Software

ii. Compliance Applications

iii. Customer Relationship Management Software

iv. Management Support Software

v. Logistics Management Software

vi. Legal matter management

vii. Industry Specific Applications

4.5 Key Features and Controls for Business Applications

A business application is selected and implemented for a specific business purpose. The IS Auditor has to assess whether the business objectives from implementing the particular business application will be achieved.

4.6 Application Controls

As per COBIT's management guide: "Application controls are a subset of internal controls that relate to an application system and the information managed by that application. Timely, accurate and reliable information is critical to enable informed decision making. The timeliness, accuracy and reliability of the information are dependent on the underlying application systems that are used to generate, process, store and report the information. Application controls are those controls that achieve the business objectives of timely, accurate and reliable information. They consist of manual and automated activities that ensure that information conforms to certain criteria what COBIT refers to as business requirements for information. Those criteria are effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability.

4.6.1 Internal Controls

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines internal control as: "a process, affected by an organisation's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations

- Reliability of financial reporting
- Compliance with applicable laws and regulations"

COSO defines control activities as the policies and procedures that help ensure management directives are carried out.

4.7 Objectives of Application Controls and key Business Information Requirements

4.7.1 Objectives

Application controls are intended to provide reasonable assurance that management's objectives relative to a given application will be achieved. Management's objectives are typically articulated through the definition of specific functional requirements for the solution, the definition of business rules for information processing and the definition of supporting manual procedures. Examples include:

(i) **Completeness**: The application processes all transactions and the resulting information is complete.

(ii) **Accuracy**: All transactions are processed accurately and as intended and the resulting information is accurate.

(iii) **Validity:** Only valid transactions are processed, and the resulting information is valid.

(iv) **Authorisation:** Only appropriately authorised transactions are processed.

(v) **Segregation of duties:** The application provides for and supports appropriate segregation of duties and responsibilities as defined by management.

4.7.2 Information Criteria

Key business requirements for information also called as information criteria need to be present in information generated. These are:

1. **Effectiveness:** Deals with information being relevant and pertinent to the process as well as being delivered in a timely, correct, consistent and usable manner.
2. **Efficiency:** Concerns the provision of information through the optimal (most productive and economical) use of resources.
3. **Confidentiality:** Concerns the protection of sensitive information from unauthorised disclosure.
4. **Integrity:** Relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
5. **Availability:** Relates to information being available when required by the process now

and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

6. **Compliance:** Deals with complying with the laws, regulations and contractual arrangements to which the process is subject, i.e., externally imposed business criteria as well as internal policies.

7. **Reliability:** Relates to the provision of appropriate information for management to operate the organisation and exercise its fiduciary and governance responsibilities.

The specific key quality requirements may vary for different organisations based on specific business needs.

4.7.3 Application Controls Objectives

COBIT provides best practices for application controls which can be used as a benchmark for implementing or evaluating application controls. The COBIT control objectives and control practices provide the best collection of controls which are generic and can be customised and used as benchmark for implementation or used as assessment criteria for any application audit. COBIT defines six control objectives for application controls:

1. **Source Data Preparation and Authorisation:** Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Errors and omissions can be minimised through good input form design.

2. **Source Data Collection and Entry**: Ensure that data input is performed in a timely manner by authorised and qualified staff. Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, retain original source documents for appropriate amount of time.

3. **Accuracy, Completeness and Authenticity Checks**: Ensure that transactions are accurate, complete and valid. Validate data that were input, and edit or send back for correction as close to the point of origination as possible.

4. **Processing Integrity and Validity:** Maintain the integrity and validity of data throughout the processing cycle. Detection of erroneous transactions does not disrupt the processing of valid transactions.

5. **Output Review, Reconciliation and Error Handling**: Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient and protected during transmission; verification, detection and correction of the accuracy of output occur; and information provided in the output is used.

6. **Transaction Authentication and Integrity**: Before passing transaction data between internal applications and business/operational functions (within or outside the enterprise), check the data for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.

4.7.4 Control Practices

Illustrative control practices for the control objectives as per COBIT 2019 are given below. Under each of the control objectives, there are list of control practices which need to be implemented to meet the control objectives. The control practices are to be customised and implemented as per specific requirements of the organisation. Once the control practices of specific control objective are implemented, then it can be said that the application meets the required control objectives.

4.7.4.1 Source Data Preparation and Authorisation

(i) Design source documents in a way that they increase accuracy with which data can be recorded, control the workflow and facilitate subsequent reference checking. Where appropriate, include completeness controls in the design of the source documents.

(ii) Create and document procedures for preparing source data entry, and ensure that they are effectively and properly communicated to appropriate and qualified personnel. These procedures should establish and communicate required authorisation levels (input, editing, authorising, accepting and rejecting source documents). The procedures should also identify the acceptable source media for each type of transaction.

(iii) Ensure that the function responsible for data entry maintains a list of authorised personnel, including their signatures.

(iv) Ensure that all source documents include standard components, contain proper documentation (e.g., timeliness, predetermined input codes, default values) and are authorised by management.

(v) Automatically assign a unique and sequential identifier (e.g., index, date and time) to every transaction.

(vi) Return documents that are not properly authorised or are incomplete to the submitting originators for corrections, and log the fact that they have been returned. Review logs periodically to verify that corrected documents are returned by originators in a timely fashion, and to enable pattern analysis and root cause review.

4.7.4.2 Source data collection and entry

(i) Define and communicate criteria for timeliness, completeness and accuracy of source documents. Establish mechanisms to ensure that data input is performed in accordance with the timeliness, accuracy and completeness criteria.

(ii) Use only pre-numbered source documents for critical transactions. If proper sequence is a transaction requirement, identify and correct out-of-sequence source documents. If completeness is an application requirement, identify and account for missing source documents.

(iii) Define and communicate who can input, edit, authorise, accept and reject transactions, and override errors. Implement access controls and record supporting evidence to establish accountability in line with role and responsibility definitions.

(iv) Define procedures to correct errors, override errors and handle out-of-balance conditions, as well as to follow up, correct, approve and resubmit source documents and transactions in a timely manner. These procedures should consider things such as error message descriptions, override mechanisms and escalation levels.

(v) Generate error messages in a timely manner as close to the point of origin as possible. The transactions should not be processed unless errors are corrected or appropriately overridden or bypassed. Errors that cannot be corrected immediately should be logged in an automated suspense log, and valid transaction processing should continue. Error logs should be reviewed and acted upon within a specified and reasonable period of time.

(vi) Ensure that errors and out-of-balance reports are reviewed by appropriate personnel, followed up and corrected within a reasonable period of time, and, where necessary, incidents are raised for more senior-level attention. Automated monitoring tools should be used to identify, monitor and manage errors.

(vii) Ensure that source documents are safe-stored (either by the business or by IT) for a sufficient period of time in line with legal, regulatory or business requirements.

4.7.4.3. Accuracy, completeness and authenticity checks

(i) Ensure that transaction data are verified as close to the data entry point as possible and interactively during online sessions. Ensure that transaction data, whether people-generated, system-generated or interfaced inputs, are subject to a variety of controls to check for accuracy, completeness and validity. Wherever possible, do not stop transaction validation after the first error is found. Provide understandable error messages immediately to enable efficient remediation.

(ii) Implement controls to ensure accuracy, completeness, validity and compliance to regulatory requirements of data input. Controls may include sequence, limit, range, validity, reasonableness, table look-ups, existence, key verification, check digit, completeness (e.g., total monetary amount, total items, total documents, hash totals), duplicate and logical relationship checks, and time edits. Validation criteria and parameters should be subject to periodic reviews and confirmation.

(iii) Establish access control and role and responsibility mechanisms so that only authorised persons input, modify and authorise data.

(iv) Define requirements for segregation of duties for entry, modification and authorisation of transaction data as well as for validation rules. Implement automated controls and role and responsibility requirements.

(v) Report transactions failing validation and post them to a suspense file. Report all errors in a timely fashion and do not delay processing of valid transactions.

(vi) Ensure that transactions failing edit and validation routines are subject to appropriate follow-up until errors are remediated. Ensure that information on processing failures is maintained to allow for root cause analysis and help adjust procedures and automated controls.

4.7.4.4 Processing integrity and validity

(i) Establish and implement mechanisms to authorise the initiation of transaction processing and to enforce that only appropriate and authorised applications and tools are used.

(ii) Routinely verify that processing is completely and accurately performed with automated controls, where appropriate. Controls may include checking for sequence and duplication errors, transaction/record counts, referential integrity checks, control and hash totals, range checks and buffer overflow.

(iii) Ensure that transactions failing validation routines are reported and posted to a suspense file. Where a file contains valid and invalid transactions, ensure that the processing of valid transactions is not delayed and all errors are reported in a timely fashion. Ensure that information on processing failures is kept to allow for root cause analysis and help adjust procedures and automated controls, to ensure early detection or prevent errors.

(iv) Ensure that transactions failing validation routines are subject to appropriate follow-up until errors are remediated or the transaction is cancelled.

(v) Ensure that the correct sequence of jobs has been documented and communicated to IT operations. Job output should include sufficient information regarding subsequent jobs to ensure that data are not inappropriately added, changed or lost during processing.

(vi) Verify the unique and sequential identifier to every transaction (e.g., index, date and time).

(vii) Maintain the audit trail of transactions processed. Include date and time of input and user identification for each online or batch transaction. For sensitive data, the listing should contain before and after images and should be checked by the business owner for accuracy and authorisation of changes made.

(viii) Maintain the integrity of data during unexpected interruptions in data processing with system and database utilities. Ensure that controls are in place to confirm data integrity after processing failures or after use of system or database utilities to resolve operational problems. Any changes made should be reported and approved by the business owner before they are processed.

(ix) Ensure that adjustments, overrides and high-value transactions are reviewed promptly in detail for appropriateness by a supervisor who does not perform data entry.

(x) Reconcile file totals. For example, a parallel control file that records transaction counts or monetary value as data should be processed and then compared to master file data once transactions are posted. Identify report and act upon out-of-balance conditions.

4.7.4.5 Output review, reconciliation and error handling

(i) When handling and retaining output from IT applications, follow defined procedures and consider privacy and security requirements. Define, communicate and follow procedures for the distribution of output.

(ii) At appropriate intervals, take a physical inventory of all sensitive output, such as negotiable instruments, and compare it with inventory records. Create procedures with audit trails to account for all exceptions and rejections of sensitive output documents.

(iii) Match control totals in the header and/or trailer records of the output to balance with the control totals produced by the system at data entry to ensure completeness and accuracy of processing. If out-of-balance control totals exist, report them to the appropriate level of management.

(iv) Validate completeness and accuracy of processing before other operations are performed. If electronic output is reused, ensure that validation has occurred prior to subsequent uses.

(v) Define and implement procedures to ensure that the business owners review the final output for reasonableness, accuracy and completeness, and output is handled in line with the applicable confidentiality classification. Report potential errors; log them in an automated, centralised logging facility; and address errors in a timely manner.

(vi) If the application produces sensitive output, define who can receive it, label the output so that it is recognisable by people and machines, and implement distribution accordingly. Where necessary, send it to special access-controlled output devices.

4.7.4.6 Transaction authentication and integrity

(i) Where transactions are exchanged electronically, establish an agreed-upon standard of communication and mechanisms necessary for mutual authentication, including how transactions will be represented, the responsibilities of both parties and how exception conditions will be handled.

(ii) Tag output from transaction processing applications in accordance with industry standards to facilitate counterparty authentication, provide evidence of non-repudiation and allow for content integrity verification upon receipt by the downstream application.

(iii) Analyse input received from other transaction processing applications to determine authenticity of origin and the maintenance of the integrity of content during transmission.

(iv) Authentication means identification, i.e. to prove you are the right person to handle or access resources whereas authorisation refers to the extent to which you can go, for example ID and password is a means for proving your authentication whereas the authorisation power will decide on what you can do after authentication. DBA can add/delete a database user, whereas an auditor is authorised to do view and printing access.

			Information Criteria						
APPLICATION AND CONTROL OBJECTIVES AND INFORMATION CRITERIA			Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Control Objective	1	Source Data Preparation and Authorisation	S	P	S	P		S	
	2	Source Data Collection and Entry	S	S	S	P		S	
	3	Accuracy, Completeness and Authenticity Checks	S	P	S	P	S	P	P
	4	Processing Integrity and Validity			P	P	P	P	P
	5	Output Review, Reconciliation and Error Handling	P	S	P	P	P	P	P
	6	Transaction Authentication and Integrity		S	P	P		P	
P = Primary		S = Secondary							

Table to the relationship between the information criteria and how achievement of those criteria can be enabled by various application control objectives. Primary and secondary are the relative importance of the information criteria.

4.8 Summary

This chapter describes the selection criteria for application systems, various application control objectives and practices.

4.9 Questions

1 Application controls shall include all except

A. Application controls are a subset of internal controls.

B. The purpose is to collect timely, accurate and reliable information.

C. It is part of the IS Auditor's responsibility to implement the same.

D. It is part of business application software.

2 As per Income Tax Act, 1961 and banking norms, all fixed deposit holders of banks need to submit their PAN or form 60/61(a form as per Income Tax Act/Rules). A bank in its account opening form, has not updated the need for form 60/61 in case PAN is not there. This defines which control lapse as per COBIT.

A. Source Data Preparation and Authorisation

B. Source Data Collection and Entry

C. Accuracy, Completeness and Authenticity Checks

D. Processing Integrity and Validity

3 In a public sector bank while updating master data for advances given, the bank employee does not update "INSURANCE DATA". This includes details of Insurance Policy, Amount Insured, Expiry Date of Insurance and other related information. This defines which control lapse as per COBIT.

A. Source Data Preparation and Authorisation

B. Source Data Collection and Entry

C. Accuracy, Completeness and Authenticity Checks

D. Processing Integrity and Validity

4 An IS Auditor observed that users are occasionally granted the authority to change system data. The elevated system access is not consistent with company policy yet is required for smooth functioning of business operations. Which of the following controls would the IS Auditor most likely recommend for long term resolution?

A. Redesign the controls related to data authentication

B. Implement additional segregation of duties controls

C. Review policy to see if a formal exception process is required

D. Implement additional logging controls.

5 An IS Auditor, processes a dummy transaction to check whether the system is allowing cash payments in excess of Rs.20,000/-. This check by auditor represents which of

the following evidence collection technique?

A. Inquiry and confirmation

B. Re-calculation

C. Inspection

D. Re-performance

6 An IS Auditor is performing a post implementation review of an organisation's system and identified output errors within an accounting application. The IS Auditor determined that this was caused by input errors. Which of the following controls should the IS Auditor recommend to management?

A. Recalculations

B. Limit Checks

C. Run-to-run total

D. Reconciliation

7 RBI instructed banks to stop cash retraction in all ATMs across India from April 1, 2013. This was result of few ATM frauds detected. This action by RBI can be best classified as:

A. Creation

B. Rectification

C. Repair

D. None of above

8 A central antivirus system determines whether each personal computer has the latest signature files and installs the latest signature file before allowing a PC to connect to the network. This is an example of a:

A. Directive control

B. Corrective Control

C. Compensating Control

D. Detective Control

9 Company's billing system does not allow billing to those dealers who have not paid advance amount against proforma invoice. This check is best called as:

A. Limit Check

B. Dependency Check

C. Range Check

D. Duplicate Check

10 While posting message on FACEBOOK, if user posts the same message again, FACEBOOK gives a warning. The warning indicates which control.

A. Limit Check

B. Dependency Check

C. Range Check

D. Duplicate Check

4.10 Answers and Explanations

1 C. It represents what auditor verifies but not that what he/she implements. Rest is part of the definition and purpose of application controls.

2 A. is the correct answer as the source data capture is not proper. Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Errors and omissions can be minimised through good input form design.

3 C. This ensures that transactions are accurate, complete and valid. Validate data that were input, and edit or send back for correction as close to the point of origination as possible.

4 C. is the correct answer. Policy is not a static document. When an exception is a regular requirement, the best control is to modify the policy accordingly.

5 D. is the correct answer. The IS Auditor may process test data on application controls to see how it responds.

6 D is correct. For finding the anomaly between input and output, reconciliation is the best option. Re-calculation and run-to-run total will provide the same result as earlier and limit check is a data validation control.

7 B. is the right answer. A, is not an answer as action by RBI is based on fraud detection. Repair is done to rectify an error which has occurred in a working system.

8 B. is the correct answer. After detecting the deficiency, it is correcting the situation hence it is a corrective control.

9 B. Dependency check is one where value of one field is related to that of another.

10 D. is the answer as this is a duplicate check.

Chapter 5

Application Controls Review of Specialised Systems

5.1 Learning objectives

An IS auditor has to be aware of the controls that have been put in place in business applications. He / She may have to review the same as a part of auditor's risk assessment procedure. As per SA200 on ""Overall Objectives of the Independent Auditor and the conduct of an audit in accordance with standards on Auditing", compliance procedures are tests designed to obtain reasonable assurance that those internal controls on which audit reliance is to be placed are in effect. As per ISACA ITAF 1007 "Assertions", IS Audit and assurance professional shall review the assertions against which the subject matter will be assessed to determine that such assertions are capable of being audited and that the assertions are sufficient, valid and relevant.

5.2 Review of Application Controls

5.2.1 Need for Application Control Review

The review is necessary for IS auditor to draw the conclusions for:

(a) How much reliance he/she can put on entities' business application system?

(b) Planning IS audit procedures.

(c) In case application controls are found in-effective to achieve the stated business objectives, then IS Auditor needs to plan for alternate audit procedure.

5.2.2 How to perform Application Control Review

As per ISACA ITAF 1205.1 "Evidences", IS audit and assurance professionals shall obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the engagement results. The procedures used to obtain evidence include:

1. Inquiry and confirmation
2. Re-performance
3. Recalculation
4. Computation
5. Analytical Procedures

6. Inspection
7. Observation
8. Other Generally Accepted Methods

5.3 Review of Business Application Controls through use of Audit Procedures

As per SA 500, “Audit Evidences”, auditor while designing tests of controls shall see whether the controls so put in place are effective.

(a) Inquiry and confirmation: IS Auditor may prepare a checklist to enquire and confirm whether the said controls are in place. This process shall evaluate existence of controls. A sample checklist for IS Auditor is included at end of chapter.

(b) Re-performance: IS Auditor may process test data on application controls to see how it responds. This process shall evaluate the effectiveness of controls.

5.4 Application Controls Review for Specialised Systems

Changes in technology are very fast. A separate section for these systems has been incorporated to help IS Auditor put a focused approach to audit these systems.

5.4.1 Artificial Intelligence (AI)

A computer is an electromechanical machine that contains no live elements. However, it is used for simulating human working in a given situation which involves thinking and reasoning, solving complex problems, doing calculations, etc. Computer history shows that computers are good at making calculations of repetitive nature speedily. In fact, in the beginning, computers were used mainly for this purpose. However, with the advancement in technologies, the concept of Artificial Intelligence (AI) has found wide applications. AI is the theory and development of computer systems so as to be able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages. The applications of AI can be classified into three major categories:

(i) Cognitive Science: This is an area based on research in disciplines such as biology, neurology, psychology, mathematics and allied disciplines. It focuses on how human brain works and how humans think and learn. Applications of AI in the cognitive science area are Expert Systems, Learning Systems, Neural Networks, Intelligent Agents and Fuzzy Logic

(ii) Robotics: This technology refers to robot machines with artificial intelligence and human-like physical capabilities. This includes applications that give robots visual perception, capabilities to feel by touch, dexterity and locomotion.

(iii) Natural Languages: Being able to 'converse' with computers in human languages is the goal of research in this area. Interactive voice response and natural programming languages, closer to human conversation, are some of the applications. Virtual reality is another important application that can be classified under natural interfaces.

IS Auditor's Role

IS auditor has to be conversant with the controls relevant to these systems when used as the integral part of the organizations business processes or critical functions and the level of experience or intelligence used as a basis for developing software. The errors produced by such systems would be more critical as compared to the errors produced by the traditional systems. More details are given in Module 6.

5.4.2 Data Warehouse

Dataware house is defined, "as a Subject-oriented, integrated, non-volatile, collection of data to support management's decision-making process and help in making future policies based on actual historical transactional data. It is a Central Repository of clean, consistent, integrated & summarized information, extracted from multiple operational systems, for on-line query processing."

In other words, a core data warehouse is where all or majority of data of interest to an organisation are captured and organised to assist reporting and analysis. DWs are normally instituted as large relational databases. In some cases, data warehouse holds fully normalised data to support the flexibility to deal with complex and changing business structure.

Data Marts represent subsets of information from the core DW selected and organised to meet the needs of a particular business unit or business line. Data marts may be relational databases or some form of online analytical processing (OLAP) data structure. Data marts have a simplified structure compared to normalised DW.

Data warehousing system is used for getting valuable information for making management decisions and making future policies. Generally, data is processed by TPS (Transaction Processing Systems), also known as operational systems. These systems are responsible for day-to-day functioning of business transactions, whereas Data warehouse is used for helping in decision making process.

Customers depositing and withdrawing money, applying for loans, opening accounts in a bank are examples of Transactions Processing Systems. In contrast, Data warehouse involves integration of related data obtained from various sources like TPS, CRM as well external sources like market trends data etc.

IS Auditor's Role

IS Auditor should consider the following while auditing data warehouse:

1. Credibility of the source data
2. Accuracy of the source data

3. Complexity of the source data structure
4. Accuracy of extraction and transformation process
5. Access control rules
6. Network capacity for speedy access

5.4.3 Decision Support System (DSS)

DSS are information systems that provide interactive information support to middle management through analytical models. DSS are designed to be ad hoc systems for specific decisions by individual-managers. These systems answer queries that are not answered by the transactions processing systems. Typical examples are:

1. Comparative sales figures between two consecutive months for different products with percentage variation to total sales.
2. Revenue and Cost projections on a product mix.
3. Evaluation of different alternatives, leading to the selection of the best one.

IS Auditor's role

As the system shall be used for decision making purposes of the management, the auditor must be concerned with the,

1. Credibility of the source data
2. Accuracy of the source data
3. Accuracy of extraction and transformation process
4. Accuracy and correctness of the output generated
5. Access control rules

5.4.4 Electronic Funds Transfer (EFT)

The electronic mode of payment has made a lot of impact on the way business is conducted. All big, medium and small businesses, banks, users, government departments, logistics providers, customers, service receivers, service providers, exporters, importers, sellers, buyers use EFT for their business and personal transactions. Immense growth of EFT has led to a new set of risks associated with such transactions. Reserve Bank of India (RBI) has issued detailed guidelines for banks to follow for EFT transactions. RBI has specified in its NEFT guidelines that Banks need to create procedural guidelines, for the purpose of:

(i) Verifying that a payment instruction, a communication authorising a payment instruction or an NEFT Data File is authorised by the person from whom it purports to be authorised; and

(ii) For detecting errors in the transmission or the content of a payment instruction, a communication or an NEFT message.

IS Auditor's role

The major concern shall be:

1. Authorisation of payments.
2. Validation of receivers' details, for correctness and completeness.
3. Verifying the payments made.
4. Getting acknowledgement from the receiver, or alternatively from bank about the payment made.
5. Checking whether the obligation against which the payment was made has been fulfilled if not whether there are adequate procedures to account for and handle such transactions.

5.4.5 E-commerce

Other than buying and selling goods on the Internet, E Commerce (Electronic Commerce) involves information sharing, payment, fulfilment of contractual obligations of the parties participating in e-commerce transactions, service and support.

Risks of E-commerce

- the identity and nature of relationships with e-commerce trading partners;
- the integrity of transactions;
- electronic processing of transactions;
- systems' reliability;
- privacy issues;
- return of goods and product warranties;
- taxation and regulatory issues.

IS Auditor's role

IS Auditor's responsibility shall be to assess whether the transactions have:

1. Authorisation
2. Authentication
3. Confirmation
4. Whether the payment gateway is secured or not.

5.4.6 Point of Sale System (PoS)

As the name indicates, a PoS is intended to capture data at the time and place of transaction which is being initiated by a business user. It is often attached to scanners to read bar codes and magnetic cards for credit card payment and electronic sales. They provide significant cost and time saving as compared to the manual methods. They also eliminate errors that are inherent in manual systems (when the data is subjected to transcription errors while a user enters data from a document into the system). POS processing may involve batch processing or online processing. These are generally used in big shopping malls or departmental stores.

IS Auditor's role

1. In case there is batch processing, the IS auditor should evaluate the batch controls implemented by the organization.
2. Check if they are in operation,
3. Review exceptional transaction logs.
4. Whether the internal control system is effective to ensure the accuracy and completeness of the transaction batch before updating.
5. The IS auditor will have to evaluate the controls for accuracy and completeness of on-line transactions.
6. RBI guidelines regarding "Cash withdrawal at Point of Sale (POS) - Prepaid Payment Instruments issued by banks: need to be validated in case such transactions are taking place.

5.4.7 Automatic Teller Machines (ATM)

An ATM (Automated Teller Machine) is a specialized form of the point of sales terminal. It is designed for unattended use by a customer of a financial institution. ATMs generally allow cash deposits, cash withdrawals and a range of banking operations like accepting requests for cheque books or account statements. The facility of ATM can be within a bank, across local banks and amongst the banks outside a region. ATMs transfer information and money over communication lines. These systems provide a high level of logical and physical security for both the customer and the ATM machine.

IS Auditor's Role

The following are the guidelines for internal controls of ATM system which the auditor shall have to evaluate and report:

(a) Only authorized individuals have been granted access to the system.

(b) The exception reports show all attempts to exceed the limits and reports are reviewed by the management.

(c) The bank has ATM liability coverage for onsite and offsite machines.

(d) Controls on proper storage of unused ATM cards, Controls on their issue only against valid application form from a customer, Control over custody of unissued ATM cards, Return of old/ unclaimed ATM cards, Control over activation of PINs

(e) Controls on unused PINs, Procedure for issue of PINs, Return of PINs of returned ATM cards.

(f) Controls to ensure that PINs do not appear in printed form with the customer's account number.

(g) Access control over retrieval or display of PINs via terminals

(h) Process of mailing cards to customers. Whether cards are sent in envelops with a return address that do not identify the Bank. Whether cards and PINs are mailed separately with sufficient period of time (usually three days) between mailings.

(i) Procedures of handling retracted/rejected transactions.

Presently, there are more than 2,50,000 ATM machine installations in India. Government of India has already indicated that it wants to further enhance the usage of ATM in India, as this allows banks to reach remote corners without being physically present. This creates a scope for the IS Auditor for a separate ATM Audit. RBI has issued detailed set of instructions for banks to follow.

Most of the banks manage their ATM Switch ecosystem through shared services of third-party ATM Switch Application Service Providers (ASPs) for shared services for ATM Switch applications. Since these service providers also have exposure to the payment system landscape and are, therefore, exposed to the associated cyber threats, the RBI has directed that certain baseline cyber security controls shall be mandated by the banks in their contractual agreements with these service providers. These pertain to implementation of measures to strengthen the process of deployment and changes in application softwares in the ecosystem; continuous surveillance; implementation of controls on storage, processing and transmission of sensitive data; building capacity for forensic examination; and making the incident response mechanism more robust. The IS auditors undertaking audit of ATM Switch Services may refer to these guidelines for providing assurance services.

5.5 Summary

This chapter covered various specialized systems and their related audit processes.

5.6 Questions

1 Which of the following business purposes can be met by implementing Data warehouse in an organisation?

A. Business continuity can be ensured in case of disaster.

B. Data in the data ware house can work as a backup

C. The data in the warehouse can be used for meeting regulatory requirements.

D. Business decisions can be taken and future policies can be framed based on actual transactional data.

2 Which of the following is a characteristic of a decision support system (DSS)?

A. DSS is aimed at solving highly structured problem.

B. DSS combines the use of models with non-traditional data access and retrieval functions.

C. DSS emphasizes flexibility in decision making approach of users.

D. DSS supports only structured decision-making tasks.

3 Which of the following audit tools is MOST useful to an IS auditor when an audit trail is required?

A. Integrated test facility (ITF)

B. Continuous and intermittent simulation (CIS)

C. Audit hooks

D. Snapshots

4 A retail company recently installed data warehousing client software in multiple, geographically diverse sites. Due to time zone differences between the sites, updates to the warehouse are not synchronized. This will affect which of the following most?

A. Data availability

B. Data completeness

C. Data redundancy

D. Data accuracy

5 The cashier of a company has rights to create bank master in TALLY. This error is a reflection of poor definition for which type of control:

A. User Controls

B. Application Control

C. Input Control

D. Output Control

6 An employee has left the company. The first thing to do is to:

A. Hire a replacement employee.

B. Disable his/her access rights.

C. Ask the employee to clear all dues/advances.

D. Escort employee out of company premises

7 As part of auditing Information Security of a multinational bank, an auditor wants to assess the security of information in ATM facilities. Under which privacy policy should he look for details pertaining to security guards and CCTV surveillance of ATM's?

A. Physical Access and Security Policy

B. Acceptable use of Information Assets Policy

C. Asset Management Policy

D. Business Continuity Management Policy Key.

8 Neural Networks and Fuzzy Logics are classified under which category of Artificial intelligence?

A. Cognitive Science

B. Robotics

C. Natural Sciences

D. Virtual Reality

9 In an inter school competition on Artificial Intelligence, four children develop software which performs the following different functions respectively. Which of them is a correct example of the use of basic Artificial Intelligence?

A. Predictive & self-learning word-processing software

B. A calculation software which arrives at the arithmetic total of figures keyed in

C. A password system which allows access based upon keying in of the correct password

D. A software which rejects invalid dates like 32nd March 2019.

10 Which are the business activities which are strong contenders for conversion to e-commerce?

A. Those that are paper-based, time consuming & inconvenient for customers

B. Those relating to software development

C. Those relating to the 'electronic' aspects of commerce

D. Those that are not paper-based, speedy & convenient for customers.

5.7 Answers and Explanations

1 Correct answer is D. Purpose of Data warehouse is to take business decisions and frame future policies based on the analysis of transactional data. It cannot act as an alternative to backup. Purpose of the data ware house is not for business continuity nor is it for regulatory requirements.

2 Correct answer is B. It goes with the purpose and definition of decision support system.

3 Correct answer is D. Snapshot is the right answer as in this technique, IS auditor can create evidence through IMAGE capturing. A snapshot tool is most useful when an audit trail is required. ITF can be used to incorporate test transactions into a normal production run of a system. CIS is useful when transactions meeting certain criteria need to be examined. Audit hooks are useful when only select transactions or processes need to be examined.

4 Correct answer is B. One of the major bottlenecks in data ware house is time synchronisation as the data of different time zones is merged in data ware house. It ultimately results in in-complete data for decision making purposes.

5 Correct answer is A. User controls are not properly defined. User controls need to be defined based on NEED TO DO and NEED TO DO basis. The above is reflection of a greater problem of improper assessment of user profiles created in the system.

6 Correct answer is B. the first thing to do as soon as an employee leaves the company is to disable his/her access rights in system. This needs to be done to prevent frauds being committed. Other answers may be valid but are not the first thing to do.

7 Correct answer is A. Physical security describes security measures that are designed to restrict unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks). Physical security involves the use of multiple layers of interdependent systems which include CCTV surveillance, security guards, Biometric access, RFID cards, access cards protective barriers, locks, access control protocols, and many other techniques. B is incorrect - An acceptable use policy (AUP), also known as an Acceptable Usage policy or Fair Use policy, is a set of rules applied by the owner or manager of a network, website or large computer system that restrict the ways in which the network, website or system may be used. C is incorrect – This policy defines the requirements for Information Asset’s protection. It includes assets like servers, desktops, handhelds, software, network devices etc. Besides, it covers all assets used by an organization- owned or leased. D is incorrect – This policy defines the requirements to ensure continuity of business-critical operations. It is designed to minimize the impact of an unforeseen event (or disaster) and to facilitate return of business to normal levels.

8 Correct answer is A. Cognitive Science. This is an area based on research in disciplines such as biology, neurology, psychology, mathematics and allied disciplines. It focuses on how human brain works and how humans think and learn. Applications of AI in the cognitive science are Expert Systems, Learning Systems, Neural Networks, Intelligent Agents and Fuzzy Logic. B, C and D are incorrect. B. Robotics: This technology produces robot machines with computer intelligence and human-like physical capabilities. This area includes applications that give robots visual perception, capabilities to feel by touch, dexterity and locomotion. C. Natural Languages: Being able to 'converse' with computers in human languages is the goal of research in this area. Interactive voice response and natural programming languages, closer to human conversation, are some of the applications. D. Virtual reality is another important application that can be classified under natural interfaces.

9 Correct answer is A. The word-processing software pops up suggested words based upon the first few words keyed in by the user. Also, when the user keys in a new word which is not available in its repertoire, it adds it to its collection & reflects it as an option the next time similar letters are initiated. In effect, the software is able to observe & record patterns and improves through ‘learning’. The other answers in Options B to D involve the basic computing functions of a computer which are based on a ‘go / no-go’ logic which does not involve pattern recognition or further learning. Hence, the correct answer is only as in Option A which displays characteristics of artificial intelligence.

10 Correct answer is A. Maximum mileage can be gained from e-commerce by converting those business activities which are paper-based, time consuming & inconvenient for customers as indicated in Option A. This will help us reduce paperwork, accelerate delivery & make it convenient for customers to operate from the comfort of their homes as also at any other place of their convenience. Hence, the other options are wrong.

Chapter 6

IT Enabled Assurance Services

6.1 Learning Objectives

This chapter provides an overview of different types of audit engagements that can be undertaken by the IS auditors. 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. A brief overview is provided so that interested ISAs can venture into these new areas.

6.2 Introduction

As information systems presence has become an indispensable part of our day to day living and as enterprise processes have become inseparable from IT, it is becoming increasingly critical to ensure safe and secure access to information from a computing environment and make it available to authorized persons & processes anyone at any point of time. This heavy reliance on information from information systems has become the very edifice of enterprises today. Information has to be available with necessary security safeguards as the information misused can lead to loss of revenue, reputation and non-compliance with regulations thereby impacting the very survival of enterprises. There are new types of tech-savvy computer fraudsters who by using their technical expertise can exploit information for committing frauds. Hence, ensuring security of any IS environment is of utmost importance within the organization as the loss of it can not only lead to huge financial losses but the enterprise can become liable for damages for loss of private data of customers as also 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 geometric progression growth. Enterprise managements look for assurance on security and value addition due to the use of 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.

6.3 Classification of Audits

An information technology audit, or information systems audit, is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals and objectives.

These reviews may be performed in conjunction with a financial statement audit, internal audit, or other forms of attestation engagements. IT audits are also called IS audits and Computer audits or IT/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 are as follows:

- **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 activities.
- **Information Processing Facilities**: An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.
- **Systems Development**: An audit to verify that the systems under development meet the objectives of the organization and to ensure that the systems are developed in accordance with generally accepted standards for systems development.
- **Management of IT and Enterprise Architecture**: An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.
- **Client/Server, Telecommunications, Intranets, and Extranets**: An audit to verify that telecommunication controls are in place on the client (computer receiving services), server, and on the networks 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. HIPPA is a US legislation that provides data privacy and security provisions for safeguarding medical information.
- **Operational Audit:** An operational audit is designed to evaluate the internal control structure in a given process or area. Audits of application in operation 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, IS Auditors are now placing more emphasis on risk and control-based audit approach. This kind of audit relates to financial information integrity and reliability.
- **Integrated Audits:** An integrated audit combines financial and operational audit steps. An integrated audit is also performed to assess the overall objectives within an organization, related to financial information and assets' safeguarding, efficiency and

compliance.

- Administrative Audits: These are oriented to assess issues related to the efficiency of operational productivity within an organization.
- IS Audits: This process collects and evaluates evidence to determine whether the information systems and related resources adequately safeguard assets, maintain data and system integrity and availability, provide relevant and reliable information, achieve organizational goals effectively, consume resources efficiently, and have, in effect, internal controls that provide reasonable assurance that business, operational and control objectives will be met and that undesired events will be prevented or detected and corrected, in a timely manner.
- Specialized Audit: Within the category of IS audits, there are a number of specialized reviews that examine areas such as services 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 audit specialized in discovering, disclosing and following up on frauds and crimes. The primary purpose of such a review is the development of evidence for review by law enforcement and judicial authorities.
- Control Self-Assessment: 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 the required controls and assist them in doing self-assessment. Therefore, setting the evaluation criteria and executing the evaluation are carried out by the business owners themselves. It is clear that proper guidance and follow-up are required to optimize the added value of this type of engagement within the enterprise. Especially with regard to approach, tools and reporting, the auditors should clearly lead the way and verify whether assessors are using the existing guidelines.
- Internal Audit/Compliance Reviews: Performed by a third party who is not involved in the functioning of the enabler, but who is employed by the same enterprise as the business owners of the enablers. Commonly, in a (medium- to large-sized) enterprise, the evaluation criteria are set and the review is performed by the internal audit or compliance department. This type of review is more independent than a self-assessment because the auditor is not involved in the functioning of the enabler and therefore contributes to the reliability/credibility of the evaluation outcome. Good practices and consistent guidance are required to optimize the added value of this type of engagement.

6.4 IT Enabled Services

There is a wide variety of services that can be offered by the IS Auditors in every area of IT implementation depending on their areas of technical expertise. IS Auditors can provide assurance or consulting services at various stages of technology deployment right from conception to post-implementation. Below is an illustrative sample problem statement with proposed solutions and listing of service opportunities for IS Auditors.

Problem: There are inadequate IT management practices in the enterprise.

Solution	Opportunity for an IS Auditor
Policies should be drafted and enforced around the environment	• Create appropriate policies that meet the business objectives. • Review IT Policies – part of consulting assignment
Procedures should arise from the policies	• Assist in development of the procedures that employees should follow. Review procedures and provide recommendations for improvements.
Appropriate application software should be selected and implemented	• Assist in application selection and implementation. • Participate as a Project Management Office (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	• Design, develop necessary workflows that are to be enforced through the application software/information systems. • Perform a BPR (Business Process Re-engineering) on information system requirements and provide recommendations.
Perform risk assessment and rank the risks	• Perform risk assessment exercise on the existing workflows and processes and identify those areas of high risk that need a higher level of attention. This is part of activities that managements need perform.
Ensure appropriate segregation of duties by ensuring right access is given to the right employees	• Provide advice in designing the roles and responsibilities of the employees. • Review existing roles and responsibilities and identify conflicts in segregation of duties.
Training is to be provided	• Provide necessary training to the employees regarding the new workflows, procedures, applications etc.

6.5 Fraud

Fraud is the wrongful or criminal deception intended for personal financial or other gains. Fraud is a deception deliberately practiced in order to secure unfair or unlawful gain. Defrauding people or organizations of money or valuables is the usual purpose of fraud. It may sometimes involves obtaining benefits without actually depriving anyone of money or valuables. For example, obtaining a driver's license by way of false statements. The establishment of a strong internal control environment is necessary to deter against fraud perpetration. For internal controls to be effective, they must be constantly evaluated for effectiveness and changed as business processes change.

6.5.1 Fraud Detection

Information technology has immensely benefited enterprises in terms of increased quality of information delivery. However, widespread use of information technology and Internet has led to enhanced risks resulting into perpetration of errors and frauds. Fraud is any act meant to deceive and to obtain illegal, and undue advantage. Detecting frauds in IT environment poses its own challenges since the data is in digital format and a fraudster can easily erase his tracks.

Management is primarily responsible for establishing, implementing and maintaining a framework and design of IT controls to meet internal control objectives. A well-designed internal control system provides a good deterrence against frauds and also an opportunity for their timely detection. However, internal controls may fail where these are circumvented by exploiting vulnerabilities or through management facilitated weaknesses in controls or collusions. Legislations and regulations cast significant responsibilities on management, IS Auditors and the audit committee regarding detection and disclosure of any fraud, whether material or not. Understanding the auditee´s business and the risks the organization faces is a critical step for developing an effective audit plan focussing on most sensitive areas. IS Auditors should observe and exercise due professional care in all aspects of their work. Entrusted with assurance functions, IS Auditors should ensure reasonable care while performing their work and be alert to the potential fraud opportunities.

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. During the course of assurance assignments, the IS Auditors may come across instances or fraud indications. The IS Auditor may, after careful evaluations, communicate the need for a detailed investigation to appropriate authorities within the organization. In the case of major fraud indications or if the risk associated with the detection is high the IS Auditor should consider communicating to the audit committee in a timely manner.

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 their 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. **LODR of SEBI:** 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 has also released the National Cyber Security Policy. This policy aims at protecting information and information infrastructure in cyberspace and building capabilities to prevent and respond to cyber threats. It aims to reduce vulnerabilities and minimize damage from cyber incidents through a combination of factors such as institutional structures, people, processes and technology.

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 do not occur randomly, but result from opportunities available. Thus the goal should be to eliminate the root causes that result in frauds 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 is dependent on the circumstances in which it was obtained. Audit evidence is more reliable when it is obtained from independent sources outside of the entity being audited. Further, evidence obtained directly by the IS Auditor is more reliable than obtained indirectly. The IS Auditor should focus more on obtaining external evidences than internally.

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 should obtain formal representations from the management as and when required. However, it should also be noted that written representations do 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.

6.5.2 Cyber Fraud Investigation

Cyber frauds are perpetrated using information technology systems rather than traditional methods of paper and pen. Cyber fraud investigation procedures are similar to a usual fraud investigation, such as

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

Fraud risk assessment is the tool that helps identifying potential fraud risk areas and also assessing effectiveness of internal controls. IS Auditors need to confirm that regular risk management processes are in place, and that commensurate controls have been implemented to mitigate the risks identified.

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

A Sample Cyber fraud risk assessment list is given below:

Cyber Fraud	Likelihood	Impact	Internal Controls
Theft – Unauthorised access to computer Hardware. (e.g. Data centres, Server rooms, network devices etc.)	Low	High	1. Key Cards 2. Security Guards 3. Visitor Logs 4. Circuit Cameras 5. Back up & Recovery Plans 6. Physical access controls

			through biometrics `etc.
Identity theft – 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 ex-employee access
Information theft - 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
Copyright Infringement – Unauthorised access to Software and Databases. (e.g. Software piracy, Peer-to-peer file sharing, etc.)	Medium	High	1. Block peer-to-peer sharing 2. Internet Surveillance 3. Software Licensing 4. Information Sharing Policy 5. Protection of Software code

A holistic approach to *fraud deterrence and prevention* would be strengthening the governance and management framework. IS Auditor could assist in evaluating control framework and assessing the adequacy thereof and related policies. Sample questions for such assessments and reviews for each of seven components adapted from COBIT 2019 are given below:

1. **Policies and Procedures:** Whether the organisation has a documented and approved Cyber Fraud Governance and Management Program.

2. **Processes:** Does the organization have approved security policy and direction that senior management conduct cyber fraud risk assessment regularly and evaluate whether remedial measures are implemented to address cyber fraud risks.

3. **Organisation Structures:** Whether the organisation has clearly defined roles and responsibilities in relation to cyber fraud management which meets both regulatory and stakeholder requirements.

4. **Culture, Ethics and Behaviour:** Does management conduct periodic employee awareness programs and training in relation to corporate governance, compliance and cyber fraud.

5. **Information Flows and Items:** 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.

6.5.3 Cyber Forensics: Digital Forensics

By definition, computer forensics is the "process of identifying, preserving, analysing 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 helps 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 manual 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 evidence 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 etc.)
- Providing assurance that the analysis is based on copies that are identical to the original evidence (could be documentation, checksums, timestamps etc.)

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

Some terms related with evidence are given below:

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.

6.5.4 Fraud investigation Tools and Techniques

Data analysis technologies using Computer Assisted Audit Techniques (CAAT) are the most effective tools and techniques to detect 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 analysis variances.
4. Outliers: to identify 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.

6.6 Some Case Studies of Frauds and Lessons

Case Study 1: Cosmos Bank Fraud

Pune based Cosmos Bank became a victim of cyber-attack in August 2018 that caused the bank over Rs 90 crore loss. The fraud began with a malware attack. Malware is a malicious software that is normally sent as a link to the intended target. Once clicked, it can install executable codes and scripts. It is normally avoided by using anti-malware and antivirus software, and firewalls. In this case, the malware compromised a digital system responsible for settling cash dispensation requests raised at ATMs. As soon as one swipes a card, a request is transferred to the core banking system (CBS) of the bank. If the account has enough money, the CBS will allow the transaction. It is suspected that the fraudsters used cloned debit cards of bank's customers. In this case, the malware created a proxy system that bypassed the CBS and approved a series of 14,800 fraudulent transactions to withdraw Rs 80.5 crore - Rs 78 crore through 12,000 transactions in 28 countries, the rest in India. Another Rs 13.5 crore was transferred to a Hong Kong-based entity using SWIFT (Society for Worldwide Interbank Telecommunications).

One of the control measures against malware is to have upgraded and tested operating system. RBI, the banking regulator had pointed out that as in August 2018, many ATMs were still running on Windows XP and other unsupported software. RBI had directed all the banks to upgrade their software by June 2019.

As per industry experts, continuous monitoring and surveillance and deployment of Incidence Response Teams is required to prevent such attacks.

Case Study 2: The WorldCom fraud

WorldCom fraud was one of the biggest crime cases in USA. WorldCom was one of the biggest telecom companies in USA. It had cooked books to hide falling profitability, and inflated net income and cash flow by recording expenses as investments. This is a popular example of using technology for fraud detection. The Internal Auditors had found around $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 population 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. This was one of the crimes that led to the Sarbanes-Oxley Act in July 2002, which strengthened disclosure requirements and the penalties for fraudulent accounting.

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 3: The $54 million fraud

This is a typical example of how lack of segregation of duties could lead to a phenomenal fraud.

Rita Crundwell, the controller and treasurer of Dixon, 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 Sewer Capital Development Account). 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. Auditors must ensure the existence of internal controls with systems designed to prevent or deter these types of frauds. Also, regular fraud risk assessments should be conducted to Identify areas of risk where theft or manipulation are likely to occur.

Case Study 4: 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, the then Chairman of the company, did. They must also be conscious of the fact that anything can be faked in this modern technology driven world and that they need to continuously update their skills and knowledge in order to keep up with the new challenges.

Case Study 5: Bangladesh Central Bank Fraud

Bangladesh Central Bank was defrauded in February 2016, when thirty-five fraudulent instructions were issued by security hackers via the SWIFT network to illegally transfer close to US $1 billion from the Federal Reserve Bank of New York account belonging to Bangladesh Bank. The heist was linked to a customized malware attack that compromised SWIFT software used to transfer funds. SWIFT is a Belgium-based cooperative of 3,000 organizations that maintains a messaging platform used by banks to transfer money across borders, often in real time. It was the bank's systems or controls that were compromised, not the SWIFT software. Five of the thirty-five fraudulent instructions were successful in transferring $101 million, with $20 million traced to Sri Lanka and $81 million to the Philippines. The Federal Reserve Bank of New York blocked the remaining thirty transactions, amounting to $850 million, due to suspicions raised by a misspelled instruction. All the money transferred to Sri Lanka has since been recovered

The attack was waged against Bangladesh Bank, the nation's central bank. It was the account of the bank with SWIFT, rather than that of the bank's customers, that was taken over. They used these credentials to authorise about three dozen requests to the Federal Reserve Bank of New York to transfer funds from the account of Bangladesh Bank. While hackers can successfully access many systems without insider assistance, in this case, almost certainly insider knowledge of how the system operates was used to overcome the fraud detection controls. This knowledge could easily have come from a current employee at SWIFT or Bangladesh Bank.

The malware used to compromise a computer used for SWIFT transactions was designed to hide traces of fraudulent payments from the bank's local database collections. What's more, once money is transferred via SWIFT, it's typically not reversible. Multiple banks and transfers may be involved in completing a transaction, all taking place within seconds. And because multiple banks and accounts are involved, by default, the transfers are not reversible when disputed. The malware was able to be installed on the SWIFT software computer because the attacker was in Bangladesh Bank's network with access - presumably with enough access to override any locally installed security software. The perpetrators managed to compromise Bangladesh Bank's computer network, observe how transfers are done, and gain access to the bank's credentials for payment transfers. Later the Governor of Bangladesh Bank stated that he had foreseen cyber security vulnerabilities one year ago and had hired an American cyber security firm to bolster the firewall, network and overall cyber security of the bank. However, the bureaucratic hurdles prevented the security firm from starting its operations in Bangladesh until after the cyber heist

The key defense against such attack scenarios remains for users to implement appropriate security measures in their local environments to safeguard their systems - in particular those used to access SWIFT - against such potential security threats. Such protections should be implemented by users to prevent the injection of malware into, or any misappropriation of, their interfaces and other core systems. As per experts, the banks should be using the very same controls over their own systems that they expect of their own customers. Further, SWIFT transactions should be conducted only on computers that are isolated from other devices on banks’ networks. It should be a dedicated computer for its single task.

6.7 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. Managements must ensure they implement adequate and appropriate internal controls. IS Auditors can assist organisations in not only investigating and detecting fraud but also play a proactive role in helping them maintain effective fraud management program that would include fraud deterrence, prevention and detection, investigation and prompt response.

6.8 Summary

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

6.9 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 As a measure of IT General controls, an organization decides to separate those who can input data from those that can reconcile or approve data. Is this a good move? Why?

A. Yes, it is a good move; it can help prevent unauthorised data entry.

B. No, it is not a good move; the person who inputs the data is the best person to approve the data too.

C. Yes, it is a good move; inputting data & reconciling data requires different skills.

D. No, it is not a good move; data entry errors would be compounded.

9 A holistic approach to deterrence & prevention of fraud would be:

A. Strengthening of Governance and Management framework

B. Focussing on integrity of new recruits

C. Establishing severe punishment for fraud

D. Compensating employees adequately to minimize temptation

10 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.

6.10 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 and value of transactions give an indication of the maximum potential loss through fraud. Answer D is incorrect since gross risk less existing controls give net risk.

3 B. The password control weaknesses mean 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 controls 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 database 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 A. Segregation of duties is an important control tool whereby, conflicting roles in particular, are segregated and handled by different individuals. It reduces the risk of fraud since one person cannot independently commit any fraud but would need to collude with the second. Also, since the output of one individual may become the input for another, an independent accuracy check of one person's work by another person becomes a built-in reality. Hence, the answer in Option A is correct.

9 A. A holistic approach to deterrence and prevention of fraud would require strengthening of governance and management framework. The answers in options B to D address the issue in bits and pieces and, hence, are not the right answers. Answer at Option A alone is correct.

10 A. An IS auditor's responsibility for detecting fraud includes evaluating fraud indicators and deciding whether any additional action is necessary or whether an additional 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.

References

www.icai.org

www.isaca.org

www.csoonline.com

www.businessdictionary.com

www.sans.org

CISA Review Manual

Information Systems Control and Audit by Ron Weber

NIST Guidelines

ITAF 3rd edition

ISO/IEC 27001 standards

Appendix 1

RFP from Bank for IS Audit of Application Software

Background: This is a private sector bank with branches all over India. It is using a number of applications – both developed In-house and Outsourced for its business operations. It wishes to have these application solutions audited as per the scope of audit given below.

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 Efficiency & 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 in relation to the application package

Inter-alia, the scope shall include the following:

1. Whether the design of the software conforms to the Requirements Specifications.
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 financial transactions?
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.
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. Today the Max Infotech Group is a significant player in the Indian software industry with a gross sales turnover of Rs 10.20 Billion in 2018-19. The Max Infotech Group offers a range of IT enabled services. The services of the Group are divided into the specific business units covering specific business interests. Max Infotech has over 5000 employees located in 10 ITPs and 20 marketing offices in India and abroad. Max Infotech has implemented SAP Ver. X and has been using it successfully for 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 processes and enhancing services to its customers. The senior management of Max Infotech has been very proactive in directing the management and deployment of Information Technology. Most of the mission critical applications in the company have been computerised. The IT department of Max Infotech has developed Information Systems Controls (Policies, Procedures, Practices and Organisation Structure) as envisaged by the management for ensuring uniformity and standardization in implementation of IT Solutions across the company. The internal audit team of the company has been well trained in IT and has gained extensive experience in auditing all IT applications and they have also specific competency in all the key functionalities of SAP.

Need for SAP Application and Logical Access 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 stabilized and standardized 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.

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 2019, 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 this assignment is to conduct Logical Access Controls Review of SAP by using the latest and globally recognised standard COBIT 2019 issued by the ISACA, 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 system operational risks and ensure that the information systems are implemented 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 in-person discussions with the internal audit team of Max Infotech on 7th March 2019 at Bangalore. The detailed scope of review and methodology to be 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 will be from security\controls perspective and would involve:

A. Review of IT Resources as relevant

a. Operating Software - Access controls

b. Telecommunications Software - Access Controls

c. RDBMS - Access Controls

d. SAP - Major focus area – Configuration of Parameters and Access Controls

e. Application controls at various stages such as Input, Processing, Output, Storage, Retrieval and transmission so as to ensure Confidentiality, Integrity and Availability of data.

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

Our Approach/Methodology

Audit Approach

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

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

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

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

In tune with terms and scope of reference of the assignment, we will adapt the methodology from COBIT®. Specific Control Objectives\Management Guidelines of the relevant IT process of Logical Access controls shall be selected for this assignment after obtaining understanding of the organisation structure, deployment of information systems 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:

1. Discussions with the
    - Internal Audit Team
    - Systems\Implementation Team
    - Users and user management
2. Review of Operating Systems (OS) documentation
3. Examination of OS access rights
4. Review of Oracle\SAP Manuals
5. Examination of selected Modules access profiles
6. Observation of the Users and the systems in operation
7. Review of access controls over Computers as relevant
8. 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:

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 led by Mr. Abraham. The team would be a blend of professionals with extensive experience in Management, Information Systems and Auditing. The team includes Chartered Accountants, IT Professionals, Management Consultants and Certified Information System Auditors. The senior members of the team are:

- Abraham
- Ramprakash
- Ravindra Jain
- Hariram

Logistic Arrangements

Infrastructure Required

It will be necessary for Max Infotech to appoint one coordinator who will be part of the discussions on the work plan initially and continue to work with our team till the assignment is complete. Max Infotech will make available necessary systems, software resources and support facilities required for completing the assignment within the agreed time-frame. During the course of the assignment, we will require following:

- Three Nodes with Read only access to SAP.
- One Laptop with Windows 10/Microsoft office 2013 or higher version.
- 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 Comments 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 estimated time for the assignment is approximately 12 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 are Rs. x.xx Lakhs (Rupees xxx only) to be paid as follows:

- 50% Advance on Proposal acceptance
- Balance 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 (OS)

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 OS is accessed and Access Logs should show details as to the users accessing the OS, 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".

Findings

1. System Users have blank user-ids:

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 ids and passwords 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 reusing the previous five passwords.

Management comment: Agreed. 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: Agreed. 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 detailed tables of SQL Statements can be obtained from ABC, IT Department. 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. The 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 was created during the time of data conversion. This user-id has been disabled so that transactions cannot be entered using this user-id.

Past Employees having ID in User Table

Rating: High

There are 19 users who have user IDs including ex-employees.

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 current users. All other users will be disabled.

Transactions with amount as Null in FA Trans table

Rating: Medium

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

Implications

This 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

- controls of their in-house package - Financial Accounting and Loan Processing System (FALPS),
- Logical access controls of FALPS, and

Conduct Implementation audit of General Controls at 2 select branches with specific emphasis on implementation of FALPS.

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 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 was also agreed to. Broadly the overall scope of review primarily from security / controls point of view 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.

Broad 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 per Audit Plan and Program, which were discussed with the statutory auditors and ABC's senior management. We have used the COBIT issued by ISACA, 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 Oracle as RDBMS using latest version of FALPS with copy of data of Bangalore Branch (up to 31st March 2019). We have also visited and reviewed operations at two branches at Mangalore and Hassan.

Audit Reports

We issued a draft report outlining our issues and recommendations and obtained feedback from the IT Department. Further, a meeting was held with IT department represented by Mr. Sam, AGM (IT) and Mr. Ram, AGM (Finance and Accounts) where the issues and recommendations were discussed in detail. The IT Department has been very proactive in incorporating our suggestions. The issues rectified so far are given 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 annexures 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 deptt and the 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 Control issues of Oracle
6. Review of Financial data using SQL: Highlighting data integrity issues in existing data

Overall Conclusions

Based on our review, our overall conclusions on specific areas are as follows:

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. This may also lead to inconsistencies in data and is a major concern area. 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 ISACA, USA and Security and Control Practices as outlined in COBIT 5 also issued by ISACA as applied to ABC operations for review of Application software and implementation. 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 the IS Auditor to Prepare Himself for Providing Assurance services in E-Commerce

1. How many (approximately) of the businesses you audit will be electronic in that there is no paper, or other non-electronic forms of audit trail available?
2. In general, as an auditor, what special steps or approach would you take when auditing a business that is engaged in eCommerce compared with a comparable business not engaged in electronic commerce?
3. Which national or international standards or pronouncements would you use or are using in undertaking an audit of a business engaged in electronic commerce?
4. To what extent would you want that records and audit trails of eCommerce transactions be maintained and in what form?
5. How would you assure the management that records, and audit trails are being properly created?
6. To what extent would you recommend that records and audit trails of eCommerce transactions be maintained over time?
7. To what extent do you foresee that records and audit trails of eCommerce transactions will be combined with other transactions or otherwise consolidated, so that the transactional trail is not lost?
8. How do you satisfy yourself that records and audit trails of eCommerce transactions have not been altered?
9. How would you test the above – through review of system controls or substantive testing?
10. If you find that that records and audit trails of eCommerce transactions are inaccessible either through being stored remotely, or through the effects of data security mechanisms, or otherwise, how would you, as auditors, audit the same?
11. 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?
12. How would you address the following issues and problems you could be facing in practice when carrying out audits of businesses engaged in eCommerce?

- Accessing initial transaction data
- Processing of the transaction by accounting systems
- Identifying suitable sources of confirmation
- Determining the system processing “rules”
- Storage and retrieval of the eCommerce records, and
- Forming an opinion as to the timeliness, completeness and accuracy of the Transaction data.

13. How many of your present clients do you perceive could be engaged in electronic commerce?
14. What specific approaches, solutions, methods, procedures or techniques do you need to develop to assist in the auditing of businesses engaged in electronic commerce?
15. What approaches, solutions, etc. do you anticipate might help you in the future when auditing businesses engaged in electronic commerce?
16. In what way would the solutions, methods, etc. you devised for auditing non-eCommerce clients differ from auditing the eCommerce Clients?
17. Do you think there are differences in business-to-business eCommerce compared with business-to-consumer eCommerce that would warrant different audit considerations and if so, what are the considerations?

Appendix 7

Specimen Report Format

<table>
<tr><th>Sr #</th><th>Reported Area</th><th>Recommendations</th><th>Management Comments</th></tr>
<tr><td>4.0</td><td>AUDIT AREA– Asset Management</td><td></td><td></td></tr>
<tr><td>4.1</td><td>Improper Asset Management
➢ Fixed asset register does not reflect the clear ownership of the asset.
➢ Many assets were not having tags as required by Asset Tagging Policy.
<table>
<tr><td rowspan="2">Root Cause</td><td></td><td>Technology</td><td></td><td>Process</td><td>🟦</td><td>People</td><td></td><td>Others</td></tr>
<tr><td colspan="8">➢ Non-Compliance to security policy</td></tr>
<tr><td>Risk</td><td colspan="2">Very High</td><td>High</td><td colspan="2">🟦</td><td>Medium</td><td>Low</td><td>Negligible</td></tr>
<tr><td>Reason for rating</td><td colspan="8">➢ Risk of Theft/Misuse
➢ Risk of system crash due to temperature and
➢ humidity</td></tr>
</table></td><td>Asset register should reflect the ownership and tagging should be as per policy.
<table>
<tr><td rowspan="2">PO support required for resolution</td><td>Yes</td><td>No</td></tr>
<tr><td></td><td>🟦</td></tr>
</table></td><td>.
<table>
<tr><td>Name</td><td></td></tr>
<tr><td>Designation</td><td></td></tr>
<tr><td>Timelines</td><td></td></tr>
</table></td></tr>
<tr><td>5.0</td><td>AUDIT AREA- Physical and Environmental Controls</td><td></td><td></td></tr>
<tr><td>5.1</td><td>Weak Controls on Laptop checking
➢ On 6/08/2019, it was observed that at M office, Laptops are not being checked while leaving the office.
➢ The access control system at the entire 1st Floor at K office is not operational.
<table>
<tr><td rowspan="2">Root Cause</td><td></td><td>Technology</td><td></td><td>Process</td><td>🟦</td><td>People</td><td></td><td>Others</td></tr>
<tr><td colspan="8">➢ Non-Compliance to security policy</td></tr>
<tr><td>Risk</td><td>🟦</td><td>Very High</td><td>High</td><td>Medium</td><td>Low</td><td>Negligible</td></tr>
<tr><td>Reason for rating</td><td colspan="8">➢ Risk of Theft/Misuse</td></tr>
</table></td><td>Visitors’ laptops should be checked while entering and leaving the office.
Access control system should be made operational.
<table>
<tr><td rowspan="2">PO support required for resolution</td><td>Yes</td><td>No</td></tr>
<tr><td></td><td>🟦</td></tr>
</table></td><td>
<table>
<tr><td>Name</td><td></td></tr>
<tr><td>Designation</td><td></td></tr>
<tr><td>Time lines</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr>
<td>5.2</td>
<td>Monitoring not done for preventive maintenance of AC
The preventive maintenance of air conditioning at K office for data centre is not being monitored at all. The Admin deptt. is not having even copy of preventive maintenance schedule, a pre-requisite for monitoring and compliance, as agreed between Bharti and Nu Tech Engineers
<table>
<tr><td rowspan="2">Root Cause</td><td></td><td>Technology</td><td></td><td>Process</td><td>🟦</td><td>People</td><td></td><td>Others</td></tr>
<tr><td colspan="8">➢ Non-Compliance to security policy</td></tr>
<tr><td>Risk</td><td>🟦</td><td>Very High</td><td>High</td><td>Medium</td><td>Low</td><td colspan="3">Negligible</td></tr>
<tr><td>Reason for rating</td><td colspan="8">Risk of system crash due to temperature and humidity</td></tr>
</table>
</td>
<td>Preventive maintenance schedule should be maintained and monitored.
<table>
<tr><td rowspan="2">PO support required for resolution</td><td>Yes</td><td>No</td><td></td></tr>
<tr><td></td><td>🟦</td><td>🟦</td></tr>
</table>
</td>
<td>
<table>
<tr><td>Name</td><td></td></tr>
<tr><td>Designation</td><td></td></tr>
<tr><td>Timelines</td><td></td></tr>
</table>
</td>
</tr>
<tr>
<td>6.0</td>
<td>AUDIT AREA- Communications and Operations Management.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1</td>
<td>Weak Backup Controls
➢ The B Backup and Recovery Management version 2.2 is dated 13/8/2015, with no date of revision
➢ Backup schedules are not drafted so as to give clear direction for storage of backups.
➢ In case of all the servers, except M-KL (10.0.0.0), monthly back-up was not kept on-site.
➢ Offsite backup is not kept in fire proof cabinet.
➢ The prescribed format, FM Backup & Recovery Request Form, is not being used.
➢ In case of server (10.0.0.0.), monthly backup is required to be kept for 7 years. As explained to us, immediate six months' data should be kept onsite and rest offsite. However, it was noticed that some tapes of 2016 and 2017 were also kept on-site.
<table>
<tr><td rowspan="2">Root Cause</td><td></td><td>Technology</td><td></td><td>Process</td><td>🟦</td><td>People</td><td></td><td>Others</td></tr>
<tr><td colspan="8">➢ Lack of clear directions in back up schedule and non adherence of policy.</td></tr>
<tr><td>Risk</td><td>🟦</td><td>Very High</td><td>High</td><td>Medium</td><td>Low</td><td colspan="3">Negligible</td></tr>
</table>
</td>
<td>Backup schedule should be suitably amended to provide clear directions for backup storage as per policy.

Offsite backups should be stored in fireproof cabinet.
<table>
<tr><td rowspan="2">PO support required for resolution</td><td>Yes</td><td>No</td></tr>
<tr><td></td><td>🟦</td></tr>
</table>
</td>
<td>
<table>
<tr><td>Name</td><td></td></tr>
<tr><td>Designation</td><td></td></tr>
<tr><td>Timelines</td><td></td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td><table><tr><td>Reason for rating</td><td>➢ Delay in restoration in case of need
➢ Offsite backups are at risk.</td></tr></table></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2</td>
<td>Improper Media Management
➢ Media Dispatch/ Receive Form is not being used for movement of blank media.
➢ The Inventory Records are not being maintained properly. Receipt of media is not being recorded.
➢ Annual Media Inventory Reconciliation is not being taken care, since the Inventory Records were started to maintain from 7/11/2006
<table>
<tr><td rowspan="2">Root Cause</td><td>Technology</td><td>Process</td><td>🟦</td><td>People</td><td>Others</td></tr>
<tr><td colspan="5">➢ Non adherence to process.</td></tr>
<tr><td>Risk</td><td></td><td>High</td><td>🟦</td><td>Medium</td><td></td><td>Low</td></tr>
<tr><td>Reason for rating</td><td colspan="6">➢ Delay in restoration in case of need</td></tr>
</table></td>
<td>Media should be managed as per defined process.
<table>
<tr><td rowspan="2">PO support required for resolution</td><td>Yes</td><td>No</td></tr>
<tr><td></td><td>🟦</td></tr>
</table></td>
<td><table><tr><td>Name</td></tr><tr><td>Designation</td></tr><tr><td>Timelines</td></tr></table></td>
</tr>
<tr>
<td>7.3</td>
<td>Unwanted files on the Servers
➢ It was observed that file deletion on the server is not followed after any activity as unwanted and unspecified files were found on the server and also in the recycle bin.
➢ Logs from the months of April, May, June, July and August were found on the Syslog server. G says that logs older than 60 days should be deleted from the servers.
<table>
<tr><td rowspan="2">Root Cause</td><td></td><td>Technology</td><td></td><td>Process</td><td>🟦</td><td>People</td><td></td><td>Others</td></tr>
<tr><td colspan="8">➢ Lack of security
➢ Non-Compliance with security Policy</td></tr>
<tr><td>Risk</td><td></td><td>High</td><td>🟦</td><td>Medium</td><td></td><td>Low</td></tr>
<tr><td>Reason for Rating</td><td colspan="8">➢ These files may contain sensitive open information and dangerous executables.
➢ Performance of the server is impaired.</td></tr>
</table></td>
<td>All files that are not required on the server should be completely deleted from the server.
<table>
<tr><td rowspan="2">PO support required for resolution</td><td>Yes</td><td>No</td></tr>
<tr><td></td><td>🟦</td></tr>
</table></td>
<td><table><tr><td>Name</td><td></td></tr><tr><td>Designation</td><td></td></tr><tr><td>Timelines</td><td></td></tr></table></td>
</tr>
<tr>
<td>7.4</td>
<td>Improper Content Filtering for WEB
Internet content filtering is done on the squid proxy and no dedicated program is used to do this such as (Websense or</td>
<td>Consider applying a dedicated program</td>
<td></td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>
IWSS). Using only the squid proxy for the filtering is not a strong measure to do the web filtering.
Database for the web content filtering is not strong enough to catch all the websites on the Internet.
<table>
<tr><td rowspan="2">Root Cause</td><td>Technology</td><td></td><td>Process</td><td>🟦</td><td>People</td><td></td><td>Others</td></tr>
<tr><td colspan="7">➢ Lack of security focus</td></tr>
<tr><td>Risk</td><td></td><td>High</td><td>🟦</td><td>Medium</td><td></td><td>Low</td><td></td></tr>
<tr><td>Reason for Rating</td><td colspan="7">➢ It is a Gateway for vulnerabilities</td></tr>
</table>
</td>
<td>
for the Internet content filtering to reduce the vulnerabilities and malicious attacks from Internet.
<table>
<tr><td rowspan="2">PO support required for resolution</td><td>Yes</td><td>No</td></tr>
<tr><td></td><td>🟦</td></tr>
</table>
</td>
<td>
<table>
<tr><td>Name</td><td></td></tr>
<tr><td>Designation</td><td></td></tr>
<tr><td>Timelines</td><td></td></tr>
</table>
</td>
</tr>
</table>

Notes

Notes