IT AUDIT MANUAL (ITAM)

AFROSAI-E

1st Edition

November 2017

African Organisation of English-Speaking Supreme Audit Institutions

Printed in South Africa

First Printing, 2017

ISBN 978-0-6399943-2-1

AFROSAI-E

www.afrosai-e.org.za

TABLE OF CONTENTS

ABBREVIATIONS

CAATs - Computer Assisted Audit Techniques

CIA - Confidentiality, Integrity and Availability

CISA - Certified Information Systems Auditor

COBiT- Control Objectives for Information and related Technology

COSO - Committee of Sponsoring Organisations

ERP - Enterprise Resource Planning

ICT - Information and Communication Technologies

IS - Information Systems

ISACA - Information System Audit & Control Association

ISO - International Standards Organisation

IT - Information Technology

ITAF – Information Technology Assurance Framework

ITIL - Information Technology Infrastructure library

KPI - Key performance indicators

SAI - Supreme Audit Institutions

TOGAF - The Open Group Architecture Framework

1. CHAPTER 1: INTRODUCTION TO IT AUDITING

1.1. Introduction

Government entities have increasingly adopted Information and Communication Technologies (ICT) to conduct their functions and to deliver various services. The continuous development of ICTs has made it possible to capture, store, process and deliver information electronically. This transition to electronic processing has necessitated significant changes in the environment in which Supreme Audit Institutions (SAIs) carry out their work. There is therefore need for auditors to gain assurance on such computerised systems to derive appropriate audit conclusions. IT systems are also commonly referred to as Information Systems (IS).

1.2. What is IT Auditing?

IT Audit is the process of deriving assurance on whether the development, implementation, support and maintenance of information systems meets business goals, safeguards information assets and maintains data integrity. In other words, IT Audit is an examination of the implementation of IT systems and IT controls to ensure that the systems meet the organisation's business needs without compromising security, privacy, cost, and other critical business elements.

1.3. IT Audit Objectives

The objective of IT Audits is to ensure that the IT resources allow organisational goals to be achieved effectively and use resources efficiently. IT audits may cover IT applications, IT operations, IT governance, ERP Systems, IS Security, acquisition of the business solution, System Development, and Business Continuity – all of which are specific areas of IS implementation, or could to look at the value proposition the IS Systems may have fulfilled.

Some examples of audit objectives are:

- Review of the controls of the IT systems to gain assurance about their adequacy and effectiveness.
- Evaluation of the processes involved in the operations of a given area such as a payroll system, or financial accounting system.
- Evaluation of the performance of a system and its security, for example, a railway reservation system.
- Examination of the system development process and the procedures.

1.4. Mandate for IT Audits

The mandate of SAI for IT audit shall be derived from the overall mandate provided to the SAI to conduct audits. Some SAIs may also have specific mandate for conducting IT Audits or audit of Information Systems.

For many SAIs, the mandate to conduct Financial Audits, Performance Audits, and Compliance audits will be a sufficient mandate to conduct IT Audits. This is because the IT systems support the core operations of an entity which may include financial systems. Thus, IT Audits may not need any additional mandate.

The specific mandate, if provided, should address jurisdiction of audit for auditing IT Systems, which are utilised by the entity to fulfil its functional objectives. It should also provide for timely, unfettered, direct and free access to all necessary documents and information from the entity, both manual and electronic, whether the function or any of its part is insourced or outsourced.

1.5. Types and Scope of IT Audits

IT audits may be carried out as a separate review of information systems or in conjunction with a financial statements audit, a review of internal controls, and/or as Performance Audits of IT Systems or IT Applications. The scope of IT audits also supports Specialised, forensic and Information Systems (IS) development projects Audits.

Outlined below is what each audit would entail:

- **IS Audit**

  The 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 organisational goals effectively, consume resources efficiently and have, in effect, internal controls that provide reasonable assurance that business, operational and control objectives will be me and that undesired events will be prevented, or detected and corrected in a timely manner.

- **Financial audit**

  Financial audit seeks to assess the correctness of an organisation's financial statements. IT audit comes in the financial audit to evaluate whether the information systems and related resources (including information) adequately safeguard data integrity.

- **Compliance Audits**

  Compliance audit include specific tests of controls to check for adherence to specific regulations and standards. These audits often overlap traditional IT Audits but may focus on particular systems or data.

- **Performance auditing**

  This is an independent, objective, and reliable examination of whether government undertakings, systems, operations, programmes, activities or entities are operating in accordance with the principles of economy, efficiency, and effectiveness and whether there is room for improvement. IT Auditors shall examine the IT systems implemented with respect to the criteria of economy, efficiency, and effectiveness and value to the citizen. (ISSAI 5300)

IT Audits can cover other specialised reviews that examine specific areas, such as outsourcing, or have specific objectives such as digital forensics.

Irrespective of the type of audit, the IT auditor would be required to assess the policies and procedures that guide the overall IT environment of the audited entity, ensuring that the corresponding controls and enforcement mechanisms are in place.

From the set objectives of the IT Audit, the IT Auditor should decide on the scope of audit. The scoping of the IT Audit would involve deciding the extent of audit scrutiny, the coverage of IT systems and their functionalities, IT processes to be audited, locations of IT systems to be covered, and the period to be covered. It will be, essentially, setting or delineating the boundaries of the audit.

1.6. Overview of the IT Audit process

IT auditing follows the same stages with a Regularity Audit. However, the method and tools used for gathering audit evidence may vary. These stages can be broadly classified **as follows:**

- **Pre-engagement activities** – which includes an assessment of the objectivity, integrity and technical capacity of audit staff and establishing the budgeted time for the audit. It also includes gaining a common understanding and expectations through issuing an engagement letter.
- **Understanding the entity**
- **Risk Assessment -** during which auditors gains understanding of the auditee's environment, identifies and evaluate risks and materiality on an institutional level. This process will also establish and ensure that the auditor has considered all relevant factors surrounding the environment within which the client operates. The overall strategic plan is at this point discussed with the auditee.
- **Performing the Audit -** here the auditor is expected to understand the detailed processes for each audit component, design audit programs, and document the performance of the programs by completing the templates provided.
- **Audit reporting** – the final management letter that arise from the audit process. At the end of each part the related working papers can be found.

A Risk based audit approach should be used when conducting an IT Audit. This involves identification of the risk elements in the entity being assessed along with weighted risk scores based on specific evaluation criteria and thus identifying priority area to be audited. This weighted risk score may involve the auditor identifying the impact and likelihood of an adverse effect. Risks may be categorised high, medium and low with the auditor assigning an appropriate measure.

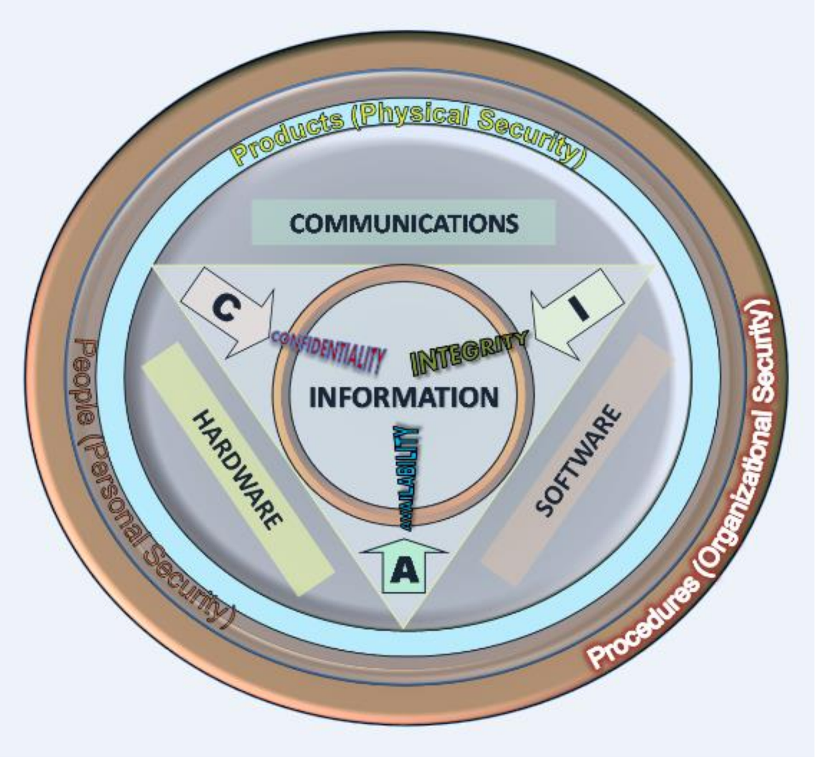
ISSAI 5300 requires the auditor to prepare audit documentation that is sufficiently complete and detailed to provide an overall understanding of an audit. The review of the documentation should enable any other IT auditor to reach the same audit conclusions. There is no standard format for IT audit documentation in ISSAIs. Further, the formats may differ from SAI to SAI. There may be certain level of standardisation within each SAI in terms of checklists, specimen letters, organisation of working papers, etc.

Throughout the audit process, quality control should be maintained to ensure that audit objectives are met.

1.7. Linkages between Financial Auditing and IT Auditing

ISSAI 1315 specifies the auditor's responsibility to identify and assess the risks of material misstatement, through understanding of the entity and its environment. In a computerized environment it is therefore important to understand how controls can affect financial statements. The auditor should obtain an understanding of the information system, including the related business processes, relevant to financial reporting.

The focus of auditing IT controls is the assessment of **Confidentiality, Integrity and Availability (CIA)** of information system resources as outlined in the diagram below.


Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
AVAILABILITY
A
HARDWARE
SOFTWARE
People (Personal Security)
Procedures (Organizational Security)

Financial auditing on the other hand is concerned with true and fair presentation of financial statements. The auditor should assess whether assertions such as Occurrence, Completeness, Accuracy, Cutoff, Classification, Existence and Valuation were met to be able to express an appropriate opinion.

The linkage between the two is that the IT control objectives (**Confidentiality, Integrity and Availability)** may have an impact on the financial assertions. Assessing these IT controls helps the auditor give an assurance or otherwise of the free and fair presentation of financial statements produced using information systems and their processes.

1.8. What is the role of the IT Auditor in a Financial Audit

It is quite clear from the ISSAIs that the auditor needs to review controls during the financial audit. The role of the IT auditor in the financial audit process is to assist the financial auditor in determining if reliance can be placed on the controls the entity developed and the effectiveness of the IT control environment as well as the application environment. The outcome of the results from the work performed by the IT auditor will determine the approach the regulatory auditor will take during the audit.

The planning of the general control audit should also be done during the planning phase of the financial audit, as well as the testing of controls. The outcomes of the general controls audit will assist to determine the overall audit strategy the financial auditor will take. Should an application audit be performed the execution of the audit will take place during the execution phase of the regulatory audit. If there are any material findings, the auditor should report the findings to management during the reporting phase of the financial audit, after taking into consideration and testing any compensating controls that relate to the specific weakness in the controls.

Whilst the focus of IT control assessment is CIA of information system resources, it is important where possible to map IT Audit findings to financial audit assertions. In many cases the financial auditor will not be certain on how the lack of general controls can affect the financial statements. The lack of IT controls will have an indirect effect on the financial statements and in some situations these risks can be quantified in monetary terms, for example the use of Computer Assisted Audit Techniques (CAATs) to determine when personnel were on vacation and transactions were approved.

At the end of the day, the financial auditor should sign off on the work performed by the IT auditor, as required by ISSAI standards and as previously stated should be included in the annual general audit report which is issued by the Auditor-General.

2. CHAPTER 2: STANDARDS AND FRAMEWORKS

2.1. Introduction

Many frameworks, standards, guidelines and tools exist to provide guidance to the auditor in completing an information systems audit. The auditor should be aware of those available when performing the IT audit and can use them as reference tools.

2.2. Standards

Standards are a set of operational or technical measures, procedures or practices. Standards provide more detailed information on how managers and functional specialists are expected to conduct certain aspects of their duties. The auditor should adhere to these standards when performing an audit.

2.2.1 International Standards for Supreme Audit Institutions (ISSAI)

The Series ISSAI 5300-5399 is allocated to Guidelines on Information Technology Audits under ISSAI framework. ISSAI 5300 is an overarching, general principle ISSAI on fundamentals of IT Audit provides for framing of more specific guidelines.

Some specific ISSAIs relating to audit of information systems are:

ISSAI 5300 Guideline to guide IT Audit professionals conducting IT Audits

ISSAI 5310 Information Systems Security Review Methodology

ISSAI 5450 Public Debt Information System

2.2.2 Information System Audit & Control Association (ISACA) Standards

ISACA is a global association that engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. IS audit and assurance standards define mandatory requirements for IS auditing and reporting and inform:

- IS audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics

- Holders of the Certified Information Systems Auditor (CISA) designation of requirements.

Failure to comply with these standards may result in an investigation into the CISA holder’s conduct by the ISACA Board of Directors or appropriate committee and, ultimately, in disciplinary action. (See also ITAF)

2.2.3 Regulations and National Standards

National standards may refer to Standards by government bodies. Each organisation needs to comply with governmental and external requirements related to information systems. The auditor should consider National standards affecting information systems being audited. These will form a basis against which an entity's information system will be assessed. However, where there are no National Standards the auditor should be guided by best practice.

2.2.4 International Standards Organisation (ISO) IT Standards

The International Organization for Standardization is the world's largest developer of voluntary International Standards. International Standards give state of the art specifications for products, services and good practice, helping to make industry more efficient and effective. Developed through global consensus, they help to break down barriers to international trade.

Some standards applicable to IT audit are:

- ***ISO 20000 (IT operations)***

  ISO 20000 is the first standard on IT service management and includes the design, transition, delivery and improvement of service requirements and provide value for both the customer and service provider.

- ***ISO 27000 (IT security)***

  The standard establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organisation

- ***ISO 31000 (Risk)***

  Assist organisations in effectively managing the risks in an environment full of uncertainty. It assists organisations increasingly to achieve their objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.

- ***ISO 38500 (Governance)***

  ISO 38500 provides a framework for effective IT governance for top management to understand and fulfil their legal, regulatory and ethical obligations in respect of the organisations' use of IT. It sets out six principles for good corporate IT governance, namely:

  - ✓ Responsibility
  - ✓ Strategy
  - ✓ Acquisition
  - ✓ Performance
  - ✓ Conformance
  - ✓ Human behaviour

2.3. Frameworks

A framework is a formal statement that provides context and board guidance with respect to policy themes or clusters. Also provides the supporting structure within which specific policies and other instruments can be understood in strategic terms. Explains why the entity sets policy in the area for example:

2.3.1 IT Assurance Framework (ITAF)

The ISACA Information Technology Assurance Framework (ITAF) is a comprehensive and good-practice-setting model that:

- Provides guidance on the design, conduct and reporting of IT audit and assurance assignments

- Defines terms and concepts specific to IT assurance.

ITAF establishes standards that address IT audit and assurance professional roles and responsibilities; knowledge and skills; and diligence, conduct and reporting requirements ITAF provides a single source through which IT audit and assurance professionals can seek guidance, research policies and procedures, obtain audit and assurance programmes, and develop effective reports.

2.3.2 Control Objectives for IT (COBIT)

Control Objectives for Information and related Technology (COBiT) is a control framework for IT governance, which defines the reasons IT governance is needed, the stakeholders and what it needs to accomplish. It is a roadmap to good IT governance. COBIT provides good practices across a domain and process framework and presents activities in a manageable and logical structure. It is focused more on control, less on execution. These practices will help optimise IT-enabled investments, ensure service delivery and provide a measure against which to judge when things do go wrong. COBIT focus on the following:

CobiT defines the business to be responsible for defining functional and control requirements and to use automated services, whereas the IT is responsible to automate and implement business functional and control requirements and to establish controls to maintain the integrity of application controls.

2.4. ITIL (IT Infrastructure library)

It is a set of practices that focuses on aligning IT with business objectives. It provides the organisation with a baseline from which it can plan, implement and measure the deliverables. ITIL v3 consists of 5 volumes, namely:

- ITIL Service strategy

- ITIL Service design

- ITIL Service transition

- ITIL Service operation

- ITIL Continual Service Improvement

2.5. Val IT

It is a comprehensive and pragmatic organising framework that enables the creation of business value from IT-enabled investments. Designed to align with and complement COBIT, Val IT integrates a set of practical and proven governance principles, processes, practices and supporting guidelines that help boards, executive management teams and other enterprise leaders optimise the realisation of value from IT investments.

2.6. Other Standards and Frameworks that the IT auditor should also be aware of:

2.6.1 COSO (Committee of Sponsoring Organisations)

It is a voluntary organisation dedicated to providing leadership to executive management and governance entities on critical aspects of organisational governance, business ethics, and internal control model against which companies and organisations may assess their control systems. COSO is supported by five organisations including the Institute of Management Accountant (IMA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Institute of Internal Auditors (IIA) and Financial Executives International (FEI).

2.6.2 Risk IT

A set of guiding principles and the first framework to help enterprises identify, govern and effectively manage IT risk.

2.6.3 The Open Group Architecture Framework (TOGAF)

It is a framework for enterprise architecture that provides an approach for designing, planning, implementing, and governing enterprise information technology architecture. TOGAF has been a registered trademark of The Open Group in the United States and other countries since 2011.

TOGAF is a high-level approach to design. It is typically modelled at four levels:

- Business,
- Application,
- Data, and
- Technology.

It relies heavily on modularization, standardization, and already existing, proven technologies and products.

2.6.4 Association Technical Standards and Best Practices

There are various organisations and associations which have developed standards and best practices to guide members. Some examples are:

Telecommunication Industry Association (TIA)

These are a set of telecommunications standards from the Telecommunication Industry Association (TIA) addressing commercial building cabling for telecommunications products and services. One the specific standards and IT Auditor can use is the TIA942- Standard for Data Centers.

Center for Internet Security (CIS)

The Center for Internet Security (CIS) is an organization dedicated to enhancing the cybersecurity readiness and response among public and private sector entities.

National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST), part of the United States Department of Commerce, publishes generally accepted principles and practices for securing information technology systems and a collection of principles and practices to establish and maintain system security.

2.6.5 Supplier/vendor Standards and specific best practice

Different vendors (e.g. Microsoft, Oracle, SAP) give recommendations regarding best practice and how to secure their products.

2.7. Guidelines

Guidelines provide guidance in applying IS Auditing Standards. The IS auditor should consider them in determining how to achieve implementation of the standards, use professional judgment in their application and be prepared to justify any departure. The objective of the IS Auditing Guidelines is to provide further information on how to comply with the IS Auditing Standards.

3. CHAPTER 3: IT RISK ASSESSMENT AND RISK BASED AUDITING

3.1. Standards on IT risk assessment and risk based audits

ISSAI 1315 requires the auditor to obtain an understanding of whether the organisation has a process for:

- Identifying business risks relevant to financial reporting objectives
- Estimating the significance of the risks;
- Assessing the likelihood of occurrence; and
- Deciding about the actions to address those risks.

ISACA standards S1202.1-3 states that 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. The IS audit and assurance professionals shall identify and assess risk relevant to the area under review, when planning individual engagements and shall consider subject matter risk, audit risk and related exposure to the enterprise.

ISSAI 5300 requires IT Audits to be carried out on a risk based approach. This Risk based audit approach involves identification of risk elements in the entity being assessed along with their potential impact and thus identifying priority area to be audited.

3.2. Risk IT principles

The Risk IT framework is about IT Risk. The connection to business is clear in the principles on which the framework is built, i.e. effective enterprise governance and management of IT risk:

- Always connects to business objectives
- Aligns the management if IT related business risk with overall enterprise risk management
- Balances the costs and benefits of managing risk
- Promotes fair and open communication of IT risk
- Establishes the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels
- Is a continuous process and part of daily activities

Risk IT defines several guiding principles for effective management of IT risk. The principles are based on generally accepted enterprise risk management principles, which have been applied to the domain of IT. The Risk IT process model is designed and structured to enable enterprises to apply the principles in practice and to benchmark their performance.

3.3. Defining IT Risk

Risk is the potential that a given threat will exploit vulnerabilities of an asset or a group of assets and thereby cause harm to the organization

IT risk is the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. IT risk consists of IT related events that could potentially impact the business. It includes both uncertain frequency and magnitude, and it creates challenges in meeting strategic goals and objectives as well as uncertainty in the pursuit of opportunities. IT risks can be categorised in different ways:

- IT service delivery risk, associated with the performance and availability of IT services, and which can bring destruction or reduction of value to the enterprise
- IT solution delivery/ benefit realisation risk, associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programmes.
- IT benefit realisation risk, associated with opportunities to use technology to improve efficiency or effectiveness of business processes, or to use technology as an enabler for new business initiatives

IT risk always exists, whether or not it is detected or recognised by an organisation hence need to be managed.

3.4. Audit risk and materiality

Audit risk can be defined as the risk that information may contain a material error that may go undetected during the audit. The IS auditor should consider the applicable other factors relevant to the organisation: customer data, privacy, availability of provided services as well as the corporate and public image as in the case of public organisation or the foundation.

Audit risk is categorised as:

- Inherent risk - the risk that an error exist that could be material or significant when combined with other errors encountered during the audit, assuming that there is no related compensating controls. It is the susceptibility to material misstatements in the absence of related controls. Inherent risk can occur because of the nature of the business.

- Control risk - the risk that a material error exists that will not be prevented or detected in a timely manner by the internal controls system e.g. controls risks associated with the manual review of computer logs can be high because activities requiring investigations are often easily missed because of the volume of logged transactions.

- Detection risk - the risk that the IS auditor uses inadequate test procedures and conclude that material misstatements do not exist when, in fact they do.

- Overall audit risk - the combination of the individual categories of risk assessed for each control objective. The objective in forming the audit approach is to limit the audit risk of the area under scrutiny so that the audit risk is at a low level at the completion of the audit.

There is an inverse relationship between risk and materiality. The lower the Materiality threshold, the more precise the audit expectations and the greater the audit risk. Thus, to gain additional assurance in instances where there is high audit risk or a lower materiality threshold, an IS auditor should compensate by either extending the scope or nature of the IS audit tests (extend the test of controls) or increasing or extending the substantive testing.

3.5. Entity's risk Management

According to ISACA, risk management is the process of identifying vulnerabilities and threats to the information resources used by an organisation in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organisation.

To develop a sound understanding of audit risk, an IS auditor should understand how the entity being audited manage risk.

Risk assessment should identify, quantify and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. The result should guide and determine the appropriate management action, priorities for managing information security risks and priorities for implementing controls to protect against the risk.

Risk assessment should be performed periodically to address changes in the environment and in security requirement and the risk situations (in the assets, threats, vulnerabilities, impact)

For risks where the risk treatment decision is to apply controls, controls should be selected to ensure that risk are reduced to an acceptable level.

3.6. Auditor's Risk Assessment

Risk Assessment is a process to identify and evaluate risks and their potential effects. It is a systematic consideration of:

- The business harm likely to result from a security failure, taking into account potential consequences of a loss of confidentiality, integrity and availability of information assets,
- The realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities and the controls currently implemented.

ISACA 1202, requires two levels of risk assessment when planning for an IS Audit:

i. Risk Assessment to develop an overall IS Audit Plan and determine priorities for the effective allocation of IS audit resources.
ii. Risk assessment of Individual Audit Engagement

3.6.1 Risk Assessment to develop an overall IS Audit Plan

A suitable risk assessment should be conducted and documented at least annually to facilitate the development of an IS audit plan. IS auditors should consider the following elements when developing the plan:

a. Full coverage of all areas within the scope of the IS audit universe, which represents the range of all possible audit activities
b. Reliability and suitability of the risk assessment provided by management
c. The processes followed by management to supervise, examine and report possible risk or issues
d. Cover risk in related activities relevant to the activities under review

The IS audit universe of most SAI is composed of many Information systems that cannot exhaustively be audited in a cycle of one year. This may be due to limited resources. Even when resources are enough, it might not be justifiable to audit some Information systems annually. Further, some applications may be mission critical applications with lapses having far reaching consequences (e.g. IFMIS) and may need more attention. The IS audit directorate should therefore use a risk assessment approach that help with the prioritisation and scheduling of the IS audit and assurance work. To reduce subjectivity in establishing the nature, timing and extent of the IS audit and the resources committed for an audit assignment, the following risk parameters (i.e. criticality of the application) may be considered:

1) Types of System (Commercial Off the Shelf or Inbuilt)
2) Whether the system relates to Critical business operation
3) Number of users of the Systems
4) Number of Interfaces to the system
5) Mode of connection to the network (intranet, extranet or web based/public domain)
6) Number of years the system has been operational
7) Volume of data in the system
8) System implementation method
9) Budget or funds processed in the system
10) Stakeholders interest
11) Prior Year Audit

The weight assigned to these factors, the impact and likelihood may vary from SAI to SAI. This information systems risk assessment can be combined with the overall risk assessment done for all the SAI clients.

3.6.2 Risk assessment of Individual Audit Engagement

Risk assessment of an individual audit engagement starts with the audit team having a full understanding of the activities in scope. During the risk assessment, professionals should consider:

- ✓ Results of prior audit engagements, reviews and findings, including any remedial activities
- ✓ The enterprise overarching risk assessment process
- ✓ The likelihood of occurrence of a particular risk
- ✓ The impact of a particular risk (in monetary or other value measures) if it occurs

In addition, the IS auditor should consider possible illegal acts that can require a modification of the nature, timing or extent of the existing procedures.

The goal of these risk assessment of Individual Audit Engagement is to reduce audit risk to an acceptably low level. Audit risk is the risk of the auditor providing an opinion that is incorrect in view of the existing facts. Audit risk is influenced by:

- ✓ Inherent risk
- ✓ Control risk
- ✓ Detection risk

3.6.2.1 Inherent risk

Inherent risk is the susceptibility of an audit area to errors in a way that could be material, individually or in combination with other errors, assuming that there were no related internal controls. Inherent risk exists independent of an audit and can occur because of the nature of a business. For example, all online information assets are exposed to hacking risk. No matter what technology driven mitigating controls are used to reduce the possibility of the threat materializing, this threat will always be there.

Inherent risk for most IS audit areas is high since the potential effects of errors ordinarily spans several business systems and many users.

3.6.2.2 Control risk

Controls are designed to reduce the possibility of a threat exploiting vulnerability and inflicting damage. Control risk is the risk that a material error exists that would not be prevented or detected and corrected on a timely basis by the system of internal control. For example, the control risk associated with manual reviews of computer logs can be high because of the volume of logged information.

Professionals should assess the control risk as high unless relevant internal controls are:

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

The audit team may hold a discussion to identify pervasive risk and ensure they are appropriately addressed.

Pervasive risks are risk that relates to the whole information systems environment and therefore affects all information system components. Example may include lack of risk assessment by management, management override of controls, management general lack of competence, management's integrity or the reliability of entity's records. Pervasive risks affect the reliability of application controls and detailed IS controls hence possibility of a high risk that the controls designed to operate at the assertion level may be ineffective

The IS auditor should use a system walk-through tests to establish the reliability of auditee's Internal control system. The aim is to answer the question: Have internal controls been implemented to address the risk? In other words, whether to use test controls or fully substantive audit approach.

Test of controls should be used when:

- Internal controls are effective and can be relied upon.
- Substantive procedures alone cannot provide sufficient appropriate audit evidence. For example, when there are many transactions.

Substantive testing should be used when:

- The control is either not in place or is ineffective
- The population of the transactions to be audited are relatively few. Test of the control in this case will not be efficient.

Compliance Test of Controls

Compliance testing is evidence gathering for the purpose of testing an organization's compliance with control procedures.

The broad objective of compliance test is to provide IS auditors with reasonable assurance that the particular control on which the IS auditor plans to rely is operating as the IS auditor perceived in the preliminary evaluation.

After test of controls, the IS Auditor may conclude that the reliance on controls is no longer appropriate in which case he should restate reliance to Low. This will necessitate more extensive substantive testing.

3.6.2.3 Substantive Test

A Substantive test substantiates the integrity of actual processing. It involves obtaining audit evidence on the completeness, accuracy or existence of activities or transactions during the audit period

In determining the level of substantive testing required, the professionals should consider the:

- Assessment of inherent risk
- Conclusion reached on control risk following compliance testing

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

3.7. Risk based Auditing

In a risk based audit, controls that address specific audit risks are identified and tested. The process normally begins with the identification of what can go wrong or risk statements that could prevent the achievement of the desired audit objectives, and proceeds to listing control objectives and ultimately preparing a work plan for testing the controls that address these risks.

The principle of the risk based approach in IT Audit is the same as for the other types of audit. This will typically entail the auditors performing the following:

- ➢ Gather information and plan
  - ✓ Knowledge of business and industry
  - ✓ Prior year's audit results
  - ✓ Recent financial information
  - ✓ Information systems and projects under implementation
  - ✓ Regulatory status
  - ✓ Inherent risk assessments
- ➢ Obtain an understanding of IT risks and internal controls
  - ✓ IT Control environment
  - ✓ Control procedures
  - ✓ Detection risk assessment
  - ✓ Risk assessment
  - ✓ Risk ranking and categorisation
- ➢ Perform compliance tests
  - ✓ Identify controls to be tested
  - ✓ Perform tests on reliability, risk prevention and adherence and organisational policies and procedures

- Perform substantive tests
  - ✓ Analytical procedures
  - ✓ Detail tests of account balances
  - ✓ Other substantive audit procedures
- Conclude on the audit
  - ✓ Create recommendations
  - ✓ Write audit report

According to WGITA, the following are the Steps in Risk-based approach for an IT Audit:

1. Identify the audit universe that would comprise the listing of all auditable organisations or units falling under the jurisdiction of an SAI.
2. List the information systems in use in the auditable organisation/units.
3. Identify factors that impact the criticality of the system for the organisation to carry out its functions and deliver service.
4. Assign weight to the critical factors. This could be carried out in consultation with the audited organisation.
5. Compile information for all the systems, across all organisations and based on cumulative scores, place the systems/ organisations in order of priority for audit.
6. Prepare an annual audit plan that should outline the priority, approach and schedule of IT Audits. This exercise could be done at annual intervals and thus could be a recurring plan.

3.8. Why risk based auditing?

The approach of risk based auditing assists the auditor in making the decision to perform either compliance testing or substantive testing. This approach assists the auditor in determining the nature and extent of testing to be carried out during the audit.

3.9. Documenting Risk Assessment

When determining the area to be audited the auditor should evaluate risks and determine the high-risk areas that should be audited. There are many risk assessment methodologies. These range from simple classification of high, medium and low, based on the IS auditor's judgment to scientific calculations that provide numeric risk rating. Outlined below is an example of how the auditor can assess risk using a risk register.

A risk register is a repository of the key attributes of potential and known IT risk issues. Attributes may include name, description, owner, expected/actual frequency, potential/actual magnitude, potential/actual business impact, disposition.

Once risk has been identified and estimated, the auditor should evaluate the risk. During the risk identification process the IS auditor identifies assets, threats, existing control, vulnerabilities and consequences. The risk estimation process involves:

- Assessment of the consequences
- Assessment of incident likelihoods and
- Quantitative /qualitative risk estimation.

A risk register can vary from simple to complex but in most cases, they include the following:

Risk Statement

A description of the current conditions that may lead to the loss, and a description of the loss. Source: Software Engineering Institute (SEI). For a risk to be understandable, it must be expressed clearly. Such a statement must include a description of the current conditions that may lead to the loss and a description of the loss. An example of a risk statement is as follows:

Because emergency changes are not being documented or approved, there is a risk that unauthorized changes to the system can be made in the production environment.

Likelihood

Probability of the occurrence of an event. The probability of occurrence of event can be classified as high, medium or low.

Impact Rating

Rating of risk based on high, medium or low. This is based on the assessment of the impact of a risk on a particular area and is normally classified as high medium or low.

Mitigation Controls

These are action to reduce the frequency and/or impact of a risk.

Residual Risk.

The remaining risk after management has implemented risk response. Where adequate mitigation controls have been put in place then the residual risk can become medium or low depending on the circumstances.

The audit focus in the risk based approach would be to cover areas with high risk.

An example of a risk register is outlined below:

Risk	Likelihood	Impact	Compensatory Controls	Residual Risk
Logical Access Controls: There is risk of unauthorized changes being made because of weak access controls	Medium	High	Satisfactory	Low

3.10. Summary

A central theme of the risk-based audit standards is iterative planning. A key component of risk-based audits is the IT risk assessment deliverable, which is considered by the audit team when determining what, if any, further audit procedures are needed to sufficiently lower audit risk to an acceptable level. The risk-based auditing standards clearly advocate continuous planning with respect to new information discovered during the audit. The risk assessment phase activities and report, however, are static. The IT risk assessment may identify controls that, if determined through testing to be operating effectively, could reduce audit risk for one or more assertions as well as the financial statement level. During this step, the IT auditor's risk assessment report should become a key and active component of audit planning. The goal is to determine if any further audit procedures are needed with respect to IT and risks of material misstatement.

4. CHAPTER 4: UNDERSTANDING IT CONTROLS

4.1. What are controls?

The IT auditor to evaluate and monitor IT controls that are integral part of the IT control environment of the organisation. The auditors should assist management by providing advice regarding the design, implementation, operation and improvement of IT controls.

Controls are all the methods, policies and procedures that ensure protection of the organisation's assets, accuracy and reliability of its records, and operational adherence to management standards.

The auditor needs to distinguish between general controls and application controls. General controls set the environment in which the IT systems are developed, operated, managed and maintained in terms of a few control procedures. Examples of general controls include the development and implementation of an IS strategy and an IS security policy, the organisation of IS staff to separate conflicting duties and planning for disaster prevention and recovery.

Application controls are specific controls unique to each computerised application. They apply to application segments and relate to the transactions and standing data. Application controls include data input validation, encryption of data transmitted, etc. For example, in an online payment application, one input condition could be that the credit card expiry date should fall beyond the date of the transaction, and details entered should be encrypted.

Applications are specific software that may include both manual and computerised procedures for transaction origination, data processing, record keeping and report preparation. An application can be divided into the following segments: data input (data origination and data entry); data communication; processing; data storage (incl. Master data); output and distribution of results.

Real time systems are applications where processing and updating of databases happen immediately with data entry. For example, users can enter transactions at a workstation and see an immediate effect on the account, i.e. the accounts are updated whenever a user enters a transaction. Real time systems allow users to improve the timeliness of management information. However, they don't include traditional controls such as batch totals.

Authorisation is the act of first comparing a proposed transaction with plans, conditions, constraints, or general knowledge of what constitutes property and then deciding if the transaction is valid and in accord with management intentions.

Validation is the act of establishing the truth, accuracy, or relevance of an amount or fact by corroborating it through re-performance, vouching, confirmation, or reconciliation. In computer programs, procedures or routines can validate data as it is entered.

4.2. Overview of general control and application controls

General controls represent the foundation of the IT control structure. It helps ensure the reliability of data generated by IT systems and support the assertion that systems operate as intended and that the output is reliable. AFROSAI-E developed a general control checklist which covers the following areas:

- IT governance
- Security management

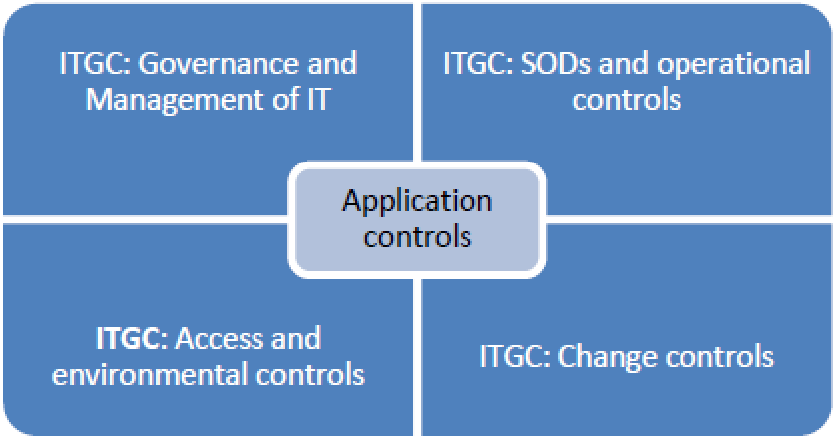
- Program change management Physical access control
- Environmental controls
- IT service continuity
- Logical access controls

Application controls are fully automated controls designed to ensure the complete and accurate processing of data, form input through to output. Application controls include:

- Completeness checks
- Validity checks
- Identification
- Authentication
- Authorisation
- Input controls
- Output control

4.3. Relationship between General IT Controls and Application Controls

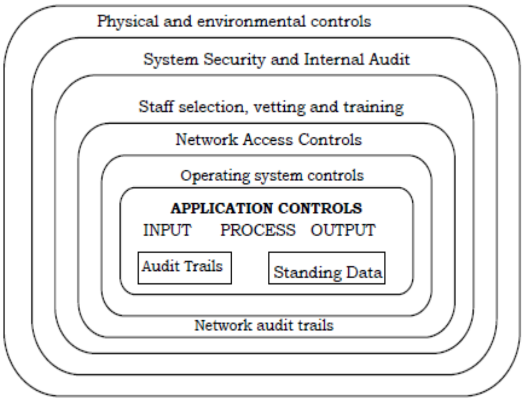
IT controls are divided into two categories, general controls and application controls. The categories depend upon a control's span of influence and whether it is linked to any particular application.


ITGC: Governance and Management of IT
ITGC: SODs and operational controls
Application controls
ITGC: Access and environmental controls
ITGC: Change controls

At the boundary, there are general controls (ITGC) that include IT governance, separation of duties, access rules and change procedures that establish a framework for overall control of the IT activities. They act as foundation onto which specific application controls can be added.

At the application-specific level, there are controls to authorise and validate transaction origination (input controls), ensure accurate and complete processing (processing controls) and generate validated outputs (output controls) that together form the application controls. In financial systems, these are specific control procedures over the accounting applications which can provide assurance that all transactions are authorised and recorded, processed completely, accurately and on a timely basis. Application controls may consist of manual procedures carried out by users (user controls) and automated procedures performed by the computer software.

The IT controls framework


Physical and environmental controls
System Security and Internal Audit
Staff selection, vetting and training
Network Access Controls
Operating system controls
APPLICATION CONTROLS
INPUT
PROCESS
OUTPUT
Audit Trails
Standing Data
Network audit trails

The design and implementation of IT general controls can have significant impact on the effectiveness of the application controls. In a way, general controls provide the applications with the resources they need to operate and ensure that unauthorised changes cannot be made to either the applications (i.e. they protected from reprogramming) or the underlying databases (the large collection of transaction data). Meanwhile, the application controls operate on individual transactions and ensure that they are correctly input, processed and output.

We can think of the layers of control being concentric (like an onion) in which we start in the middle of the onion with the financial statements and work our way out through successive layers of control. These layers, when put together should reduce the risk that the financial statements will contain material errors due to IT control risk.

4.4. IT General Controls

The general controls are the foundation of the IT control structure. These are concerned with the general environment in which the IT systems are developed, operated, managed and maintained. General IT controls establish a framework of overall control for the IT activities and provide some assurance that the overall control objectives are satisfied. Also included in general controls are pervasive controls. These controls are designed to manage and monitor the IT environment and therefore, affect all IT related activities.

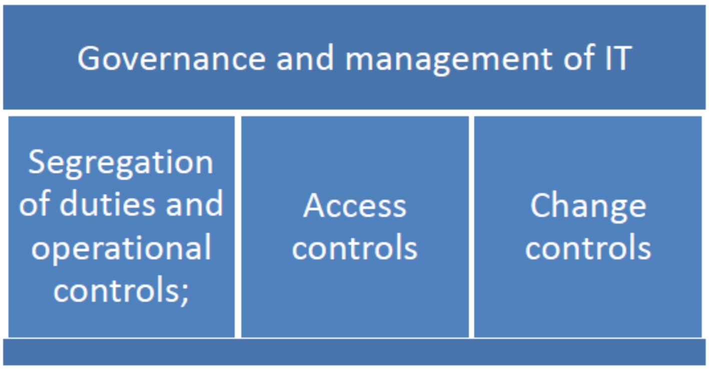
General IT controls are concerned with the entity’s IT infrastructure, including any IT related policies, procedures and working practise. The control procedures would govern segregation of duties, usage of IT assets, acquisition and maintenance of IT application, access controls and data centre operations.

These controls are not specific to individual transaction streams or particular accounting packages or financial applications.

The auditor’s primary role is to deliver assurance on internal controls operating in an entity. Where the entity operates in an IT environment, the auditor needs to evaluate the design, implementation and compliance with the IT control framework. Every control area is based on a set of control objectives that seeks to mitigate a control risk, and the auditor needs to assess whether the deployed controls are adequate to meet the objective or not. In case of general controls, it is important for the auditor to understand the broad categories and extent of general controls in operation, evaluate the management attention and staff awareness in the organisation for the same, and find out how effective the controls are in order to deliver assurance. If general controls are weak, they severely diminish the reliability of controls associated with individual's IT applications.

4.4.1 Major categories of general controls:

The major categories of general controls are shown in figure below:

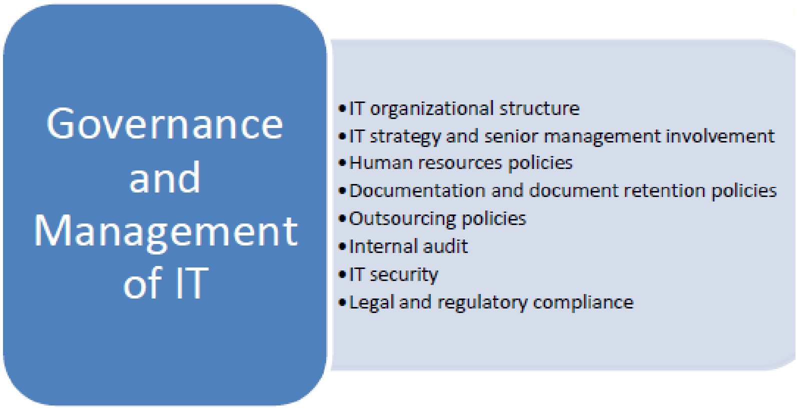

Governance and management of IT
Segregation of duties and operational controls;
Access controls
Change controls

4.4.1.1 Governance and management of IT

This is an integral part of the organisation's governance and consists of the leadership and organisational structures and processes that ensure that IT systems sustain business goals and strategy. At a broad level, the general controls have a top down flow driven by the Governance and management of IT. It lays down the control environment and sets the foundation for establishing sound internal control practices and reporting at functional levels for management oversight and review.

The higher-level controls set by management defined policies sets the tone at the top in terms of attention. Auditors need to understand and evaluate the different components of the IT governance structure to determine whether the IT decisions, directions, resources, management and monitoring support the organisation's strategies and objectives.

To carry out the assessment, the auditor needs to know the key components of IT governance and management. The auditor needs to be aware of the risks associated with the inadequacy of each component in an entity.


Governance and Management of IT
•IT organizational structure
•IT strategy and senior management involvement
•Human resources policies
•Documentation and document retention policies
•Outsourcing policies
•Internal audit
•IT security
•Legal and regulatory compliance

The first two components i.e. IT organisation structure and IT relate to the governance structure which enables a foundation for design and alignment of IT strategy and processes to the business objectives.

Control objectives - To ensure that in IT infrastructure planning, implementation and maintenance, there exists an active involvement of senior level management so that IT is given the proper recognition, attention or resources it requires to meet business objectives.

Control risk - In absence of proper top management involvement in drawing up of IT strategy, allocation of resources through structured steering committee procedures, there is an inherent risk of the IT function not serving the business needs. This may give rise to problems with the financial systems being unable to meet new reporting requirements (which may occur due to a change in national accounting standards, or a change in government requirements).

Poor reporting structures leading to inadequate decision making - This may affect the client's ability to deliver is services and may affect its future as a going concern (one of the fundamental accounting principles).

Inappropriate or no IT planning leads to business growth being constrained by a lack of IT resources.

HR policies

The extent to which the information systems can support business objectives of an entity depend on the human resources that make the system work.

Control objective - To ensure that organisation has put sound staffing and training procedures in place to reduce the risk of errors, omission and commissions made by the entity staff.

This would be achieved by putting in place:

- Organisational charts laying down clear job descriptions of all staff including IT staff. These should depict lines of reporting and management. The charts enable all staff to know how they fit in, and whom to inform when problems are encountered. Staff planning policy to ensure that there are enough appropriately skilled personnel to run different applications / modules in the current systems as well as meet future staffing requirements.

- Staff recruitment policies for employment of permanent staff, temporary staff, contractors and consultants. These include background checks, confidentiality agreements, and codes of conduct. New employees should be made aware of their roles and responsibilities in respect of security matters.

- Training policy on the basis of assigned roles and incremental / planned change to IT infrastructure. IT training is often costly and should be controlled by training plans and budget.

- Conditions of engagement including code of conduct, job rotation, special controls and vacation policies. Special contracts are entered when IT departments call specialists, contractors and consultants for once off jobs. There should be policies which require those on special contracts to adhere to established policies and procedures.

- Staff assessment policies for incentives / promotions/ demotions based on predefined measurable criteria. The assessment procedures should be seen to be fair and equitable and understood by all employees.

- Termination policies that define the steps to be taken when an employee's services are no longer required. These should address voluntary termination / involuntary / immediate termination and include security measures.

- Notification of other employees: Arrange final pay routines to ensure that that person is removed from the payroll; return of company property, including personal laptop computers, pagers.

Control risk - In the absence of a well-designed HR policy and procedure, there may be repeated instances of data loss, high frequency of data errors, unauthorised data and program amendments, system unavailability and lack of business continuity attributable to error and omissions caused by people due to incomplete understanding of job roles, fraud, hardware /software failure and high staff attrition.

Documentation and document retention policies

Documentation of information systems, applications, job roles, reporting systems and periodicity is an important reference point to align IT operations with business objectives.

Appropriate documentation retention policies enable tracking and managing iterative changes to information architecture in an entity.

Control objective - Proper documentation of the information architecture and job roles, reporting systems, and periodicity is an important reference point to align IT operations with business objectives. Appropriate documentation retention policies enable tracking and managing iterative changes to information architecture in an entity.

Control objective- Proper documentation of the information architecture and job roles aim to ensure that standardised work practices are followed for each job role and incidences / maintenance and iterative changes to the architecture can be managed without inhibiting business processes.

The entity needs to have a policy on documentation of systems, processes, job roles that emphasises on updating, version control, backup and retention. Entities that have adopted quality certifications would have policies on document production, approval and issue, as well as on policies on controlling changes to existing documents.

Apart from requirement for documentation retention that provide audit trail for independent assurance on internal controls and financial reporting, there may be other, non-audit requirements, which require the client to retain transaction documentation, e.g. customs regulations, taxation regulations, and company legislation requirements.

Control risk - The risks associated with inadequate documentation policies include unauthorised working practise being adopted by IT staff, increase in the number of errors being made by operations staff; higher recovery time from disruptions. For example, if a client's network is not adequately documented and a problem occurs with the wiring, those tasked with carrying out repairs would have difficulty in locating where the failure had occurred.

Outsourcing policy

IT outsourcing allows the entity management to concentrate their efforts on core business activities, the need for outsourcing may also be driven by the need to reduce running costs.

Control objective - Where an entity outsources or intends to outsource its IT activities it needs to ensure that IT activities remain aligned with business objective, security, confidentiality and availability of data is protected, and there is no disruption to business processes.

The objective is met by the entity building in the considerations of availability, integrity, confidentiality and security of entity data along with the entity's exclusive ownership of the data into the contract agreement with the outsourcing partner. Wherever the entity enters into an outsourcing model where responsibility for some business operations is assigned to the partner, the management retains ultimate accountability for the effectiveness of that outsourced environment and for developing and implementing appropriate controls and processes internally.

Control risk - In absence of appropriate outsourcing policy and procedures, the entity faces the risk of non-availability of operational/financial data, lack of security of data and data integrity, breach of confidentiality, disruption to business continuity and loss of goodwill.

Internal audit

Management has ultimate responsibility for ensuring that an adequate system of internal controls is in place.

Control objective - The management needs to obtain periodic assurance that the different controls related to the business processes working in an IT environment, are in place, are followed at the related operational levels and are adequate to cover the risk of IT functions becoming misaligned with business objectives.

For the purpose, the management puts policies and procedures in place to obtain assurance on adequacy of by relying on the review work carried out by internal auditors.

The external auditor can review the client's internal audit function as part of the overall control structure (since they prevent, detect and correct control weaknesses and errors). An assessment will enable the external auditor to decide if they can use or place reliance on internal audit's work.

Control risk - In absence of adequate internal audit involvement, the management may not be able to obtain timely, reliable, periodic information about the adequacy of and compliance to the control framework established throughout the organisation.

IT security policy

It is important that the entity establishes an IT security policy for protection of information assets which clearly states the organisation's position.

Control objective - The top management of the entity needs to define the security framework that enables detailed physical and logical access controls for different categories of information assets in a consistent manner.

IT security policies are normally expressed in the form of a concise narrative, i.e. a few pages of text. The policy requires senior management approval if it is to have any weight, and consequently should be approved at board level or equivalent. The policy should be available to all employees responsible for information security. Where the entity has operational staff with access to IT systems the policy should lay down the elements:

Elements of an IT security policy	➢ Definition of information security (objectives and scope including data confidentiality) ➢ Detailed security principles, standards and compliance requirements ➢ IT department personnel should not have operational or accounting responsibilities ➢ Definition of general and specific responsibilities for all aspects of information security ➢ Use of information assets and access to email, internet ➢ Mode and method of access Backup procedures ➢ Procedures to deal with malicious software /programs ➢ Elements of security education and training Process for reporting suspected security incidents Business continuity plans ➢ Methods of communicating to staff the policy and procedures adopted for IS security

Responsibility for IT security is normally assigned to a security administration function. In smaller clients this function may be a part-time job carried out by a member of staff known as the IT security officer. Larger clients would be expected to have dedicated IT security personnel.

Legal and regulatory compliance

The legal and regulatory requirements may include;

- Data protection and privacy legislation to protect personal data on individuals'
- Computer misuse legislation to make attempted computer hacking and unauthorised computer access a criminal offence
- Banking and finance regulations, where banks may have to undergo regular reviews if they wish to continue operating; and
- Copyright laws to prevent he theft of computer software

The entity should be aware of the legal requirements at the location (s) in which it operates and take appropriate measures to ensure compliance.

Control risk - Non-compliance could result in action varying from a warning letter to prosecution or even closure of the business.

4.4.1.2 Segregation of duties and operational controls

The organisation needs to define jobs roles in a manner that implements a division between tasks and responsibilities at different staff levels/functions.

Control objective - The basic idea underlying segregation of duties (SoD) is that no employee or group of employees should be in a position both to perpetrate and to conceal errors or fraud in the normal course of their duties. Separation of duties is a proven way of ensuring that transactions are properly authorised, recorded, and that assets are safeguarded. Separation of duties occurs when one person provides a check on the activities of another.

4.4.1.3 Access Control

Access control is a security technique that can be used to regulate who or what can view or use resources in a computing environment. It is dividend in two main types: Physical and logical access controls. Physical access control limits access to building, group of buildings, rooms or computer-based IT system. Logical access limits connections to computer networks, system files and data.

In a government environment, access control is important because many government entities process sensitive data and privacy concerns limit who should view various parts of the information. Access control ensures that only users with the process credentials have access to sensitive data.

4.4.1.4 Change Controls

Change control is a systematic approach to managing all changes made to a product or system. The purpose is to ensure that no unnecessary changes are made, that all changes are documented, that services are not unnecessarily disrupted and that resources are used efficiently.

4.4.2 Effect of pervasive controls on the audit

The auditor should also take into consideration the effect of pervasive controls during the audit. Pervasive controls can be defined as those controls which are designed to manage and monitor the information systems environment and therefore affects all IS – related areas.

ISACA auditing guidelines states that auditors should perform a preliminary assessment of the controls over the function which they will be auditing. This preliminary assessment should include identifying and evaluating the effect of pervasive controls. During the planning of the audit the auditor will need to identify all pervasive controls which are applicable to the different audit objectives and will need to ensure that there are sufficient procedures to address all the applicable pervasive controls.

If the pervasive controls have a significant impact on the audit objective, the auditors' audit plan cannot only focus on the detailed controls but should also address the pervasive controls. Where it is impossible to test the pervasive controls (or where it is not practical), auditors need to report the limitation of the scope of the audit.

Where the auditor finds that pervasive controls are satisfactory, they can reduce the number of detailed control testing, since the strong pervasive controls will contribute to the assurance which may be obtained by auditors in relation to the detailed control. However, where the pervasive controls are not satisfactory, auditors need to increase the number of detailed control tests to obtain sufficient evidence that the controls are working efficiently.

When reporting the audit results back to the management of the audited entity, auditors should also address the weaknesses found in pervasive controls, even though the controls were not part of the original scope of the audit.

In cases where pervasive controls are significant to the detailed controls but the pervasive control was not tested by the auditors, auditors need to bring this to the attention of management together with a statement of the potential effect on the audit findings, conclusions and recommendations.

For example, if the auditors were auditing the acquisition of a new software package or the development of the package and did not find an IT strategy document, then the auditors need to report to management that the IT strategy document was not available for review or does not exist. The effect of the lack of the IT strategy would be that IT investments may not be aligned to business objectives. It should be however noted that in such a case of missing strategy or policy, the auditor should review and document ICT management practices and resource allocation to assess whether it is aligned to business objectives.

4.4.3 Knowledge of key documents to assist completing the general computer controls review

There are various documents the auditor can request to gain an understanding of the entity and the IT environment in which it operates:

IT strategy - an IT strategy describes how the IT department can assist the organisation in achieving its objectives and is an integral part of the business strategy. The IT strategy relates to the long-term direction an organisation wants to take in leveraging IT for improving business processes.

IT budget: The current budget should be reviewed to establish whether it's sufficient and whether IT activities are prioritized.

IT governance structure - this include the most recent organisation chart of the organisation, job descriptions for the key IT positions. Key IT positions include:

- System administrator
- Security administrator
- Database administrator
- Systems analyst
- Application programmers
- System programmers

To evaluate the performance of an IT system, an IT auditor will be required to get some preliminary information. The knowledge of entity working paper contains some of the preliminary information that an IT auditor can obtain

4.5. IT Application controls

Controls embedded in business process applications are commonly referred to as application controls.

Application controls refer to controls over the processing of transactions and data within an application system and, therefore, are specific to each application. While the general IT controls in an entity set the tone for the overall control environment for the information systems, application controls are built into specific applications to ensure and protect the completeness, accuracy, validity, integrity, reliability and confidentiality of information. Therefore, the objectives of application controls generally involve ensuring the:

- Data prepared for entry/input are complete, valid and reliable
- Data converted to an automated form and entered into the application accurately, completely and on time
- Data are processed by the application completely and on time, and in accordance with established requirements;
- Output is protected from unauthorised modification or damage and distributed in accordance with prescribed policies.

4.5.1 What Application Controls include

Application controls do include manual procedures which operate in proximity to an application. These controls are not only built into specific applications, but also surrounding business processes. For example, a data entry clerk may require a data input form to be signed before it is entered onto the system. The combination of manual and automated controls chosen is often a result of cost and control considerations at the design stage of an application.

4.5.2 Importance of Application Controls

The application controls have an important role in the information processing environment to ensure confidentiality, integrity and availability of information. In an entity where the general control environment is reasonably well laid, the auditor needs to obtain an assurance that transactions are properly initiated, authorised, processed, and recorded. Since application controls are closely related to individual transactions it is easier to see why testing the controls will provide the auditor with assurance on the accuracy of a particular account balance. The auditor may also need to evaluate whether the manual activities necessary to supplement and support the automated activities are being completed appropriately.

For example, testing the controls in a payroll application would provide assurance as to the payroll figure in a client's accounts. It would not be obvious that testing the client's general IT controls (e.g. change control procedures) would provide a similar level of assurance for the same account balance.

4.5.3 Application control objectives

Application controls seek to provide assurance that management's business objectives relative to a given application are achieved. It is done by ensuring that data preparation and entry is authorised, complete, valid and reliable, data integrity is maintained through processing; output is protected from unauthorised modification and is distributed in accordance with prescribed policies

4.5.4 Application categorisation

Automated solutions implemented will typically take one of the following forms:

- Management information systems - these solutions are designed to automate the collection and processing of information related to the execution and financial aspects of the enterprise core activities, but also relate to the collection and processing of information about enterprise processes, resources and customers. Common examples include integrated enterprise resource planning (ERP) systems that automate the collection and processing of financial information and the data warehouse or similar executive information systems/ decision support systems (EIS/DSS) used to support business decision making.

- Process automation system - these solutions are designed to automate the specific activities within the process. An example of process automation is a robotic system used in automobile industry.

It is important for auditors to understand application categorisation in terms of processing routines to be able to identify and evaluate application controls which are specific to each category. The two broad categories are batch data entry systems and real-time systems. The former is normally associated with legacy financial systems. Transactions are normally passed by users to a central IT or finance data input section, where they are batched up and entered into the computer in batches. In real time systems, users and enter transactions at a workstation ad see an immediate effect on the account balances, i.e. the accounts are update whenever a user enters a transaction. Real time systems allow users to correct errors immediately and improve the timeliness of management information. However, they don't include traditional controls such as batch totals.

4.5.5 Categories of application controls

Application security controls	Input controls	Processing controls	Output controls	Masterfile and standing data controls
Logical access controls (allocating different privilege levels and menus to individual users Automated activity logs Management and audit trails	Data entry / field validations (e.g. validation of entered credit card numbers) Work flow rules (e.g. routing and signoff of purchase request) Field entries being enforced based on predefined values (e.g. pricing information)	Business rules Automated calculations Management and audit trails	Reconciliation Review and follow-up of application generated exception reports	SODs built into applications

4.5.5.1 Data input controls

Irrespective of whether a financial system is manual or computer based, the validity of entries is best ensured by some method of authorisation.

Control objectives

The input controls seek to validate and authenticate the acts of source data preparation, authorisation and entry so that accurate, reliable and complete data is accepted by the application in a timely manner.

A significant proportion of these measures are designed at the development stage of an application during different stages of systems development after the business rules are laid down at the requirements definition. While data input can be manual, or system interface driven, errors and omissions can be minimised through good input form design, adequate segregation of duties regarding the origination and approval of input documents, and plating relevant authenticity, accuracy and completeness checks (with menu options or interactive message).

Elements of input controls

Authorisation of input	Manual procedure/ supervisory level authorisation of data on data entry form. E.g. authorisation of bill of entry details by for processing in customs applications
Completeness of input data	Completeness check to ensure that all the key transaction information has been entered before the transaction can be posted to the accounts. E.g. in an online ticketing application, date of journey/nature of ticket/ names of passenger/ identity numbers are key fields without which transaction would be rejected by the system
Data input validation	Automated validity checks on the data presented to the system. E.g. journey data falls outside the booking open period.
Duplicate checks and matching	Comparing new transactions with transactions previously posted to the same account. E.g. check against duplicate invoices.
Matching procedure for dealing with rejected input	Subsequent correction measures /prompts enabling re-input. E.g. clearance of suspense items

Input control risk

In absence of proper input controls, there is a risk of erroneous or fraudulent processing and that the application would not be able to deliver business objectives.

With real time processing systems, some of the control measures like reconciliation of input and output of batch totals for ascertaining completeness of input, retention of data origination documents for audit trail are not available. However, real time systems embed other compensating controls within the application like interactive data completeness / validation prompts, logging of access attempts, etc.

4.5.5.2 Processing controls

Control objectives

These are measures that seek to protect data integrity, validity and reliability and guard against processing errors throughout the transaction processing cycle - from the data is received from the input subsystem to the time data is dispatched to the database, communication or output subsystem. They ensure that valid input data is processed only once and that detection of erroneous transactions do not disrupt the processing of valid transactions. They seek to enhance the reliability programs that execute instructions to meet specific user requirements.

The control procedures include establishing and implementing mechanisms to authorise the initiation of transaction processing and to enforce that only appropriate and authorised applications and tools are used. They routinely verify that processing is completely and accurately performed with automated controls, where appropriate. They control types may include checking for sequence and duplication errors, transaction /record counts, referential integrity checks, control and hash totals, range checks and buffer overflow.

In real time systems, some of the compensating controls would be one for one checking, retrospective batching exception and suspense account reporting.

Control risk

Processing errors may emerge due to wrong mapping of business rules, inadequate testing of program code, or inadequate control over different versions of programs to restore integrity of processing after a problem occurs. In absence of necessary processing control practices, there could be repeated erroneous transactions affecting business objectives and goodwill.

4.5.5.3 Output controls

Control objectives

Output controls are measures built into the application that seek to protect data processed by an application from unauthorised modification and distribution.

The control processes include proper definition of outputs, desired reports at the system design and development stage, proper documentation of report extraction logic, controls limiting access to processed data, output review, reconciliation and review.

Control risk

In absence of adequate output control measures there is a risk of unauthorised modification/deletion of data, creation of wrongly customised management reports and breach of data confidentiality.

4.5.5.4 Master files/ standing data controls

Master files are data files which contain semi-permanent financial or reference data which may be used by several applications to process. The data stored in the master file is known as standing data. Applications call upon the reference data in master files to process their transactions.

For example, a master file may contain standing data on the price of goods for sale. When a sale is made the application requires the user to enter the variable transaction data such as the quantity of goods sold. The application then calls upon standing price data in a master file and combines the unit price with the quantity of goods sold. The application then calls upon standing price data in a master file and combines the unit price with the quantity to get the total value of the sale.

Standing data may include pay rates for each grade; supplier details (reference number, address, telephone number, and credit terms); customer details; employee bank account numbers; inflation rates and indices, overhead rates, system administration data.

4.5.5.5 Use of standing data

Due to the nature, standing data is used to process many transactions. For example, the VAT standing data may be used to determine tax liabilities on hundreds or thousands of organisations transactions. The client should have controls in place to ensure that amendments to standing data are authorised; users are held accountable for any changes made; the standing data is up to date and accurate; and the integrity of the master files is maintained.

As standing data errors have a far-reaching effect it is normal for controls over the data to be more stringent than controls over individual transactions.

4.5.5.6 Master file control processes

The types of controls a client may use to protect standing data have already been covered in this module, i.e. physical and logical access controls. These controls should ensure that only authorised users can gain access to, create, amend or delete standing data.

The controls may be implemented at both the application level and the installation level. Individual transactions have to be authorised and the same principal applies to changes to master file data. Hence the client should have procedures and controls for making amendments to master file data. These may include filing out data amendment and another user commits the amendment using automated permissions.

Audit logs are useful as they can help identify individual users who make unauthorised amendments. Ideally the audit log should record what records or fields were amended, when they were amended, from what to what, and who made the amendment.

4.5.6 User categorisation and application security controls

To map the application security control process the auditor needs to understand the roles of responsible actors dealing with an application. The three principal entities are application owner (having overall responsibility for the strategic contribution the system makes to business objectives e.g. finance manager for an accounting application), application administrator (responsible for access, support and security functions and reports to the application owner) and system user (having limited access privilege to particular modules/routines). The application security controls limit access for different user categories; create transaction and activity logs for audit trail.

The auditor needs an understanding of the nature of processing routine of the input data (batch entry/real time), the transaction flow ad outputs, the major transactions involved and data files maintained, and the volume of transactions. The auditor should use judgment when assessing the application controls and should be careful when putting forwards recommendations for improvements. Excessive details in transaction logging may add to entity cost overheads, and may not indicate desired trails. Where an entity uses off the shelf financial packages with standard access control mechanisms, the auditor should ascertain what access controls are available and determine whether the client has configured them properly in sync with defined SODs.

Implement effective identification and authentication mechanisms

Entities should have application security policies and procedures in place concerning user identification and authentication. Management should have created an environment where all users have their own unique IDs and passwords, or other mechanisms, such as tokens and biometrics to access any part of the information system and applications that allow them to execute functional responsibilities in line with their job descriptions. In addition, it is important to understand the mechanisms used to assign access privileges for applications under assessment. An evaluation of identification and authentication controls includes consideration of the following factors:

- How do the users access the application?
- Are users required to enter user name/ID and password for each application?
- Do all users have an individual and unique ID that would allow the user's activities to be recorded and reviewed?
- What are the password parameters (i.e. length character requirements, etc)?
- How often does the application require the user to change the password?
- Are there any instances of users having multiple IDs and passwords?
- Are there any instances of users sharing IDs or passwords?
- What other IDs and passwords does the user have to enter before accessing the sign-in screen for the application?
- Does the user enter a network ID and password?
- Does management maintain and review a current list of authorized users?
- Does management periodically review the user list to ensure that only authorized individuals have access, and that the access provided to each user is appropriate?
- Is public access (non-entity employees) permitted to the application?
- Is access permitted via the Internet? If so, how is this access controlled?

The knowledge of the application security design and function enables the auditor to assess the effectiveness of the security controls over the other levels of authentication, especially when weaknesses are identified at the application security layer, as those weaknesses may be mitigated by stronger controls at other levels.

4.5.7 Audit Trails

Audit trails provide a chronological record of user activities. They can be used to document when the user logged in, how long the engaged in various activities and what they were doing. Management should decide on the activities to be logged as maintaining a record of every activity can consume computer resources. The auditor should establish the following amongst other things:

- The type of activities which are logged in the system
- Are security logs created and reviewed?

- Are the transactions/logs reviewed by the business owners?

- Does management monitor access within the application (i.e. unauthorised access attempts, unusual activity etc.)?

- Does the application generate reports to identify unauthorized access attempts?

4.5.8 System Administrator's authority and responsibility

A Systems Administrator is a person responsible for administering use of a multiuser computer system, communications system, or both.

Since data management systems are supported by one or more operating systems, the auditor should obtain an understanding of the role of the data management system administrators. There should be a distinct segregation between the data management system administrator and the operating system administrator. The operating system administrator may need access to the data management system, but should have limited access. Likewise, the data management system administrator may need access to the underlying operating system, but should have only the access necessary to manage the data management system functionality.

The auditor should also evaluate the segregation between the data management system administrator and personnel in charge of reviewing audit and transaction logs.

The data management system administrator should not have access to the audit logs within the data management system. These logs should be reviewed by a security administrator.

There should also be a separation between the functional aspects of the data management system environments. Data management system access should be consistent with the functional separation of duties within the application environment. Users that are developers should have access to the development environment only, and consequently only the development data management system. Users that require access to production should only have access to the production data management system.

5. CHAPTER 5: OVERVIEW OF PLANNING

In today's environment, IT audit plays a substantial role in most financial audits. In most organisations, IT controls are very important and the IT auditor must come in at the planning phase of the audit to evaluate IT controls to determine whether a controls reliance audit approach can be used.

During an IT Audit, the auditor will assess the general and application control environment to determine whether reliance can be placed on the controls or if additional testing needs to be performed. The result of this assessment should be communicated adequately to the financial (or other) auditor so that the financial audit takes the findings into consideration in their audit approach. As discussed in the previous session on risks, a risk based audit approach is used to assess risk and to assist the auditor's decision to either take a compliance testing or substantive testing audit approach.

The IT auditor should understand the overall audit objective as the nature, timing and extent of IT audit procedures vary depending on the audit objective. As mentioned in Chapter 1, the different types of IT audits have varying overall engagement objectives. If the audit is in support of a financial or other audit, the IT Auditor needs to have an understanding of the objectives of such audit.

The first step outlined in the risk based approach in chapter 3 of gathering information and planning. The auditor must gain an understanding the entity's key operations and key business processes. To plan an audit, the auditor obtains a general understanding of the entity's IS infrastructure, which include review key organization documents including:

- IT strategy and policy documents
- IT function's organization structure
- IT budgets and operational plans
- Qualifications and competence of key IT staff
- IT system designs, blue prints, user manuals and business process procedures

The review of these documents helps the auditor in having a detailed understanding of business rules, transaction flows and application module interactions. The auditor will then identify the key critical control points in the design of the entity's information systems based on the auditor's understanding of such systems.

5.1. What Audit Standards is related to the Evaluation of Internal Controls by the Auditor

ISSAI 1300 deals with the auditor's responsibility to plan an audit of the financial statements. The standard requires the auditor to perform preliminary audit activities in understanding the entity (ISSAI 1210), effectively managing the relationship with the auditee and evaluating the compliance to ethical requirements (ISSAI 1220). In addition, the standard requires the auditor to complete an overall audit strategy for the audit, and an audit plan. The audit plan will be discussed in a later chapter.

ISSAI 1315 deals with the auditor's responsibility to identify and assess the risks of material misstatement in the financial statements, through understanding the entity and its environment, including the internal control. The standard requires the auditor to obtain an understanding of the internal control which is relevant to the audit. Although most controls relevant to the audit are likely to relate to financial reporting, not all controls that relate to financial reporting are relevant to the audit (par. A 42 - A65). Furthermore, the standard also requires the auditor to obtain an understanding of the information systems, including the related business processes, relevant to financial reporting (par. A81 - A85)

5.2. The Audit Process Flow

In the performance of system reviews, IT auditors are likely to encounter two scenarios, and these are;

- IT auditors performing a purely IT system review e.g. System development audit or network security review

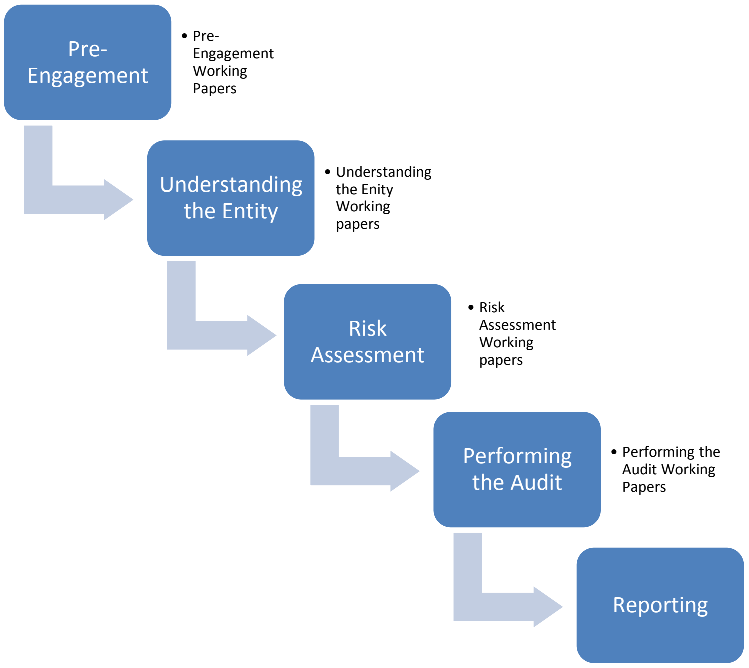
- IT auditors performing an integrated audit with Regulatory, Performance or compliance auditors

The audit process flow followed by IS auditors in both scenarios follows typically the same stages as the financial or other audit process.

Template working papers have been drafted to incorporate IT related issues that were not previously captured in other working papers. This is in a quest to ensure that both the IT and Non-IT control and risk thereon are adequately evaluated at all stages of the audit.

The working papers (templates) when completed adequately will ensure full compliance with the requirements of ISSAIs and other internationally accepted standards.

The following are the stages and proposed working papers (templates)


Pre-Engagement
• Pre-Engagement Working Papers
Understanding the Entity
• Understanding the Enity Working papers
Risk Assessment
• Risk Assessment Working papers
Performing the Audit
• Performing the Audit Working Papers
Reporting

Refer to Appendixes for Working Paper Templates

5.3. Materiality

According to ISACA Standards 1204, the following key concepts are highlighted on materiality;

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

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

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

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

- Absence of controls or ineffective controls

- Significance of the control deficiencies

- Probability of these weaknesses resulting in a significant deficiency or material weakness

In an integrated audit, IT auditors will be required to work within the overall materiality that will be set by regulatory auditors for all financial issues. However, this does not exclude the IT auditors from considering materiality in the review of IT issues. ISSAI 5300 requires IT Auditors to consider materiality throughout the (IT) audit process.

However, materiality of an IT Audit issue should be decided under the overall framework for deciding materiality in an SAI. The perspective of materiality would vary depending on the nature of IT audit. Materiality for public sector financial, performance and compliance auditing, of which IT audit is a part are discussed in ISSAIs 200, 300 and 400. (ISSAI 5300)

5.4. Information System Prioritisation

After IT system have been identified at the strategic level through the system documentation and IT infrastructure checklist, IT auditors will then be required to decide which system they will audit and report on.

Prioritisation of such system will be dependent on the financial impact, systems impact critical functions or assets, materials, customers, decision making, and how close to real time they operate, stakeholder concerns, public interest, regulatory requirements and consequences for society.

In an integrated audit, the financial impact will be one of the key factors that will be used to prioritise the systems to be audited. The following table can be used to help with the prioritisation of systems as auditors will be required to audit the system processing material figures.

Understanding the information system relevant to financial reporting. Reference to the ISSAI 1315, 18.				
Application name	**Classes of transactions/ account balances** **(refer to the Regulatory Auditors Lead Schedule)**		**Description and purpose of the application**	**Is the system relevant to the audit?** Give a brief evaluation regarding materiality, the diversity and complexity of the entity's operations and the complexity of the systems. *
	Classes of transaction	**Amount**		
e.g. IFMIS	Procurement items	30,000	It is an integrated financial management system which manage 90% of Government expenditure	The amount and material and the system cover the 90% of the Government expenditure

5.5. Audit Programs

5.5.1 What is an audit program?

An audit program is a series of steps or procedures to be performed to meet the audit objective.

5.5.2 Why should an IT auditor prepare/develop an audit program?

ISSAI 1230 in the financial audit guidelines deals with the auditor's responsibility to prepare audit documentation for an audit of financial statements. The auditor should record various aspects of the audit together in one document with cross-references to the supporting working papers.

ISACA Standard 1201 on Engagement Planning states that the IT auditor should develop and document an IS audit or assurance engagement project plan.

The audit plan will assist auditors in preparing an IT audit programme. The pre-requisite step in developing the audit programme will be to have a clear understanding of the audited entity and its Information Systems ***(IDI Hand Book)***

Further they should develop and document an audit programme and/or plan detailing the nature, timing and extent of the audit procedures required to complete the audit.

These audit procedures should be documented in a manner that will permit the IT auditor to record completion of the audit work and identify work that remains to be done. As the work progresses, the IT auditor should evaluate the adequacy of the programme based on information gathered during the audit. When IT auditor determines that the planned procedures are not sufficient, they should modify the programme accordingly.

The audit program is based on the scope and objectives of the IT audit, and includes procedures to obtain sufficient, relevant and reliable evidence to draw and support audit conclusions and opinions.

Following the completion of the audit planning matrix discussed in the previous section, the auditor should come up with a detailed audit program. The audit program will contain the detailed audit procedures needed to complete the audit.

5.5.3 Contents of an Audit programme

A best practice requires an Audit Program to contain the following;

- Description of the audit area
- Audit objectives
- Criteria and resources for each audit step
- W/p reference
- Auditor that performs the audit
- Dates the audit were performed
- Comments (e.g. If not applicable and why)
- Conclusion
- Time and extent of testing

Description of the audit area

E.g. Business Continuity Plan (BCP) - a business continuity plan is an enterprise wide group of processes and instructions to ensure the continuation of business processes - incl., but not limited to Information Technology - in the event of an interruption. It provides the plans for the enterprise to recover from minor incidents to major disruptions. The plan is usually owned and managed by the business units and a disaster management or risk prevention function in the enterprise. Functional continuity plans are subsets of the enterprise business continuity planning and support the delivery of essential business services.

Audit objective

E.g. the continuity planning audit will:

- Provide management with an evaluation of the enterprise's preparedness in the event of a major business disruption. Identify issues that may limit interim business processing and restoration

- Provide management with an independent assessment of the effectiveness of the business continuity plan and its alignment with subordinate continuity plans

Scope of the audit

E.g. the review will focus on the enterprise business continuity plan, policies, standards, guidelines, procedures, laws and regulations that address maintaining continuous business services. This will include:

- Development, maintenance and testing of the BCP

- Ability to provide interim business services and the effective and timely restoration of same

- Risk management and costs related to the BCP

Criteria and resources for each audit step

IT auditors should select criteria, against which the subject matter will be assessed. When selecting the criteria, professionals shall carefully consider choose the suitability, acceptability and source of the criteria*. (ISACA* IS Audit and Assurance Standard 1008 - Criteria)

In this section, the auditor will determine what information is needed to meet the objective and where they will get the information from. E.g. the auditor will need to obtain the IT continuity plan, test plan, implementation plan, shortcomings and resolution

W/P reference

Good practices require the auditor to create a working paper for each audit area. This will describe the work performed, issues identified and conclusions. The reference is to be used to cross-reference the audit step to the working paper that supports it.

Comments

The comments column can be used to indicate the waiving of a step or procedure relevant to the step performed. It is not to be used in place of a working paper describing the work performed.

Refer to Appendixes on each audit area

5.6. Evidence

ISACA IS Audit and Assurance Standard 1205 - Evidence has the following provisions with regards to evidence

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

- IS audit and assurance professionals shall evaluate the sufficiency of evidence obtained to su pport conclusions and achieve engagement objectives.

Audit evidence is the collection of data, records, documents, and information by the IT Auditors to substantiate their observations to the relevant stakeholder(s), at the relevant time period (at the time of audit or subsequently), sufficiently, reliably, and accurately. ***(ISSAI 5300)***

The evidence in IT Audits need to be appropriately captured and stored in a manner that they are available over time, without any change, to be utilised again. IT Auditors need to ensure that the evidence have necessary timestamps in case of a continuous transacting system, which may have the potential of updating or changing the information. ***(ISSAI 5300)***

Procedures used to gather evidence vary depending on the characteristics of the information system being audited, timing of the audit, audit scope and objectives, and professional judgement. Evidence can be gathered through the use of manual audit procedures, computer-assisted audit techniques (CAATs) or a combination of both. Professionals should select the most appropriate procedure in relation to the IS audit objective. ***(ISACA IS Audit and Assurance Guideline 2205-Evidence)***

5.7. IT Audit Tools

The SAI shall deploy appropriate IT Audit tools commensurate with the risk assessment in the audit engagement, capacity and resources available within the SAI. ***(ISSAI 5300)***

The auditor can use Generalised Audit Software or computer-assisted audit techniques (CAATs) to carry out the information analysis. Tools such as Microsoft Excel, Microsoft Access, IDEA, ACL etc. are examples of generalised audit software that provide the facility to import as well as analyse data. ***(IDI Handbook)***

CAATs are very useful to conduct, inter alia, User Log Analysis, Exception Reporting, Totalling, File Comparison, Stratification, Sampling, Duplicate Checks, Gap Detection, Ageing, Virtual Field Calculations, etc. ***(ISSAI 5300)***

6. CHAPTER 6: IT GOVERNANCE

6.1. What is IT governance?

IT Governance is the responsibility of the Board of Directors and executive management. It is an integral part of organisational governance and consists of leadership, organisational structures and processes that ensure the organisation's IT sustains and extends the organisational strategies and objectives.

The purpose of IT governance is to direct IT resources, to ensure that IT performance meets the following objectives:

- Alignment of IT with the organisation and realisation of the promised benefits;
- Use of IT to enable the organisation by exploiting opportunities and maximising benefits;
- Responsible use of IT related resources
- Appropriate management of IT risks

Fundamentally IT governance is concerned with two things: IT's delivery of value to the organisation and mitigation of IT risks. The delivery of value is mainly driven by the strategic alignment of IT with the business, whereas the mitigation of IT risks is driven by embedding accountability into the organisation.

IT governance is a continuous process which starts initially with the development of a strategy and its alignment throughout the organisation. This is followed by implementation, which should be monitored regularly.

The auditor should have an understanding of the roles and responsibilities of personnel and committees that are key for IT governance. However, it is important to understand that these positions probably exist in all organisations, they may be using a different title or one person may play several roles:

- Board of directors (Parliament) - the most senior executives and/or non-executives of the enterprise who are accountable for the governance of the organisation and have overall control of its resources.
- Ranking officer who is in charge of the total management of the organisation
- Executive management committee (senior management committee) - group of senior executives appointed on behalf of the Board of Directors to manage the day-to-day operations of an organisation.
- IT Steering committee - composed of key stakeholders from executive, business and IT management to prioritise IT enabled investment programmes in line with the organisation's business strategy and priorities; track status of projects and resolve resource conflict and monitor service levels and service improvements.
- Chief information officer (CIO) - the most senior official of the enterprise who is accountable for IT; aligning IT and business strategies; and planning, resourcing and managing

the delivery of IT services and information and the deployment of associated human resources. The CIO typically chairs the governance council that manages the portfolio.

- Chief financial officer (CFO) - the most senior official of the enterprise who is accountable for financial planning, record keeping and financial risks. Business process owners - the individual responsible for identifying process requirements, approving process design and managing process performance. In general, a business process owner must be at a high level in the organisation and have the authority to commit resources to process-specific risk management activities.

- External auditor - has sole responsibility for the audit opinion expressed and for determining the nature, timing and extent of external audit procedures. Internal auditor - means an appraisal activity established within an organisation as a service to the entity. Its functions include, amongst other things, monitoring adequacy and effectiveness of internal control.

6.2. Why is it important for the IT auditor to understand IT Governance?

IT Governance is needed to ensure that new and existing investments in IT generate value reward, and mitigate IT associated risks, avoiding failure.

IT is central to organisational success - effective and efficient delivery of services and goods - especially when the IT is designed to bring about change in an organisation. This change process, commonly referred to as “business transformation,” is now the prime enabler of new business models both in the private and public sectors. Business transformation offers many rewards, but it also has the potential for many risks, which may disrupt operations and have unintended consequences. The dilemma becomes how to balance risk and rewards when using IT to enable organisational change.

Despite efforts of the software industry to identify and adopt best practices in the development of IT projects, there is still a high rate of failure and missed objectives. Most IT projects do not meet the organisation’s objectives.

6.3. IT Governance constraints can lead to audit observations

There are many constraints that face organisations that are trying to implement an effective Governance structure, particularly when there are significant. IT investments involved. Without effective governance to deal with these constraints, IT projects will have a higher risk of failure.

Each organisation faces its own unique challenges as their individual environmental, political, geographical, economic and social issues differ. Any one of these issues can present obstacles to providing effective governance. It is the responsibility of the IT auditor to bring points to the attention of senior management and in some cases to the Board of Directors.

One would never be able to list all the inhibitors relating to IT Governance but the following are common to most organisations:

- Senior management not engaging IT: A major issue that inhibits the success of IT projects is that senior management tend to be unwilling to involve IT in the decision-making process. Management needs to work with their IT department when considering major IT investments to ensure that they are provided with the knowledge and feedback necessary to make appropriate decisions.

- Poor strategic alignment: little or no organisational value may be derived from major IT investments that are not strategically aligned with the organisation’s objectives and resources. Such poor strategic alignment means that IT may not be efficiently and effectively contributing to the achievement of the organisation’s objectives.

- Lack of project ownership: in the past many IT projects were solely in the hands of the IT department and senior management tended to steer clear of taking ownership for such projects. A lack of clear leadership from senior management puts the IT project at risk of failing to integrate its objectives with the overall objectives of the organisation. Often management “passes the buck” on to the IT department, leading to a lack of integration and alignment of IT with the overall objectives of the organisation. This creates vast inefficiencies for which IT managers are usually blamed.

- Poor risk management: poor risk management is a major constraint to the success of most IT projects. Risk management involves assessing all potential threats to the project and mitigating them. If these issues are not addressed at the onset of the project and throughout, the risk of failure is extremely high. Often, the most damaging IT risks are those that are not well understood by senior management.

- Ineffective resource management: to achieve optimum results at minimum costs, an organisation must manage its IT resources effectively and efficiently. Making sure that there are enough technical, hardware, software and most importantly human resources available to deliver IT services is key to achieving value from investments in IT.

6.4. Some key best practices which an IS auditor can look for when assessing the effectiveness of IT governance in an organisation

A key best practice is implementing an organisational structure, including an effective governance framework, with well-defined roles and responsibilities for IT stakeholders including IS auditors. Such a framework ensures that IT investments are aligned and delivered in accordance with corporate objectives and strategies. Without this framework, IT projects are more susceptible to failure however many organisations fail to consider the importance of IT governance. They take on IT projects without fully understanding what the organisation’s requirements are for the project and how this project links to the organisation’s objectives.

Identifying organisational objectives for IT is another key best practice for IT governance. Historically, senior managers saw IT projects from the limited perspective of input and output objectives. This inefficient and ineffective perspective stemmed directly from these managers’ lack of technical experience to deal with the complexity of such projects. In addition, these managers were unjustly blamed for the vast inefficiencies caused by the organisation’s failure to integrate the objectives of IT projects with the overall objectives of the organisation.

To be successful an organisation should consider all the following factors, which lead to best practices: high level framework, independent assurance, performance management reporting, resource management, risk management strategic alignment, and value delivery:

- High-level framework: including defining leadership, processes, roles and responsibilities, information requirements, and organisational structures - ensures the IT investment is aligned with the overall strategies of the organisation, maximizing the application of available IT opportunities.

- Independent assurance: in the form of internal and external audits (or reviews), can provide timely feedback about compliance of IT with the organisation's policies, standards, procedures, and overall objectives. These audits must be performed in an unbiased and objective manner, so that managers are provided with a fair assessment of the IT project being audited.

- Resource management: through regular assessments, ensure that IT has sufficient, competent, and efficient resources to meet the organisation's demands.

- Risk management: embedded in the responsibilities of the organisation's management and IT regularly assess and report IT related risks and organisational impact. Exposures of any problems are followed up, with special attention paid to any potential negative effects on the overall objectives of the organisation.

- Strategic alignment: a shared understanding between the organisation's management and the IT department enables the Board and senior management to understand strategic IT issues. IT strategy demonstrates the organisation's technology insights and capabilities and ensures that the IT investment is aligned with the overall strategies of the organisation, maximising the use of available IT opportunities.

- Value delivery: demonstrates the benefits that can be achieved from each IT investment. Such investment should always provide value to the organisation and be driven by the needs of the investing entity.

6.5. Performance management

Performance metrics is the basis for sound IT governance structure. For an organisation to have good governance, it must be able to see where true value is being added to its IT investments. Having a well-defined set of performance metrics provides management with the means to measure success and determine what areas need to be focused on to improve the effectiveness and efficiency of IT investments.

The performance metrics will consist of key performance indicators (KPI) which will help the organisation to understand how well they are performing in relation to their strategic goals and objectives.

The IT auditor uses the same metrics to ensure that management has taken sufficient and appropriate action to deal with problems. Without performance metrics to back one up, it would be difficult to gauge the progress towards achieving IT objectives.

Examples of governance metrics used by organisations:

- IT staff numbers: How does the organisation measure the value added of each activity compared with the amount of resources committed

- Outsourcing ratios: How does the organisation determine the effectiveness of its own staff and allow them to gauge their reliance on external resources

- System availability: How many hours per week is the system available compared to standard hours per week

- Mean time between failures (MTBF): What is the mean time between failures?

- Mean time to repair: What is the basic measure of the maintainability of repairable items, (it can represent the average (mean) time required to repair a failed component or device)

6.6. What are the key questions the IT auditor needs to answer when auditing IT governance

- Overall question: are the necessary leadership and organisational structures and processes in place to achieve corporate objectives and to support the organisation's strategy? (Source: WGITA)

- Leadership and organisation: do the IT organisational structure and human resources management in place support the organisation strategies and objectives?

- IT strategy: is there an IT strategy in place, including the IT direction, and the processes for the strategy's development, approval and implementation and maintenance that is aligned with the organisation's strategies and objectives?

- Policies and procedures: are there IT policies, standards and procedures and the processes for their development, approval, implementation, maintenance and monitoring in place to support the IT strategy and comply with regulatory and legal requirements?

- Quality management system: is there an IT quality management system in place to support the organisation's strategies and objectives?

- IT controls: are there sufficient IT management and monitoring of controls (e.g. continuous monitoring, QA) in place to support the organisation's policies, standards and procedures?

- Investment planning: Is there IT resource investment, use and allocation practices, including prioritisation criteria in place that are aligned with the organisation's strategies and objectives?

- Contracting: are there IT contracting strategies and policies, and contract management practices in place to support the organisation's strategies and objectives?
  Risk management: are there risk management practices in place to ensure that the organisation's IT related risks are properly managed?

- Monitoring and reporting: are there monitoring and assurance practices in place to allow the board and executive management to receive sufficient and timely information about IT performance?

- Business continuity planning: is there a business continuity plan in place to support orderly recovery of essential business operations during the period of an IT disruption?

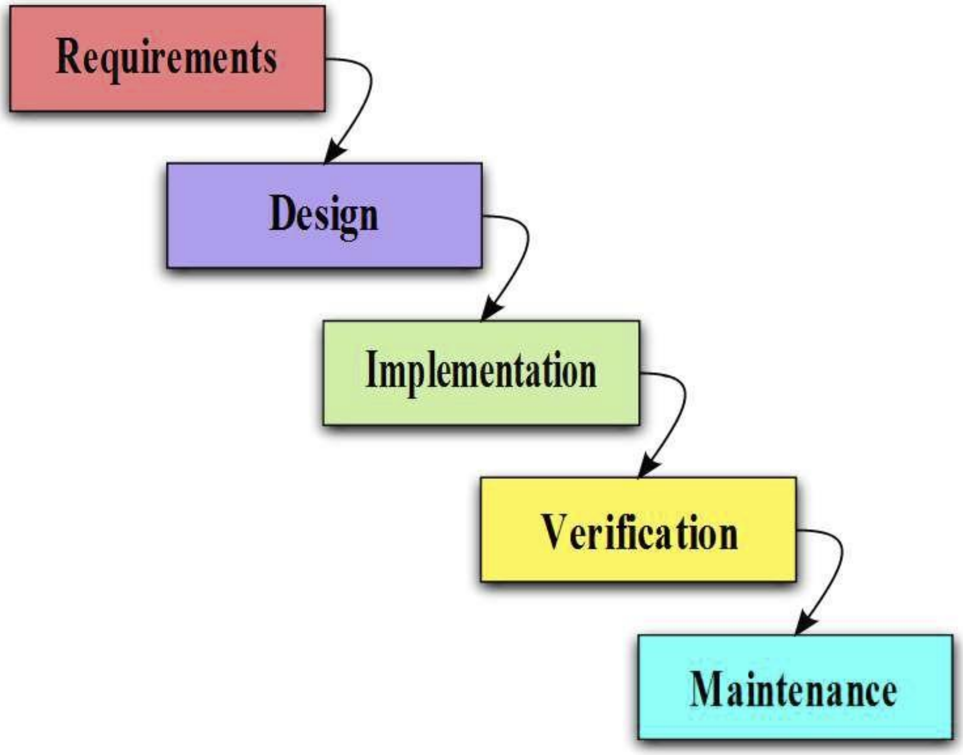
If an adverse response is provided on any of the above questions the auditor should check for the adequacy of compensatory controls. Where compensatory controls are not in place or are ineffective an audit observation should be raised.

7. CHAPTER 7: AUDIT OF INFORMATION SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

The system development life cycle (SDLC) is the process of managing the development life cycle of a newly developed system or the implementation of a system which were bought off the shelf and customised for the organisation.

SDLC - is a methodology or a systems development method wherein the system is developed in stages. Thus, project management focuses on managing the team to use the SDLC and other tools to create the product.

7.1. System development phases



The IT Auditor should note that these different phases may be broken down, split into sub phases or categories, or merged.

7.2. Why should IT auditors know about SDLC phases

The IT auditor can assist the organisation by reviewing the system development process to ensure that the developed system complies with the organization's strategy and standards. Experience with many software failures led to conclusion that it was important to develop the software in phases rather than all at once. Each phase has objectives and as an IT auditor we need to ensure that the project manager has met the objective of each phase. Unless they do this, they will most likely create a software product that does not meet the users' needs or contains many errors.

7.3. What is in each of the SDLC phases?

The different phases of the SDLC:

7.3.1 Defining user requirements

The objectives of this phase are to gather and prioritise the initial set of user needs for a business deficiency, conduct a preliminary analysis, evaluate and propose alternative solutions, describe costs and benefits and submit a preliminary analysis, evaluate and propose alternative solutions, describe cost and benefits and submit a preliminary plan to meet the need with software and hardware or other (i.e. process change) components.

Auditors need to look closely at this phase (or the deliverables from this phase, Requirements Document) if the audit is of a system under development to ensure that the entity has fully understood the system and its requirements before they build it.

7.3.2 Systems analysis and system requirements definition

The objective if this phase is to break the hardware and software portions into manageable components, define the detailed requirements for each, identify external and internal interfaces, identify relevant stakeholders, skills and tools needed to build the system, and lay out the schedule and among other items identify the risks with the program. Hold a Requirement Review to ensure that stakeholders and users understand the requirements and at the end of the phase approve the set of requirements the system will implement.

Auditors also need to look closely at the deliverables from this phase to see if stakeholders are involved in the development of requirements and the approval process.

7.3.3 System design

The objective of this phase if to take the various components of the system and design the solution in detail including screen layouts, business rules, process diagrams, pseudo code and other documentation. Peer review the design and hold a preliminary and detailed design review to get stakeholder input and concurrence.

7.3.4 Implementation (Development)

At this stage, the system developer will write the code for the various components, carry out peer review and perform unit test the code, including regression test if some code is re-used from other sources.

IS Auditors may not be involved directly at this stage but can verify the results of unit tests and regression tests. Ethically you cannot audit a system you develop.

7.3.5 Verification and validation (testing)

Integration and testing: in this phase all the various pieces (software, hardware, test equipment, etc.) are brought together and tested to ensure that it meets the requirements.

The IS Auditor at this stage will need to verify the test results or outcomes.

7.3.6 Acceptance, installation, deployment

This is the phase where the software is put into production test environment and tested by the users and after meeting the organisational criteria on acceptance testing is put into the production environment.

The Auditor will need to look at user acceptance testing documentation. The auditor may verify if a Test environment was used to carry out testing and not a Production Environment.

7.3.7 Maintenance

This phase is typically the last phase and generally includes updates and periodic fixes to the software or system to ensure it continues to meet the business objectives the team typically continues to use whichever model they used for initial development for the maintenance phase. However, if the number of changes are relatively small or do not require much resources, the team may choose a much more compressed set of phases for the maintenance. One of the main concerns with this phase is that the organisation finds that they do not have sufficient documentation of the software fix errors in the product.

It should be noted that an organisation may choose to acquire a system off shelf and may not have control over the newer versions of the system under development.

However, in this case the IT auditor may look into the acquisition process to ensure the system procured met the requirements of the organisation or system owner or system users and verify if the version in use is up to date.

Further information on IT Operations which includes the Maintenance of IT Systems can be found in the next Chapter.

7.4. An overview of SDLC models

The two widely used SDLC models are:

- Waterfall model, and
- Spiral model

Most organisations use the waterfall or the spiral model for systems development. However, for projects that are web based or those that need quicker turnaround time the Agile SDLC model provides users with a working product sooner than the waterfall or spiral model.

7.4.1 Waterfall model

The waterfall model for software or systems development is an iterative process of requirements, prototypes and improvements. This model assumes that development in each phase will be completed before moving into the next phase. That assumption is not very realistic in the real world. Changes are discovered that regularly require portions of software to undergo redevelopment.

7.4.2 Spiral model

While the waterfall model implies a linear path from start to finish through the phases (Requirements - testing) the spiral model allows incremental builds and iteration through the phases. Each version of software will repeat the cycle of the previous version while adding enhancements and greater functionality. Users and stakeholders will see a working system much earlier than the waterfall model but the functionality is not yet complete or may be limited.

7.4.3 Agile model

Both the waterfall and the spiral model are time consuming and depending on the size of the system, users have to wait many months or more before they see a working product. Agile model on the other hand provides users with working software in as soon as 30 days. However, initial software deliveries, typically every 30 days, provides users many opportunities to add requirements or request changes to delivered functions.

The agile software development method places greater emphasis on delivering working software than full and complete documentation. In the agile method, the team combines Design & Implementation, and Verification into a 30-day time period called a sprint. At the end of the 30 days the team delivers the product.

7.4.3.1 Terminology used under Agile system

Scrum is the method that implements the Agile method. The Scrum method greatly compresses all of the typical phases of software development (requirements, design, development, and test) into a 30-day time period. The development team is given a set of requirements (called sprint backlog) to implement in the next 30 days

Traditional names	Scrum names
Requirements	Product backlog, sprint backlog
Planning	Sprint planning
Development phase	Sprint
Meeting	Daily scrum
Project tracking	Burn down
Software deliverable	Build, release, increment

7.4.3.2 Scrum terms

Product backlog (requirements)

The product backlog is a list of requirements for the product. It is ordered or prioritised by the Business Owner based on such inputs like risk, business value, dependencies, date needed.

Sprint planning meeting (planning)

At the beginning of each sprint a planning meeting is held to discuss what items from the backlog will be moved to the sprint backlog

Sprint backlog (release requirements)

The sprint backlog is the list of work the Development Team must address during the next sprint. The team breaks the backlog into user stories. The team interacts with the users during the 30-day sprint which ensures that the product at the end of the sprint meets their needs.

Within the team the stories are broken down further into tasks for team members. Generally, the same team works from one sprint to the next.

Daily scrum (meeting)

This is a daily meeting of team members to discuss work related issues, anyone can be present but only the core group is allowed to speak. This meeting is generally about 15 minutes in duration and address what was done the previous day, what will be done today and if there are any issues that need to be resolved.

30-day sprint (development)

A sprint is the basic unit of development in Scrum. Sprints last between one week and one month but are typically 30 days in duration. They are "timeboxed" i.e. the duration is typically not extended and the sprint ends at the end of the 30 days.

Burn down (project monitoring)

The sprint burn down chart is a publicly displayed chart showing remaining work in the sprint backlog. Updated every day, it gives a simple view of the sprint progress. It also provides quick visualisations for reference.

Build/Release/ Increment (Deliverable)

The increment s the sum of all the Product Backlog items completed during the sprint and all previous sprints. At the end of a sprint, the increment must be done according to the scrum's team definition of done (this needs to be defined, but is generally considered to include working, tested and error free code.)

7.5. Why should auditors know about SDLC models?

We have already discussed SDLC phases. However, a IT Auditor needs to know that SDLC models are a way to look at how to implement the various phases of the SDLC. The models have certain risks that the program manager (overseeing development life cycle process) needs to address. The auditor will ask the audit related questions to ensure that the program manager is effectively managing these risks.

7.6. Considerations for IT auditors

Auditors need to understand the common system development methods so that they can audit an IT program that may be in the development phase. The phases and risks along with audit related questions are provided in the table below:

Stage of system development	Risk description	Audit related questions
Requirements	✓ Requirements not sufficiently described, reviewed, or analysed.	✓ Where are your requirements for the project documented? ✓ Who reviews the set of requirements? ✓ Who approved the set of requirements? ✓ What is your process to manage changes to the baseline requirements?
	✓ Users are not consulted for requirements	✓ How do you ensure that user input is provided in the requirements for a system?
Design	✓ Unclear design, no review of design	✓ What is your process for refining requirements if the design cannot be completed because of vague requirements? ✓ Who reviews the design of the system outside of the software group? ✓ How is the design of the system explained to the users and other stakeholders?
Implementation	✓ Errors introduced by programmers, functions left out, not conforming to prescribed interface standards.	✓ What is your process to catch coding errors during the development of the software? ✓ How do you ensure that the programmers implement all of the

		required functions they are assigned by the program manager? ✓ Where do you document your software and hardware interfaces (for input, output, data transmissions, etc.) ✓
Verification & validation (testing)	✓ Missing functionality, inadequate testing, no pass-fail criteria	✓ How do you ensure that approved requirements are traced to the system design and test? ✓ Who approves your test plan? ✓ Are users involved in the testing phase? ✓ What determines whether a test passes or fails?
Maintenance	✓ Missing documentation, ✓ lack of skills to maintain ✓ the product, too many ✓ changes to product	✓ Where do you keep documentation for the project? ✓ How do you ensure that the documentation is complete and reflect the working software? ✓ Does your team have the skill necessary to maintain the software? ✓ How do you prioritise the changes or modifications you will make to this software?
Agile model		
	✓ Documentation	✓ How do you ensure that your documentation matched the delivered product?
	✓ Testing	✓ How do you ensure that your team adequately tests

		✓ the software?
	✓ Project completion	✓ How do you know when the product is complete?
	✓	✓ Where are the products requirements documented?
	✓ Vendor fails to deliver	✓ What happens if a team is ✓ unable to deliver a product ✓ in the given (30 days, 40 ✓ days) time frame?

7.7. The Role an IT Auditor can play in Systems Implementation

As government is increasingly using information systems more, the spending on systems is very huge. A number of system weaknesses and failures are a result of bad implementation practices and it is important for the IT Auditors to play a role during systems implementation. The auditor should however take care not to play a role that compromises the SAIs ability to audit that particular system, e.g designing a control.

Some roles that the auditor can play to ensure successful completion and implementation of any new systems are:

- ➢ Identify potential vulnerabilities and points requiring control
    - ✓ In the life cycle development of the business application
    - ✓ This will facilitate efforts to ensure that proper controls are designed and implemented in the new System
- ➢ Auditor's role to advise the project team on control deficiencies, activities of appropriate controls or processes to implement and follow

These roles can be done by:

- ➢ The IS auditor can review all relevant areas and phases of the systems development project, and report independently to management on the adherence to planned objectives and company procedures
- ➢ The IS auditor can identify selected parts of the system and become involved in the technical aspects on the basis *of* his/her skills and abilities
- ➢ The IS auditor can provide an evaluation of the methods and techniques applied through the development

Auditors can refer to the WGITA guide on auditing systems development for SAIs.

8. CHAPTER 8: IT OPERATIONS AND IT KEY PERFORMANCE INDICATORS

8.1. What are IT Operations?

IT Operations are the activities involved in the day to day running of the IT systems which support the business processes of an organisation.

These may include and are not limited to:

- Procurement or Development of IT Systems
- Maintenance, Update and Security of IT Systems (Databases, Applications etc) whether managed in-house or outsourced.
- Review and Documentation of Systems
- User Policies, Training and User Support

8.2. What is a key performance indicator (KPI)?

Key performance indicators are measures that determine how well a business process is performing in enabling the goal to be reached. They are lead indicators of whether a goal will likely be reached or not, and are not good indicators of capabilities, practices and skills. They measure the activity, goals, which are the reactions the process owners must take to achieve effective process performance.

To define meaningful KPI measures that align with the goals of the organisation, the following questions need to be asked:

- What are the business/ organisation measures or requirement?
- How do these translate into IT service measure?
- How does a process support the IT service measures?
- How will I collect and analyse and measure?

Examples of KPI measures and the corresponding definitions and goals

Process	Goal (critical success factor)	KPI	Measurement architecture
SLA	✓ Improve ability to track and meet the service levels agreed on with clients	✓ Percentage increase or decrease and meeting service level targets	✓ Tracked through incident management and reported monthly
Change management (this	✓ Reduce incidents caused by unauthorised changes	✓ Percentage reduction in the number of incidents	✓ Tracked through incident management, change

may include patch management)		resulting from unauthorised access	management and reported monthly.

Note: patch management may fall under change management because the process involves making changes (like adding features) to a system, in this regard an IT Auditor should also determine that policies, standards and procedures for Patch Management are formalized, appropriate and implemented.

The KPI's should provide insight into:

- Quality - how well is the process working? Are we improving toward goals that were established for this process?
- Efficiency - is the throughput of the process sufficient?
- Compliance - is the process being followed?
- Value - are we doing what we are supposed to be doing?

8.3. Why KPI's are important for the IS auditor and how they can be used in an IT audit?

Whilst the KPI's are the responsibility of the IS operation management it is important to understand how the auditor can use of these KPIs during the audit. Key performance indicators can assist the auditor to ask questions about the performance of IS operations and help him identify potential areas of significance e.g. the number of IT incidents per month may be an indicator that there are problems with the systems.

Review of KPIs will assist the auditor to ask questions related to:

- Whether the systems are operating efficiently and effectively?
- Whether mechanisms are in place for identifying gaps in performance, addressing gaps identified, and following up on the implementation of corrective action taken as a result of evaluating of the entity's performance
- How the organisation performance does compares against other organisations?
- Identifying control issues in the entity being audited thereby helping to determine the nature, timing and extent of testing.

8.4. Internal service level agreements

8.4.1 What is an internal service level agreement

An internal service level agreement is between the IT organisation and the business owners. Failure to adhere to service level agreements affects meeting of users' requirements. The IS operations and business owners should agree on amongst other things the following IT delivery services:

- Capacity management
- IT financial management
- Availability management

Capacity management involves planning and monitoring of computing and network resources to that the available resources is used efficiently and effectively. This requires that the expansion or reduction of resources takes place in parallel with the overall business growth or reduction.

IT financial management involves ensuring that the financial systems are able to produce accurate and timely financial reports. The system should be available throughout the peak period and should be able to process large volumes of transactions without disrupting processing. Unavailability of the system might result in the organisation losing business or not meeting its expected corporate results.

IS operations and business owners, also need to agree on the availability of the system throughout the required periods as failure to avail the system when needed might have a direct impact on the business and on processing and reporting on financial transactions. System down times should therefore be minimised as this affect the processing and reporting on financial transactions. The IS auditor should review any SLAs to determine that they support the accurate and consistent processing of financial data.

8.4.2 Why internal service level agreements are important for the IS auditors

The IS auditor can make use of the internal SLA's to check on the IS operations ability to track and meet the service levels agreed on with the users. By comparing the actual service levels against the planned service levels, the IS auditor can compare the percentage increase or decrease in meeting service level targets. For example, if the IS operations and users agreed on 97% availability and the actual availability is only 70% the IS auditor should ask the organisation for the impact of failure to meet targets. IF the impact is severe then the auditor may consider this as a potential audit area.

Similar to KPIs the IS auditor should review the internal SLA's to assist in identifying control issues that are relevant to determine the scope of the audit.

8.5. External service level agreements

An external service level agreement is between the IT organisation and the business contractors, suppliers and consultant, who are external stakeholders of the business. Failure to adhere to external service level agreements affects meeting of business' requirements. The IS external stakeholder and the business should agree on amongst other things the following IT delivery services:

- Capacity management

- IT financial management
- Availability management

The treatment and importance in regard to external Service level agreement is similar to those of an internal service level agreement with exception of stakeholders and documentation. In this aspect, the IT Auditor should be aware of the guiding principle of an external Service agreement of a particular service of the audit client.

It should also be known that maintenance contract could also be used as an external service level agreement.

8.6. Data Administration practices

8.6.1 What are data administration practices?

Data administration practices are used to determine the integrity and optimisation of databases. Data management is enabled by the system software that enacts and supports the definition, storage, sharing and processing of user data, and deals with file management activities. User and system data can be organised sequentially or direct random access/ Database Management Systems (DBMS) aids creating, in organising, controlling and using the data needed by application programs. The primary functions of a DBMS include reduced data redundancy, decreased access time and basic security over sensitive data.

Data redundancy occurs in database system which has a field that is repeated in two or more tables. For instance, in case when customer data is duplicated and attached with each product bought then redundancy of data is a known source of inconsistency, since customer might appear with different values for a given attribute.

8.6.2 Why data administration practices are important for the IS auditors?

Data administration practices are important for the IS auditor because there should be sufficient and appropriate controls in place for the underlying database of key applications.

In other words, if there are adequate application controls for an application, there should be equivalent controls for underlying database because there is a risk that the controls at the application level could be circumvented by making changes directly to the database. The IS auditor should have knowledge of the technology concepts related system software and database management systems.

8.6.3 During an audit, the IT auditor can ask the following questions:

- Are there adequate change procedures in place to ensure the integrity of the database management software?
- Is data redundancy minimised by the database management system?
- Is integrity of the database management system’s data dictionary maintained?

8.7. Capacity and performance monitoring tools and techniques

8.7.1 What is capacity and performance monitoring tools and techniques?

It helps to determine whether IT services meet the organisation's objectives. Computer resources such as hardware, software, telecommunications, networks, application and data should be used for the benefit of the entire organisation. This includes providing information to authorised personnel where and when needed at a cost that is identifiable and for the benefit of the organisation. Examples of capacity and performance monitoring tools and techniques:

- Network analysers - instruments that measure the network parameters of electrical networks

- Load balancing - is a computer networking methodology to distribute workload across multiple computer or computer clusters, network links, central processing units, disk drives or other resources to achieve optimal resource utilisation, maximum throughput, minimise response time and avoid overload.

- System utilisation report - displays generic server operating system configuration, and associated utilisation information. By graphically illustrating usage on a day-to-day, week-to-week basis, including the daily hours of usage and system idle time.

8.7.2 Why is capacity and performance monitoring tools important for the IS Auditor?

The IS auditor should have knowledge of capacity planning and related monitoring tools and techniques used by the organisation and establish whether they are adequate and working properly. The review of the various IT performance monitoring reports produced by the organisation is a good source of evidence to determine if IT systems are working as intended by the organisation.

8.7.3 The IS auditor can ask the following questions:

- Are criteria used in the hardware performance monitoring plan based on historical data and analysis obtained from the IS trouble logs, processing schedules, job accounting system reports, preventative maintenance schedules and reports?

- Is there continuous review of hardware and system software performance capacity?

- Is monitoring adequate for equipment that has been programmed to contact its manufacturer without human intervention in the case of equipment failures?

8.8. Problem and incident management

8.8.1 What is problem and incident management?

Problem and incident management are the systems and practices used to determine whether incidents, problems or errors are recorded, analysed and resolved in a timely manner. Problem management aims to resolve issues through investigation and in-depth analysis of a major incident in order to identify the root cause. Once a problem has been identified and analysis of the root cause has been done it becomes a known error and a solution can be developed to address the error and to prevent future occurrences of related incidents. A mechanism should be put in place for the detection of and documentation of abnormal conditions that could lead to the identification of an error.

The IT operation section should have documented procedures for detecting and recording abnormal conditions. A manual or computerised log may be used to record these conditions. Contents should include:

- Error or fault detection date - when was the fault first detected?
- Error resolution description - resolved, pending, under investigation, no further action, or irresolvable
- Error code
- Error description - short narrative description of the fault and the source of the error
- Initials of those responsible for maintaining the log, closing the log, and Section responsible for dealing with the problem

8.8.2 Why is a problem and incident management important for the IS auditor?

The IS auditor should have knowledge of problem and incident management practices. The auditor should check for compliance to policies and procedures and may wish to examine the maintenance contracts and schedules to determine if adequate maintenance is carried out. Ultimately the key test to the adequacy of the client’s maintenance arrangements is the amount of system down-time or the number of Helpdesk incidents arising from equipment failures.

Effective hardware maintenance and problem management help prevent unexpected interruptions. Problems and delays encountered, the reason, and the elapsed time for resolution are recorded and analysed to identify recurring patterns or trends. Policies and procedures for hardware maintenance should exist and be up to date.

8.8.3 Sample Questions on IT operation

Outlined below are audit questions the IS auditor can ask IS operations staff:

- Are significant and recurring problems identified and actions taken to prevent their recurrence?
- Were processing problems resolved in a timely manner and was the solution complete and reasonable?
- Are there any recurring problems that are not being reported to IS management?

Component	**Service Level Measurement Type**	**Included in SLA?**
Availability		
Servers		
Database Servers	Required Uptime	
Application Servers	Required Uptime	
Email Server	Required Uptime	
Internet Servers	Required Uptime	
File Servers	Required Uptime	
Mainframe	Required Uptime	
Network		
WAN Segment	Required Uptime	
LAN Segment	Required Uptime	
Problem Resolution		
Servers		
Problem Resolution Business Critical Servers Priority One in less than x hours	Percentage of time achieving service level commitment	
Problem Resolution Business Critical Servers Priority Two in less than x hours	Percentage of time achieving service level commitment	
Problem Resolution Business Critical Servers Priority Three in less than x hours	Percentage of time achieving service level commitment	
Network		
Problem Resolution Business Critical LAN/WAN outage Priority One in less than x hours	Percentage of time achieving service level commitment	
Problem Resolution Business Critical LAN/WAN outage Priority Two in less than x hours	Percentage of time achieving service level commitment	

Problem Resolution Business Critical LAN/WAN outage Priority Three in less than x hours	Percentage of time achieving service level commitment
Help Desk	
Time to answer calls in less than xx seconds	Percentage of time achieving service level commitment
First call problem resolution (Resolvable calls)	Percentage of time achieving service level commitment

9. CHAPTER 9: INFORMATION SECURITY

9.1. Information security and its importance

Information is an asset and organisation should strive to secure this asset as they do other assets. Information security allows an organisation to protect their information and information resources (IT infrastructure) from unauthorised users.

What is core in information security is **C**onfidentiality **I**ntegrity **A**vailability. Information system security seeks to protect an organisation's information by reducing the risk of loss of confidentiality, integrity and availability of that information to an acceptable level. Confidentiality is concerned with that information being disclosed or available to unauthorized individuals. Integrity refers to information accuracy and completeness. Availability is that the information and other information resources must be available to those who need to assess it.

A security policy sets out how an organisation secures their information resources. The information security policy should provide for training of staff on security and ensures that they follow established procedures for data access and control. When looking at information security, the IS auditor must be aware of risks arising from personal and mobile devices which assess an organisation's information.

In coming up with an information security plan, an organisation should have

- An understanding of the organisation and scope the information security
- Have leadership commitment and plan to achieve the security objectives
- Have adequate and competent resources to achieve the information security

9.2. What are the components of information security?

There are generally 12 accepted areas for information security:

Risk assessment: Risk assessment is the process of identification, analysis and evaluating risks in the IT security infrastructure. It is the process of assessing security related risks from internal and external threats to an entity, IT assets and personnel.

Security policy: the policy is the set of laws, rules and practices that regulate how an organisation manages, protects and distributes resources to achieve specified security objectives. These laws, rules and practices must identify criteria for according individuals authority, and may specify conditions under which individuals are permitted to exercise their authority. To be meaningful, these laws, rules and practices must provide individuals reasonable ability to determine whether their actions violate or comply with the policy.

Organisation of information security:

- Communications and operations management: an organisation needs to keep track of the process and procedures they use for their business operations. It includes the set of organisational procedures and processes that ensure the correct processing of data in the organisation. This includes documenting procedures for media ad data handling, emergency procedures, network security logging and backup procedures. The objective of this category is to ensure that correct and secure operation of information processing facilities.

Documented operating procedures: operating procedures should be documented, maintained and made available to all users who need them. Control includes:

- Documentation of/for all significant system activities including start-up, close-down, back-up and maintenance
- Treatment of such documentation as a formal organisational record, subject to appropriate change authorisation, change tracking and archiving
- Provision of appropriate security for such documentation, including distribution control (see also "security of system documentation")

Asset management: refers to any system whereby things that are of value to an entity or group are monitored and maintained. It may apply to both tangible assets such as buildings or intangible assets such as intellectual property rights. Asset management is a systematic process of operating, maintaining, upgrading and disposing of assets cost effectively. For a government entity asset management is very important in the current fiscal environment because financial constraints will not allow them to replace lost or stolen assets in a reasonable manner.

Human resource security (covered in more detail in the HR controls section): Employees handling personal data in an organisation need to receive appropriate awareness training and regular updates to safeguard the data entrusted to them. Appropriate roles and responsibilities assigned for each job description need to be defined and documented in alignment with the organisation's security policy. The organisation's data must be protected from unauthorised access, disclosure, modification, destruction or interference. The management of human resources security and privacy risks is necessary during all phases of employment associated with the organisation.

Training to enhance awareness is intended to educate individuals to prevent data disclosure, recognise information security problems and incidents, and respond according to the needs of their work role. Safeguards include the following:

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

The objective of human resources security is to ensure that all employees are qualified for and understand their roles and responsibilities of their job duties and that access is removed once terminated. The three areas of Human resources security are:

- Pre-employment: this topic includes defining roles and responsibilities of the job, defining appropriate access to sensitive information for the job, and determining depth of candidate's screening levels - all in accordance with the company's information security policy. During the phase, contract terms should also be established.
- During employment: employees with access to sensitive information in an organisation should receive periodic reminders of their responsibilities and receive ongoing, updated

security awareness training to ensure their understanding of current threats corresponding security practices to mitigate such threats

- Termination or change of employment: to prevent unauthorised access to sensitive information, access must be revoked immediate upon termination / separation of an employee with access to such information. This also includes the return of any assets of the organisation that was held by the employee.

Physical and environmental security: physical and environmental security describes measures that are designed to deny access to unauthorised personnel from physically accessing a building, facility, resource, or stored information; and guidance on how to design structures to resist potentially hostile acts. Physical security can be as simple as a locked door or as elaborate as multiple layers of barriers, armed security guards and guardhouse placement.

Physical security is primarily concerned with restricting physical access by unauthorised people to controlled facilities, although there are other considerations and situations on which physical security measures are valuable (for example limiting access within a facility and or to specific assets, and environmental controls to reduce physical incidents such as fires and floods)

It is the responsibility of management to ensure that there are adequate controls in place to protect the business assets and resources. Management should carry out a proper risk assessment which will involve identifying the threats to the system & system resources, the vulnerability of the system components and the likely impact of an incident occurring. Management then identifies counter measures to reduce the level of exposure to an acceptable level.

Security inevitability incurs costs, and it can never be perfect or complete - in other words - security can reduce but cannot entirely eliminate risks, given that controls are imperfect, strong physical security applies the principle of defence in depth using appropriate combinations of overlapping and complementary controls. For instance, physical access controls for protected facilities are generally intended to:

- Deter potential intruders (e.g. using pass cards/badges and keys)

- Distinguish authorised from unauthorised people

- Delay, frustrate and ideally prevent intrusion attempts

- Trigger appropriate incident responses

Environmental controls can be defined as exposures which occur from natural events such as earthquakes, lightning, floods, power failures, etc. Areas of environmental controls management must ensure that there are proper controls in place, include:

- Fire prevention, detection and suppression systems: these systems are designed to prevent a fire from breaking out and when it occurs to deal with the fire in an efficient manner. These systems need to be maintained at least once a year.

- Protection from water damage: information processing facilities should be located preferably in a position where the equipment is less likely to get into contact with water. Even where computer facilities are located above ground level, there may still be a risk of water damage from burst pipes or leaking roofs.

- Protection and control of the power supply: the auditor’s primary concern relate to the possible impact that electricity has on the availability of the systems and the integrity of the data processed. The client’s system should have controls in place to minimise the effect of power cuts or deviations in supply. This is normally achieved through the installation of electrical surge protectors and uninterruptible power supplies (UPS).

Access control: Refers to exerting control over who can interact with a resource. Often, but not always, this involves an authority, who does the controlling. The resource can be given building, group of buildings, or computer-based information system. But it can also refer to a restroom stall where access is controlled by using a coin to open the door.

Access control is, in reality, an everyday phenomenon. A lock on a car door is essentially a form of access control. A PIN on an ATM system at a bank is another means of access control. The possession of access control is of prime importance when persons seek to secure important, confidential, or sensitive information and equipment.

In a government environment, access control is important because many government entities process sensitive data and privacy concerns limit who should view various parts of the information. Access controls ensures that only users with the process credentials have access to sensitive data.

There are basic elements to logical access controls:

- User identification: this normally involves a user identifying them to the computer with a username or logon id.

- User authentication: The computer requires confirmation that the user is who he/she says they are. This is achieved by something the user has and/or knows. Passwords are a common form of authentication. Other forms of authentication include PIN numbers, signature or biometrics.

Information systems acquisition, development and maintenance: the system development life cycle (SDLC) is a process of creating or altering information systems, and the models and methodologies that people use to develop these systems. In software engineering, the SDLC concept underpins many kinds of software development methodologies. These methodologies form the framework for planning and controlling the creation of an information system or the software development process. The deployment of the system includes changes and enhancements before the decommissioning or sunset of the system. Maintaining the system is an important aspect of SDLC. As key personnel change positions in the organisation, new changes will be implemented, which will require system.

Information security incident management: in the fields of computer security and information technology, information security incident management involves the monitoring and detection of security events on a computer or computer network, and the execution of proper responses to those events. Information security incident management is a specialised form of incident management, the primary purpose of which is the development of a well understood and predictable response to damaging events and computer intrusions.

Business continuity management: business continuity planning is the process an organisation uses to plan and test the recovery of their business processes after a disruption. It also describes how an organisation will continue to function under adverse conditions that may arise (for example natural or other disasters). For more information, refer to the chapter on business continuity and disaster recovery planning.

Compliance: the IS auditor should review and assess compliance with legal, environmental and information quality, and fiduciary and security requirements. All the security areas listed above is defined in ISO 27002, a security framework from the International Standards Organisation. In addition, ISSAI 5310 provides a framework to help in the audit of information security.

Audit: both ISSAI 5310 and ISO 27002 provide guidance to government agencies on information security practices.

10. CHAPTER 10: CHANGE MANAGEMENT

10.1. What is change management?

In IT organisations, the change management process is normally used to manage and control changes to software, hardware and related documentation. Change management is necessary where the impact of an unapproved or accidental change could have severe risks and financial consequence for an organisation. Organisations follow a defined change management procedure which requires approval from a board before being implemented into the operational environment.

10.2. Why is it important for the auditors?

Government organisations rely on their IT systems to process data. This might include financial data, healthcare, or security. Privacy and statutory laws require that all of sensitive data in an organisation be access controlled and the processing of the data have adequate controls for data reliability.

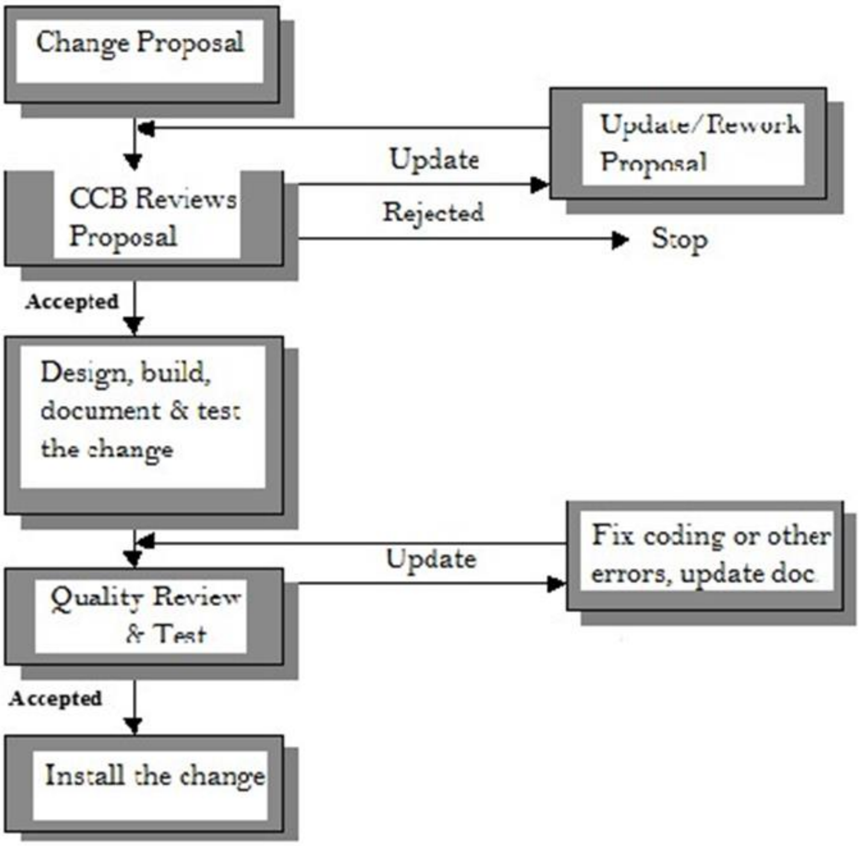
Since it is quite easy in the software world to change the code so that the processing is different or that sensitive data get corrupted or is maliciously written to a secret file, organisations have instituted change management. Change management, when implemented correctly, ensures that only authorised changes are made to the operating environment once the necessary quality checks have passed. Auditors need to assure themselves that the change management process that an organisation has implemented ensures the integrity of the data, software and related documentation.

10.3. Why are changes required to a software or hardware system?

After systems are developed and put into the operating environment users might request additional features or functions. Additionally, as the system is used, users who interact with the system may realise that some of the operations may not be correct. When a change (as a result of new functions or errors) is identified, the organisation will need to go through a change management process before fixing the software. This is to prevent the introduction of additional errors and or limit the number of changes to the system. System changes cost money to the organisation both in the development and in testing and installation costs.

10.4. What is a typical change management process?

Government organisations can have different change management processes because of the variance in the size of the IT group. However, there are common elements in a change management process. The diagram below depicts a typical change management process.



- **Change proposal/request -** this is the initial change proposal. It can be the result of an error, missing functions, or added functionality. Most organisations have a change request form with various fields or severity, size or effort, cost, schedule, and affected or related software systems. The change request form may also be called the request for change form. It may include items such as potential impact on the IT systems and services to users, the effect of not implementing the change, the resources required to implement the change and or estimated future resource requirements for maintaining this change.

- **Change control board reviews proposal** - The change request is reviewed by the change control board (CCB). The CCB is the final authority who meets and reviews the proposals on a periodic basis. The CCB is the final authority on whether a proposal is accepted or rejected. A proposal can be rejected for a number of reasons including low priority, cost and risk.

  The IS auditor should take into consideration the entities organisational structure and management committees. An organisation can have the functions of a CCB performed by a structure of the organisation which may not be called a CCB. What is key is the changes to systems be considered and authorised by management or their delegated authorities.

- **Update / rework proposal** - at times a proposal may not have sufficient detail to enable the CCB to make a decision. In this case, they may request additional detail or supporting material. These may include better cost estimates, risk mitigation strategies for change proposal or more specifics on the schedule estimate that is part of the change request.

- **Design, build, document and test the change -** once the CCB approves a change request, the project team begins working on the detailed requirements analysis, design, and updating related documents. They will build and test the change typically using a SDLC method. Once the change meets all of the requirements it is passed on to the quality assurance group (who may test is again, do a comparison to ensure no malicious code is present, check it against a previous version, etc.) and if it passes the test, it is recommended for installation in the production environment. During the design and build stage the project team will have its own set of internal change control procedures. It is also a good to note that users who requested the changes should be part of the testing process to ensure changes work as requested.

- **Install the change -** after the code has been approved by the quality assurance group, the code is installed into the production environment. The organisation needs to have either a software library or similar control to ensure that the correct version of the software is installed and that there is a way to roll back changes in case of a serious disruption as a result of the change.

	Risk	**Audit related questions**
Change request	✓ Increased likelihood of unauthorised changes being introduced to key business systems; ✓ Insufficient control over emergency changes ✓ No proper tracking of changes ✓ Reduced system availability ✓ Configuration documentation failing to reflect the current system configuration ✓ Lack of documentation of business processes ✓ Failure of updates for hardware and software changes	✓ Does the organisation have a change control policy? ✓ Is change control covered in the ICT policy if there isn't a separate policy ✓ Where is the change request form documented? ✓ Who can initiate a change request? ✓ How does the organisation track the status of change requests? ✓ What is the organisations change request numbering? (to facilitate tracking in a database) ✓ Are change requests logged and given a unique number? ✓ Are changes requests categorised and prioritised?
Change control board review proposals	✓ Increased likelihood of unauthorised changes	✓ Request change control charter

	being introduced to key systems ✓ Insufficient control over emergency changes ✓ No proper tracking of changes ✓ Reduced system availability ✓ Configuration documentation failing to reflect the current system configuration ✓ Lack of documentation of business processes ✓ Failure of updates for hardware and software changes	✓ How often does the CCB meet to review change proposals? ✓ How does the CCB handle emergency changes? ✓ What is the process to handle emergency changes once the CCB approves the change request? ✓ Request a list of approved change requests as well as rejected change requests ✓ Who approves the change request
Design, build, document & test the change	✓ Increased likelihood of unauthorised changes being introduced to key systems ✓ Insufficient control over emergency changes ✓ No proper tracking of changes ✓ Reduced system availability ✓ Configuration documentation failing to reflect the current system configuration ✓ Lack of documentation of business processes ✓ Failure of updates for hardware and software changes	✓ Can the IT group bypass the CCB change control process? ✓ What quality checks are performed on the system prior to installation? ✓ Who approves the change implementation for final installation? ✓ How many changes have your quality assurance organisation or the final approving authority accepted and rejected? ✓ What happens to rejected changes? ✓ How do you ensure that your documents are updated and stay current with the modified software? (Look for comments in the documentation that may

		indicate why changes were made)
Install the change	✓ Increased likelihood of unauthorised changes being introduced to key systems ✓ Insufficient control over emergency changes ✓ No proper tracking of changes ✓ Reduced system availability ✓ Configuration documentation failing to reflect the current system configuration ✓ Lack of documentation of business processes ✓ Failure of updates for hardware and software changes	✓ Do you have a software library from where you install the software? ✓ How do you ensure that the correct version of the software has been installed? ✓ How do you roll back changes to a previous version? ✓ When was the last time you had to roll back to a previous version? ✓ What changes have you made to your change request process as a result?

11. CHAPTER 11: AUDIT OF BUSINESS CONTINUITY AND DISASTER RECOVERY

11.1. What is a Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)

Business continuity planning refers to the process which enables an organisation to carry on with normal operations in case of disaster. The main objective of a business continuity plan is to maintain the integrity of the organisation's data together with the operational service and processing facilities and if necessary, provide a temporary or restricted service until normal services can be resumed.

Confidentiality, Integrity and Availability of Systems or Data is still a guiding principle throughout the process of the design of BCPs and DRPs.

11.2. Difference between BCP and DRP

The BCP concerns the entire organisation and refer to the process of prioritizing mission critical business processes and ensuring that they can be performed in a suitable manner after a disruption or can be recovered in a reasonable length of time. In may require the use of manual or automated processes for the business to function with limited capacity The DRP typically concerns itself with ensuring that the IT infrastructure is robust enough to recover from a disaster. The planning is also aligned with the BCP to ensure that the mission critical processes that are in the BCP and which are supported by IT systems are also considered critical by the IT department.

11.3. Importance of BCP/DRP for an IT organisation

Over the past 20years government organisations have come to rely increasingly on the availability and correct operation of their computer systems in order to discharge their statutory obligations. Computer systems often play an important role in such diverse activities as the assessment and collection of taxes and customs revenues, the payment of state pensions and social security benefits; and in processing national statistics (births, deaths, crime, diseases, etc,). Indeed, many activities could now be carried out effectively - if at all - without the support of computers.

Loss of power, industrial action, fire, malicious damage can all have disastrous effects on computer systems. It may take an organisation many weeks to resume effective business operations if they do not have a workable BCP in place.

Critical services or products are those that must be delivered to ensure survival, avoid causing injury, and meet legal or other obligations of an organisation, BCP is a proactive planning process that ensures critical services or products are delivered during a disruption.

11.4. The Plan

An entity should have policy that should be the base for development of BCP/DRP. This policy or the details BCP/DRP should at least cover

- The organization’s overall target for recovery or Recovery Strategy
- Empowers people involved in BCP/DRP
- Recovery Objectives – time & point
- Invocation
- Dependencies
- Recovery Teams
  - ✓ Infrastructure - identification
  - ✓ Applications - identifications
  - ✓ Co-ordination and Logistics
  - ✓ Public Relations and Monitoring
  - ✓ Business Teams
- Recovery Test Checklist
- Recovery Procedures

11.5. Why audit BCP/DRP

BCP/DRP ensures that the business process and IT infrastructure of an organisation are able to support mission needs after a disaster or other disruption. Government agencies serve many mission critical needs, if these services are disrupted for sufficiently long periods of time, it will lead to both financial and other losses. Auditors need to ensure that all government agencies have a BCP/DRP process that ensures that the agency can continue to serve citizens.

11.6. Audit of BCP/DRP

There are certain phases that government organisations should take to plan their recovery strategies. There are no fixed names for these phases and some might be done multiple times to further refine the impact or analysis. The IT auditors can look at the stage of development of the BCP/DRP to identify relevant audit issues.

11.6.1 Business impact scenarios & threat identification

System users and IT support personnel of organisation work together to assess the criticality of each business system within the review’s boundary, and to identify the range of threats that might prevent their correct operation. Threat identification and analysis is the process of looking at potential threats and evaluating how the will affect the business. Threats may include natural disasters and human events such as bombs etc.

The objectives of the business impact review are to identify the organisation's business systems and rank them in order of importance to the business. Within the business impact review there are some phases, which include

- **Business impact scenarios** - identifying potential business impacts will involve considering various "business impact scenarios". For example, business impact scenarios for a government organisation that administers social security benefits might include the following which are considered important to the organisation:

  - ✓ State pension and social security benefit claims cannot be processed;
  - ✓ Benefit payments cannot be made
  - ✓ Loans cannot be recovered
  - ✓ Accounts cannot be produced.

  Identifying impact scenarios will involve distinguishing between what is realistic and what is not. This will require a combination of judgment and a good all-round understanding of the business.

- **Measuring business impacts or business impact analysis** - having identified realistic business impact scenarios which will affect critical business functions, the related business impacts are then measures by the organisation. These might include for example, how cost of overtime working increased, or the cost of repairs, etc. will affect business operations. For an organisation measuring impact analysis is determining what mission functions are critical and what will it cost if they are not recovered in a defined period. Generally, if not conducting a business function leads to significant operational limitation.

  Business impacts are estimates of the potential damage to the business that would be caused by an impact scenario taking place. They are estimated for each critical business process, or group of processes, and it is important to recognise that they will vary with time. In general, the longer a scenario continues, the more severe its impact on the business will be.

- **Defining recovery deadlines & recovery documentations** - once the organisation can calculate or estimate the financial or other loss of not be able to perform critical functions, they can begin to create recovery deadlines. These timelines are dependent on the agency but for example they could use a category list such as:

  - ✓ Category 1: recovery times within "n" minutes
  - ✓ Category 2: recovery times within "n" hours
  - ✓ Category 3: recovery times within "n" days
  - ✓ Category 4: recovery times within "n" weeks
  - ✓ Category 5: criticality varies according to date
  - ✓ Category 6: applications that is not critical

- **Recovery documentation** - recovery documentation lists the required resources needed to be available when recovering from a disaster. The asset management functions from the information security area is utilised by the organisation to ensure that the required resources are in the presumed location, at the right configuration and are in good working order. The recovery documentation is utilised to make a solution design in the next phase.

- **Risk reduction methods** - during the review the team should identify any areas in which risk of disaster could be reduced by the application of additional controls. However, because the review is not intended to be a detailed review of IT security, this aspect should be confined to more obvious disaster prevention controls.

- **Reporting to management** - the management report from the business impact review will summarise how much the organisations stand to lose from a disaster or other incident, and how quickly these losses would mount up. The report will therefore identify the key business processes ranked in their order of criticality to the business and for each one describe:

  - ✓ The form that the damage or loss to the organisation is likely to take
  - ✓ How the degree of damage or loss is likely to escalate after the incident
  - ✓ The minimum staffing, facilities and services that will be necessary to resume an emergency level of service
  - ✓ The maximum tolerable time for both emergency and full-service recovery.

11.6.2 Recovery strategy definition

During the recovery strategy stage of planning, the review team should identify any threats that could be reduced by implementing stronger preventative and detective controls. Stronger controls will reduce the overall risk of a disaster occurring, and will help to prevent serious damage should the disaster occur by ensuring early detection and management.

11.6.3 Solution design

The goal of solution designs is to create a solution using the organisation assets that will enable continued business functions after a disruption. The organisation may utilise external and internal resources and will typically balance cost against recovery time. Certain functions may be required to be conducted manually and the solution design will document the process for this. Solution design also includes specific backup and recovery procedures that the organisation needs to follow so that the data is backed up in a periodic basis. Recovery procedures ensure that the backed-up data is able to be recovered and that sufficient versions of backups are stored both at the local site and at a remote site.

In coming up with a strategy and solution, an organisation will have to set their Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for the information systems. These will essentially determine the DRP solution design that will be implemented.

The RTO is the period or duration within which a business process must be restored in the event of an un-foreseen eventuality.

RPO is the acceptable data loss in case of disruption of operation management would be willing accepts. For instance, if the RTO is set to 2 hours, then an offsite mirrored back-up should be maintained as a BCP/DRP solution.

The more mission critical a system is for the entity operations, the less the RTO and RPO it will have.

11.6.4 Implement and test

This phase is where the organisation puts in solution together and individually tests various components and conducts a full-scale test. A full-scale test is disruptive to the organisation and may not be done often. However, the testing of components is conducted periodically. There are various approaches the organisation can use to test the plan:

- ➢ Live testing - should be carried out under conditions that are as realistic as possible. The test should be based in a major scenario and involve transferring the live workload on the key systems under test to a standby system. It should also be carried out under the control of the crisis management team at the emergency control centre, and include relocation of some business users in line with the test scenario and the plan requirement. The overall test should aim to prove that:
    - ✓ The system under test can be recovered on the standby computer
    - ✓ The correct system and data files being backed up
    - ✓ The standby system remains compatible with the main system
    - ✓ Telecommunication links can be switched to the standby site.
    - ✓ Procedures for relocating personnel in an emergency work
    - ✓ User support services can be provided
- ➢ System recovery - recovery systems, particularly on a standby computer, is an exercise that also ought to be carried out periodically. Even if the recovered system only carries simulated workload, the exercise will at least provide assurance that aspects of the plan remain workable. Variations on this type of testing might include:
    - ✓ Unannounced tests
    - ✓ Random selection of staff to be involved in the test, reducing the workforce and excluding some key members of the team;
    - ✓ Disabling major system components to stimulate failures.
- ➢ Standby utilities - these tests mainly include standby supplies for electricity, water and telecommunications. The standby generators and UPS should be tested at least monthly under full load. During an emergency, the standby power supply might need to maintain key computer systems, their supporting environmental equipment and communication systems.

- Practice evacuations - it can be used to exercise both the continuity planning manager and the emergency control centre, but are most useful for maintaining personnel awareness.

- Dry running - involves taking a board game approach. An imaginary scenario is created and the team involved talk through their roles in implementing the plan and managing recovery.

11.6.5 Evaluating the results and updating the plan

Evaluating the results - testing is not simply a matter of going through the motions; the objective must be to prove that the plan is workable. Testing should therefore be underpinned by criteria that can subsequently be used to evaluate the test results. Test criteria will normally be time related and include:

- Time to restore the system under test - if this is excessive and business operations cannot be restored within the critical deadline, then either further testing will be necessary to improve familiarity with implementing the plan, or it will need to be modified in some respect.

- Time to reconnect users to the system under test - restoring a batch system might pose different problems to those presented by an online system where problems might be experienced with diverting telecommunication circuits and restoring networks. Time to distribute printed output - if printed outputs are produced centrally can these be distributed to the correct recipients?

- Processing load - it is possible that the standby system, when recovered, might not be able to process the necessary volume of traffic or offer a satisfactory response time, even taking account of the possibility that a reduced level of service might be acceptable under emergency conditions.

A problem log must be kept in which to record all problems that arise during testing. Following the test, problem data should be classified by type and ranked severity. This information will provide further criteria against which to judge the overall success of the test. It will also provide indicators where the plan should be adjusted.

Updating the plan - perhaps the most important requirement is that the plan should have recognised “owner”, that is a manager who is accountable to the Board for maintenance of the continuity plan. Lack of an owner will inevitably result in the plan falling into obsolescence.

11.6.6 Risk and audit considerations

Application software forms the operational backbone of the organisation. Should a disruption occur the organisation should at the shortest time possible recover from the disruption? The IT continuity and disaster recovery plans address the IT exposures and solutions based in the priorities and framework of the business continuity plan. The role of the auditor is to review the plan and provide management with an evaluation of IT preparedness in the event of a disruption and to identify any issues that may limit business processing. The auditor also provides management with an independent assessment relating to the effectiveness of the IT continuity plan and its alignment with the business continuity plan.

The following are risks associated with business continuity planning:

- Failure of plans to reflect changes to business needs, applications or technology;
- Failure of plan to assess the situation and implement alternate processes to fit unforeseen situations
- Inappropriate or incomplete recovery plans and processes, resulting in delayed restoration of processing
- Incomplete or untested interim processing and logistics plans
- Inadequate training and staff not prepared to execute the plan effectively and quickly
- Inadequate or unavailable staffing resources to restore processes on a timely basis
- Unavailability of backup data, inability to locate media when needed, or inability to transport data within the prescribed time frame.
- Regulatory violations resulting in loss of customer confidence
- Increased costs for continuity management due to ineffective focus on risks and costs or failure to prioritise services recovery based on business need
- Lack of development of realistic threat scenarios based upon potential circumstances and events

Examples of procedures the auditor can perform to address the risks:

- Determine whether the organisation has a business continuity and disaster recovery plan;
- Determine if team member roles and responsibilities have been assigned at an appropriate level of authority
- Determine if a business impact assessment has identified all critical and necessary business functions and their resource dependencies
- Review the risk assessment and determine if it documents the mitigating steps that are in place to address these threats
- Determine if recovery time objectives have been assigned to all critical business process components

12. CHAPTER 12: IT OUTSOURCING

12.1. What is IT outsourcing?

The outsourcing of IT services provides the customer with flexibility and cost savings by transferring the services, infrastructure or applications processing to a supplier (the outsourced company or service provider). Outsourcing may also be part of an organisation's risk mitigation strategy. Outsourcing can also provide a form of risk transfer.

The scope of the outsourced activities can include:

- Operating infrastructure (data centre and related processes) at either the data centre of the customer or the supplier;
- Processing of a proprietary application by the servicer (application services provider) Systems development or maintenance of application
- Managing the network
- Managing the information security infrastructure and supporting processes
- A combination of any of these and other business and technology processes

The outsourcing contract is the legal document that establishes the scope, terms, conditions, legal liabilities, responsibilities and remedies between parties. The explicit and comprehensive description of these issues is essential to a successful relationship between the customer and supplier. The issues vary depending on the type of outsourcing, but include:

- Ownership or lease of hardware, software licenses, etc.
- Employee transfer (where data centre is conveyed) Applications licensed
- Intellectual property terms
- Rights to audit the environment and third-party assurance of controls
- Billing
- Recourse and remediation of unsatisfactory performance
- Renewal or termination of services
- Legal breach of data liability

The SLA is one of the primary metrics used to measure performance. It can address number of transactions processed, timeliness of processes, age of issues remaining unresolved, etc., depending on the type of outsourcing relationship. The SLA provides the auditor and management with the evidence to support the evaluation of the customer/supplier relationship.

The relationship between the customer and supplier is another critical control and process. The outsourcing of a process transfers operational responsibility to the supplier. The customer retains responsibility for the management of and adherence to policies, procedures and regulatory requirements. If the supplier fails to provide appropriate controls and/or performance based upon the contract terms, the customer may have legal recourse. However, the regulatory authorities will generally hold the customer responsible for failure to comply with regulations, including penalties that may result. In addition, the remedies for failure to provide adequate performance levels are limited. Financial penalties can provide negative reinforcement (supplier will lose money unless in compliance) because there is a point where the supplier has more to lose by continuing the relationship than by breaking the contract. The costs associated with termination of services can be expensive, and the transfer of processes can range from disruptive catastrophic. Ownership of an access to intellectual property can affect the viability of the enterprise and need to be addressed. Relationship management of the customer and supplier is essential.

The retained organisation changes its focus from providing operational processes to ensuring that the supplier and the operational interfaces within the organisation have the appropriate communications, performance reviews and incentives to achieve the agreed-upon objectives. It is also the retained organisation's responsibility to verify that appropriate controls are in effect to ensure that the organisation fulfils its contractual obligations and cannot be seen as impeding the supplier's performance. It is necessary for the retained organisation to have the necessary qualifications focusing on technical, managerial and relationship management expertise.

Outsourcing changes the assurance and audit process. When processes are owned and executed by the business, the internal audit function is responsible for performing the appropriate procedures to satisfy its charter to provide assessment of internal controls. The transfer of a process to a supplier may change how the audit function is achieved. Of the supplier provides a service that is proprietary or is a shared service centre, it may be reluctant to permit the customer's audit function from performing audit procedures, citing other customer confidentiality or disruption to the supplier's operations. A third-party audit assessment of the supplier's processes, performed by a recognised professional, is an accepted alternative to direct customer assurance procedures. The objectives, scope and audit procedures of each third-party audit differ according to the needs of those engaging the auditor and the services provided by the supplier.

The supplier's auditor can provide two types of reports: type one report provides a description of the supplier's processes and controls at a specific point in time, and the auditor's opinion as to whether the descriptions are fairly presented and are suitable designed to achieve the related control objectives; type two report utilised the objectives if the first report, but also includes testing of controls to determine if they are operating with adequate effectiveness to achieve the related control objectives over a period of at least six months. The third-party report or document provided by the supplier should provide the customer with recommended procedures that they should implement to support and complement the controls provided by the supplier. The customer should analyse the third-party reports and perform a gap analysis against the audit charter and other standards, to determine if additional assurance procedures are required, potentially requiring supplier permission access to facilities.

Management of the relationship is one of the most critical points in the outsourced environment. This role is the interface between supplier and customer's management, often the retained organisation. It is this group that ensures that the contract terms are satisfied; the billing process is accurate; supplier performance is satisfactory; and issues during day-to-day processes are identified, escalated to the appropriate management teams and satisfactorily resolved. Since most outsourcing problems relate to relationship management issues, the audit focuses on this as a major component of the review.

The IT outsourcing audit addresses several phases of outsourcing:

- Evaluation of the IT outsource requirements;
- Evaluation of the supplier selection process;
- Evaluation of the contract negotiation and finalisation process
- Review if the outsource implementation and transfer of processes
- Review of the production steady-state outsource environment
- Review of the renewal/ termination process

12.2. What are the advantages of outsourcing?

- Staffing flexibility - outsourcing will allow operations that have seasonal or cyclical demands to bring in additional resources when you need them and release them when you're done.
- Staff development - if a project requires skills that the organisation does not currently have, they can outsource the development when they train internal staff. Additionally, depending on the physical locations of the vendor the organisation may be able to give internal staff work alongside the vendor personnel for a period of time.
- Cost reductions from outsourcing - outsourcing typically results in cost reductions by shifting labour and other costs to the vendor who has a lower labour cost. IT organisations look to outsource tasks which would be more costly to complete in-house.
- On call experts - outsourcing enables the organisation to have on call experts waiting in the wings to assist with existing or emerging issues. The company is able to quickly respond to changing business needs (new mission or taking on additional functions) with the help of the expert.
- A larger workforce - still another advantage to outsourcing is the benefit of enjoying a larger workforce when necessary without the hassle of maintaining a larger staff. Outsourcing companies can bring in additional employees on a contract basis during times of prosperity without worrying about having to lay them off or keep them utilised when the surge of work begins to wane.
- Flexibility - is another considerable advantage of outsourcing work. Even the most well-planned projects may suddenly end up behind schedule or under a time crunch due to minor errors, changes in plans, or other incidental activities.
- Cloud computing - is a form of outsourcing where the organisation outsources data processing to computers owed by the vendor. Outsourcing may also include utilising the vendor's computers owned, backup and provide online access to the organisation data. The organisation will need to have a robust access to the internet if they want their staff or users to have ready access to the data or even the application that process the data. In the current environment, the data or applications are also available from mobile platforms.
- Risk mitigation - an organisation may find that outsourcing and having some services or processes off their premises is an effective strategy to handle risks that may be associated to having those same services managed by themselves. For instance, a process such as a country preparing for an election may print ballot papers overseas (outsource) yet that country has

the capacity to print them itself. Other examples with banks, printing of money, processing of online payments, immigrant visa processing, passports etc. So apart from the aspect of providing better services, outsourcing may help reduce risks associated with such sensitive processes being handled in house.

12.3. IT outsourcing risks and audit questions

Risks associated with outsourcing	**Audit questions**
Difficulty in accessing outsourced system for audit purposes	✓ Does the organisation have a clear right to audit clause in their outsourcing contract which mentions audit by the organisation or a third party appointed to audit the outsourced system by the organisation?
Solutions failure to meet business and user requirements	✓ Determine if the supplier provides a manual of suggested or required user controls ✓ Perform a gap analysis of supplier suggested controls to those controls in effect at the enterprise and identify control gaps.
Contractual discrepancies and gaps between business expectations and supplier capabilities	✓ Determine that formal legal approval is documented according to contract approval procedures ✓ Verify that there is a clear understanding of which party has intellectual property ownership ✓ Determine if the problem resolution process is clearly delineated for both parties.
System security and confidentiality compromised	✓ Verify that security access levels for both party's representatives are clearly defined ✓ Review operating system controls to ensure that the operating systems within the scope of the outsourcing agreement are configured for maximum security, achieve the assurance objectives in the operating system audit program, and adhere to minimum enterprise policies and procedures.
Invalid transactions or transactions processed incorrectly	✓ Review applications maintenance and support controls to ensure that change management is designed and configured for maximum security, and achieves the assurance objectives in the change management audit program, and

	adheres to the minimum organisational policies and standards,
Poor software quality, inadequate testing and a high number of failures	✓ Verify that the SLAs established in the supplier contract are measurable for quality of the services provided by the supplier. ✓ Verify the existence of an incident/problem tracking system.
Unclear responsibilities and accountability	✓ Define a process to continuously monitor all agreed-upon service levels. ✓ Provide regular and formal reporting of SLA performance, including deviations from the agreed-upon values, and distribute this report to different levels in the organisation. ✓ Perform regular reviews to forecast and identify trends in service level performance.
BCP or DRP plans not effectively covering outsourced systems or not covering them at all.	✓ Do the organisation's BCP and DRP effectively cover areas or aspects of Systems or Business processes that are Outsourced? ✓ Does the Outsourced entity have a BCP or DRP of their own which is complementary to the one of the organisation outsourcing to them, and are these covered in the SLAs?

12.4. How can some outsourcing risks be mitigated or managed?

The SLA is the primary tool or documented agreement between the organisation and the vendor to whom the services are outsourced. By putting critical or important elements in the SLA, the vendor and the organisation are committing to certain conditions. These conditions manage the risks that the vendor does not deliver on time, by stipulating time constraints and identifying penalties or other profit reduction methods. Another way the SLA managed risk is by requesting the types and detail of project documents on applications developed by the vendor.

In addition, the SLA should define the services the vendor is expected to perform as well as the technical parameters for those services since it is a legally binding agreement between the vendor and the organisation.

An ideal SLA should include:

- ➢ The types of services that will be performed by the vendor;
- ➢ Allocation of responsibilities between the organisation and the vendor;

- The services that will be measured, measurement period, duration, location and reporting timelines (defect rates, response time, help desk staffing hours, etc.)
- Time to implement new functionality, rework levels
- Type of documentation required for applications developed by the vendor;
- Location where services are to be performed
- Frequency of backup, data recovery parameters
- Termination and data delivery methods and formats
- Incentive and penalty clauses

13. CHAPTER 13: AUDIT OF ERPS

13.1. Introduction to Enterprise Resource Planning (ERP) Systems

Traditionally, the various mission areas of an organisation like finance, sales and human resources were built around individual missions and did not necessarily have common business focus or processes. The different department functioned independent from each other and in most instances, each department had its own individual application system, or a number of systems to support. In some cases, the different software programmes were able to interface with each other, but this was not generally the case. This approach resulted in time delays, additional costs, the need for reconciliation of data and data redundancy when issuing reports or reconciling accounts in the traditional approach management heavily relied on manual controls, for example purchase orders were manually retrieved from the paper files and stapled to the invoice, prior to the authorisation of payment.

An ERP application seeks to do away with this fragmented approach to the business information management by integrating diverse functions which exchange information between them. The main purpose of an ERP system is to facilitate the flow of information between all business functions within an organisation and manage the connections with external stakeholders. An ERP system can run on a number of different hardware and network configurations, typically employing a database as a repository for information.

The ERP system is a packaged business software system that allows the entity to:

- Automate and integrate the majority of its business processes
- Share common data and practices across the entity
- Produce and access information in a real-time environment

Examples of ERP systems

- SAP
- Oracle
- ACCPAC
- EPICOR

IFMIS

Integrated Financial Management Information System (IFMIS) or Integrated Financial Management System (IFMS) is a common information and communication technology (ICT) platform which integrates core public financial management functions (e.g. budgeting, treasury operations, accounting, cash/debt management, auditing/reporting) to ensure efficient management of public resources. IFMIS/IFMS is an ERP distributed across many ministries or departments. The IS auditor should get to know how their IFMIS is implemented to be able to identify areas of weaknesses. The controls at all the entities determine the overall reliability of the system. For instance, the central system may require complex passwords for log in, having a department where officers share accounts or paste passwords on the computer will make increase system risk.

13.2. Characteristics of ERPs

Characteristics of an ERP system:

- Integrated system that operates in real time; Common database
- Consistent look and feel throughout each module
- Installation of the system without elaborate application / data integration by the IT department

13.3. Benefits of ERP systems

ERP systems automate information processing across business functions. Data is available across different but integrated applications and the organisation has better understanding of their business process and how data flows between them. In an ERP environment, every business transaction is recorded in the Financial Accounting and controlling module automatically and the processing is inline and in real time. Management has access to up-to-date information on how the entity is performing.

ERP systems are implemented to support the operations of an organisation and to be successful all modules should be fully integrated into all different significant processes. The auditor should ensure that they have an understanding of the environment in which the organisation operates as well as the regulatory environment to enable the auditor to identify the technical, applications and behaviour risks associated with the system and the environment in which it operates.

13.4. Why should an auditor worry about ERP systems?

Since ERP systems automate most of the manual processes that were in place the auditor must ensure that appropriate controls are in place. Specifically, with ERP systems there is much greater emphasis on automated controls, logical access security and configuration controls. The web enablement of ERP systems and the integration of back-end ERP systems with front end web enabled systems continue to transform business process and technical infrastructure. All of these add risks of ERP implementation and the auditor will need to look at what the organisation has done to mitigate the risks.

13.5. Risks associated with implementation of ERPs

The implementation of ERP systems has been shown to have additional risks which the IT auditor needs to look into when auditing ERP systems.

Firstly, unlike a normal application which sets out to automate a particular business process the ERP application also automates interrelationships between diverse business functions. This involves different functions understanding each other’s roles, and some processes need to be re-engineered to fit in.

An important first step is complete project planning documentation. The organisation must ensure that all project planning documents are completed. In most instances organisations will use vendors to assist with the implementation of the ERP system. If the project documentation is not completed, the risk exists that the system will not be functioning effectively, the system is not properly configured and cost overruns can occur.

Audit related questions

- Who is managing the implementation of the ERP system
- What is their experience in managing EPR systems
- Where are the organisations business processes for finance, human resource, payroll, etc. documented?
- How are you ensuring that the ERP program / project manager get the most current business process document?
- Where are the ERP project related documents?
- Who reviews and approves the project related documents?

Some of risk associated with ERPs includes:

13.6. Management commitment

if management does not demonstrate their commitment to the project, the risk of failure exists. Staff members may be of the opinion that why do they need to be committed to the project when management is not committed.

Audit related questions

- Has the ERP project obtained senior management commitment?
- Are various business owners available to discuss how they operate their business processes?
- Has management devoted sufficient time to planning the ERP implementation by requesting staff to make time available to the project, assist the project with their questions and review project related documents?
- Has senior management committed to the ERP implementation schedule and the time it takes to tune the system to produce value added data

13.7. Data conversion

The switch from a legacy system to standardised and integrated systems increases the complexity of the conversion process. Sometimes new data which was not available on the legacy system to the new system would be needed. Another risk associated with the data conversion of the old system to the new system is that incorrect data could be migrated to the new system. The organisation should also ensure that the data from the old legacy system should be accessible when the need arises.

Audit related questions

- Where have you documented the data requirements for the ERP project?
- Where have you identified your data aps and how do you plan to define the source and type of data
- How are you ensuring that the data is clean, i.e. is not missing fields, contains the right elements, etc.?

13.8. Return on investment

Implementing an ERP system is a huge investment of time and money. The amount of cash required would not even be considered by management, given the fact that such an outlay is not guarantee to the said benefits but subject to proper implementation, training, and use. Most of the ERP systems don't reveal their value until after the organisation have had them running for some time and can concentrate on making improvement on the business processes that are affected by the systems.

Audit related questions:

- Have you estimated the cost of your implementation?
- Have you estimated your ERP implementation schedule?
- What is your risk management strategy for when the schedule slips and cost rise?
- When do you expect start realising the benefits of the ERP implementation?

13.9. User requirements

User expectations and requirements should be properly documented and managed. User requirements should be included in the project documentation and all parties should agree on the requirements. If user requirements are not properly documented the risk of scope creep exists. This means that as the project progresses more and more additional requirements are made, and the possibility exists that the deadline might not be achieved.

Audit related questions:

- How are you managing your user expectations?
- What is your plan to prioritise and manage user requirements?

13.10. External consultants

When implementing systems, most organisations rely on the use of consultants to implement systems. The risk exist that the knowledge is not transferred to staff in the organisation and the organisation will start to depend heavily on consultants.

Audit related questions:

- How are you ensuring that you will be able to support the ERP system after implementation?
- Where is the documentation for the ERP?

- Have you trained your internal staff in the IT organisation on the ERP software?
- Are consultants given access rights to the ERP

Other challenges experienced with ERP (including IFMIS) implementations are

- Lack of Internal capacity
- Resistance from users (as a security concern)
- Data migration and storage
- Customization to meet specific business use
- Funding to keep infrastructure updated
- No controls

13.11. Operation of an ERP application

Modules in an ERP heavily rely on each other. To appreciate audit of ERPs, we need to understand the relationship and data flows among modules. It is therefore good practice to adopt a process/cycle approach as opposed to modular approach od auditing the ERPs.

ISACA audit Program for Oracle EBS and SAP uses this process/cycle audit approach. In addition, the programs include some key configurations which need to be done.

A typical ERP system will contain the following modules:

13.12. General ledger

- Finance - the financial module is the core of many ERP software systems. It can gather financial data from various functional departments and generates financial reports such as general ledger, trail balance, balance sheet and quarterly financial statements. The following areas are covered in the financial module.
- General ledger - general ledger is the central repository for all of the financial data. All the other modules feed data to the general ledger, and financial reports, such as the income statement and balance sheet, etc. are generated out of the general ledger.

The various functionalities provided by the general ledger are as follows:

- Import data from subsidiary ledgers in the form of journals
- Enter journals directly into the general ledger to record actual and budget transactions Enter encumbrance journals to track encumbrances through the purchase approval process and to control spending against budgeted amounts;
- Correct actual, budget and encumbrance information
- Review account balances online or through standard reports or ad hoc queries

Risks relating to the general ledger

- Bank reconciliations are not performed regularly
- Duplicate journals are posted to the general ledger
- Journals are not recorded in the correct accounting period Unauthorised changes to the chart of accounts

Audit related queries

- Are bank statements reconciled to the general ledger regularly?
- Ensure that journals are only posted once to the general ledger

13.13. Purchasing and payables

Purchasing modules

The purchasing module is used to create and maintain suppliers, enter requisitions and request for quotations and, issue purchase orders. The purchasing module integrates with other modules in the following manner:

- Payables module - when invoices are created in payables and matched against a purchasing order, the purchase order data is copied from purchasing to payables.
- General ledger module - purchasing transfers commitment information to the general ledger and the form of encumbrance journals

Payables module

The payables module is used to enter invoices received from suppliers and make payments issuing EFT/ cheques. The payables module integrates with other modules in the following manner:

- Purchasing module - purchase order information for matching against invoices is obtained from the purchasing module. The supplier database is also shared between purchasing and payables
- General ledger module - the accounting entries are passed out to the general ledger

Risks relating to the purchasing and payables module

- Entity may use unapproved vendors
- Unauthorised requisitions can be processed on the system
- Purchase orders may not comply with the relevant procurement policies and procedures
- Cancelled purchase orders may be processed for payment.

Audit procedures the auditor can perform

- How do you prevent the use of unapproved suppliers via the ERP system?
- How do you control unauthorised personnel entering requisitions on the system?
- Who grants access to various components of the ERP system and who approves the access privilege
- How do you prevent personnel bypassing or overriding access controls in the ERP system?

13.14. Cash management

Cash management entails the following:

- Accessing budget information, cash collection, receipts and banking by ministries, releases from Treasury and payments
- Reconciliation of bank accounts (manual or online)
- Different banking arrangements
- Cash forecasting

Risks relating to the cash management receipts

- Not all cash received are recorded
- Captured cash receipts maybe inaccurate, incomplete, and not in a timely manner

Audit related questions

- How do you ensure that all cash received are recorded on the ERP
- How do you ensure that all cash received are entered accurately, completely and on a timely basis

13.15. Receivables

Accounts receivables and miscellaneous receipts information are processed and integrated in to the general ledger.

Risks associated with receivables:

- Poor debtor management
- Irregular payments by debtors
- Duplication of debtors
- Bad debt write-offs may not be valid.

Audit related questions

- Review the system to determine whether proper controls are built in the ERP to properly manage debtors

- Request a list of all debtors captured on the ERP and test for duplication

- Request the policy managing the write off of bad debt and test whether application controls were built into the ERP to comply with the policy

13.16. Budgeting

The public-sector budgeting module provides the approved budget and supplementary budget information to the general ledger.

Budgets are prepared and transferred into the general ledger module for appropriation and execution. The available budget information is passed onto Public Sector Financials for issue of accounting warrants. The accounting warrant information is used by purchasing, payables, and general ledger modules in order to transact.

Risks associated with the budgeting module:

- Funds are released in excess of the budget

- Unauthorised budget revisions are made on the ERP Inaccurate budget reports

Audit related questions

- How does the auditor test the release of funds which are in excess of the budget?

- Review the budget revisions procedures, and ensure that controls are built into the ERP that only appropriate personnel can make the necessary changes to the budget

- Review budget reports and confirm the accuracy and the completeness of the reports

- Check whether the Chart of accounts is configured in line with the relevant public financial management laws and regulations?

13.17. Sales and marketing module

Sales module implements functions of order placement, order scheduling, shipping and invoicing. Sales module is closely integrated with organisations e-commerce websites. Many ERP vendors offer online store front as part of the sales module. ERP marketing module along with CRP supports lead generation, direct mailing campaign and other marketing works.

13.18. Inventory

Inventory module facilitates processes of maintaining the appropriate level of stock in a warehouse. The activities of inventory control involve identifying inventory requirements, setting targets, providing replenishment techniques and options, monitoring items usages, reconciling the inventory balances and reporting inventory status. Integration of inventory control module with sales, purchase, finance modules allows ERP systems to generate vigilant executive level reports.

13.19. Human resource management

The HR management module streamlines the management of human resources. It maintains a complete employee database including contact information, salary details, attendance, performance evaluation and promotions of all employees.

13.20. Production module

Production planning optimises the utilisation of manufacturing capacity, parts, components and material resources using historical data.

13.21. Application security

Application security is aimed at the following:

- Continued availability of the system
- Integrity of the information stored on the system
- Preservation of confidentiality of data in store and transit
- Adherence to trust and obligation requirements in accordance with applicable laws and regulations.

Risks

- Failure to identify operating system deficiencies
- Unauthorised access
- Loss of confidentiality Loss of privacy
- Unavailability of the system / business continuity Breach of laws and regulations
- Irregularities, fraud, wrong doings, errors and omissions
- Loss of audit trail
- Failure to identify security threats.

Password parameters differ from one entity to another, but the ICT policies should clearly indicate the acceptable rules, which the IT auditor should test the systems against. Outlined below are some of the audit procedures and audit of the questions which the auditor may look at:

- Review the logical access controls in place for the ERP system and match it to the job descriptions
- The auditor should review the following settings:
  - Auditor should also ensure that the password length, composition, history and other parameters are in line with the policy of the organisations

- Default passwords should be changed when the ERP is implemented

- User should only have three attempts to enter an incorrect password before the system locks the user out

- Powerful user roles/profiles, including default super user accounts should assigned in line with functional responsibilities

- Access to critical tables/databases should be granted the basis of a business need

- Auditor should ensure that the audit trail is enabled on the ERP and that the audit trail is reviewed regularly.

The modules mentioned are typical common modules. ERP modules will vary in organisations depending on system and industry e.g an ERP in a university will have modules an ERP in a municipality won't have.

13.22. Tools available to assist the auditor in performing an ERP audit

There is a vast number of tools available to assist the auditor with an ERP audit. Some of the tools available include:

- SAP – Audit Information System – the auditor is able to extract various reports relating to business and system audit.

- Audit vault – can be used to audit oracle

- ACL – scripts can be run to extract data direct from tables as well as to get specific alerts

- IDEA

- All major ERP vendors have courses which the auditor can attend to assist him in his understanding of how specific ERP system works, which transaction Ids will be needed to obtain certain information from the system.

14. CHAPTER 14: REPORTING

14.1. Reporting standards

ISSAI 1700 - ISSAI 1700 (Forming an opinion and reporting on financial statements) stipulates that the auditor's opinion has to be reported in the form as specified by the standard.

ITAF (A professional practices framework for IT assurance) provides guidance on the design, conduct and reporting of IT audit and assurance assignments, defines terms and concepts specific to IT assurance and establishes standards that address IT audit and assurance professional roles and responsibilities, knowledge and skills, and diligence, conduct and reporting requirements.

At the end of each audit the auditor should prepare a written report, as appropriate, setting out the findings in an appropriate form. The content should be easy to understand and free from vagueness or ambiguity, include only information which is supported by competent and relevant audit evidence, and be independent, objective, fair and constructive.

- Ideally, IT Audit is a part of a financial audit
- IT Audit finding may be reported as a part of the financial audit management letter if the weaknesses uncovered are material, these could include
    - ✓ Classification of the finding;
    - ✓ Description of the finding;
    - ✓ Implication;
    - ✓ Recommendation;
    - ✓ Management response; and auditor's comments
- Some SAI's summarize the management letter and issue them as public reports in line with ISSAI 1700 Practice Note (PN) 5

ISSAI 1706 has options to include IT issues in a Financial Audit Report under sections:

- Emphasis of Matter
    - Significant internal control weaknesses
    - Propriety issues
- Other Matter
    - Control weaknesses

14.2. Levels of reporting

The auditor should report on their findings in a timely manner and should be constructive and useful to the audit entity. The auditor may report to many different bodies, depending upon why the audit was carried out. For example:

- ➢ The auditor may have been asked by the audit entity to carry out the control review
- ➢ The funding or sponsoring body may have requested the review
- ➢ The review may have been part of an annual financial audit and the auditors' findings may be incorporated in the annual audit report
- ➢ The audit may have been commissioned on behalf of a regulatory body.

The levels of reporting can be executed irrespective of the above, but the reporting requirements of each of the above will vary from one client to another and from one SAI to another. The auditor should determine who the final recipient of the report will be and adjust the report accordingly.

There are three levels of reporting in the audit process:

- ➢ **The discussion draft** - the reporting process begins with the discussion of the first draft. This draft is sent to the client's middle management prior to the closing meeting. The draft is then included as a matter for discussion in the closing meeting. This allows any inflammatory wording, factual errors or inconsistencies to be identified, corrected or eliminated at an early stage. Once the client and the auditor have discussed the contents of the discussion draft, the auditor makes the necessary amendments and sends the client the first Formal draft.
- ➢ **The management letter (formal draft)** - is given to the client so that they can respond to the observation raised. This allows management to concentrate on the findings, conclusions and recommendations in the formal draft which they receive. At this point it is the duty of management to formally write to the auditor comments/responses to all the findings.
- ➢ **Audit report (final audit report)** - when client's comments are received, the auditor then prepares a response indicating the audit position, this is achieved by putting together the auditor's comments and the client's response in one report which is the Audit Report

14.3. Elements of standard reports

Each SAI generally has one or more report types and templates that they use for various types of reports. However, there are some common themes in all audit reports. Given below are two standard reporting formats that may be used for reporting findings of financial audit and an IT audit report respectively. These formats are based on ISSAI 1700.

14.4. Financial audit report

14.4.1 *The auditor's standard report*

An auditor presents a standard report which contains the opinion formed by the auditor. The key elements required for auditor's report to meet International auditing standards are:

- The report is in writing

- The report has a title that clearly indicates that it is the report of an independent auditor

- The report is addressed as required by the circumstances of the engagement. This is usually specified in law or regulation.

The auditor issues a standard report when he or she has formed an unmodified opinion.

Contents of a report - the auditor's standard report shall include the following nine sections: **Introductory paragraph**

The introductory paragraph:

- Identifies the entity whose financial statements have been audited; States that the financial statements have been audited;

- Identifies the title of each statement that comprises the financial statements;

- Refers to the summary of significant accounting policies and other explanatory information;

- Specifies the date or period covered by each financial statement comprising the financial statements.

Management's responsibility for the financial statements

The report includes a section with the heading "management's responsibility for the financial statements". This section describes the responsibilities of those in the organisation that are responsible for the preparation of the financial statements. The auditor may use the wording of the law or regulation to describe these responsibilities if they are considered equivalent to the wording in the standard auditor's report

Auditor's responsibility

The report has a section with the heading "auditor's responsibility" that states that the responsibility if the auditor is to express an opinion on the financial statements based on the audit and indicates that the audit was conducted in accordance with International Standards on Auditing (ISSAIs) or in accordance with the SAIs legal mandate. The report has a brief description of an audit. Where the financial statements are prepared in accordance with a fair presentation framework, the description of the audit in the auditor's report refers to "the entity's preparation and fair presentation of the audit in the auditor's report refers to "the entity's preparation of financial statements that give a true and fair view", as appropriate in the circumstances. The auditor's report states whether the auditor believes that the audit evidence the auditor has obtained is sufficient and appropriate to provide a basis for the auditor's opinion.

Auditor's opinion

The report includes a section with the heading "Opinion: which presents the opinion formed on basis of the auditing evaluation. When expressing an unmodified opinion on financial statements prepared, the wording of the unmodified opinion is dependent on which financial reporting framework is used. In accordance with a fair presentation framework, the auditor's opinion, unless otherwise required by law or regulation, uses one of the following phrases, which are regarded as being equivalent

14.5. Other Reporting Considerations

Public reporting

The auditor should take into consideration that some issues that may be reported in an IS audit may severely increase the vulnerability of that system to access by unauthorised persons. The SAI should come up with ways of how such matters are tabled in Parliament and corrective measures taken.

Communication with Regularity Auditors & Reporting on key financial information systems

IT Auditors should always have in mind the financial (or other) auditors who are auditing financials produced by the information systems being audited. Weaknesses identified, especially those affecting reliance on the system to produce true and fair financial statements, should be communicated and discussed with the Financial Auditors. The auditor should reduce the technical jargon to make the issues understandable by the financial auditor.

Key financial systems, typically the IFMIS, produce the bulk of the financial statements which are audited by the SAI. Herein lies the importance of the IT Auditors auditing these systems and communicating control weaknesses to the FA teams. Where additional audit procedures need to be performed by the Financial Auditor at the ministries or agencies, this should also be communicated to the RAs stating the extent of procedures and implications of findings on their audit work. Consideration of the Financial Auditors competence to performs those procedures should also be discussed.

15. REFERENCES

- AFROSAI-E regularity audit manual
- CISA Item Development Guide
- CISA Review Manual - 2011 & 2015
- COBIT 5
- http://www.intosaiitaudit.org/intoit_articles/25_p30top35.pdf
- IFRS – reporting requirement on IT issues
- ISACA Audit Program: Business Continuity Management Audit/Assurance Program (Sep 2011)
- ISACA Audit Program: Crisis Management Audit/Assurance Program (Aug 2010)
- ISACA Audit Program: IT Continuity Planning Audit/Assurance Program (Jan 2009)
- ISACA Audit Program: Mobile Computing Security Audit/Assurance Program (Oct 2010)
- ISACA Audit Program: Outsourced IT Environments Audit/Assurance Program (Jan 2013)
- ISACA Board briefing on IT governance 2nd Edition 2003
- ISACA Standard and guidelines
- ISO 27001
- ISO 27002
- ISO/IEC 38500 Corporate Governance of Information Technology
- The Risk IT Framework
- The Risk IT Practitioner’s Guide
- *ISSAIs 1220 and 1330*
- ISSAI 5300, 1220, 1315, 1330, 5450, 5310
- Manual for Information Technology Audit- India
- Report on the Committee on the Financial aspects of Corporate Governance, Sir Adrian Cadbury, London, 1992 ISBN 0 85258 9131
- WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions