

Information Technology Audit Manual

State audit institution Information Technology Audit Methodology (SITAM)

2015

1. PREFACE	3
1.1 MANUAL CONTENTS.....	3
1.2 INTRODUCTION	4
1.3 INFORMATION TECHNOLOGY AUDIT PARTICULAR STANDARDS.....	6
2. MANUAL MAINTENANCE	7
2.1 GENERAL RULES	7
2.2 AUTHORITY	8
2.3 CONDITIONS.....	8
2.4 TIMING.....	10
2.5 PROCEDURE	11
3. CONFIDENTIALITY POLICY.....	15
3.1 CONFIDENTIALITY	15
3.2 RIGHTS	16
3.3 LEGAL RECOURSE.....	16
4. INFORMATION TECHNOLOGY AUDIT	17
4.1 IT AUDIT DEFINITION AND OBJECTIVE	17
4.2 NEED FOR IT AUDIT	17
4.3 APPLICATION OF IT AUDITS	18
4.4 IT CONTROLS.....	19
4.5 APPLICATION CONTROLS	19
4.6 SAI ROLE IN IT AUDITS.....	20
5. SAI IT AUDIT METHODOLOGY (SITAM).....	21
5.1 OVERVIEW	21
5.2 SITAM ROAD MAP	22
5.3 SITAM APPROACH.....	23
5.4 SITAM IT CONTROLS.....	24
5.5 IT HEALTH CHECK.....	26
5.6 ASSESS IT COMPLEXITY	26
5.7 ASSESS IT CONTROL MATURITY.....	27
5.8 DETERMINE IT AUDIT REQUIREMENTS	29
6. PLANNING.....	31
6.1 UNDERSTAND AUDIT OBJECTIVES AND SCOPE OF THE IT AUDIT.....	31
6.2 UNDERSTAND THE ORGANIZATION.....	32
6.2.1 <i>Understand the management and organization</i>	<i>32</i>
6.2.2 <i>Understand the external and internal factors affecting the operations</i>	<i>32</i>
6.2.3 <i>Understand the key business processes and operations.....</i>	<i>32</i>
6.2.4 <i>Understand the applications supporting the business process</i>	<i>33</i>
6.2.5 <i>Understand the IT infrastructure</i>	<i>33</i>
6.3 IDENTIFY AND UNDERSTAND SYSTEMS RELEVANT TO AUDIT SCOPE.....	34
6.4 IDENTIFY CRITICAL CONTROL POINTS.....	34
6.5 IDENTIFY IT CONTROLS RELEVANT TO AUDIT OBJECTIVE.....	35
7. EXECUTION.....	36
7.1 IT AUDIT EXECUTION	36
7.1.1 <i>Perform Walkthroughs</i>	<i>37</i>
7.1.2 <i>Design Test of IT Controls</i>	<i>37</i>
7.1.3 <i>Execute Test of IT Controls</i>	<i>38</i>
7.1.4 <i>Document and Evaluate the Results</i>	<i>38</i>
7.1.5 <i>Respond to Ineffective IT Controls</i>	<i>39</i>
7.1.6 <i>Determine the Level of Reliance of IT Controls Relevant to Audit Scope</i>	<i>39</i>
7.2 IT GENERAL CONTROLS.....	40
7.2.1 <i>Overview</i>	<i>40</i>
7.2.2 <i>Organizational and Management Controls</i>	<i>42</i>
7.2.3 <i>Change Management</i>	<i>43</i>
7.2.4 <i>Access Controls</i>	<i>44</i>
7.2.5 <i>IT Operational Controls.....</i>	<i>46</i>

7.2.6	Security Management	49
7.2.7	Business Continuity Management	50
7.3	APPLICATION CONTROLS	52
7.3.1	Overview	52
7.3.2	Data Input	54
7.3.3	Data Processing.....	55
7.3.4	Data Output.....	56
7.3.5	Master Data Setup and Maintenance	57
7.3.6	Interface Strategy and Design	58
8.	REPORTING	59
8.1	OVERVIEW	59
8.2	REPORTING FOR FINANCIAL AUDITS	60
8.3	REPORTING FOR PERFORMANCE AUDITS	60
9.	APPENDICES	62
	THIS SECTION INCLUDES THE FOLLOWING APPENDICES:	62
	APPENDIX A: COMPUTER ASSISTED AUDIT TECHNIQUES AND TOOLS	63
	APPENDIX B: IT HEALTH CHECK TOOL OVERVIEW.....	69
	APPENDIX C: DETAILED IT AUDIT ASSESSMENT TOOL OVERVIEW	70
	APPENDIX D: LEADING PRACTICES, FRAMEWORKS, AND STANDARDS	74
	ISO27001:2005.....	74
	BS 25999: 2006	76
	PAYMENT CARD INDUSTRY – DATA SECURITY STANDARD (PCI – DSS).....	77
	COBIT FRAMEWORK	78
	CAPABILITY MATURITY MODEL INTEGRATION (CMMI)	80
	TOGAF FRAMEWORK	81
	APPENDIX E: TECHNICAL TERMS USED IN THE MANUAL.....	82
	APPENDIX F: IT AUDIT CHECKLIST.....	83

1. Preface

1.1 Manual Contents

The IT Audit manual encompasses methodologies that will be followed in addressing and performing information technology audits by the State Audit Institution (hereinafter 'SAI'). The manual also includes reference to detailed IT General controls and Application controls to be used in the course of audits. For that purpose, the manual has been divided into the following sections and indices:

Preface

This section provides a quick overview of SAI as an organization, manual contents, its format, and basic policy statements on manual usage responsibility and authority.

Manual Maintenance

This section depicts the periodic review process of SAI IT audit methodology. Authority, conditions, and timing leading to such exercise are part of this section. The amendment policy and related form are also part of this section.

Confidentiality Policy

This section provides a broad reiteration of the confidentiality policy of SAI in dealing with the manual as being restricted to the use of SAI employees. The section also depicts the policy and procedure of distributing the manual to new and existing employees as well as its distribution following a change in it. Distribution of the manual is based on a preset suggested form created for that purpose. This section also provides a guide on legal recourse based on applicable rights in case of non-compliance with the policy statements stated in this section.

Applicable Methodology and Standards

This section has a direct reference to the relevant international, regional and local, if any, auditing standards that it is based upon and the need to review such standards that are applicable to SAI whenever a change occurs.

Overview

This section provides an overview of the importance of IT and IT Audits for government entities in the recent period. Additionally, this section provides a brief overview of the:

- Objective of IT Audits
- IT Audit Standards
- Understanding the IT Environment
- Overview of IT General Controls and Application Controls

SAI IT Audit Road Map and Approach

This section provides a graphical representation of the overall IT Audit Methodology for SAI. It clearly lists the various phases and steps involved in conducting an end-to-end IT Audit.

Preliminary IT Assessment

This section involves the IT Health Check of the IT Complexity and IT Controls Maturity for the entity's IT environment. The results of this preliminary assessment provide the basis for determining the IT Audit requirements for the auditee. A Preliminary IT Assessment Tool shall be used to meet the objective of this phase.

Planning

The planning section of the audit provides a detailed insight into the activities to be carried out in the planning phase. The key steps in this phase include:

- Understanding Audit Objectives and Scope of IT Audit: This phase aims to identify what kind of an audit needs to be carried out (supporting financial or performance audits) along with the scope of the IT audit

- **Understand the Business:** This phase enables the auditor to obtain and document an understanding of the auditee sufficient to plan and perform the audit in accordance with applicable auditing standards and requirements.
- **Identify and Understand Systems Relevant to Audit Scope:**
- **Identify Critical Control Points:** This phase provides the auditor and overview of identification and documentation of critical control points in the design of auditee's IT systems based on the auditor's understanding of such systems, key areas of audit interest, and IT risk.
- **Identify IT Controls Relevant to Audit Objectives:** This phase helps the auditor to identify control categories and control domains that are relevant to the IT audit.

Execution

This section guides the auditor to use information obtained in the planning phase to evaluate the effectiveness of IT controls (ITGCs and Application Controls). The key steps in this phase include:

- **Perform Walkthroughs:** This phase guides the IT auditor to test the design effectiveness of IT controls
- **Design Test of IT Controls:** This phase guides IT auditors to perform an appropriate mix of audit procedures to obtain sufficient, appropriate evidence to support their conclusions while assessing the operating effectiveness of IT controls
- **Execute Test of IT Controls:** Based on the information obtained in the design phase, the IT auditor tests the operating effectiveness of IT controls
- **Document and Evaluate the Results:** In this phase the IT auditor uses the Detailed IT Audit Assessment Tool to document the results of the Walkthroughs and Test of Controls of each control within the IT General Controls and Application Controls
- **Respond to Ineffective IT Controls:** In this phase the auditor lists control objectives that are rated ineffective and identifies a response for them
- **Determine the Level of Reliance of IT Controls Relevant to Audit Scope:** Based on inputs gathered from previous phases, the IT auditor provides a conclusion whether to provide "Rely" or "No-Rely" on IT controls

This section also provides an in-depth description of the IT General Controls and Application Controls

Reporting

This phase provides an overview of summarizing the results of the audit, drawing conclusions on the individual and aggregate effect of all identified IT control weaknesses on audit risk and audit objectives. This phase also highlights differences between reporting requirements for financial and performance audits.

1.2 Introduction

The Purpose of this manual

This manual provides a methodology for performing information system control audits (IT audits) in accordance with universally accepted practices in this area. This manual provides a methodology for assessing the effectiveness of IT controls, and the IT controls that auditors evaluate when assessing the confidentiality, integrity, and availability of information and IT systems. IT controls consist of those internal controls that are dependent on information systems processing and include general controls and application controls. This manual focuses on such IT General Controls and Application Controls.

This manual is intended for the auditors of State Audit Institution (SAI) to assist in performing IT audits as part of both financial and performance audits

Enhanced Role of IT in Government Entities in Oman

The use of Information Technology (IT) within government entities in Oman has become increasingly significant in recent years owing to the following:

- His Majesty's Vision on IT
- Implementation of Digital Oman Strategy initiatives by Oman IT Authority (ITA).

His Majesty's Vision on IT

His Majesty Sultan Qaboos Bin Said emphasized the importance of Information Technology and Communications in the following message in the Annual session of the council of Oman in November 2008.

"Information technology and communications have now become the main elements that move forward the development process in this third millennium; therefore, we have accorded our attention to finding a national strategy to develop the skills and abilities of citizens in this domain with the aim of further developing e-government services. We are closely following the important steps that we have made in this regard. We call upon all government institutions to speedily enhance their performance, and to facilitate their services, by applying digital technology in order to usher the Sultanate into the constantly evolving spheres for applying knowledge."

Sultan Qaboos bin Said

The Annual Session of the Council of Oman

November 2008

Digital Oman Strategy Initiatives

The ITA developed Digital Oman Strategy to transform Oman by empowering its people, through the eOman initiative, besides opening up job opportunities for nationals in the IT sector, within the digital society. The goal includes a significant improvement in the quality of services the government provides to its citizens.

The implementation of the strategy began in 2003 with the following focus areas:

- Setting up a unified e-Government architecture including IT infrastructure, applications and shareable databases of services and public information
- Connect government entities with secure ICT network
- Availing broadband communications throughout the Sultanate to individuals and businesses
- Creating an IT governance framework, standards and guidelines for national ICT infrastructure, and a security framework
- Simplifying and streamlining all government processes by business process reengineering
- Enabling customer-centric e-Government services for both individuals and businesses and streamlining them within the common IT infrastructure
- Enabling easy access to timely and relevant public information accessible to all through a wide range of delivery channels
- Developing plans and policies for training and development of human resources in IT while enhancing existing competencies
- Empowering consumers with IT skills and knowledge through awareness and training campaigns and enabling them to perform their duties more efficiently and conveniently
- Deploying ICT education and training programs suitable for various segments of the society based on systematic studies and comprehensive planning

- Creating formal and informal communication channels between government organizations, academic institutions, private sector and individuals

In view of the above, government entities have become increasingly dependent on information systems to carry out their operations and to process, maintain, and report essential information. Majority of operations of Government entities are supported by automated systems and electronic data, and they would find it difficult to carry out their operations without these information assets. The effective and efficient management of IT is vital to the success of most entities.

1.3 Information Technology Audit Particular Standards

Principles, methodologies, and standards included in this manual is the result of development work accomplished by the State Audit Institution, which has developed the manual in light of principles, methodologies, and standards that are considered as international best practices in IT auditing in particular and in governmental auditing in general.

Professional resources referred to being leading practice resources during the development of the manual is represented in the following main professional standard setting bodies' resources:

- Information Systems Audit & Control Association represented by the IT Audit Standards and Cobit® Framework
- ISO 27001:2005 (Information technology — Security techniques — Information security management systems — Requirements)
- ISO 20000: 2005 (Information technology — Service management — Specifications)
- ITIL Infrastructure Library (ITIL) Version 3
- BS 25999: 2006 (Business Continuity Management)
- Institute of Internal Auditors represented by the International Standards for the Professional Practice of Internal Auditing
- International Organization of Supreme Audit Institutions represented by INTOSAI Standards as well as the branching regional organizations' standards including the ARABOSAI, AFROSAI, CAROSAI, EUROSAI, SPASAI if different from the INTOSAI
- Oman eGovernment Architecture Framework (OeGAF)

Reference to the above resources has been in the context of referring to international leading practices representing the auditing professional body only. SAI has developed its own standards based on its own audit environment needs and legal requirements, but at the same time, this has been done in line with such international leading practices. Thus, all related copyright disclosures and requirements have been adhered to in that context.

In addition to IT auditing standards, IT auditors need to be aware of other laws, regulations, or other authoritative sources that may impact the conduct of an IT audit. The IT audit work carried out by State Audit Institution (SAI) should be guided by international standards or the IT auditing standards applicable for Sultanate of Oman.

2. Manual Maintenance

2.1 General Rules

Auditing standards, including IT Auditing standards, are a content of dynamic nature that should be periodically reviewed and updated to reflect any changes internally or externally.

To ensure that manual sections are maintained and updated, SAI IT Audit Unit designated Head should assign responsibility for particular sections to specific personnel after attaining the approval of the IT audit unit standards committee.

Each section should be specifically assigned to an employee (resource person) in the IT Audit Unit.

While separate sections' maintenance are distributed, one senior employee may be responsible for coordinating all manual section development, implementation, and ongoing reviews to be raised to the committee, being represented in the designated IT Audit Unit Head.

This employee's job responsibilities, authority, and monitoring requirements should be clearly detailed in his/her job description in relation to development and amendments of the manual section responsible of.

The designated IT Audit Unit Head could possibly hold the post of the Head of the IT Audit Unit.

SAI's IT Auditors should maintain a schedule listing each section, the employee responsible for the section, the date the section was adopted, the date it was last reviewed or revised, and other pertinent data.

Ongoing training regarding SAI IT Audit manual sections is an integral part of the continuous improvement and maintenance process.

The objective of any training program should be to reinforce management's and staff's understanding of what IT audit standards are, how they were created, how they should direct the Unit's activities, and the benefits derived from establishing such standards in various sections of the manual.

2.2 Authority

The authority to review standards in SAI is directly related to the type of review under question. If the review process entails a change in the methodology or standards leading to a change in the SAI founding law and its amendments, then such an authority is vested in the Cabinet of Ministers of the Sultanate of Oman. In such cases, SAI acts as a consultant to the Cabinet of Ministers in recommending and justifying changes to the SAI founding law.

If the review process entails a change in the methodology or standards without any resulting change in the SAI founding law and any amendments thereto, then such an authority is vested internally in the President of SAI who in turn assigns and delegates such authority to various sectors and divisions within SAI. This is further elaborated in the procedure section relating to a change request process and the resulting amendment procedures in the manual.

As a result, SAI's IT Auditors will manage any internal changes in its own methodology and standards represented in this manual as a result of a need for a change not affecting SAI's establishing law.

SAI will be having the option and right to consult external professional organizations in attaining advice on such changes.

2.3 Conditions

Conditions leading to such a change or a group of changes will be either internal or external in nature. Any changes in the laws, rules, and regulations could lead to a necessity in changing SAI standards and methodology in whole or in part:

2.3.1 External conditions:

Such conditions are represented in changes in the laws, rules, and regulations that are mostly external in nature. In anytime that the laws and regulation are amended in whole or in part, SAI could review and amend its own audit methodology and standards insofar their relation to the laws and regulation.

External conditions leading to a change in the IT auditing standards could be resulting from an identifiable change in pattern represented in international professional auditing standards. Such changes are reflected in the standards particular to the following professional bodies:

- Information Systems Audit & Control Association represented by the IT Audit Standards and Cobit® Framework
- ISO 27001:2005 (Information technology — Security techniques — Information security management systems — Requirements)
- ISO 20000: 2005 (Information technology — Service management — Specifications)
- ITIL Infrastructure Library (ITIL) Version 3
- BS 25999: 2006 (Business Continuity Management)
- Institute of Internal Auditors represented by the International Standards for the Professional Practice of Internal Auditing
- International Organization of Supreme Audit Institutions represented by INTOSAI Standards as well as the branching regional organizations' standards including the ARABOSAI, AFROSAI, CAROSAI, EUROSAI, SPASAI if different from the INTOSAI
- Other whenever applicable
- SAI will review and amend its own audit methodology and standards insofar their relation to the above mentioned standards, and especially particular components of the manual that do reflect similar concepts portrayed in the other international standards being referred to above.

2.3.2 Internal conditions:

Any of the following list of internal organizational conditions could lead to a change in SAI's audit methodology or standards, in whole or in part. This could be represented in the following conditions:

- Changes in functions and activities of SAI due to internal changes in the functional or organizational structure
- Changes in internal business processes
- Changes in delegation of authority structures
- Changes in job roles, duties, and descriptions of employees
- Changes in SAI internal financial or employee related articles
- Changes in SAI services

SAI will review and amend its own audit methodology and standards insofar their relation to the above mentioned standards, and especially particular components of the manual that do reflect similar concepts portrayed in the other international standards being referred to above.

2.4 Timing

Timing and frequency of review of standards is either periodic & cyclical in nature or non-cyclical conditions based, explained in the following:

Periodic Cyclical Changes: To be able to enforce a 'culture of change', the change management process should be periodic in nature. To elaborate, any system reflecting a business process that is based on a methodology or a standard is not perfect in nature; thus, it requires a review over a period of time regardless of any internal or external conditions instigating a change. Thus, SAI will periodically review its audit standards and methodology at least once every five years.

Non-Cyclical Conditions Based Changes: Timing of such changes is directly linked to the necessity and urgency of such a change due to a requirement by law or a change in international auditing or accounting standards or other professional standards of international standard setting bodies and professional organizations' standards as stated in section 2.3.1.

Timing of such changes, if urgent in nature, then should be tied to the requirement of the law or a professional standard in setting a particular deadline to meet.

In other instances, where international standards or the law have not set a particular deadline, then professional judgment of SAI should apply in setting its own deadline to be within a maximum of a five-year period from the date of issuance of a particular law, regulation, or standard.

It should be also noted that such a review exercise is directly related to what SAI primarily follows, in whole or in part, as a result of a change in standards, practices, or methodologies of such standard setting bodies.

It should also be a matter of policy, in cases when SAI does not follow a particular standard setting body, and if such body issues a new standard, practice, or methodology, then SAI should at least consider the implications and compare to its own standards, practices, or methodologies from a benchmarking point-of-view that could eventually lead to a change in the latter at SAI.

2.5 Procedure

Two main sources of change requests could be accommodated. One is originating from within the IT Auditors, and the other being received from other SAI entities including other sectors, departments, or personnel.

If the request is internal, then each manual section has a responsible employee (resource person) who overlooks any developments, amendments, and as a result raises such requests to the appropriate authorities as indicated earlier.

If the request is external, then such a request should be received from a departmental manager at least. The request should be justified in that it relates to the audit being performed by another department.

This measure is introduced by SAI to limit and minimize instances where SAI could audit the same entity or issue more than once. It also creates a level of common awareness among all SAI sectors and the audits being performed by each, which would eventually lead to better audit coverage.

If the change request is from within the IT Auditors, then the following procedures apply:

- The requesting employee in the IT Auditors (resource person) has to fill out the Request for Amendment Form (see enclosed form 2.a. Request for Amendment Form) and address it to the Head of IT Audit Unit.
- The Head of IT Audit Unit conducts a review of the request.
- If the request is feasible, then the Head of IT Audit Unit forwards the same to the IT Audit Unit Head.
- The Head of IT Audit conducts a review of the request.
- If the request is feasible, then the Head of IT Audit forwards the same to the Standards Development Committee.
- The Standards Development Committee then convenes based upon the request from the IT Audit Unit Head.
- The committee reviews the request and considers the following implications as a result of a possible change to the contents of the manual:
 - i. Review human resource capabilities and discuss changes in personnel requirements;
 - ii. Review management information systems and discuss potential changes in IT requirements;
 - iii. Evaluate legal, regulatory, and accounting issues, and solicit comments from appropriate professionals if and when needed;
 - iv. Evaluate cross manual required changes as a result of a change in the IT Audit manual.
- If the committee partially approves on such changes, pending a partial change in the content of a request, then the request is returned back to the Head of IT Audit who will coordinate with the Head of IT Audit Unit to perform the required changes.
- The new changes are forwarded again to the Standards Development Committee to follow the same review and approval procedure.
- If the committee approves on such changes, then the request is forwarded to the President of SAI for final approval.
- If not approved, then the President of SAI refers back the process to the committee for further deliberation or for closure if the request is not considered appropriate for consideration by SAI.
- If approved, then the following implementation activities are taken into account by the IT Auditors:
 - i. The amendments are addressed by the Head of IT Audit and distribute the changes to the resource person responsible for including the amendments in the particular manual sections.
 - ii. The resource person performs the required changes and attains the approval of the Head of IT Audit Unit and the Head of IT Audit on the changes performed.
 - iii. Any changes are then printed and added to the manual sections and any required forms and other related materials are also included by the resource personnel.

- iv. Any new sections (including forms) are then distributed to the other relevant SAI departments or other resource personnel within the IT Auditors through the 1.4.1 Manual Distribution Form.
- v. After distribution, the resource personnel update form 2.5.2 Manual Maintenance Schedule included in this section of the manual.
- vi. IT Auditors coordinates with the Training Department to conduct a training session on the changes as a result.
- vii. IT Audit Unit Standards Development Committee monitors for compliance with the new standards.

2.5.1 Request for Amendment Form

Name of entity requesting amendments: _____

Section/s Reference: _____

Manual Section: _____

Section Name: _____

Description of needed amendments:

Proposed amendments:

Proposed by: _____ (Requesting Employee)

Reviewed by: _____ (Head of Employee)

Approval by: _____ (The Head of IT Audit)

Approval by: _____ (Standards Development Committee)

Final Approval by: _____ (SAI President)

Implementation Date: _____ (Set by IT Audit Unit Head)

Resource Person's Signature: _____ (Upon Final Approval)

2.5.2 Manual Maintenance Schedule

Section No.	Employee Responsible	Date First Adopted	Date Last Reviewed	Other Comments
1				
2				
3				
4				
5				
17				

3. Confidentiality Policy

3.1 Confidentiality

The manual and its contents are strictly for internal use and are as such treated as highly confidential material based on the general SAI confidentiality policy to follow:

- SAI's confidential and proprietary information is its most valuable asset and includes but is not limited to its own internal information as well as the information of its auditees.
- The latter information is SAI property and is protected by copyright and applicable laws.
- Every employee has the responsibility to safeguard it, to never disclose it, intentionally or inadvertently.
- Confidential information relating to SAI or to its audited entities could include the following:
 - i. Names and lists of employees
 - ii. List of applications used
 - iii. Type of network devices used
 - iv. Configuration information
 - v. Device specific policies
 - vi. Information related to missing controls
 - vii. Technical data not published previously
 - viii. Organizational matter information
- On the other extreme, information which is regarded as non-confidential is that which is – and accepted to be – openly discussed with outsiders within the context of “publicly disclosed” material and information.
- Classification of Confidential Information:
 - To guide employees in the handling of confidential information, including that contained in e-mails, SAI has established the following classifications:
 - i. “SAI CONFIDENTIAL: INTERNAL USE ONLY”
Information with this classification is not highly sensitive and can be distributed within SAI without restrictions. Examples of information included in this category are internal telephone listings, e-mail address listings and audit manuals.
 - ii. “SAI CONFIDENTIAL: NEED-TO-KNOW”
This information is more sensitive and valuable than “Internal Use Only” documents. Its dissemination is limited to employees who need the information to do their jobs. Information in this category might include policy information, device configuration information, technology inventory etc.
 - iii. “SAI CONFIDENTIAL: REGISTERED”
This is the most sensitive of all information. Registered documents must be numbered and each copy assigned to a specific recipient. These documents must be kept in a secure place at all times and should not be duplicated, except by their originator. Information in this category may include results from previous audits including information on missing controls.
- Disclosure of Confidential Information:
To enable the accomplishment of SAI's mission, from time to time SAI's proprietary information could be disclosed to auditees. However, such disclosure should never be done without carefully considering its potential benefits and risks. If SAI determines in consultation with an employee's manager and other appropriate SAI management level that disclosure of confidential information

is necessary for the purpose of completion of a particular IT audit, the employee must then contact the Head of IT Audit before any disclosure takes place.

- Specific policies have also been established on who may communicate information to the press and the community at large. All inquiries or calls from the press should be referred to the Office of the President of SAI or those delegated this responsibility by the President.
- Requests for Confidential Information:
 - i. Written Requests – All written requests for information to be provided by SAI shall be forwarded to the Office of the President of SAI. He will then decide whether such information should be disclosed to the requesting party after instructing the related Division Head.
 - ii. Verbal Requests – All verbal requests will be referred to the Office of the President of SAI. If the President of SAI is not present, such requests will be referred to the available Division Head. If none are present, such requests will be forwarded to the Office of the President of SAI for follow-up on a later date. If the request is by telephone or a personal visit to the SAI premises, the requestor will be referred to the Office of the President of SAI. If unavailable, the requestor should be asked to provide their name, entity name, telephone number and address, if possible. Also they should be asked the reason for the request and a brief description of the information desired. This information should be written down and forwarded to the Office of the President of SAI for follow-up. In all cases, verbal requests for any type of information should be limited.
- Electronic Mail:
 - i. E-mail is not always the most secure way to send or receive information. Do not forward or send email containing confidential information outside of the SAI's network.
 - ii. If there is a business need to communicate with someone outside SAI, confirm with your immediate supervisor in the IT Audit Team that an appropriate non-disclosure agreement has been signed before emailing information outside the network.
- Verbal Communication:
 - i. All employees need to use discretion when verbal communication is being used outside of SAI such as at social gatherings, conferences, and meetings.
 - ii. Do not give any information to the press or any market entity. Refer all press calls to the Office of the President of SAI.

3.2 Rights

All SAI rights are reserved as per local laws, rules and regulations pertaining to this publication.

No part of this manual may be reproduced, stored in any system or form, or transmitted in any form by any means – electronic, mechanical, photocopied, recorded, or otherwise – without the prior written consent of the State Audit Institution.

3.3 Legal Recourse

Violation of the above 'Rights' clause subjects an individual or an entity to applicable legal proceedings as per the laws of the Sultanate of Oman.

This manual is also subject to unauthorized use protection as per the internal articles and by-laws of the SAI as well as the Confidentiality policy stated above.

4. Information Technology Audit

4.1 IT Audit Definition and Objective

IT Audit is “the process of collecting and evaluating evidence to determine whether an IT system has been designed to meet the following objectives:

- Produce timely, accurate, complete and reliable information outputs,
- Ensure confidentiality, integrity, availability and reliability of data
- Adhere to relevant legal and regulatory requirements,
- Allow organizational goals to be achieved effectively and use resources effectively”.

4.2 Need for IT Audit

Use of IT Systems has brought about radically different ways of processing, recording and controlling information and has combined many previously separated functions. The potential for material system errors has thereby been greatly increased causing great costs to the organization.

The highly repetitive nature of many IT applications means that small errors may lead to large losses. For example, an error in the calculation of salaries to be paid to employees in a manual system will not occur in each case, but once an error is introduced in an IT system, it will affect each case. This makes it imperative for the auditor to test the underlying processes and to identify the vulnerabilities in an IT system.

Government entity employing the use of IT has objectives and expectation of what it intends to achieve from the large investment made in technology. Reasons for implementing IT within the organization include:

- Obtain business value through reduced costs,
- Greater effectiveness,
- Enhanced efficiency, and/or
- Increased service delivery.

It is against the above objectives that an IT auditor is required to provide assurance of effectiveness and efficiency of IT Systems.

Typically, the entity's goals and objectives in utilizing technology to support business processes include:

- Confidentiality;
- Integrity;
- Availability;
- Reliability; and
- Compliance with legal and regulatory requirements

Underpinning these goals and objectives is the need to ensure information technology and the controls supporting such technology, assists the organization to achieve its objectives (effectiveness) with an optimum use of resources (efficiency).

- Confidentiality: concerns the protection of sensitive information from unauthorized disclosure. Consideration needs to be given to the level of sensitivity of the data, as this will determine how stringent controls over its access should be. Management need assurance of the organization's ability to maintain confidentiality of information, as a compromise in confidentiality could lead to adverse visibility and loss of reputation, particularly where the information relates to sensitive information.

- **Integrity:** refers to the accuracy and completeness of information as well as to its validity in accordance with organization's requirements and expectations. This is an important audit objective to gain assurance on because it provides assurance to both management and external report users that the information produced by the organization's information systems can be relied and trusted upon to make important decisions.
- **Availability:** relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities. Given the high-risk nature of keeping important information stored on computer systems, it is important that organizations gain assurance that the information they need for decision-making is available when required. This implies ensuring that the organization has measures in place to ensure business continuity and ensuring that recovery can be made in a timely manner from disasters so that information is available to users as and when required.
- **Reliability:** refers to the degree of consistency of a system or the ability of a system (or component) to perform its required function under stated conditions. Reliability is an important audit objective in order to provide assurance that the system consistently operates and performs its stated functions as expected.
- **Compliance with Legal and Regulatory Requirements:** deals with complying with those laws, regulations and contractual obligations to which the organization is subject, that is, externally imposed business criteria. Management and key stakeholders require assurance that necessary IT Controls have been put in place, as there is a potential risk that the organization could incur penalties should legal and regulatory procedures not be enforced.

Increasing use of computers for processing organizational data has added new dimensions to the review and evaluation of internal controls for audit purposes. The IT controls are of great value in any IT system and it is an important task for an auditor to ensure the following:

- Adequate IT controls exist
- IT controls work effectively to ensure results and achieve objectives
- IT controls should be commensurate with the risk assessed so as to reduce the impact of identified risks to acceptable levels
- Evaluate the adequacy of IT controls in IT systems to mitigate the risk of loss due to errors, fraud, disasters or incidents.

4.3 Application of IT Audits

IT audit is part of the overall audit process, as IT audit can be applied in the implementation of:

- Financial Audits
- Performance Audits

It is important to have an understanding of the above types of IT audits that can be conducted. This understanding is required so that the development of audit programs and procedures is appropriately focused and their execution will ultimately satisfy the specific audit objectives

The objectives of undertaking an IT audit as a component of a financial audit include:

- Concluding on the effectiveness of controls over the information technology systems that have an impact on the processing of financial information.
- Where IT audit is involved in the performance audit, the objectives of the audit are further defined by what role IT is playing in the audit:
- Understanding how well management capitalizes on the use of information technology to improve its important business processes;
- Understand the pervasive effect of information technology on the auditee's important business processes;

- Understanding how auditee's use of information technology for the processing, storage and communication of information affects the internal control systems and consideration of inherent risk and control risk;
- Identifying and understanding the controls that management uses to measure, manage and control the information technology processes;
- Seek assurance that all aspects of the IT systems, including necessary controls, are being effectively enforced; and
- Examine the efficiency and effectiveness of a business process/government program and IT audit will be involved because IT is considered critical to the organization.

4.4 IT Controls

IT controls are set of policies, procedures and systems used to mitigate the risks associated with the IT environment and application systems.

IT controls are designed to provide reasonable assurance that the IT Systems achieve the following objectives:

- Produce timely, accurate, complete and reliable information outputs,
- Ensure confidentiality, integrity, availability and reliability of data
- Adhere to relevant legal and regulatory requirements,
- Allow organizational goals to be achieved effectively and use resources effectively

These controls are broadly classified into two categories:

- IT General Controls (ITGC)
- Application Controls

IT General Controls (ITGCs)

IT General Controls (ITGCs) create the environment in which the application systems and application controls operate.

IT General Controls (ITGCs) are concerned with the auditee's IT infrastructure, including any IT related policies, procedures and working practices. They are not specific to individual transaction streams or particular accounting packages or financial applications. In most instances the general controls elements of an IT review will concentrate on the auditee's IT department or similar function.

Examples include IT policies, standards and guidelines pertaining to IT security and information protection, application software development and change controls, segregation of duties, business continuity planning, etc.

4.5 Application Controls

Application controls pertain to specific IT applications. They include controls that help to ensure the proper authorization, completeness, accuracy and validity of transactions, maintenance and other types of data input. Examples include:

- Completeness checks: controls that ensure all records were processed from initiation to completion.
- Validity checks: controls that ensure only valid data are input or processed.
- Identification: controls that ensure all users are uniquely and irrefutably identified.
- Authentication: controls that provide an authentication mechanism in the application system.
- Authorization: controls that ensure only approved business users have access to the application system.

- Input controls: controls that ensure data integrity fed from upstream sources into the application system.

Application controls are unique to an application and may have a direct impact on the processing of individual transactions. These controls are used to provide assurance (primarily to management) that all transactions are valid, complete, authorized and recorded.

Since application controls are closely related to individual transactions it is easier to see why testing the controls will provide the auditor an assurance on the accuracy of a particular account balance. For example, testing the controls in a payroll application would provide assurance on the payroll figure in an auditee's accounts. It would not be obvious that testing the auditee's general IT controls (e.g. change control procedures) would provide a similar level of assurance for the same account balance.

4.6 SAI Role in IT Audits

As part of State Audit Institute's role in Sultanate of Oman, SAI performs independent financial and performance audit for the government entities. SAI auditor shall also carry out IT audits (as a component of Financial or Performance Audits). In IT audit supporting the financial audit, SAI shall evaluate the effectiveness of applicable IT General Controls and Application Controls to conclude whether to rely or not rely on data generated from financial systems. In IT audit supporting performance audit, SAI shall evaluate the effectiveness of relevant controls based on the scope and objective of the audit.

5. SAI IT Audit Methodology (SITAM)

5.1 Overview

SAI IT Audit Methodology (SITAM) is a framework developed for State Audit Institution to determine IT Audit requirements for the audited entity, and to provide the guidelines for carrying out detailed IT Audit (as a component of Financial or Performance Audits). The SITAM consists of four key phases:

- **Preliminary IT Assessment:** in which the IT Audit requirements of the auditee shall be determined.
- **Planning:** in which the IT auditor identifies the audit objective and scope, obtains an overall understanding of auditee's process, operations, and infrastructure, identifies key areas of audit interests, and determine the IT controls that shall be tested and evaluated as per audit scope.
- **Execution:** in which the IT auditor performs walkthroughs and test of IT controls, and evaluates the effectiveness of these controls. In this phase, the IT auditor also determines the level of reliance that can be placed on the IT controls relevant to audit scope.
- **Reporting:** in which the IT auditor document all findings and observation of the audit, and reports the findings relevant to audit scope to auditee's management.

5.2 SITAM Road Map

The following is the State Audit Institution IT Audit Methodology (SITAM) Road Map which encompasses the phase of the IT audit as well as the key aspects of each phase:

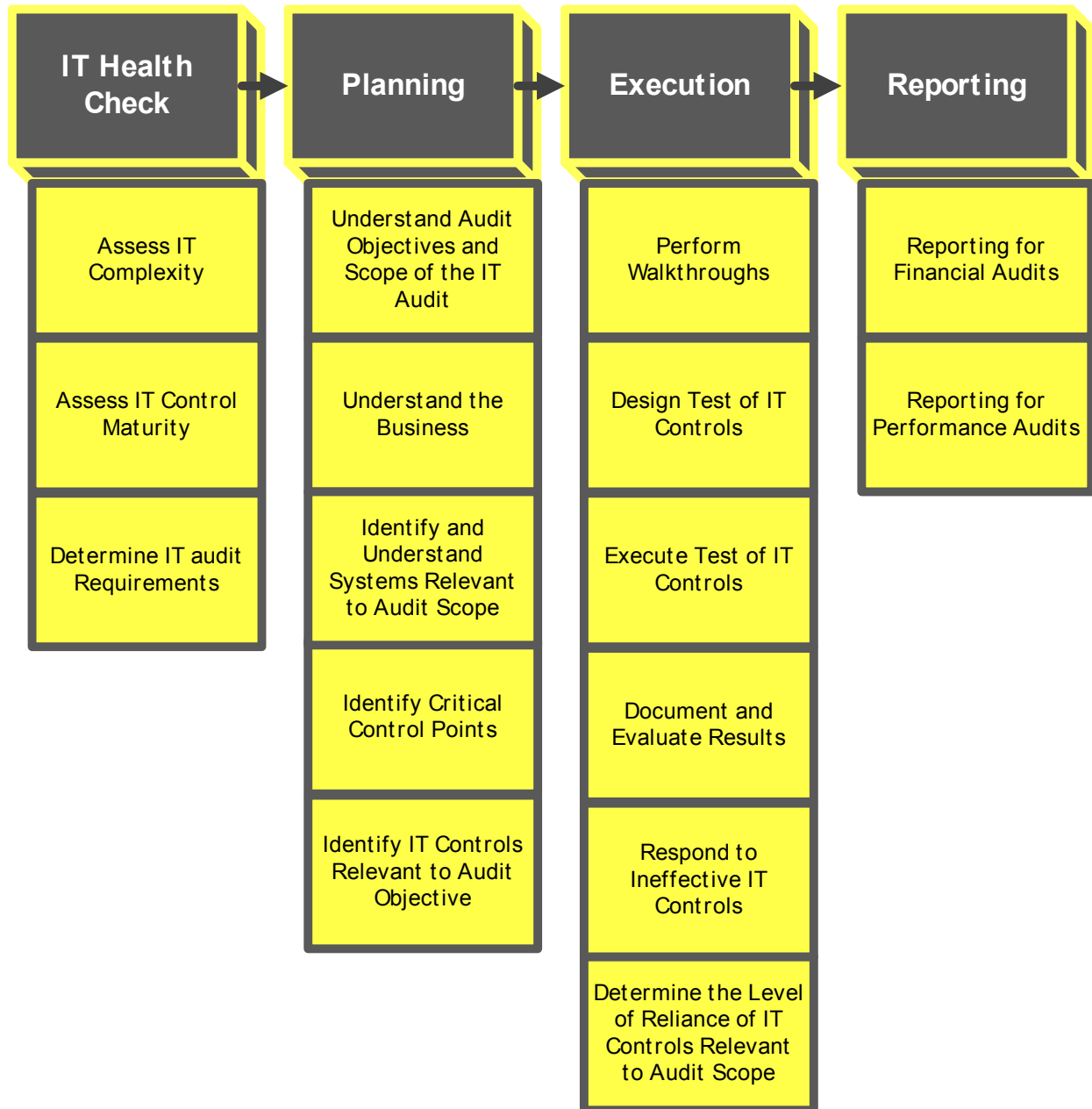


Figure 1.0 (SITAM Road Map)

5.3 SITAM Approach

The figure below represents the approach that SAI auditors shall follow to conduct IT audits (supporting financial and performance audits) as per SITAM. Further details of the activities in each phase (Preliminary IT Assessment, Planning, Execution, and Reporting) will be provided in the manual.

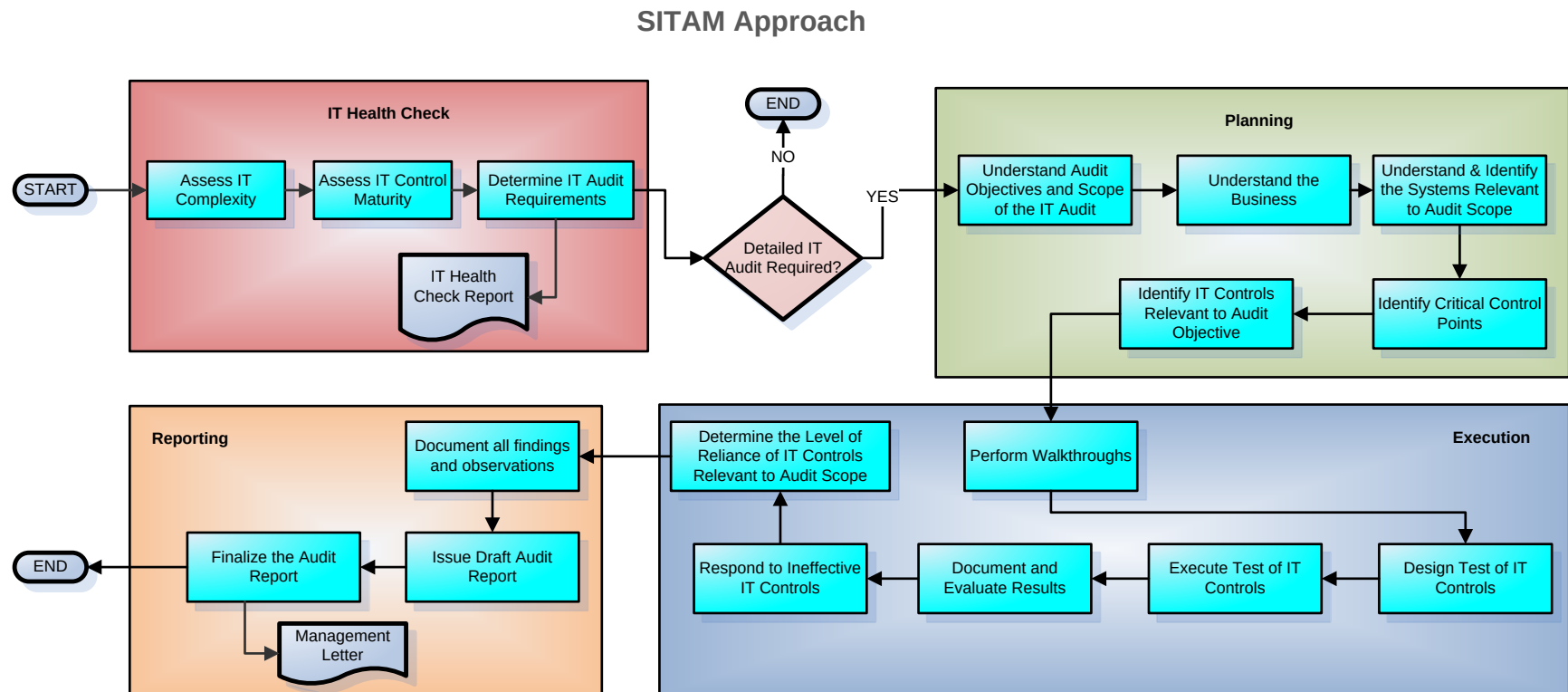


Figure 2.0 (SITAM Approach)

5.4 SITAM IT Controls

IT controls are structured in SITAM as following:

- **Control categories:** consist of 2 broad categories viz. IT General Controls and Application Controls. Each control category comprises of various domains that address different areas in Information Technology e.g. Change Management
- **Control Domain:** is a set of control objectives that aim to establish a complete area in Information Technology. Each domain addresses a unique area of Information Technology.
- **Control Objective:** are statements or desired result or purpose. Control objectives in a domain aim to achieve a different purposes that contribute towards the overall purpose of a domain
- **Control:** Controls: are statements that provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected. Controls of similar type make a control objective

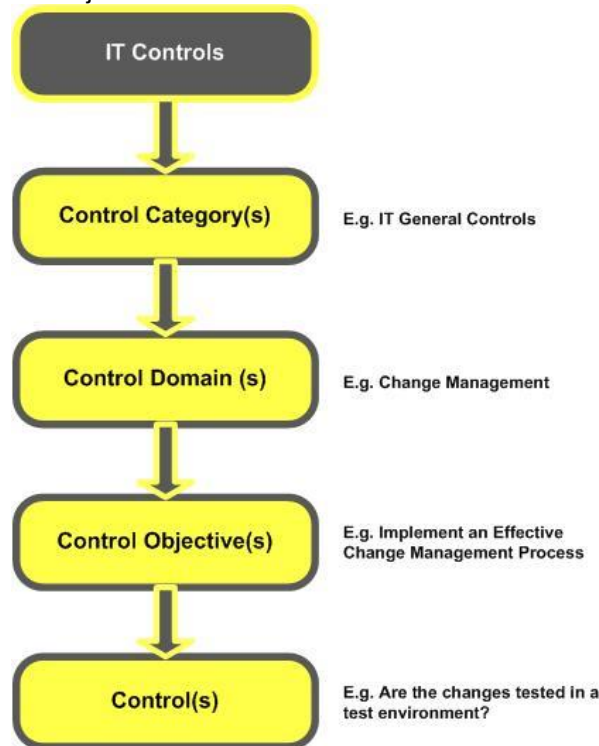


Figure 3.0 (SITAM IT Control Structure)

As per SITAM, there are two control categories within IT Controls: IT General Controls (ITGCs) and Application Controls. The Control Domains in ITGCs are: organizational and management controls, change management, access controls, IT operational controls, security management, and business continuity management. The Control Domains in Application Controls are: data input, data processing, data output, master data setup and maintenance, and interface controls. Moreover, description of control domains and associated control objectives is provided later in this manual.

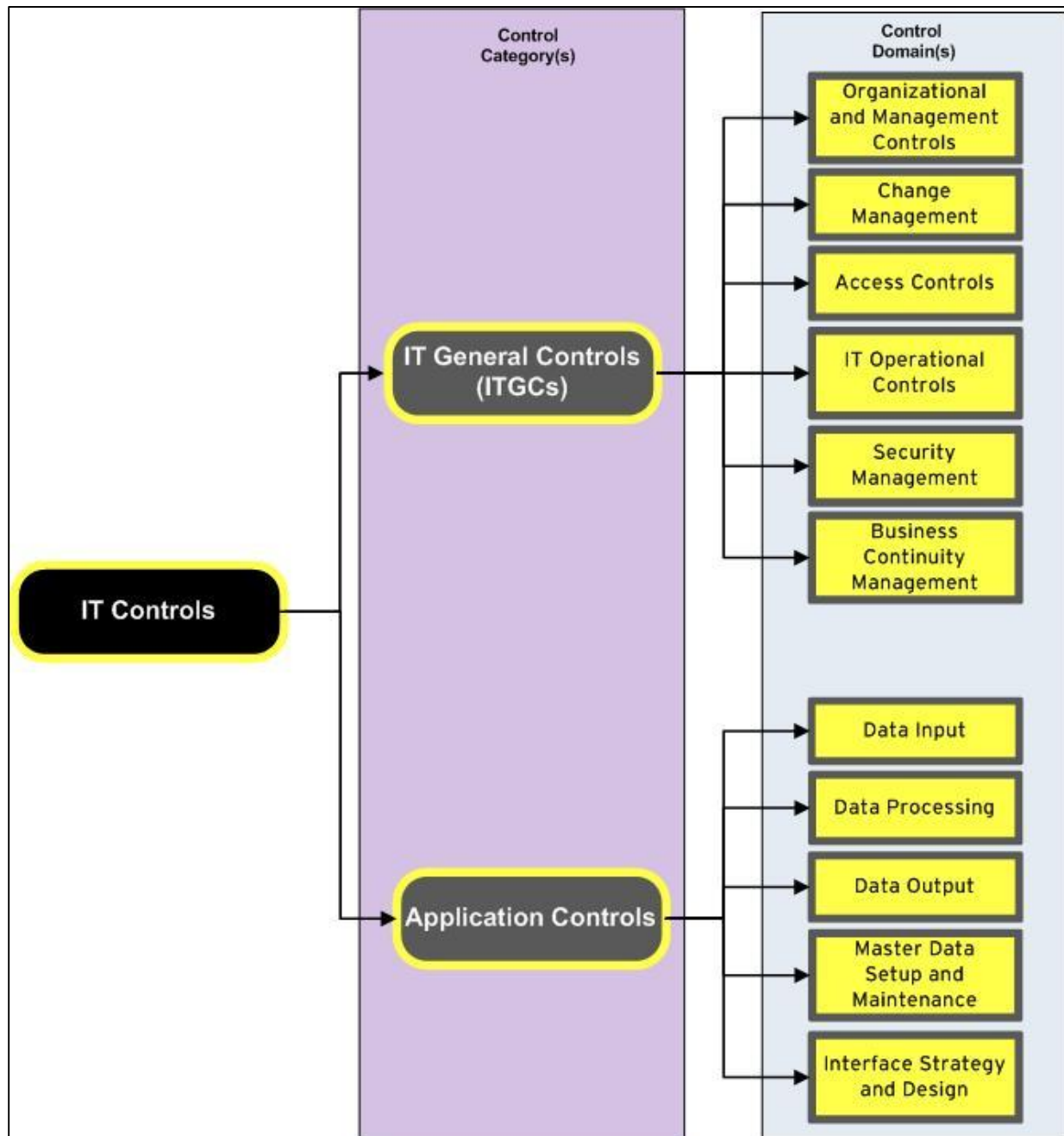


Figure 4.0 (SITAM IT Control Categories and Control Domains)

5.5 IT HEALTH CHECK

As per SITAM, the first phase of the IT Audit encompasses the IT Health Check to assesses the IT Complexity and IT Controls Maturity of the auditee.

The results of IT Health Check provide the basis for determining the IT Audit requirements for the auditee. The Preliminary IT Assessment Tool shall be used to meet the objective of this phase. For further details on the IT Health Check Tool, refer to Appendix 1: IT Health Check Tool Overview.

The figure below illustrates the key steps involved in IT Health Check phase:

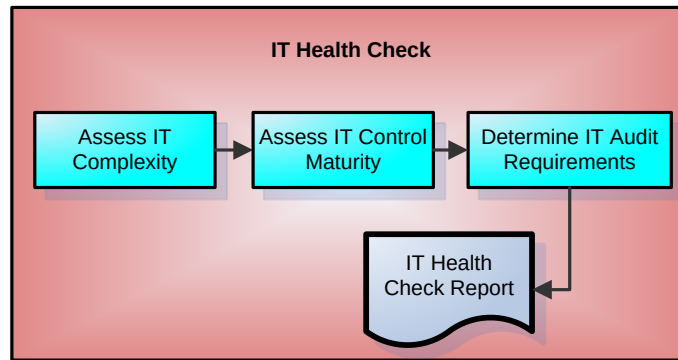


Figure 5.0 (SITAM IT Health Check Phase)

5.6 Assess IT Complexity

It is necessary for the auditor to obtain a clear understanding of the IT environment in which the IT Systems operate to be able to provide adequate assurance on IT Audit objectives. This will ultimately determine the nature and scope of the audit to be undertaken. This will also ensure that the auditor has focused their work in the appropriate areas so that the auditor has an appropriate basis upon which to make final assessment of the IT environment.

The Preliminary IT Assessment Tool shall be used by the Auditor to gather information on the auditee's IT environment. The questions included in the tool assess the technology, people, and reliance of the data generated from the IT Systems, to determine auditee's IT environment complexity.

The tool will assign the following ratings to the IT Complexity based on the responses obtained from the auditee in this phase:

- Simple
- Moderate
- Complex

The figure below represents the IT Complexity Assessment questions:

ID	Question	Response	Comments
A1.	Is the number of significant Business Applications supported by IT more than 3?		
A2.	Does the auditee have an ERP System or any other enterprise integrated systems?		
A3.	Does the auditee have a website hosted in the premises?		
A4.	Does the auditee have web based applications accessed by citizens?		
A5.	Is the number of servers and network devices more than 30?		
A6.	Is number of remote locations serviced by the IT department more than 10?		
A7.	Does auditee have remote connection facility for the users?		
A8.	Does auditee have Wireless Connection enabled or any other form of non wired connection (GPRS, GPS, VSAT etc.)?		
A9.	Is the number of sections in the IT Department more than 3?		
A10.	Is the total Strength of the IT Department more than 15?		
A11.	Does the audit team place reliance on the reports or calculations generated or performed by IT applications?		

Figure 6.0 (IT Complexity Assessment Questions)

5.7 Assess IT Control Maturity

During the IT Health Check phase, the auditor should gain a high level understanding of IT controls' maturity in the auditee's environment.

The Preliminary IT Assessment Tool shall be used to gather information from the auditee to understand the IT Controls Maturity. The questions included in the tool assess key IT controls to determine auditee's IT Controls Maturity. The tool will assign the following ratings to the IT Control Maturity based on the responses obtained from the auditee in this phase:

- Low
- Medium
- High

The figure below represents the IT Control Maturity Assessment questions:

ID	Question	Response	Comments
B.1	Does the auditee have an IT Strategy aligned with business requirements?		
B.2	Has the auditee established an IT Planning or Steering Committee?		
B.3	Does the auditee have a structured IT organizational chart?		
B.4	Is segregation of duties implemented in auditee's IT organizational structure to prevent any conflict of interests?		
B.5	Does the auditee have a documented IT manual (policies and procedures)?		
B.6	Does the auditee have an acceptable use policy on Internet and e-mail usage?		
B.7	Does the auditee have a change management process (e.g. changes are raised, documented, classified, authorized, tested, approved)?		
B.8	Are procedures for emergency changes documented and		

	implemented?		
B.9	Does the auditee have an access control policy based on business requirements?		
B.10	Does the auditee use a registration and de-registration process for granting access to all information systems and services?		
B.11	Are the access privileges assigned to users limited to their job requirements?		
B.12	Are the user access rights reviewed regularly, and in cases of promotion, demotion or termination of employment?		
B.13	Does the system enforce users to use complex passwords as per the password policy?		
B.14	Are systems left logged off or protected with screen/keyboard locking mechanism when unattended or when not in use?		
B.15	Are account lockouts being enforced after a pre-defined number of unsuccessful login attempts?		
B.16	Are audit logs containing user activities, exceptions, and security incidents recorded and retained for defined periods?		
B.17	Are audit logs reviewed regularly?		
B.18	Does the auditee control and monitor physical entry of personnel?		
B.19	Does the auditee carry out maintenance of their systems and devices as per manufacturer recommendations?		
B.20	Are only authorized maintenance personnel allowed to carry out repairs and service of equipments?		
B.21	Are procedures defined for electronic media usage and disposal?		
B.22	Are essential business data and software backed up as per business requirements?		
B.23	Is the backup data restored regularly?		
B.24	Does the auditee have an information classification scheme that fulfills the business requirements?		
B.25	Does the auditee have an anti-malware application installed on their system?		
B.26	Is the anti-malware application updated regularly?		
B.27	Does the auditee maintain an up-to-date inventory of assets?		
B.28	Is the risk assessment exercise carried out regularly and whenever systems, applications, facilities, or other conditions change?		
B.29	Does the auditee perform a vulnerability assessment and penetration testing exercise at least annually?		
B.30	Is there mechanism for obtaining timely information about technical vulnerabilities of IT systems?		
B.31	Are patches tested before they are installed?		
B.32	Does the auditee have a documented Business Continuity Plan (BCP)?		
B.33	Has the auditee implemented and tested the Business Continuity Plan (BCP)?		

Figure 7.0 (IT Control Maturity Assessment Questions)

5.8 Determine IT Audit Requirements

Once IT Complexity assessment and IT Control Maturity assessment are completed; the IT Audit requirements for the auditee should be defined based on the matrix below (Figure 8.0). For example, if the IT environment complexity is “COMPLEX”, and the IT controls maturity is “LOW”, then it is recommended to conduct detailed IT audit immediately, whereas if the IT environment complexity is “SIMPLE”, and the IT controls maturity is “HIGH”, then it is advised to implement the recommendations included in the IT Health Check report. The IT Health Check Tool shall determine the IT Audit requirements for the auditee; based on the IT complexity and IT control maturity ratings.

IT AUDIT REQUIREMENTS			
IT ENVIRONMENT COMPLEXITY →	SIMPLE	MODERATE	COMPLEX
IT CONTROLS MATURITY ↓			
LOW	IT IS RECOMMENDED TO CONDUCT DETAILED IT AUDIT IN THE LONG TERM	IT IS RECOMMENDED TO CONDUCT DETAILED IT AUDIT IN THE SHORT TERM	IT IS RECOMMENDED TO CONDUCT DETAILED IT AUDIT IMMEDIATELY
MEDIUM	IMPLEMENT THE RECOMMENDATIONS INCLUDED IN THE IT HEALTH CHECK REPORT	IT IS RECOMMENDED TO CONDUCT DETAILED IT AUDIT IN THE LONG TERM	IT IS RECOMMENDED TO CONDUCT DETAILED IT AUDIT IN THE SHORT TERM
HIGH	IMPLEMENT THE RECOMMENDATIONS INCLUDED IN THE IT HEALTH CHECK REPORT	IMPLEMENT THE RECOMMENDATIONS INCLUDED IN THE IT HEALTH CHECK REPORT	IT IS RECOMMENDED TO CONDUCT DETAILED IT AUDIT IN THE LONG TERM

Figure 8.0 (IT Audit Requirements Matrix)

The tool will also generate a summary of findings (Figure 9.0) that includes:

- The IT Complexity of the auditee
- The IT Control Maturity of the auditee
- The IT Audit Requirements for the auditee

 State Audit Institution		 ERNST & YOUNG <i>Quality In Everything We Do</i>	
Summary			
Auditee Name:	<XYZ Auditee>		
Date:	<Date>		
IT Complexity	COMPLEX		
IT Control Maturity	MEDIUM		
IT Audit Requirments	<u>IT IS RECOMMENDED TO CONDUCT DETAILED IT AUDIT IN THE SHORT TERM</u>		
NOTE: <u>MAKE SURE THAT ALL THE QUESTIONS IN IT COMPLEXITY ASSESSMENT AND IT CONTROL MATURITY ASSESSMENT ARE ANSWERED</u>			

Figure 9.0 (Example of IT Health Check Tool Summary of Findings)

Finally, the IT Auditor should prepare a IT Health Check Report which shall include summary of the findings and corresponding recommendations, and share the report with the auditee's management.

6. Planning

As per SITAM, if the IT Health Check determines that the auditee requires a detailed IT audit, the IT auditor shall start the planning phase of the IT Audit. The planning phase of the audit provides a detailed insight into the activities to be carried out in the planning phase. The key steps in this phase include:

- Understanding Audit Objectives and Scope of IT Audit: This phase aims to identify what kind of an audit needs to be carried out (supporting financial or performance audits) along with the scope of the IT audit
- Understand the Business: This phase enables the auditor to obtain and document an understanding of the auditee sufficient to plan and perform the audit in accordance with applicable auditing standards and requirements.
- Identify and Understand Systems Relevant to Audit Scope:
- Assess IT Risk: In this phase the auditor gets an overview of assessing and documenting, on a preliminary basis, the nature and extent of IT risk that relates to the key areas of audit interest.
- Identify Critical Control Points: This phase provides the auditor and overview of identification and documentation of critical control points in the design of auditee's IT systems based on the auditor's understanding of such systems, key areas of audit interest, and IT risk.
- Identify IT Controls Relevant to Audit Objectives: This phase helps the auditor to identify control categories and control domains that are relevant to the IT audit.

The figure below illustrates the key steps involved in Planning phase:

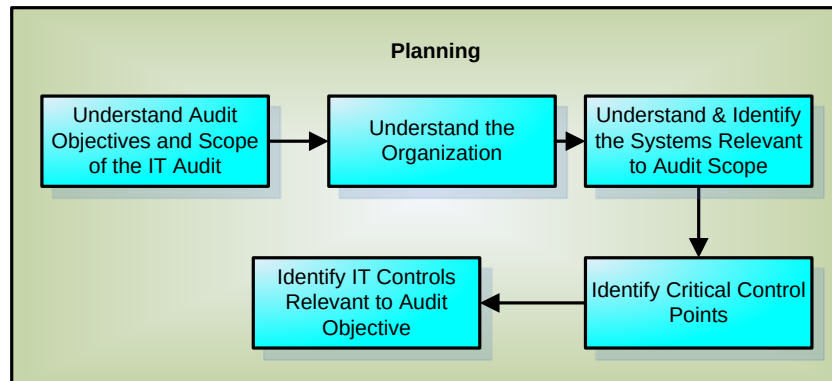


Figure 10.0 (SITAM Planning Phase)

6.1 Understand Audit Objectives and Scope of the IT Audit

The nature, timing, and extent of IT controls audit procedures vary depending upon the audit objectives. Typical IT controls' audit objectives include the following:

- To support financial statement audits by, for example, assessing the effectiveness of IT controls related to financial systems to conclude whether to rely or not rely upon financial data.
- To supplement IT performance audits by assessing the effectiveness of security within the context of a broader systems review.
- To support other performance audits, such as assessing data reliability or how well an information system protects the confidentiality, integrity, and availability of data and the effect of this level of protection on program performance.

- To determine the effectiveness of IT controls, not in support of another audit, so that any risks are identified. Such audits may be designed to provide a conclusion on the effectiveness of IT controls and describe any material weaknesses and other significant deficiencies, or merely describe any IT control weaknesses without an overall conclusion as to the effectiveness of IT controls.

The auditor should also determine and document the appropriate scope of the IT controls audit, including

- The organizational entities to be addressed (e.g., entity wide, selected system(s), etc.);
- The breadth of the audit (e.g., overall conclusion on IS control effectiveness, review of a specific application or technology area, such as wireless or UNIX, etc.);
- The types of IT controls to be tested:
- ITGC and/or application level controls to be tested, or selected components; or
- All levels of the auditee's information systems, or selected levels

If the IT controls audit is performed as part of another audit, the auditor should understand the overall audit objectives and how the IT controls audit will integrate with the audit. The auditor should reach a common understanding of objectives with the audit team responsible for the overall audit.

6.2 Understand the Organization

The auditor should obtain and document an understanding of the auditee sufficient to plan and perform the audit in accordance with applicable auditing standards and requirements. In planning the audit, the auditor obtains information that will provide an overall understanding of the auditee, such as its mission, size and location, organization, business, strategies, risks, and internal control structure. Understanding auditee's operations in the planning process enables the auditor to identify, respond to, and resolve problems early in the audit.

6.2.1 Understand the management and organization

To plan the audit, the auditor obtains a general understanding of the auditee's and the IT function's organizational structure, including key members of the auditee and IT management. The auditor's main objective is to understand how the auditee is managed and structured.

6.2.2 Understand the external and internal factors affecting the operations

The auditor should identify significant external and internal factors that affect the auditee's operations, particularly IT. External factors might include:

- IT budget
- External systems users
- Current political climate
- Relevant legislation

Internal factors might include

- Size of the auditee
- Number of locations
- Structure of the auditee (centralized or decentralized)
- Complexity of operations
- IT management structure
- Impact of information systems on business operations
- Qualifications and competence of key IT personnel
- Turnover of key IT personnel.

6.2.3 Understand the key business processes and operations

The auditor should document any significant factors that could affect the IT controls audit, including the auditor's risk assessment. The auditor should also obtain a general understanding of the auditee's

business processes, particularly those processes most closely related to the audit objectives. Business processes are the primary functions that the auditee performs in accomplishing its mission. Examples of typical business processes include:

- Mission-related processes, typically at the program or subprogram level
- Financial management processes, such as collections, disbursements, or payroll; and
- Other support processes, such as human resources or security.

6.2.4 Understand the applications supporting the business process

Understanding the auditee operations and business processes includes understanding how applications are used to support key business processes. The auditor should obtain and review documentation, such as design documents, blueprints, business process, procedures, user manuals, etc., and interview knowledgeable personnel to obtain a general understanding of each significant IT application that is relevant to the audit objectives. This includes a detailed understanding of:

- Business rules (e.g. removing all transactions that fail edits or only selected ones based on established criteria),
- Transaction flows (e.g. detailed study of the auditee's internal controls over a particular category of events that identifies all key procedures and controls relating to the processing of transactions), and
- Application and interfaces (transactions leave one system for processing by another, e.g. payroll time card interfaces with pay rate file to determine salary information).

The auditor should identify and document the key business processes that are relevant to the audit objectives. For each key business process, the auditor should identify:

- Key business process name
- Process owner
- Application(s) supporting the process

In addition, for each Application supporting the key business process, the auditor should identify and document:

- Computing Platform
- Operating System Name and Version
- Database Management System
- Source of Application
- Changes to Application
- Whether it has connectivity to the Internet
- Whether the application performs shared processing with other entities

6.2.5 Understand the IT infrastructure

The auditor should obtain and document a general understanding of the structure of the auditee's networks as a basis for planning the IT controls audit. The auditor's understanding includes a high-level view of the auditee's network architecture that the auditee uses to implement relevant key business processes. Such an understanding helps the auditor to assess risk, identify potential critical control points on a preliminary basis, understand technologies that may be subject to audit, and identify key locations. The auditor generally should request documentation of such information from the auditee, including both high-level and detailed network schematics. The auditor should obtain the following information about the network architecture, generally documented in network schematics:

- Internet presence;
- Firewalls, routers, and switches;
- Intrusion detection or prevention systems;
- Critical systems, such as Web and mail systems, file transfer systems, etc.;
- Network management systems;
- Connections to other external organizations;
- Remote access—virtual private network and dial-in; and

- Wireless connections.

6.3 Identify and Understand Systems Relevant to Audit Scope

The auditor should identify key areas of audit interest, which are those that are critical to achieving the audit objectives. For a financial audit, this would include key financial applications and data and related interface systems. For a performance audit, this would include key systems that are likely to be significant to the audit objectives. For each key area of audit interest, the auditor should document relevant general support systems and major applications, including:

- The operational locations of each key system or file,
- Significant components of the associated hardware and software (e.g., firewalls, routers, hosts, operating systems),
- Other significant systems or system level resources within scope, and
- Prior audit problems reported.

The auditor should also identify all access paths into and out of the key areas of audit interest. By identifying the key systems, files, or locations, the auditor can concentrate efforts on them. The auditor generally should prioritize important systems, files, or locations in order of importance to the audit objectives. The auditor may characterize these items by the sensitivity or significance of the information processed, monetary value of the transactions processed, or presence or number of key edits or other controls performed by a business process application.

The auditor should obtain and document an understanding of the information processing steps performed in information systems that are significant to the audit objectives, including:

- The manner in which transactions are initiated;
- The nature and type of records and source documents;
- The processing involved from the initiation of transactions to their final processing, including the nature of computer files and the manner in which they are accessed, updated, and deleted; and
- For financial audits, the process used to prepare auditee's financial statements and budget information, including significant accounting estimates, disclosures, and computerized processing.

6.4 Identify Critical Control Points

The auditor should identify and document critical control points in the design of auditee's IT systems based on the auditor's understanding of such systems, key areas of audit interest, and IT risk. Critical control points are those system control points that, if compromised, could allow an individual to gain unauthorized access to or perform unauthorized or inappropriate activities on auditee systems or data, which could lead directly or indirectly to unauthorized access or modifications to IT systems in scope. Control points typically include external access points to auditee's networks, interconnections with other external and internal systems, system components controlling the flow of information through auditee's networks or to the key areas of audit interest, critical storage and processing devices, and related operating systems, infrastructure applications, and relevant business process applications. Typical control points also include network components where business process application controls are applied. As the audit testing proceeds and the auditor gains a better understanding of auditee's information systems, of control weaknesses, and of the related risks, the auditor should periodically reassess the critical control points. Based on information obtained during audit planning, the auditor should identify those critical control points in auditee's IT systems that are significant to the effectiveness of security over the key areas of audit interest. An analysis of critical control points includes consideration of alternate work sites.

In identifying critical control points and in planning and performing the assessment of IT controls, auditors apply the concept of control dependencies. A control dependency exists when the effectiveness of an internal control is dependent on the effectiveness of other internal controls. An assessment of the effectiveness of information system controls over a critical control point includes testing the effectiveness of controls over other control points upon which the security of the critical control point is dependent.

As the auditor performs the IT controls audit, based on the auditor's assessment of risk and the results of audit tests, the auditor may determine that it is necessary to modify the scope of the audit, including revisions to the critical control points. For example, if significant IT control weaknesses are identified during the audit, it may not be necessary to perform all planned tests of IT controls. If testing is reduced due to the identification of significant weaknesses, the auditor should document such a decision. Also, testing may result in the identification of additional risks, and critical control points, and or control dependencies; the auditor should determine whether to adjust the scope for them.

6.5 Identify IT Controls Relevant to Audit Objective

Based on the results of audit planning and other procedures performed, the auditor should identify the control categories and control domains that are relevant to the IT audit. In doing this, the auditor considers the audit objectives and audit scope, the extent of IT risk and the preliminary understanding of IT controls.

The IT auditor should clearly document the IT control categories and control domains that are relevant to the audit objective and scope. For the reason that, only the specified control domains shall be included in the scope of test of controls, as well as only ineffective controls of the specified domain(s) will be reported to the auditee's management.

7. Execution

7.1 IT Audit Execution

As per SITAM, the subsequent phase after “Planning” is “Execution”. The figure below illustrates the key steps involved in Execution phase:

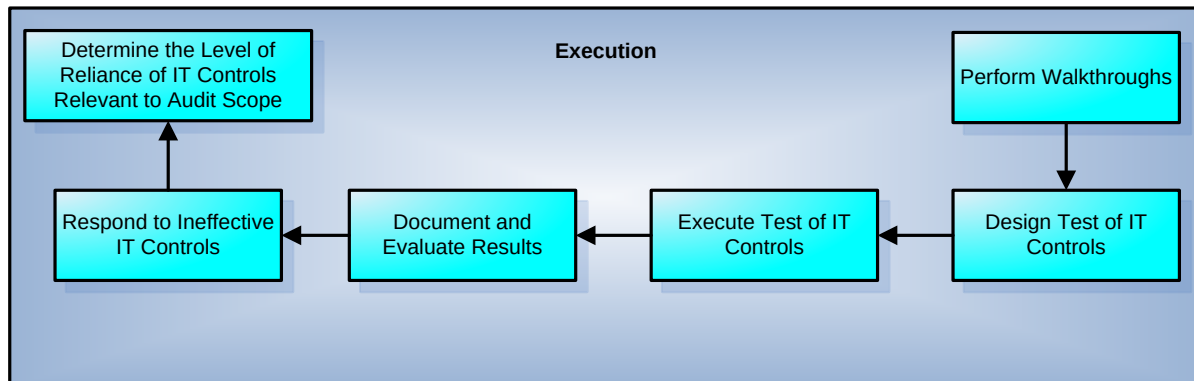


Figure 11.0 (SITAM Execution Phase)

In the execution phase of the IT audit, the auditor uses information obtained in the planning phase to evaluate the effectiveness of IT controls (ITGCs and Application Controls). As an outcome of this phase, the IT auditor should define the level of reliance that can be placed on the IT controls relevant to the audit scope.

The IT auditor shall be able determine the effectiveness of IT Controls after series of tests and evaluation achieved by performing the following:

- Perform Walkthroughs
- Design Test of IT Controls
- Execute Test of IT Controls

The IT auditor must evaluate both design effectiveness and operating effectiveness of IT controls.

- Design Effectiveness
 - Relates to whether controls are suitably designed to mitigate a particular risk or what can go wrong
 - Design effectiveness is evaluated at a “point in time” through a walkthrough
- Operating Effectiveness
 - Relates to whether the control actually operates as designed
 - Operating effectiveness is evaluated “over time” through testing

The IT auditor shall use the Detailed IT Audit Assessment Tool to document the results of walkthroughs and Test of Controls. The tool will evaluate these results and assign a rating for the effectiveness of the control objective, control domain, and control category. For further details on the Detailed IT Audit Assessment Tool, refer to Appendix 2: Detailed IT Audit Assessment Tool Overview.

If the IT auditor has determined that an IT Control deficiency exists, the auditor should:

- Identify and test compensating controls
- Perform other substantive procedures

The output of the steps above shall assist the IT auditor to conclude whether or not to rely on the IT controls relevant to the audit scope.

7.1.1 Perform Walkthroughs

In this phase, the IT auditor should test the design effectiveness of the IT controls. When testing the design effectiveness, the auditor shall evaluate whether controls are suitably designed to mitigate a particular risk. The auditor should perform walkthroughs of all the controls that are listed in the control domain relevant to the audit objective and scope. The auditor shall use the list of controls provided in the Detailed IT Audit Assessment Tool.

7.1.2 Design Test of IT Controls

To assess the operating effectiveness of IT controls, auditors should perform an appropriate mix of audit procedures to obtain sufficient, appropriate evidence to support their conclusions. Such procedures could include the following:

- Inquiries of IT and management personnel can enable the auditor to gather a wide variety of information about the operating effectiveness of control techniques. The auditor should corroborate responses to inquiries with other techniques.
- Questionnaires can be used to obtain information on controls and how they are designed.
- Observation of the operation of controls can be a reliable source of evidence. For example, the auditor may observe the verification of edit checks and password controls. However, observation provides evidence about controls only when the auditor was present. The auditor needs other evidence to be satisfied controls functioned the same way throughout the period.
- Review documentation of control policies and procedures. For example, the auditee may have written policies regarding confidentiality or logical access. Review of documents will allow the auditors to understand and assess the design of controls.
- Inspection of approvals/reviews provides the auditor with evidence that management is performing appropriate control checks. The auditor may combine these tests with discussions and observations.
- Analysis of system information (e.g., configuration settings, access control lists, etc.) obtained through system or specialized software provides the auditor with evidence about actual system configuration.
- Data review and analysis of the output of the application processing may provide evidence about the accuracy of processing. For example, a detailed review of the data elements or analytical procedures of the data as a whole may reveal the existence of errors.
- Re-performance of the control could be used to test the effectiveness of some programmed controls by reapplying the control through the use of test data. For example, the auditor could prepare a file of transactions that contains known errors and determine if the application successfully captures and reports the known errors.

In determining the appropriate timing for tests of IT controls, the auditor should consider appropriate factors, including, among other things, whether the audit objectives relate to a specific point in time or to a period of time, the nature of the evidential matter that is available (evidence of the proper operation of many IT controls is available only at the time of the test), the extent of information system risk, the significance or criticality of the IT control to the audit objectives, and the effectiveness of entity-wide and security management controls in reasonably assuring that IT controls operated consistently during the relevant period. Audit procedures may include a selection of specific items (e.g., access forms). In addition, the auditor may need to determine, among multiple instances of a type of network component, which specific components to test. For example, the auditee may have many internet access points or multiple instances of a data base. The auditor should exercise judgment in determining the number of items to select and the method used to select them. Generally, such judgment would include consideration of the related information system risk, the significance or criticality of the specific items in achieving the related control objectives, the location of the network component in relation to the key areas of audit interest, and the extent of consistency in the configuration of the components.

7.1.3 Execute Test of IT Controls

Based on the information obtained from the “Design Test of IT Controls” phase, the IT auditor should test the operating effectiveness of IT controls. The auditor shall perform this exercise on a tiered basis, starting with the IT general controls, followed by the application controls. In this phase the IT controls are tested to confirm that they operate as designed. The auditor shall execute test of controls of all the controls listed in control domain(s) relevant to audit scope.

7.1.4 Document and Evaluate the Results

The IT auditor shall use the Detailed IT Audit Assessment Tool to document the results of the Walkthroughs and Test of Controls of each control within the IT General Controls and Application Controls categories as shown in (Figure 12.0). The response can be:

- **“YES”**: If the control is fully compliant with design and operating effectiveness requirements
- **“PARTIAL”**: If the control is partially compliant with design and operating effectiveness requirements
- **“NO”**: If the control is not compliant with design and operating effectiveness requirements

The figure below illustrates how IT auditor shall document the results through use of the Detailed IT Audit Assessment Tool:

DETAILED IT AUDIT ASSESSMENT TOOL			
ITGC - CHANGE MANAGEMENT			
ID	Control	Response	Comments
A. Implement an Effective Change Management Process			
A.1	Is the change management process documented?	NO	
A.2	Are the changes raised, documented (e.g., Change Request Form) and classified?	YES	
A.3	Are the changes assessed for the impact, urgency, cost, benefits and risk of the changes?	YES	
A.4	Are the changes approved or rejected by authorized personnel, depending on the type, size, and risk of change?		
A.5	Are the changes handled by authorised and competent personnel?	YES PARTIAL NO	

Figure 12.0 (Example of Detailed IT Audit Assessment Tool)

Based on the results documented, the tool will determine the effectiveness at the control objective level, domain level, and control category level as shown in the figures below.

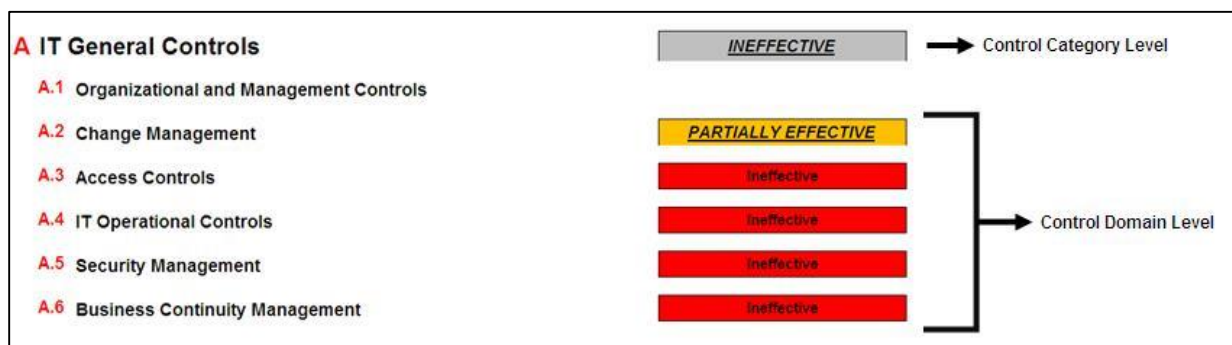


Figure 13.0

(Example of the Control Category and Control Domain Rating in Detailed IT Audit Assessment Tool)

For further details regarding ITGCs and Application Controls domains and control objectives, refer to 7.2 IT General Controls and 7.3 Application Controls.

7.1.5 Respond to Ineffective IT Controls

Once the IT auditor has obtained the rating of effectiveness of each control category, control domain, and control objective from the Detailed IT Audit Assessment Tool, the auditor shall list the control objectives that are rated ineffective. The auditor should respond to ineffective control objectives in the following manner:

- **Identify and test compensating controls**
The auditor should identify and test other IT controls or manual controls that can sufficiently reduce the risks (associated with the ineffective control) to an acceptable level. If compensating control(s) are present, then the ineffective control objective's rating can be changed accordingly, and consequently reliance can be placed on that specific domain. These observations should be documented and reported, as compensating controls are not replacements for the controls listed in Detailed IT Audit Assessment Tool.
- **Perform other substantive procedures**
If the auditor is not able to neither identify nor effectively test compensating controls, other testing procedures should be performed to obtain reasonable assurance that the risk of associated with the ineffective control objective did not occur. If such evidence can be obtained, then the control objective(s) rating shall remain the same, however reliance can be placed on that specific domain. These observations should be documented and reported.

If the auditor cannot identify compensating controls or perform other substantive procedures, then the control objective rating shall remain "ineffective", and controls shall not be relied upon.

7.1.6 Determine the Level of Reliance of IT Controls Relevant to Audit Scope

Based on information obtained from the phases above, the IT auditor should be able to conclude the level reliance on IT controls relevant to audit scope. The conclusion can be "Rely on IT Controls Relevant to Audit Scope" or "No Rely on IT Controls Relevant to Audit Scope". For example, if the IT control domains relevant to the scope are ineffective, then conclusion shall be "No Rely on IT Controls Relevant to Audit Scope".

Furthermore, based on the objective and scope of the audit, the reliance can be placed either at the control category level or at the control domain level. For example, if a comprehensive audit is required, then all the control domain(s) listed in Detailed IT Audit Assessment Tool shall be tested and evaluated, and the reliance will be placed at the control category level (e.g. ITGCs). Whereas, if the audit is only concerned about change management, then controls listed under Change Management Domain shall be tested and evaluated, and reliance will be placed at that specific control domain level.

7.2 IT General Controls

7.2.1 Overview

General controls are concerned with the organization's IT infrastructure including any IT related policies, procedures and working practices. They are not specific to individual transaction streams or particular accounting packages or financial applications. In most instances the general controls elements of an IT review will concentrate on the organization's IT department or similar function. General Controls include controls over data centre operations, system software acquisition and maintenance, access security and application system development and maintenance. They create the environment in which the application systems and application controls operate. Examples include IT policies, standards and guidelines pertaining to IT security and information protection, application software development and change controls, segregation of duties, business continuity planning, IT project management, etc.

As per SITAM, the evaluation of IT general controls includes the following six domains:

- **Organizational and Management Controls**
- **Change Management**
- **Access Controls**
- **IT Operational Controls**
- **Security Management**
- **Business Continuity Management**

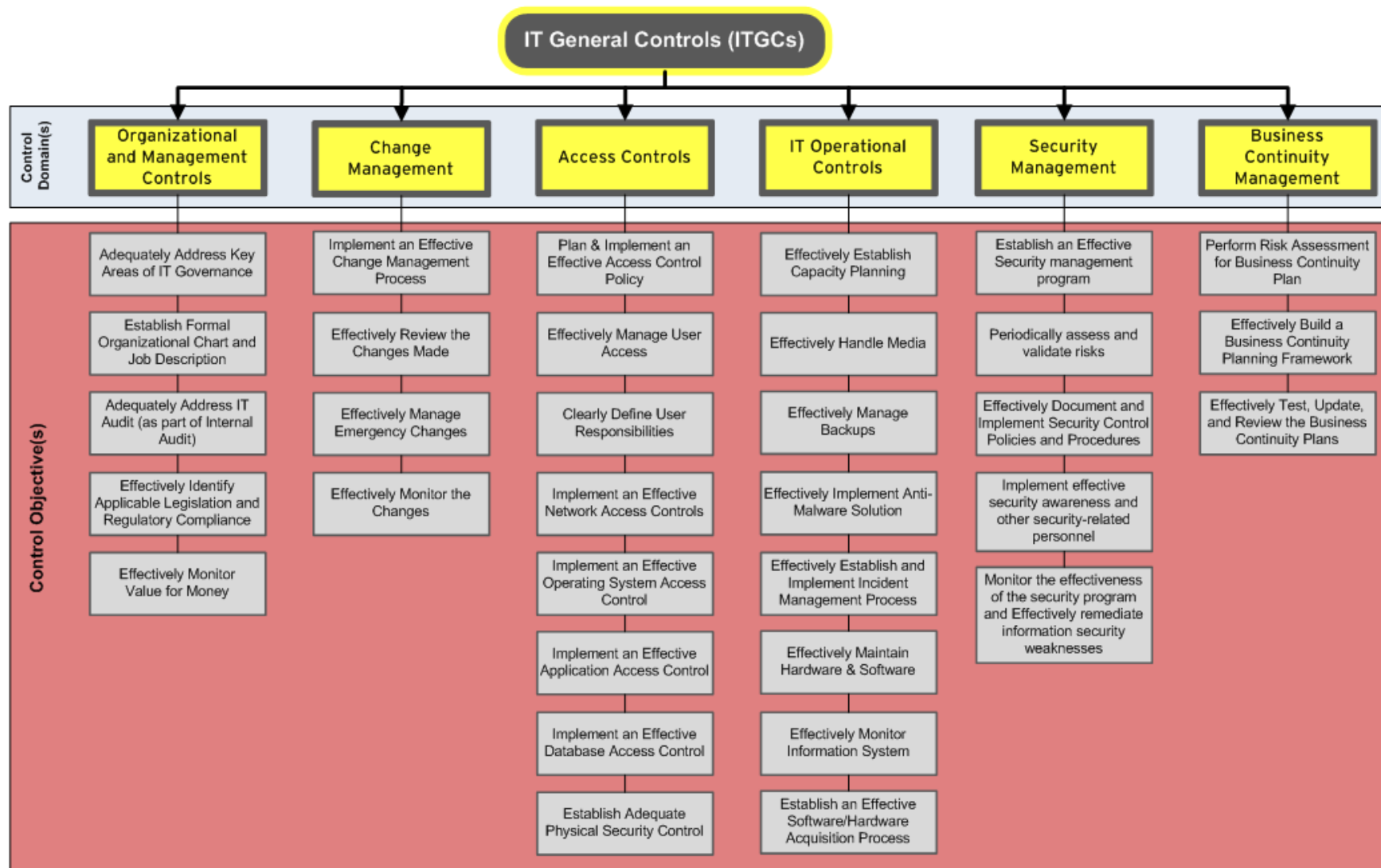


Figure 14.0 (SITAM IT General Controls' domains and control objectives)

7.2.2 Organizational and Management Controls

This domain addresses the high level controls adopted by management to ensure that the IT systems function correctly and that they are satisfying business objectives.

A. Adequately Address Key Areas of IT Governance

The control objective provides an overview of IT governance, the activities comprising an IT governance program and those that may be considered important. The control objective addresses the following topics from a management perspective such as:

- IT mission and vision
- IT strategic plan aligned with business goals and vision
- Technological strategy and standards IT Investments
- IT organizational structure (high level)

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

B. Establish Formal Organizational Chart and Job Description

This control objective ensures that a formal IT organization structure exists with all staff knowing their roles and responsibilities supported by clearly defined job descriptions. This control objective addresses the following:

- Allocation of IT responsibilities to be done in accordance with the organization's IT policy
- Responsibilities for carrying IT processes to be clearly identified
- Review of organization structure to be done at set intervals

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

C. Adequately Address IT Audit (as part of Internal Audit)

This control objective ensures that management has ultimate responsibility for ensuring that an adequate system of internal controls is in place. Management enforce policies and procedures and get assurance that the controls are in place and adequately reduce identified risks by relying on the review work carried out by internal auditors.

This control objective addresses the following:

- Carrying out IT audits on regular basis
- Allotting roles and responsibilities for IT audits
- Building up skills to carry out IT audits
- Using audit tools to carry out IT audits

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

D. Effectively Identify Applicable Legislation and Regulatory Compliance

This control objective includes controls to avoid breaches of any law, statutory or regulatory obligations by the use of IT systems. The design, operation, use, and management of information systems may be subject to statutory and regulatory requirements. Advice on specific legal requirements should be sought from the organization's legal advisers or suitably qualified legal practitioners.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

E. Effectively Monitor Value for Money

This control objective includes controls to assess whether or not the auditee has obtained the maximum benefit from the IT related goods and services it acquires and/ or provides, within the resources available to it. It not only measures the cost of goods and services, but also takes account of the mix of quality, cost, resource use, fitness for purpose, timeliness and convenience to judge whether or not, when taken together, they constitute good value.

7.2.3 Change Management

The objective of change management is to ensure all changes are assessed, approved, implemented and reviewed in a controlled manner.

Change refers to changes to both hardware and software. Hardware includes the computers, peripherals and networks. Software includes both the system software (operating system and any utilities) and individual applications. The scale of change can vary considerably, from adjusting a system's internal clock, to installing a new release of an application or operating system. The effect that a change has on the operation of the system may be out of proportion to the size or scale of the change made.

A. Implement an Effective Change Management Process

This control objective ensures that:

- Changes have a clearly defined and documented scope;
- Only changes that provide business benefit are approved, e.g. commercial, legal, regulatory, statutory;
- Changes are scheduled based on priority and risk;
- Changes to configurations can be verified during change implementation;
- The time to implement changes is monitored and improved where required

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

B. Effectively Review the Changes Made

This control objective ensures that all changes should be reviewed for success or failure after implementation and any improvements recorded.

- A post-implementation review should be undertaken for major changes to check that:
 - The change met its objectives;
 - The customers are satisfied with the results;
 - There have been no unexpected side effects.
- Any nonconformity should be recorded and corrective actions should be taken.
- Any weaknesses or deficiencies identified in a review of the change management process should be fed into plans for improving the service.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

C. Effectively Manage Emergency Changes

Emergency changes are sometimes required and where possible the change process should be followed but some details may be documented retrospectively. Where the emergency process bypasses other

change management requirements, the change should conform to these requirements as soon as practicable.

The objective of this control objective is to ensure that emergency changes can be justified by the implementer and reviewed after the change to verify that it was a true emergency.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

D. Effectively Monitor the Changes

The objective of this control objective is to ensure that change records are analyzed regularly to detect increasing levels of changes, frequently recurring types, emerging trends and other relevant information. The results and conclusions drawn from change analysis should be recorded and acted upon.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

7.2.4 Access Controls

The objective of access control is control access to information and systems. Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements. Access control rules should take account of policies for information dissemination and authorization.

A. Plan & Implement an Effective Access Control Policy

This control objective ensure that an access control policy should be established, documented, and reviewed based on business and security requirements for access. Access control rules and rights for each user or group of users should be clearly stated in an access control policy. Access controls are both logical and physical and these should be considered together. Users and service providers should be given a clear statement of the business requirements to be met by access controls.

Additionally, this control objective also ensures that the access control policy ensures key points such as:

- Security requirements of individual applications;
- Identification of all information related to the business applications and the risks the information is facing;
- Policies for information dissemination and authorization, e.g. the need to know principle and security levels and classification of information;
- Consistency between the access control and information classification policies of different systems and networks;
- Relevant legislation and any contractual obligations regarding protection of access to data or services.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

B. Effectively Manage User Access

This control objective ensures that authorized user access and to prevent unauthorized access to information systems. Formal procedures should be in place to control the allocation of access rights to information systems and services. The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access

to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

User Access typically focuses on the following:

- A formal user registration and de-registration procedure be in place for granting and revoking access to all information systems and services
- The allocation and use of privileges be restricted and controlled
- The allocation of passwords be controlled through a formal management process
- Management should review users' access rights at regular intervals using a formal process

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

C. Clearly Define User Responsibilities

This control objective ensures prevention of unauthorized user access, and compromise or theft of information and information processing facilities. The co-operation of authorized users is essential for effective security. Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment. A clear desk and clear screen policy should be implemented to reduce the risk of unauthorized access or damage to papers, media, and information processing facilities.

User Responsibilities related to access control include the following:

- Follow good security practices in the selection and use of passwords
- Ensure that unattended equipment has appropriate protection
- Adopt a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

D. Implement an Effective Network Access Controls

The objective of network access controls is to prevent unauthorized access to networked services. Access to both internal and external networked services should be controlled. User access to networks and network services should not compromise the security of the network services by ensuring:

- Appropriate interfaces are in place between the organization's network and networks owned by other organizations, and public networks;
- Appropriate authentication mechanisms are applied for users and equipment;
- Control of user access to information services is enforced.

This control objective ensures the following:

- Users are provided with access to the services that they have been specifically authorized to use.
- Appropriate authentication methods are used to control access by remote users.
- Automatic equipment identification is considered as a means to authenticate connections from specific locations and equipment.
- Physical and logical access to system ports is controlled.
- Groups of information services, users, and information systems are segregated on networks.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

E. Implement an Effective Operating System Access Control

The objective of operating system access controls is to prevent unauthorized access to operating systems. Security measures should be used to restrict access to operating systems to authorized users. The measures should be capable of the following:

- Authenticating authorized users, in accordance with a defined access control policy;
- Recording successful and failed system authentication attempts;
- Recording the use of special system privileges;
- Issuing alarms when system security policies are breached;
- Providing appropriate means for authentication;
- Where appropriate, restricting the connection time of users.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

F. Implement an Effective Application Access Control

The objective of application access controls is to help an organization assure the confidentiality, integrity, and availability of information assets, and provide reasonable assurance that application resources and data are protected against unauthorized:

- Modification,
- Disclosure,
- Loss, and
- Impairment

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

H. Establish Adequate Physical Security Control

This control objective prevents unauthorized physical access, damage, and interference to the organization's premises and information. Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference. The protection provided should be commensurate with the identified risks.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

7.2.5 IT Operational Controls

This domain ensures the correct and secure operation of information processing facilities. Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating procedures.

A. Effectively Establish Capacity Planning

This control objective requires the use of resources to be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance. This control objective further requires:

- Capacity requirements to be identified for each new and ongoing activity
- System tuning and monitoring to be applied to ensure and where necessary, improve the availability and efficiency of systems
- Detective controls to be put in place to indicate problems in due time
- Projections of future capacity requirements to take account of new business and system requirements and current and projected trends in the organization's information processing capabilities.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

B. Effectively Handle Media

This control objective addresses prevention of unauthorized disclosure, modification, removal or destruction of assets and interruption to business activities.

Effective Media handling requires that:

- Media be controlled and physically protected.
- Appropriate operating procedures should be established to protect documents, computer media (e.g. tapes, disks), input/output data and system documentation from unauthorized:
 - disclosure
 - modification
 - removal and
 - destruction

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

C. Effectively Manage Backups

This control objective requires backups of data and software to be carried out by an organization on a regular basis. Routine procedures should be established to implement the agreed back-up policy and strategy for taking back-up copies of data and rehearsing their timely restoration.

This control objective addresses the following typical aspects of information backup:

- Defining the necessary level of back-up information;
- Produce accurate and complete records of the back-up copies and documented restoration procedures;
- The extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements of the organization
- Storing the back-ups at a remote location
- Back-up information should be given an appropriate level of physical and environmental protection
- Testing back-up media regularly to ensure that they can be relied upon for emergency use when necessary

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

D. Effectively Implement Anti-Malware Solution

This control objective aims to protect the integrity of software and information from malware. Precautions are required to prevent and detect the introduction of malicious code and unauthorized mobile code. Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs. Users should be made aware of the dangers of malicious code. Controls should be introduced to prevent, detect, and remove malicious code and control mobile code.

This control objective requires:

- Documenting and circulating an anti-malware policy
- Installing updated anti-malware solutions on the system
- Allotting roles and responsibilities to manage anti-malware
- Education users on the risks related to anti-malware

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

E. Effectively Establish and Implement Incident Management Process

This control objective ensures a consistent and effective approach to the management of information security incidents. Responsibilities and procedures should be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of information security incidents. Where evidence is required, it should be collected to ensure compliance with legal requirements.

An incident management processes requires the following:

- Process to report information security events
- Process to report security weaknesses
- Allocating responsibilities and procedures for incident management
- Process to learn from information security incidents
- Process to collect evidence

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

F. Effectively Maintain Hardware & Software

This control objective requires hardware and software to be correctly maintained to ensure its continued availability and integrity.

Effective hardware and software maintenance includes:

- Hardware and software to be maintained as per vendor specifications only
- Frequency to be set to maintain hardware and software
- Maintain records of all maintenance activities

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

G. Effectively Monitor Information System

This control objective addresses detection of unauthorized information processing activities. Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified. An organization should comply with all relevant legal requirements applicable to its monitoring and logging activities. System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.

This control addresses the following key points related to monitoring:

- Audit logging
- Monitoring system use
- Protection of log information
- Retaining administrator and operator logs

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

G. Establish an Effective Software/Hardware Acquisition Process

This control objective addresses the controls related to Software/Hardware acquisition process. These controls aim to ensure smooth and structured process for the acquisition of the software and hardware.

The following should be considered:

- Corporate procurement process
- Effective communication between stakeholders
- Functional and technical analysis and design
- Training
- Testing strategy and plan
- Implementation and roll-back plan
- Post implementation review

7.2.6 Security Management

The objective of security management is to lay foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. The security management program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Overall policies and plans are developed at the organization-wide level. System and application-specific procedures and controls implement the organization-wide policy. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

A. Establish a security management program

This control objective requires the organization to have policies, plans, and procedures that clearly describe the organization's security management program. The security management program should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security and those who own, use, or rely on the organization's computer resources. As part of this organization-wide program, the organization should have a security management structure in place at the system and application levels. Thus, in managing a particular operating system or network device, the organization should have a clearly assigned structure and responsibilities for the security of the operating system and device. Similarly, the organization should have a clearly assigned structure and responsibilities related to particular business process applications. The security program policies, plans, and procedures should be kept up-to-date and revised to reflect system and organizational changes, problems identified during plan implementation, and security control assessments or audit reports.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

B. Periodically assess and validate risks

This control requires the organization to carry out a comprehensive risk assessment to develop or modify the organization's security policies and security plans. Such assessments are important because they help make certain that all threats and vulnerabilities are identified and considered, that the greatest risks are addressed, and that appropriate decisions are made regarding which risks to accept and which to mitigate through security controls. Appropriate risk assessment policies and procedures should be documented and based on the security categorizations.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

C. Document and implement security control policies and procedures

This control objective requires that security control policies and procedures should be documented and approved by management. They should also appropriately consider risk, address general and application controls, and ensure that users can be held accountable for their actions. Control policies and procedures may be written to be more general at the organization-wide level and more specific at the systems (for example, specific configurations) and application levels (for example, user access rules for specific applications). Also, a formal disciplinary process should be established for personnel who fail to comply with established IT control policies and procedures.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

D. Implement effective security awareness and other security-related personnel

This control objective requires an ongoing security awareness program to be implemented that includes first-time training for all new employees, contractors, and users; periodic refresher training for all employees, contractors and users; and distribution of security policies detailing rules and expected behaviors to all affected personnel. The information security program must include security awareness training for not only agency personnel but also contractors and other users of information systems that support the organization's operations and assets.

This training must cover

- Information security risks associated with users' activities and
- Users' responsibilities in complying with agency policies and procedures designed to reduce these risks.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

E. Monitor the effectiveness of the security program and effectively remediate information security weaknesses

An important element of risk management is ensuring that policies and controls intended to reduce risk are effective on an ongoing basis. This control objective requires effective monitoring of IT controls to evaluate or determine whether they are appropriately designed and operating effectively to achieve the organization's control objectives. Senior management's awareness, support, and involvement are essential in establishing the control environment needed to promote compliance with the organization's information security program. Senior management should balance the emphasis on security with the larger objective of achieving the organization's mission. To do this effectively, top management should understand the organization's security risks and actively support and monitor the effectiveness of its security policies.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

7.2.7 Business Continuity Management

The objective of having a business continuity plan and associated controls is to ensure that the organization can still accomplish its mission and it would not lose the capability to process, retrieve and protect information maintained in the event of an interruption or disaster leading to temporary or permanent loss of IT systems. Losing the capability to process, retrieve, and protect information can significantly affect an organization's ability to accomplish its mission. If business continuity controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can

cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. Given these severe implications, it is critical that an organization have in place:

- Procedures for protecting information resources and minimizing the risk of unplanned interruptions
- A plan to recover critical operations should interruptions occur

A. Perform Risk Assessment for Business Continuity Plan

This control objective requires events that can cause interruptions to business processes be identified, along with the probability and impact of such interruptions and their consequences on the organization. Business continuity risk assessments should be carried out with full involvement from owners of different departments. This assessment should consider all departments. It is important to link the different risk aspects together, to obtain a complete picture of the business continuity requirements of the organization. The assessment should identify, quantify, and prioritize risks against criteria and objectives relevant to the organization, including critical resources, impacts of disruptions, allowable outage times, and recovery priorities. Depending on the results of the risk assessment, a business continuity strategy should be developed to determine the overall approach to business continuity. Once this strategy has been created, endorsement should be provided by management, and a plan created and endorsed to implement this strategy.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

B. Effectively Build a Business Continuity Planning Framework

This control objective require plans to be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of critical business processes.

This control objective also addresses the following:

- Identification and agreement of all responsibilities and business continuity procedures;
- Identification of the acceptable loss of information and services;
- Implementation of procedures to allow recovery and restoration of business operations and availability of information in required time-scales
- Operational procedures to follow pending completion of recovery and restoration;
- Documentation of agreed procedures and processes

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

C. Effectively Test, Update, and Review the Business Continuity Plans

This control objective ensures that business continuity plans are tested and updated regularly to ensure that they are up to date and effective.

Business continuity plan tests should ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when a plan is invoked. The test schedule for business continuity plan(s) should indicate how and when each element of the plan should be tested. Each element of the plan(s) should be tested frequently.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

7.3 Application Controls

7.3.1 Overview

A business process application is a combination of hardware and software that is used to process business information in support of a specific business process. Application level controls, commonly referred to as “application level controls” or “application controls” are those controls over the completeness, accuracy, validity, confidentiality and availability of transactions and data during application processing. The effectiveness of application level controls is dependent on the effectiveness of organization-wide and system level general controls. Weaknesses in organization-wide and system level general controls can result in unauthorized changes to applications and data that can circumvent or impair the effectiveness of application level controls.

The evaluation of application controls includes the following four domains:

- **Data Input**
- **Data Processing**
- **Data Output**
- **Master Data Setup and Maintenance**
- **Interface Strategy and Design**

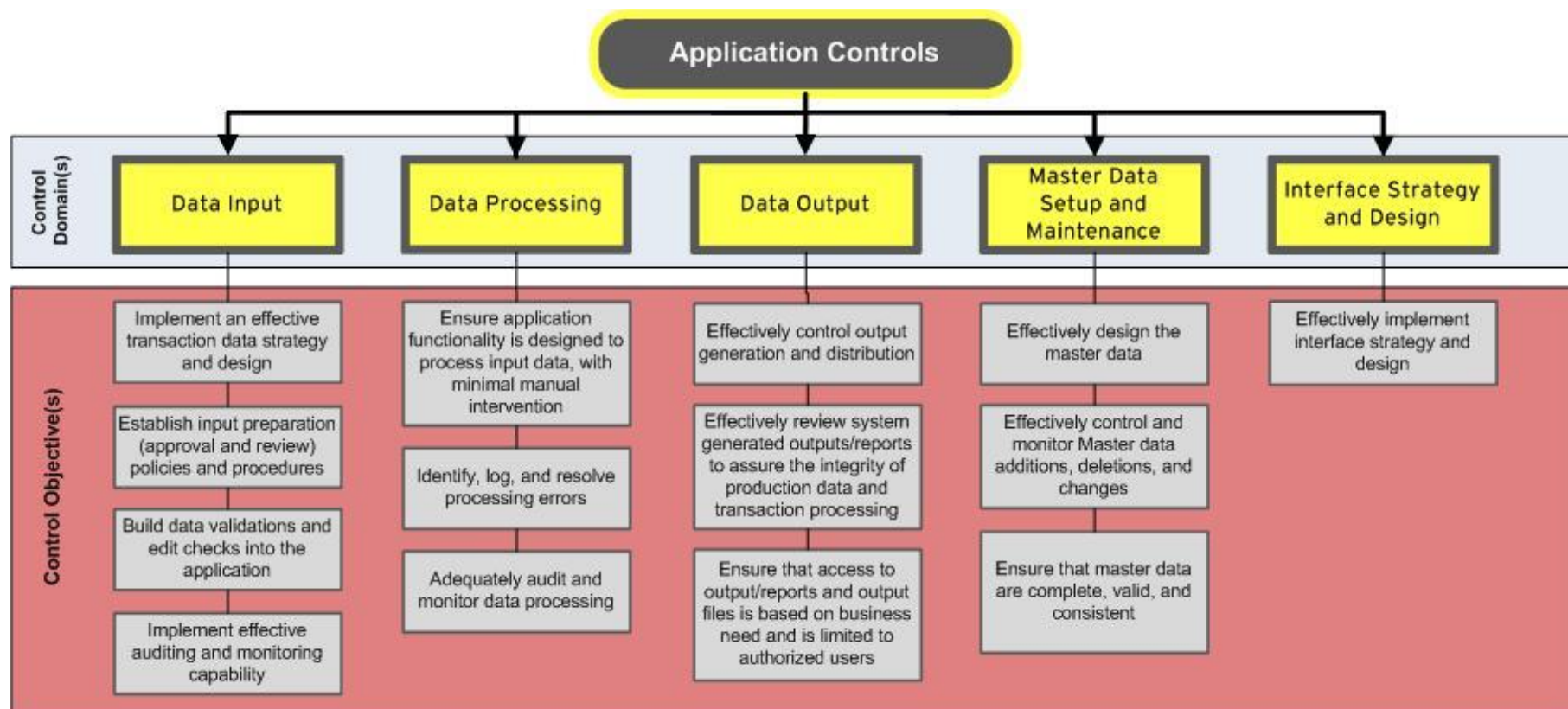


Figure 15.0 (SITAM Application Controls' domains and control objectives)

7.3.2 Data Input

The objective of this domain is to ensure that the procedures and controls reasonably guarantee that:

- The data received for processing are genuine, complete, not previously processed, accurate and properly authorized, and
- Data are entered accurately and without duplication.

Input control is extremely important as the most important source of error or fraud in IT systems is incorrect or fraudulent input. Controls over input are vital to the integrity of the system.

A. Implement an effective transaction data strategy and design

This control objective requires that the organization have an appropriate data strategy and design (how the data are organized into structures to facilitate retrieval while minimizing redundancy). The design of transaction data elements is a critical factor in helping to assure the quality of data as well as its interrelationship with other data elements. Data standards should be defined and maintained, but may vary depending upon the specific requirements of the organization, including regulatory requirements, and database or application-based standards.

A clearly defined data strategy minimizes data redundancies fundamental to an efficient, effective transaction processing function. Poor data quality may lead to a failure of system controls, process inefficiencies, and inaccurate management reporting.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

B. Establish input preparation (approval and review) policies and procedures

This control objective requires that the organization should have policies and procedures in place to reasonably assure that all authorized source documents and input files are complete and accurate, properly accounted for, and transmitted in a timely manner for input to the system. Among these, management should establish procedures to reasonably assure that all inputs into the application have been processed and accounted for; and any missing or unaccounted for source documents or input transactions have been identified and investigated. Finally, procedures should be established to reasonably assure that all source documents (paper or electronic form) have been entered and accepted to create a valid transaction.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

C. Build data validations and edit checks into the application

This control objective requires input data to be validated and edited to provide reasonable assurance that erroneous data is prevented or detected before processing. In many cases, application owners and programmers will build application input edits directly into the application to limit the number of errors that are input into the application. Edits are used to help assure that data are complete, accurate, valid, and recorded in the proper format. Edits can include programming to identify and correct invalid field lengths or characters, missing data, incorrect data, or erroneous dates.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

D. Implement effective auditing and monitoring capability

As part of the data input process, data entry errors may occur. These errors can occur during manual or automated entry of data. This control objective requires management to have procedures to identify and correct any errors that occur during the data entry process. Error handling procedures during data entry should reasonably assure that errors and irregularities are detected, reported, and corrected.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

7.3.3 Data Processing

The objective of this domain is to ensure complete and accurate processing of input and generated data. The objectives for processing controls are to ensure that:

- Transactions processing is accurate;
- Transactions processing is complete;
- Transactions are unique (i.e. no duplicates);
- All transactions are valid; and
- The related IT processes are auditable

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

A. Ensure application functionality is designed to process input data, with minimal manual intervention

This control objective ensures that application processing of input data is automated and standardized. Design documentation supporting the processing design exists for validation and change control purposes. The version of application, data and files to be processed are appropriate and current.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

B. Identify, log, and resolve processing errors

System entries use transaction logs to reasonably assure that all transactions are properly processed and identify the transactions that were not completely processed. Procedures need to be implemented to identify and review the incomplete execution of transactions, analyze and take appropriate action. Additionally procedures need to be implemented to monitor overrides applied to transaction processing in a timely manner.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

C. Adequately audit and monitor data processing

This control objective ensures that management has implemented procedures to reconcile the data input with the data processed by the application. Monitoring procedures should provide details of data to be added / modified during the processing, and expected result. System audit logs should be reviewed for exception. The organization should maintain a process log and the log are reviewed for unusual or unauthorized activity. Procedures to monitor, in a timely manner, overrides applied to transactions including maintenance of override logs should be implemented.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

7.3.4 Data Output

This objective of this domain is to ensure that system output is complete, accurate and correctly distributed. A well-controlled system for input and processing is likely to be completely undermined if output is uncontrolled. Reconciliation carried out at the end of the output stage can provide very considerable assurance over the completeness and accuracy of earlier stages in the complete cycle.

The objective of output controls ensure that all output is:

- Produced and distributed on time,
- Fully reconciled with pre input control parameters,
- Physically controlled at all items, depending on the confidentiality of the document and
- Errors and exceptions are properly investigated and acted upon

A. Effectively control output generation and distribution

This control objective ensures that management has procedures in place to reasonably assure that content and availability of output and data are consistent with

- End users' needs
- Sensitivity
- Laws and regulations
- Confidentiality of data
- Valid user access.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

Procedures are required to monitor replication of output data used in management reports or other communications within or outside the organization. User access to output data is aligned with the user's role and confidentiality/sensitivity of information.

B. Effectively review system generated outputs/reports to assure the integrity of production data and transaction processing

This control objective requires management to identify key outputs/reports to track processing results. Procedures need to be documented to:

- Review processed results, where applicable and
- Monitor, in a timely manner, overrides applied to transactions, including maintenance of override logs.

Additionally, procedures need to be implemented to review critical output data or control reports on a timely basis.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

C. Ensure that access to output/reports and output files is based on business need and is limited to authorized users

This control objective requires access to reports be restricted to those users with a legitimate business need for the information. Users should have appropriate authorization for accessing reports, including the appropriate level of security clearance where applicable.

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

7.3.5 Master Data Setup and Maintenance

This domain requires Master/Standing data file controls for integrity and accuracy of master and standing data files.

Three key control areas specific to master data controls are:

- The controls related to design and configuration of master data (preventive)
- The procedures external to the system (detective and preventive)
- The monitoring of master data design compliance (detective)

Master data is also subject to access controls (activities to create and maintain master data are controlled by access privileges)

A. Effectively design the master data

This control objective requires master data elements to be designed to minimize the risk of erroneous master data. This control objective also ensures the following:

- An entry is required in all key fields (e.g. address and account number)
- Null values or invalid values are not accepted in the required fields.
- For financial applications, account assignments (asset, liability, income and expense) are accurately defined

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

B. Effectively control and monitor Master data additions, deletions, and changes

This control objective requires controls over master data for:

- Changes to the configuration of the master file,
- Validity of all master file records,
- Completeness and validity of master file data,
- Consistency of master data among modules, and
- Approval of changes to master file data

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

C. Ensure that master data are complete, valid, and consistent

This control objective requires master data to be reviewed on a regular basis, duplicates are identified and removed or blocked, and unused data is identified and blocked. Policies and procedures for master data maintenance should be documented and must include:

- Approval requirements;
- Data quality criteria;
- Data owner;
- Supporting documents;
- Backup procedures in the event of a disaster or data corruption error;
- Archival policies

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

7.3.6 Interface Strategy and Design

This domain includes controls that address the

- Timely, accurate, and complete processing of information between applications and other feeder and receiving systems on an on-going basis
- Complete and accurate migration of clean data during conversion

The objectives of interface controls are to:

- Implement an effective interface strategy and design
- Implement effective interface processing procedures that require:
- Interfaces to be processed completely, accurately and only once in the proper period
- Interface errors to be rejected, isolated and corrected in a timely manner
- Access to interface data and processes be properly restricted and data is reliable and obtained only from authorized sources

A. Effectively implement interface strategy and design

This control objective requires an interface strategy for each interface that includes:

- The interface method
- Data fields being interfaced
- Controls to reasonably ensure a complete and accurate interface
- Schedule
- Assignment of responsibilities
- System balancing requirements and
- Security requirements

(Refer to the Detailed IT Audit Assessment Tool for list of controls under this control objective)

8. Reporting

8.1 Overview

After completing the execution phase, the auditor summarizes the results of the audit, draws conclusions on the individual and aggregate effect of all identified IT control weaknesses on audit risk and audit objectives. The auditor then reports the results of the audit.

As per SITAM, the key activities involved in the Reporting phase are illustrated in the figure below:

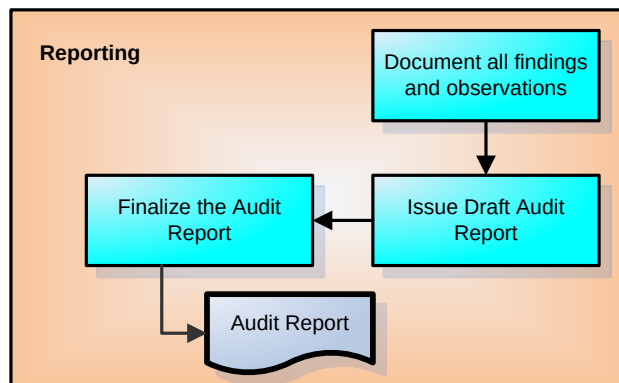


Figure 16.0 (SITAM Reporting Phase)

The auditor evaluates the effect of any weaknesses on the auditee's ability to achieve each of the control category, control domains, and control objectives relevant to scope of the audit.

The Detailed IT Audit Assessment tool shall provide the summary of findings in which the control category(s), control domain(s), and control objective(s) are evaluated. However, if compensating controls were found for the ineffective control objectives, then the final conclusion may change. In absence of strong compensating controls, overall IT controls are unlikely to be effective, and thus overall conclusion shall be "no rely on IT Controls relevant to audit scope".

If achieving the audit objectives does not require an overall conclusion on IT controls or only relates to certain components of the auditee, the auditor's assessment would not necessarily identify all significant IT control weaknesses. For example, a limited review of controls over a type of operating system may not identify any significant weaknesses. However there may be very significant weaknesses in other areas that the auditor may not be aware of because of the limited scope of the audit. Consequently, the auditor should evaluate the potential limitations of the auditor's work, and the needs and expectations of users. The auditor may determine that, because the limitations are so significant, the auditor:

- Will communicate the limitations to the audited entity, those charged with governance, and those requesting the audit
- Clearly report such limitations on the conclusions in the audit report

For example, in reporting on an audit of an operating system, the auditor may clearly report that the scope of the assessment was limited to the operating system. Consequently, additional IT control weaknesses may exist that could impact the effectiveness of IT controls related to the operating system and to auditee as a whole. The auditor should document and report the effect of identified IT control weaknesses in terms of the audit objectives.

Moreover, it is important to report IT control weaknesses in terms that are understandable to individuals who may have limited expertise in Information Technology. In this regard, the auditor generally should define technical terms and avoid jargon and undefined abbreviations and acronyms. The auditor should also avoid the disclosure of sensitive information. It is recommended that the auditor provides a draft IT report to auditee for a sensitivity review to avoid disclosure of sensitive information.

8.2 Reporting for Financial Audits

Based on the results obtained from the execution phase, the auditor should conclude:

- Reliability of financial reporting—The IT general controls and application controls can be relied upon to protect the financial data from breaches of confidentiality, integrity, and availability

The auditor should issue a draft Audit Report to auditee's management in which the following are addressed:

- Summary of findings (ineffective IT controls and areas of improvements)
- Critical observations of IT controls (ITGCs and Application Controls) relevant to the audit objective and scope. For each observation the report should include:
 - Description
 - Associated Risk
 - Recommendation
- Area of improvements in IT Controls (ITGCs and Application Controls) relevant to the audit objective and scope

Finally, the auditor should discuss the draft report with the auditee's management, and then finalize and issue the Audit Report which shall also include a summarized management response from the auditee for the audit observations.

8.3 Reporting for Performance Audits

The auditor should draw conclusions on the effectiveness of IT controls relevant to the audit objectives. Depending on the audit objectives, the auditor's report will vary. For example, the auditor's report may:

- provide an overall conclusion (e.g., the auditee's IT controls are or are not effective in achieving the IT control objectives relevant to the audit) and communicate identified weaknesses;
- Compliance with applicable laws and regulations;
- limit reporting to identified weaknesses without providing an overall conclusion (e.g., "based on our work, we identified the following IT control weaknesses"); or
- if in support of a broader performance audit, report findings in the context of the audit objectives, such as how they relate to the assessment of the reliability of electronic data

Auditors should include in their audit reports the scope of their work on internal control (which includes IT controls) and any deficiencies in internal control that are significant within the context of the audit objectives and based upon the audit work performed.

The auditor should issue a draft Audit Report to auditee's management in which the following are addressed:

- Summary of findings (ineffective IT controls and areas of improvements)
- Critical observations of IT controls (ITGCs and Application Controls) relevant to the audit objective and scope. For each observation the report should include:
 - Description
 - Associated Risk

- Recommendation
- Area of improvements in IT Controls (ITGCs and Application Controls) relevant to the audit objective and scope

Finally, the auditor should discuss the draft report with the auditee's management, and then finalize and issue the Audit Report which shall also include relevant references to summarize auditee's management response for the audit observations.

9. Appendices

This section includes the following appendices:

- Appendix A: Computer Assisted Audit Techniques and Tools
- Appendix B: IT Health Check Tool Overview
- Appendix C: Detailed IT Audit Assessment Tool Overview
- Appendix D: Leading Practices, Frameworks, and Standards
- Appendix E: Technical Terms used in the manual
- Appendix F: IT Audit checklist

Appendix A: Computer Assisted Audit Techniques and Tools

Introduction	
Computer Assisted Audit Techniques and Tools (CAATTs), are computer based tools and techniques which permit auditors to increase their productivity as well that of the audit function in gathering audit evidence by exploiting the power and speed of computer. CAATTs have the ability to improve the range and quality of audit and fraud investigation results. It has nowadays become an integral part of the whole audit work. CAATTs may also provide effective tests of control and substantive procedures where there are no input documents or a visible audit trail, or where population and sample sizes are very large. This is done by making use of the wide range of techniques and tools to automate the test procedures for evaluating controls, obtaining evidence and data analysis. The auditor can use CAATTs as an integral part of the whole audit work to gather audit evidence independently. CAATTs provide a means to gain access and to analyze data for a predetermined audit objective and to report the audit findings with emphasis on the reliability of the records produced and maintained in the system.	
Objectives	
The overall objectives and scope of an audit do not change when an audit is conducted in an Information Technology environment. The application of auditing procedures may, however, require the auditor to consider techniques known as Computer Assisted Audit Techniques (CAATTs) that use the computer as an audit tool. CAATTs may be used in performing various auditing procedures and improving the effectiveness and efficiency of obtaining and evaluating audit evidence. CAATTs are often an efficient means of testing a large number of transactions or controls over large population by: • Analyzing and selecting samples from a large volume of transaction, • Applying analytical procedures, and • Performing substantive procedures. CAATTs make remote and continuous auditing possible. By installing file interrogation tools at remote locations, auditors could continuously monitor activities and report any exceptions to the home office. CAATTs may be used in performing various auditing procedures, including the following: • Tests of details of transactions and balances, for example, the use of audit software for recalculating interest or the extraction of invoices over a certain value from computer records. • Analytical review procedures, for example, to identify inconsistencies or significant fluctuations. • Use of expert system, for example, in the design of audit programs and in audit planning and risk assessment. • Tests of general controls, for example, to test the setup of configuration of the operating system or access procedures to the program libraries. • Sampling programs to extract data for audit testing. • Tests of application controls, for example, to test the function of programmed control. • Creation of electronic working papers, for example, by downloading the general ledger for audit testing. • Recommitting calculations performed by the entity's accounting systems.	
Major Steps in using CAATTs	
The major steps to be undertaken by the auditor in the usage of CAATTs are to: • Set the objectives of the CAATTs application; • Determine the content and accessibility of the entity's files and data,	

- Identify the specific files or databases to be examined;
- Understand the relationship between the data tables where a database is to be examined;
- Define the specific tests or procedures and related transactions and balances affected;
- Define the output requirements;
- Arrangement with the user and IT departments, if appropriate, for copies of the relevant files or database tables to be made with the appropriate cut off data as per the period of audit and time;
- Identify the personnel who may participate in the design and application of the CAATTs;
- Refine the estimates of costs and benefits;
- Ensure that the use of the CAATTs is properly controlled and documented;
- Arrange the administrative activities, including the necessary skills and computer facilities;
- Reconcile data to be used for the CAATTs with the accounting records.
- Execute the CAATTs application;
- Evaluate the results.

Types of CAATTs

CAATTs can be split into two discreet areas of operation namely to validate programmes/systems (functionality of the programmable controls) and to analyze data files. Discussed below are some CAATTs that fall in this category.

CAATTs Used to Validate Programmes/Systems

Program Code Review

Program review involves a detailed examination of programme coding. It generally involves a fair degree of programming skill and a thorough knowledge of programme specification. By reading programme source codes, auditors should identify any of the following:

- **Identify Erroneous Code:** The use of code review to identify erroneous code is well established. Thus auditors can use code review to determine whether program code complies with its specifications.
- **Identify Unauthorized Code:** Without directly examining a program's source code, auditors are unlikely to identify unauthorized code in a program. Unauthorized code often is triggered by a specific data value or combination of data values. For example, a fraudulent programmer might modify a program so it does not print out details of his or her own account when it is overdrawn.
- Similarly, he or she might modify a program to exclude transactions having certain account number and data values from normal data validation process. Unless auditors submit test data having these specific values and have a way of checking that the test data has traversed all execution paths in the code that is their focus, they are unlikely to detect this unauthorized code.
- **Identify Ineffective Code:** Auditors can examine whether code is ineffective in two ways. First, they can evaluate whether the code meets the documented program specifications. Second, they can examine whether the code meets user requirements. Moreover, assuming the program specifications are correct, design errors that results in the program not complying with specification are also prevalent.
- **Identify Inefficient Code:** Code review also can allow auditors to identify inefficient segments of code. For example, in a sequence of tests of transaction types, the tests might not have been ordered according to their frequency of occurrence. As a result, the program executes more of its code than it would have to if the tests were recorded. Auditors might also use code review to identify the existence of the instructions that execute inefficiently on the hardware/software platform used.
- **Identify Non-Standard Code:** Non-standard code takes a variety of forms. For example, it could be code that does not comply with organizational standards covering data item names or internal documentation. Alternatively, it could be code that does not employ structured programming control structures. Whatever the nature of the nonstandard code, often it manifests other defects in the code – for example, unauthorized code or erroneous code.

Program Code Comparison This procedure involves the auditor comparing two versions of the source or object code of the program; one version - called the “blue print” - has known attributes and the auditor determines whether the other version has the same attributes. The auditor uses this technique for two reasons: First, to check whether the software given to him for audit is same as the one in operation; Second, to check whether any changes have been made in the code with respect to earlier versions, and if so, whether adequate change management procedures were followed. Utility programs are available that will compare two versions of a program, and report difference between the two.	
Parallel Simulation Parallel simulation involves the creation of an independent set of code that emulates the function of the area being tested. The results can be compared to those produced by the application itself. Parallel simulation is a useful tool enabling the auditor to re-perform all or part of the application being tested. Usually this would be performed on the area of the application of audit interest. This is a good way to prove the accuracy of calculations and processing procedures within the system without affecting the system itself. The auditor will need a good knowledge of the system and of the procedures to be replicated, and programming experience.	
Integrated Test Facility An Integrated Test Facility (ITF) is a technique that is sometimes used in auditing complex application systems. It provides an in-built testing facility through the creation of a dummy department or branch within the normal accounting system. Banks sometimes create a test branch within their Customer Accounting System that is used both for audit testing and training tellers in the use of the terminal system.	
Interactive Testing Facility Tracing A trace allows the auditor to analyse each step of a program. By performing a trace it is possible to see how each line of code has an effect on any data being processed or the program itself. For example, if a program is not totaling transactions correctly, a trace can highlight where exactly the error is occurring. Snapshot A snapshot is a utility which allowed the auditor to freeze a program at a given point and give the auditor a view of data at a particular point within a program or system. It is then possible to check on the values of a transaction and the processing that has been going on as the program was running. The snapshot is quick and relatively easy to use although it has a limited function and is specific. This is very useful for identifying potential errors in the mathematical calculations being carried out on a transaction. A good example of a snapshot would be a line of code in a program that produced a halt and output the value of a particular variable.	
CAATTs Used to Analyze Data Files	These are CAATTs which are primarily used on data files. Of course, results of data analysis can indirectly help the auditor to reach conclusions regarding the quality of programs. However, these CAATTs do not directly test validity of programs unlike those discussed earlier.
File Interrogation Software File interrogation involves various tests performed on a data file such as to check control totals, duplicate entries, missing entries, abnormal transactions, select samples, etc. The tests can be performed by using SQL statements, writing programmes specific to the system being audited, or by	

using generalized audit software. Discussed below are two types of file interrogation software.

Generalized Audit Software

The auditor may face a problem to deal with systems having diverse characteristics: different hardware and software environments, different data structures, different record formats, and different processing functions. With resource constraints it is often not feasible to develop specific programs for every system that will extract, manipulate and report data required for audit purposes. For this reason generalized audit software has been developed that is capable of handling a wide variety of different systems. With the development and marketing of generalized audit software like ACL and IDEA, the auditor has been provided with a powerful tool that can add tremendously to the auditor's efficiency with minimum IT-skill requirement.

The various analytical techniques that can be employed over data using generalized audit software for audit conclusion are:

- Reasonableness and Completeness tests
- Gap and duplication tests
- Period over period and similar comparisons
- Regression analysis
- Statistical analysis
- Transaction matching
- Data mining

Specialized Audit Software

Some types of audit software packages are now available that are oriented toward a specific industry in which an auditor works. They differ from the generalized audit software discussed earlier in two ways:

- First, since they are oriented toward a particular industry, they provide high-level commands that invoke common audit functions needed within the industry. For example, in the banking industry, they might use a single command to invoke logic that would check for account kiting. If generalized audit software were used to check for kiting, several commands might be required to express the logic needed for various tests.
- Second, industry-specific audit software may run on a smaller number of hardware/software configurations than generalized audit software. Indeed, industry specific audit software may have been developed to access the data maintained by a specific generalized application package that is in widespread use within the industry. Accordingly, the file definitions, record definitions, and field definitions used by the application package may be incorporated in the audit software package, and so do not have to be defined by the auditor each time the audit software package is run.

Embedded Audit Module

An embedded audit module is a technique that is generally used with a computer system that handles very high volumes of data. As its name implies, it's an audit application that is permanently resident within the main processing system. The embedded audit module examines each transaction as it enters the system. Every time a transaction occurs that meets the selection criteria, transaction details are logged before the transaction is allowed to continue for further processing. The audit log is periodically scanned, analyzed and reports are printed for follow up

With embedded audit software, the IT Auditor should be involved in system design and the techniques will have to be developed and maintained within the organization's application programs/systems.

Categories of CAATTs

File Downloading Tools

Using microcomputer-based package, auditors must first receive the data from the host system before it can be processed. There are many methods of data transfer available:

- Small files can be copied directly from floppy disk to the hard disk of the auditor's PC. Larger file may be compressed using a utility such as WINZIP before transfer and decompressed after transfer;
- Data can be downloaded from a reel tape, and most tape readers will be able to access the data;
- Data can be transferred from PC to PC via a parallel or serial cable;
- Data can be downloaded across a network, and its speed is high;
- Data can be downloaded via a modem, although the transfer rate is not very fast, it is also acceptable for smaller files.

The method used to transfer data depends on the hardware used by the auditor and SAI. File downloading tools are usually used by the CAATTs specialists to transfer clients' data to the auditor's PC. It is carried out by the use of tape management tools, such as Depot, Tarsus, Fdump and Tapeuti. etc

Auditor also can use Online Database Connectivity (ODBC) to access windows file. The CAATTs user can specify the particular source of data for interrogation from within the file interrogation software and invoke the relevant ODBC driver for that source. In this way direct access between the file interrogation software and the data source can be maintained.

Sometimes data needs to be manipulated after download, and then it can be put into a format that can be easily be imported into an interrogation package. There are several ways to manipulate data:

- Data can be manipulated using a simple editor such as DOS Text Editor;
- There is a range of Off-the-shelf software to manipulate downloaded data. For example, print files can be manipulated using Auto Import or Monarch. Software Bridge enables the user to translate files from one format to another.
- It is also common to write file manipulation software in house to fix downloaded data. This could take the form of removing padding characters from downloaded data blocks or splitting a downloaded file into small sub files containing different record types.

File Interrogation Software is the most widely used, and auditor can use it to deal with the massive volumes of data involved. This kind of software usually provides for a wide variety of functions for collecting and analyzing audit evidence, such as:

- Selecting records that confirm to particular criteria;
- Printing selected records for detailed examination;
- Printing totals and subtotals from an accounting file;
- Searching for duplicate transactions;
- Searching for gaps in sequence;
- Comparing the contents of two files, and printing either record matches or exceptions;
- Sorting and merging files in preparation for other audit tests.
- Aging

Report Generators Tools

Such tools facility querying and formatting data in a desired format from a file.

System Security/Review Tools

Software that can help an auditor plan a system review and provide computer generated recommendations, for instance, Enterprise Security Management Software.

Planning Tools

Software that can aid the auditor in planning the auditing.

Programming Tools for Specific Tasks (Bespoke Programme): Tools usually written by CAATTs specialists to perform a specific function.

Structured Query Language (SQL)

Structured Query Language (SQL) is the standard language designed to extract data from relational database systems and includes the capability of manipulating both the structure of a database and its data. An SQL interface can be found in database management systems such as Microsoft Query, Microsoft Access, ORACLE, INFOMIX, DB2, INGRES, Dbase IV, etc. SQL is able to perform many mathematical functions: counting, totaling, averaging, multiplication. SQL is also able to generate complex reports using a wide range of conditions: where, between, having, like.

Illustrations on the use of CAATTs

The following audit steps can be performed by auditor using CAATTs while auditing different areas of operation

Payroll Applications

- Identification of changes in exemption, gross pay, rates and salary amounts
- Reporting of entries against authorization records for new or terminated employees
- Identify duplicate direct deposit numbers
- Compare pay rates with ranges for the employees' classification
- Identify persons on payroll with no work address, contact numbers, etc.
- Reconcile salaries by job or by project etc.
- Match vendor and employee names, addresses, phone numbers, etc.
- Identification of duplicate employee names, addresses, phone numbers, etc.

Data Reliability

Where CAATTs are used to extract information for data analysis the auditor should verify the integrity of the information system and IT environment from which the data are extracted. The reliability of the source of the information used provides reassurance on the findings generated. So ensuring the reliability of data is crucially important.

There are many verification techniques and procedures that can be used by the auditor:

- Interviewing agency personnel associated with the information system;
- Reviewing and examining the related policies, procedures, and documentation;
- Observing the related activities and operations;
- Analyzing, testing, and evaluating the security relevant and security critical aspects of system hardware, software, firmware, and operations.

Several measures can be taken to ensure the reliability of data in electronic computer systems. The first step is to use reliable collection methods. This means that data will be legally obtained from reliable sources, preferably 'primary' sources rather than 'secondary' sources. The next step to consider is the method by which data is 'captured' from the source. Staff will need to be trained in techniques designed to optimize accurate input and to ensure a safe working environment. One of the best ways to ensure the accuracy of data is to apply data verification techniques.

CAATTs can be used to extract sensitive programs/system information and production data that should be kept confidential. The auditors should safeguard the program/system information and production data with an appropriate level of confidentiality and security. In doing so, the auditor should consider the level of confidentiality and security required by the organization owning the data and any relevant legislation.

Appendix B: IT Health Check Tool Overview

IT Health Check Tool		
Users of the Tool	Auditor(s) of State Audit Institution	
Objective	The tool objective is to assess IT Complexity and IT Control Maturity of the auditee, and then determine the IT Audit requirements.	
When to use the tool	This tool shall be used in the IT Health Check phase.	
How to use the tool	First, the information of the auditee must be recorded in tool. Then the Auditor shall gather the information on IT complexity and IT control maturity from the auditee and record the responses ("YES" or "NO") in the tool.	
Tool Functionality	Based on the responses recorded, the tool shall assign rating for auditee's IT complexity ("SIMPLE", "MODERATE", or "COMPLEX") and IT control maturity ("LOW", "MEDIUM", or "HIGH"). Once the ratings are assigned, the tool will determine the IT Audit requirements of the auditee.	
Tool Modules	Auditee Data	Contains the information of the auditee such as auditee name, date of the assessment, preparer name, approver name, and the interviewees' names.
	IT Complexity Assessment	Contains a list of questions which the IT Auditor shall use to gather and record information on IT complexity of the auditee. The rating of auditee's complexity will be shown in this module.
	IT Control Maturity Assessment	Contains a list of questions which the IT Auditor shall use to gather and record information on IT control maturity of the auditee. The rating of auditee's complexity will be shown in this module.
	IT Audit Requirements	Contains the matrix which will determine the IT Audit Requirements of the auditee. The tool shall determine the IT Audit requirements of the auditee based on the responses recorded in IT Complexity Assessment and IT Control Maturity Modules.
	Summary	Contains the summary of the IT Health Check which includes auditee name, data of the assessment, IT Complexity Rating, IT Control Maturity Rating, and IT Audit Requirements of the auditee.

Appendix C: Detailed IT Audit Assessment Tool Overview

Detailed IT Audit Assessment Tool		
Users of the Tool	Auditor(s) of State Audit Institution	
Objective	This tool is used to document and evaluate the results of walkthrough and test of IT General and Application controls within the auditee's	
When to use the tool	The tool shall be used while doing the walkthroughs and test of controls in the Execution phase.	
How to use the tool	The auditor should record the responses ("YES", "NO", "PARTIAL") for each control (listed under the control domain relevant to the scope of the audit) based on the results of the walkthroughs and test of controls.	
Tool Functionality	Based on the responses recorded by the IT auditor for each control, the tool shall assign a rating of "Effective", "Partially Effective", or "Ineffective" for the control objective, control domain, and control category.	
Tool Modules	Auditee Data	Contains the information of the auditee such as auditee name, date of the assessment, preparer name, approver name, and the interviewees' names.
	ITGC - Organizational & Management Controls	Contains the control objectives of Organizational Management Control Domain. Under each control objective, the controls are listed in a question format. The IT auditor shall record the responses for these controls based on the walkthroughs and test of controls results.
	ITGC - Change Management	Contains the control objectives of Change Management Control Domain. Under each control objective, the controls are listed in a question format. The IT auditor shall record the responses for these controls based on the walkthroughs and test of controls results.
	ITGC - Access Control	Contains the control objectives of Access Control Domain. Under each control objective, the controls are listed in a question format. The IT auditor shall record the responses for these controls based on the walkthroughs and test of controls results.
	ITGC - IT Operational Controls	Contains the control objectives of IT Operational Control Domain. Under each control objective, the controls are listed in a question format. The IT auditor shall record the responses for these controls based on the walkthroughs and test of controls results.
	ITGC - Security Management	Contains the control objectives of Security Management Control Domain. Under each control objective, the controls are listed in a question format. The IT auditor shall record the responses for these controls based on the walkthroughs and test of controls results.
	ITGC - Business Continuity Management	Contains the control objectives of Business Continuity Management Control Domain. Under each control objective, the controls are listed in a question format. The IT auditor shall record the responses for these controls based on the walkthroughs and test of controls results.
	Application Controls -	Contains the control objectives of Data Input Control Domain.

	Data Input	Under each control objective, the controls are listed in a question format. The IT auditor shall record the responses for these controls based on the walkthroughs and test of controls results.
	Application Controls - Data Processing	Contains the control objectives of Data Processing Control Domain. Under each control objective, the controls are listed in a question format. The IT auditor shall record the responses for these controls based on the walkthroughs and test of controls results.
	Application Controls – Data Output	Contains the control objectives of Data Output Control Domain. Under each control objective, the controls are listed in a question format. The IT auditor shall record the responses for these controls based on the walkthroughs and test of controls results.
	Application Controls – Master Data Design & Maintenance	Contains the control objectives of Master Data Design and Maintenance Control Domain. Under each control objective, the controls are listed in a question format. The IT auditor shall record the responses for these controls based on the walkthroughs and test of controls results.
	Application Controls – Interface Controls	Contains the control objectives of Interface Control Domain. Under each control objective, the controls are listed in a question format. The IT auditor shall record the responses for these controls based on the walkthroughs and test of controls results.
	Summary	Contains the overall rating of “Effective”, “Partially Effective”, or “Ineffective” for control categories (ITGCs and Application Controls), and corresponding control domains and control objectives.

Below is the list of questions to be asked during the evaluation of the IT environment complexity:

ID	Question	Response	Comments
A1.	Is the number of significant Business Applications supported by IT more than 3?		
A2.	Does the auditee have an ERP System or any other enterprise integrated systems?		
A3.	Does the auditee have a website hosted in the premises?		
A4.	Does the auditee have web based applications accessed by citizens?		
A5.	Is the number of servers and network devices more than 30?		
A6.	Is number of remote locations serviced by the IT department more than 10?		
A7.	Does auditee have remote connection facility for the users?		
A8.	Does auditee have Wireless Connection enabled or any other form of non wired connection (GPRS, GPS, VSAT etc.)?		
A9.	Is the number of sections in the IT Department more than 3?		
A10.	Is the total Strength of the IT Department more than 15?		
A11.	Does the audit team place reliance on the reports or calculations generated or performed by IT applications?		

The following table shows the questions as suggested by the tool to assess the maturity of IT controls:

ID	Question	Response	Comments
B.1	Does the auditee have an IT Strategy aligned with business requirements?		
B.2	Has the auditee established an IT Planning or Steering Committee?		
B.3	Does the auditee have a structured IT organizational chart?		
B.4	Is segregation of duties implemented in auditee's IT organizational structure to prevent any conflict of interests?		
B.5	Does the auditee have a documented IT manual (policies and procedures)?		
B.6	Does the auditee have an acceptable use policy on Internet and e-mail usage?		
B.7	Does the auditee have a change management process (e.g. changes are raised, documented, classified, authorized, tested, approved)?		
B.8	Are procedures for emergency changes documented and implemented?		
B.9	Does the auditee have an access control policy based on business requirements?		
B.10	Does the auditee use a registration and de-registration process for granting access to all information systems and services?		
B.11	Are the access privileges assigned to users limited to their job requirements?		
B.12	Are the user access rights reviewed regularly, and in cases of promotion, demotion or termination of employment?		
B.13	Does the system enforce users to use complex passwords as per the password policy?		
B.14	Are systems left logged off or protected with screen/keyboard locking mechanism when unattended or when not in use?		
B.15	Are account lockouts being enforced after a pre-defined number of unsuccessful login attempts?		
B.16	Are audit logs containing user activities, exceptions, and security incidents recorded and retained for defined periods?		
B.17	Are audit logs reviewed regularly?		
B.18	Does the auditee control and monitor physical entry of personnel?		
B.19	Does the auditee carry out maintenance of their systems and devices as per manufacturer recommendations?		
B.20	Are only authorized maintenance personnel allowed to carry out repairs and service of equipments?		
B.21	Are procedures defined for electronic media usage and disposal?		
B.22	Are essential business data and software backed up as per business requirements?		
B.23	Is the backup data restored regularly?		
B.24	Does the auditee have an information classification scheme that fulfills the business requirements?		
B.25	Does the auditee have an anti-malware application installed on their system?		
B.26	Is the anti-malware application updated regularly?		
B.27	Does the auditee maintain an up-to-date inventory of assets?		
B.28	Is the risk assessment exercise carried out regularly and whenever systems, applications, facilities, or other conditions		

	change?		
B.29	Does the auditee perform a vulnerability assessment and penetration testing exercise at least annually?		
B.30	Is there mechanism for obtaining timely information about technical vulnerabilities of IT systems?		
B.31	Are patches tested before they are installed?		
B.32	Does the auditee have a documented Business Continuity Plan (BCP)?		
B.33	Has the auditee implemented and tested the Business Continuity Plan (BCP)?		

Appendix D: Leading Practices, Frameworks, and Standards

ISO27001:2005

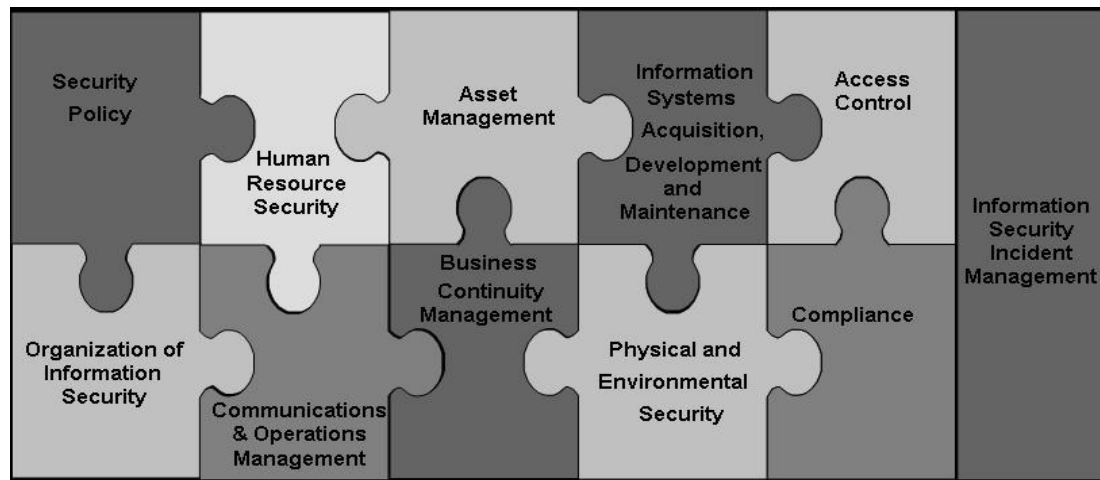
ISO 27001 is an information security standard designed to give organizations a means for providing clients, partners and regulators assurance of compliance to an internationally recognized set of information security controls. Its sister document, ISO 27002 describes 133 best practices for information security, along with detailed implementation advice. Together, the two documents create a certifiable framework for protecting organizations information assets.

ISO/IEC 27001 is the only auditable international standard which defines the requirements for an Information Security Management System (ISMS). The standard is designed to ensure the selection of adequate and proportionate security controls. It offers a business-led approach to implement best practices for information security management that are suited to the unique needs of the organization. Information security is characterized within ISO 27001 as the preservation of Confidentiality, Integrity and Availability.

Drawing on the concept of risk management, the standard enables all types and sizes of organizations to create an information security management system that is most appropriate for their needs. The standard is not prescriptive, as controls that are not applicable for a particular organization can be omitted, and additional controls not specified in the standard can be included to address unusual circumstances. It essentially enables organizations to identify its key information assets, assess risks to those assets and select and implement controls from global best practices to reduce the risk exposure of an organization.

ISO 27001 is centered on the protection of information assets that are critical to business operations. The standard embraces the concept of defense-in-depth. Controls are implemented at various levels to ensure the protection of the assets ranging from controls to protect the information itself, the operating system on which it resides, the applications used to access it, the networks on which they are used, the people using the applications and even the premises housing all these components. Layers are also built in terms of activities, procedures and policies to govern each process.

The management system is a dynamic entity, enabling organizations to proactively identify new threats and vulnerabilities to its information assets periodically and ensure compliance with the acceptable risk profile. The standard is divided into 11 domains of information security which are further divided into 39 control objectives and 133 controls that can be applied to address information security requirements.



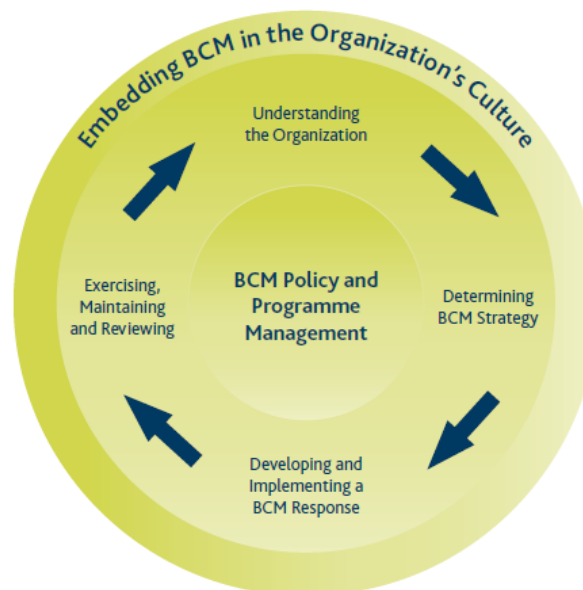
Organizations can get certified on the standard by a qualified accredited certifying body. This provides independent assurance that information security measures have been implemented as per global standards. It allows organizations to demonstrate the effectiveness of their information security initiatives to their business partners, potentially reducing the need for multiple audits by customers. Public recognition of this organizational commitment towards protecting information can be leveraged against competition. The ISO 27001 certification is now a benchmark within an industry sector, and providing secure environment/services to customers is increasingly becoming a major competitive advantage.

BS 25999: 2006

Risk and business continuity management is, without doubt, due diligence. Planning for crisis or disaster is an aspect of management that can only be short changed at your peril. However, it is a complex science, and not a five minute job. There are of course a range of tools to assist and to help create process. However, efforts have been made to create a generally accepted framework for business continuity management. The framework of standard so developed was called as BS 25999 published in November 2006 by British Standard Institution.

BS 25999-1:2006 is a code of practice that takes the form of guidance and recommendations. It establishes the process, principles and terminology of business continuity management (BCM), providing a basis for understanding, developing and implementing business continuity within an organization and to provide confidence in business-to-business and business-to-customer dealings.

BS 25999-1:2006 has been developed by practitioners throughout the global community, drawing upon their considerable academic, technical and practical experiences of BCM. It has been produced to provide a system based on good practice for BCM.



It is intended to serve as a single reference point for identifying the range of controls needed for most situations where BCM is practiced in industry and commerce, and to be used by large, medium and small organizations in industrial, commercial, public and voluntary sectors.

The benefits of BS 25999 are widespread and cover three critical areas:

- **Resilience:** Proactively improves your resilience when faced with the disruption of your ability to achieve key objectives
- **Delivery:** Provides a rehearsed method of restoring your ability to supply critical products and services to an agreed level and timeframe following a disruption
- **Management:** Delivers a proven capability for managing a disruption and protecting your reputation and brand

Payment Card Industry – Data Security Standard (PCI – DSS)

It is important to realize that the Payment Card Industry – Data Security Standard (PCI – DSS) addresses security of card holder information, not just IT security. Card holder information can exist in many forms it can be printed or written on paper, stored electronically transmitted by post or using electronic means, spoken in conversation or on the telephone. Whatever form the information takes, or by which means it is stored, shared or used, it should always be appropriately protected.

Almost all businesses, irrespective of their size, need to understand the scope of PCI DSS and how to implement security that is compliant with PCI DSS guidelines. In doing so, they will avoid penalties or the possibility of having their merchant status revoked and potentially being banned from accepting or processing credit cards.

Any organization that stores, processes or transmits cardholder data must comply with PCI DSS. Primarily, merchants and service providers should be compliant to this standard. Merchants are the companies that accept credit cards in exchange for goods or services. A service provider is any company that processes, stores, or transmits cardholder data, including companies that provide services to merchants or other service providers.

The PCI DSS version 1.2, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect card holder information.

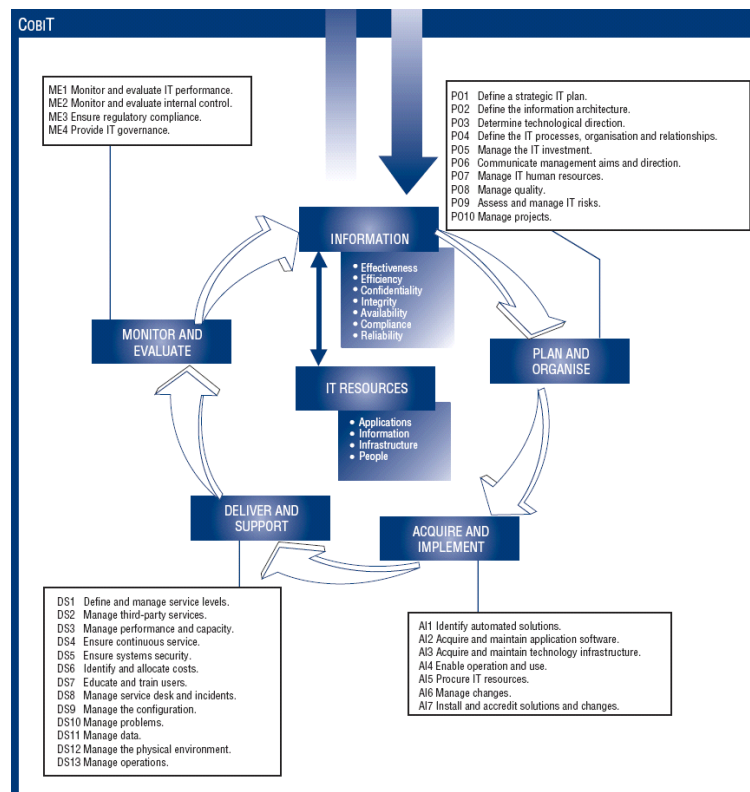
CoBIT Framework

COBIT is an acronym for Control Objectives for Information and related Technology. It is a framework created by ISACA for information technology (IT) management and IT Governance. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.

Its mission is to research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers, IT professionals and assurance professionals.

COBIT defines 34 generic processes to manage IT. Each process is defined together with process inputs and outputs, key process activities, process objectives, performance measures and an elementary maturity model. The framework supports governance of IT by defining and aligning business goals with IT goals and IT processes.

The framework provides good practices across a domain and process framework. The business orientation of COBIT consists of linking business goals to IT goals, providing metrics and maturity models to measure their achievement, and identifying the associated responsibilities of business and IT process owners. The process focus of COBIT is illustrated by a process model that subdivides IT into four domains (Plan and Organize, Acquire and Implement, Deliver and Support and Monitor and Evaluate) and 34 processes in line with the responsibility areas of plan, build, run and monitor. It is positioned at a high level and has been aligned and harmonized with other, more detailed, IT standards and good practices as COSO, ITIL, ISO 27000, CMMI, TOGAF and PMBOK. COBIT acts as an integrator of these different guidance materials, summarizing key objectives under one umbrella framework that link the good practice models with governance and business requirements.



The COBIT components include:

- Framework: Organize IT governance objectives and good practices by IT domains and processes, and links them to business requirements
- Process descriptions: A reference process model and common language for everyone in an organization. The processes map to responsibility areas of plan, build, run and monitor.
- Control objectives: Provide a complete set of high-level requirements to be considered by management for effective control of each IT process.
- Management guidelines: Help assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes
- Maturity models: Assess maturity and capability per process and helps to address gaps.

Capability Maturity Model Integration (CMMI)

Capability Maturity Model Integration (CMMI) is a process improvement approach whose goal is to help organizations improve their performance. CMMI can be used to guide process improvement across a project, a division, or an entire organization.

CMMI in software engineering and organizational development is a process improvement approach that provides organizations with the essential elements for effective process improvement. CMMI is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

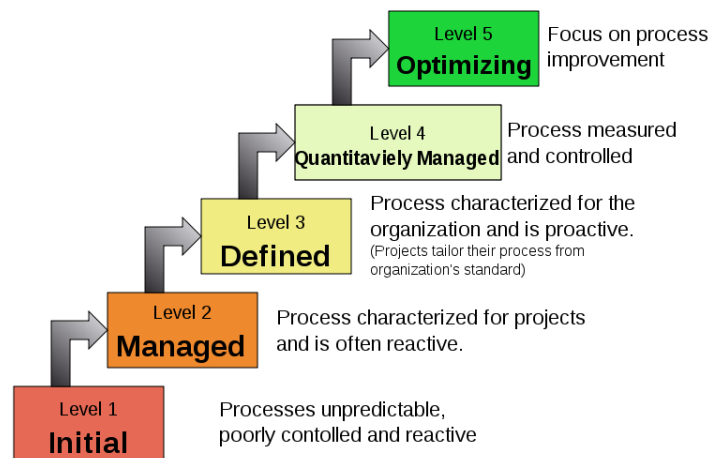
According to the Software Engineering Institute, CMMI helps integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality processes, and provide a point of reference for appraising current processes.

CMMI currently addresses three areas of interest:

- Product and service development — CMMI for Development (CMMI-DEV),
- Service establishment, management, and delivery — CMMI for Services (CMMI-SVC), and
- Product and service acquisition — CMMI for Acquisition (CMMI-ACQ).

CMMI originated in software engineering but has been highly generalized over the years to embrace other areas of interest, such as the development of hardware products, the delivery of all kinds of services, and the acquisition of products and services.

Characteristics of the Maturity levels



TOGAF Framework

The Open Group Architecture Framework (TOGAF®) is a framework for enterprise architecture which provides a comprehensive approach for designing, planning, implementation, and governance of enterprise information architecture. TOGAF is a registered trademark of The Open Group in the United States and Other countries.

TOGAF is a high level and holistic approach to design, which is typically modeled at four levels: Business, Application, Data, and Technology. It tries to give a well-tested overall starting model to information architects, which can then be built upon. It relies heavily on modularization, standardization and already existing, proven technologies and products.

An architecture framework is a set of tools which can be used for developing a broad range of different architectures. It should:

- describe a method for defining an information system in terms of a set of building blocks
- show how the building blocks fit together
- contain a set of tools
- provide a common vocabulary
- include a list of recommended standards
- include a list of compliant products that can be used to implement the building blocks

Appendix E: Technical Terms used in the manual

Policy	Intentions and direction of an organization as formally expressed by its top management
Procedure	Set of activities to perform certain process with defined roles and responsibilities
Methodology	The framework shows how processes, policies and procedures are planned, implemented, executed and measured
Integration	Interfacing and sharing inputs/ outputs
UNIX	UNIX Operating system
Cobit® Framework	Stands for Control Objectives for Information Technology, this framework is developed by ISACA for IT management and monitoring. CoBIT includes a set of tools that allows organization management to reduce the gap between audit requirements and business risks.
ISO 27001: 2005	Information security standard that enables organizations to ensure the deployment and compliance with information security requirements and IT security audit requirements.
ISO 20000 : 2005	ISO 20000 is granted to organizations implementing IT service management in compliance with ITIL leading practice and aims to improve IT service management.
25999:BS 2006	BS 25999 represents a set of activities in the form of guidelines and instructions for building and implementing IT services continuity and is considered as the basis for the design and execution of IT services continuity activities in organizations meeting agreed targets of business users and customers.
ITIL (Information Technology Infrastructure Library)	Framework and best practices derived universally from best practices implemented by public and private sectors and shows how IT is required to be organized in order to provide value to business and document processes and IT service management roles.
ITGC (Information Technology General Controls)	Set of controls implemented covering different IT and data components, systems and operations. These controls are important to ensure that proper implementation of to ensure safe deployment and execution of IT applications, programs, data and operations.
ERP (Enterprise Resource Planning)	A group of systems working together for the automation of business processes of the organization with integrated and unified manner.
INTOSAI	The International Organization of Supreme Audit Institutions
ARABOSAI	The Arab Organization of Supreme Audit Institutions
AFROSAI	The African Organization of Supreme Audit Institutions
CAROSAI	The Caribbean Organization of Supreme Audit Institutions
EUROSAI	The European Organization of Supreme Audit Institutions

Appendix F: IT Audit Checklist

IT Health Check		
1	Assess IT Complexity	√
٢	Assess IT Control Maturity	√
٣	Determine IT Audit Requirements	√
4	Preliminary IT Assessment Report	√
Detailed IT Audit Required?		
Planning		
5	Understand Audit Objectives and Scope of the IT Audit	√
6	Understand the Business	√
7	Understand & Identify the Systems Relevant to Audit Scope	√
8	Identify Critical Control Points / تحديد نقاط التحكم الحرجة	√
9	Identify IT Controls Relevant to Audit Objective	√
Execution		
10	Perform Walkthroughs	√
11	Design Test of IT Controls	√
12	Execute Test of IT Controls	√
13	Document and Evaluate Results	√
14	Respond to Ineffective IT Controls	√
15	Determine the Level of Reliance of IT Controls Relevant to Audit Scope	√
Reporting		
16	Document all findings and observations	√
17	Issue Draft Audit Report	√
18	Finalize the Audit Report	√
19	Management Letter	√