ISO/IEC JTC 1/SC 7 **N 5450**

ISO/IEC JTC 1/SC 7

Software and systems engineering

Secretariat: SCC (Canada)

Document type:	Working Draft Text
Title:	30120 1WD IT Audit V1
Status:	Send your comments, please, to Ms. Alison Holt (alison.holt@gmail.com) and Mr. Myles Ward (Myles.Ward@ird.govt.nz)
Date of document:	2012-02-29
Source:	WG40
Expected action:	COMM
Action due date:	2012-04-29
Email of secretary:	witold.suryn@etsmtl.ca
Committee URL:	http://isotc.iso.org/livelink/livelink/open/jtc1sc7

ISO/IEC JTC 1/SC 7 Nxxxx

Date: 2012-2-3

ISO/IEC 30120 WD IT Audit

ISO/IEC JTC 1/SC 7/WG40

Secretariat:

Information technology – Software Engineering – IT Audit – Audit guidelines for Governance of IT

Document type: Technical Report
Document subtype:
Document stage: (40) Enquiry
Document language: E

Contents

Page

INTRODUCTION **2**

1 SCOPE **3**

2 NORMATIVE REFERENCES **3**

3 TERMS AND DEFINITIONS **3**

4 PRINCIPLES OF AUDIT GUIDELINES FOR GOVERNANCE OF IT **4**

4.1 General 4

5 MANAGING AN AUDIT PROGRAMME **5**

5.1 General 5
5.2 Establishing the Audit programme objectives 5
5.2.1 Overview of the Audit programme 5
5.3 Establishing the audit programme 10
5.4 Implementing the audit programme 10
5.5 Monitoring the audit programme 11
5.6 Reviewing and improving the audit programme 11
6.1 General 12
6.2 Initiating the audit 12
6.3 Preparing audit activities 12
6.4 Conducting the audit activities 13
6.5 Preparing and distributing the audit report 14
6.6 Completing the audit 14
6.7 Conducting audit follow-up 14

7 COMPETENCE AND EVALUATION OF AUDITORS **15**

7.1 General 15
7.2 Determining auditor competence to fulfil the needs of the audit programme 15
7.3 Establishing the auditor evaluation criteria 16
7.4 Selecting the appropriate auditor evaluation method 16
7.5 Conducting auditor evaluation 16
7.6 Maintaining and improving auditor competence 16

ANNEX A **17**

BIBLIOGRAPHY **53**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electro technical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

ISO/IEC 30120 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software Engineering*.

Introduction

Today, Information Technology (IT) has become an important instrument for an organization to achieve such things as:

- Grow, evolve, and transform a business.
- Deliver business strategy.
- Improve organisational positioning and performance.
- Develop new opportunities.

The importance of operating and managing IT is key for the successful end to end delivery of business processes and in the production of and delivery of goods and services,..

With the switch from labour intensive processes to electronic rich environments and with organizations operating in a border-less economy, an organizations' IT is becoming more inter-connected globally and operated by a combination of partners and cloud related technologies. These networks of information systems compose an essential part of a wider social system and networks. If an IT system fails in one organisation, it has consequences and flow on effects to other systems and services. .

As IT is increasingly becoming more diversified and complex and becoming ever more coupled with front office activity in the delivery of systems and services, IT related risks are becoming more prominent and realizing value from IT is becoming increasingly difficult. The importance of good governance of IT and ensuring that IT is seen as a corporate tool as opposed to a corporate cost is increasingly becoming a crucial and complex issue for organizations to realise..

Under these circumstances, IT Audit is seen as an effective means to ensure IT risks are properly managed and the value of IT can be therefore be appropriately delivered in a controlled and well executed way. IT Audit plays a prominent role and an important object in the overall governance of IT.

The objective of this guideline is to provide guidance on IT Audit which assures efficient, effective and acceptable use of IT based on the requirements as specified in ISO/IEC 38500. Specific guidance includes management of audit programmes, conduct of audit, as well as the competence and evaluation of auditors.

This guideline should be used in conjunction with the guidance contained in ISO/FDIS 19011: *Guidelines for auditing management systems*. Texts in this guideline follow the structure of ISO/FDIS 19011. Within the structure, new guidance items are added and original items are modified in order to reflect the specific conditions applicable to IT management systems.

1 Scope

This technical report provides guidance on the auditing of IT that supports the evaluation of the governance of IT based on the principles of ISO/IEC 38500.

This guideline is applicable to an array of organsiations and is not bound by type and or size. This guideline should be used in conjunction with ISO/IEC 38500.

2 Normative references

The following referenced documents are crucial for the application of this International Guideline. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- ISO 19011: 2011(E), Guidelines for auditing management systems
- ISO/IEC 38500: 2008, Corporate governance of information technology
- (ISO/IEC TR38502:201x*, Corporate Governance of Information technology – Framework and Model)

3 Terms and definitions

For the purposes of this document, the terms and definitions provided in ISO19011 and ISO/IEC 38500 apply. In addition, the following IT Audit specific term and definitions apply**.**

3.1

Editors note: Currently **executive management** is deleted in the TR38502 discussion and ask NBs for necessity of this term in this guideline.

executive management
person or group of people who have delegated responsibility from the governing body for implementation of strategies and policies to accomplish the purpose of the organization.

3.2

governing body

group of people who are ultimately accountable for the performance of the organization

[ISO/IEC TR38502:201x]

3.3 IT management system

system of controls and processes required to achieve the strategic objectives set by the organization's Governing Body. And, the product is included to perform the strategic objectives. Management systems are subject to the policy guidance and monitoring set through organizational governance.

Note. The term Management is often used as a collective term for those with delegated responsibility to influence the achievement of objectives. This technical report uses the term Managers to avoid confusion.

4 Principles of Audit guidelines for Governance of IT

4.1 General

The guidelines from ISO 19011:2011, Clause 4.1, apply.

5 Managing an Audit programme

5.1 General

The guidelines from ISO 19011:2011, Clause 5.1, apply.

5.2 Establishing the Audit programme objectives

The guidelines from ISO 19011:2011, Clause 5.2, apply. In addition, the following IT Audit-specific guidance applies.

5.2.1 Overview of the Audit programme

Audit is a systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.

Potential areas of IT audit include the six principles set out by ISO/IEC 38500:2008. These principles are:

- Responsibility
- Strategy
- Acquisition
- Performance
- Conformance
- Human Factors.

Audit criteria for each principle can be classified into two categories: process and product. That is:

- Do relevant processes exist and operate appropriately?
- Do relevant product (documents, systems, delibables and etc) exist and are contents of the products appropriate?

In case of Responsibility, specific audit criteria includes the following:

Responsibility, Principle **Individuals and groups within the organization understand and accept their responsibilities in respect of both supply of, and demand for IT. Those with responsibility for actions also have the authority to perform those actions.**		
Category	**Audit Criteria**	**Contents**
Process	The responsibilities formulation process for current and future business objectives.	o Determining current and future business objectives. The responsibilities formulation process exist and current and future business objectives. o Ensuring effective, efficient, and acceptable use and delivery of IT
	IT responsibilities formulation process for the organization’s business objectives and performance.	o Establishing the appropriate assigned IT responsibilities. o IT responsibilities assisted by IT specialists who understand business values and processes.

Product	The appropriate IT governance mechanisms.	○ The responsibility and authority of personnel should be clearly defined and separated. ○ Their responsibilities in respect of both supply of, and demand for IT.
	The information that they need to meet their responsibilities and accountability.	○ Monitor the performance of those given responsibility in the governance of IT

In case of Strategy principle, specific audit criteria would be:

Strategy Principle **The organization's business strategy takes into account the current and future capabilities of IT; the strategic plans for IT to satisfy the current and ongoing needs of the organization's business strategy.**		
Category	**Audit Criteria**	**Contents**
Process	Appropriate risk assessment formulation Process.	○ Establishing appropriate risk assessment ○ Ensuring that IT use are subject to appropriate risk assessment and evaluation, as described in relevant international and national standards
	Business Strategy Formulation Process	○ Establishing business strategy, do there processes exist and operate appropriately to take into account the current and future capability of IT.
	IT Strategic Plan Formulation Process	○ Establishing IT Strategic Plan, there exist processes to satisfy the current and ongoing needs of the organization's business strategy, and the processes operate appropriately.
Product	Risk assessment for It	○ Risk assessment exists and its contents are appropriate
	Business Strategy	○ Business strategy exists and its contents are appropriate
	IT Strategic Plan	○ IT Strategic Plan exists and its contents are appropriate

In case of Acquisition, specific audit criteria would be:

Acquisition Principle **IT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision making. There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.**		
Category	**Audit Criteria**	**Contents**
Process	Evaluate options for providing IT Formulation Process.	○ Evaluate options for providing IT to realize approved proposals, balancing risks and value for proposed investments.

	Analysis IT acquisitions Formulation Process	o Extend ongoing analysis Formulation Process. o The supply arrangements (including both internal and external supply arrangements) support the business needs of the organization. o Monitor the extent to which their organization and suppliers maintain the shared understanding of the organization's intent in making any IT acquisition.
Product	IT investments plan	o IT investments are considered to realize the required functionalities in both the short term and the long term.
	IT development plan	o The IT development plan should be developed and aligned with the optimization plan and business requirements.
	IT asset report (systems and infrastructure)	o IT assets (systems and infrastructure) are acquired in an appropriate manner, including the preparation of suitable documentation, while ensuring that required capabilities are provided.

In case of Performance, specific audit criteria would be:

Performance Principle
IT is fit for purpose in supporting the organization, providing the services, levels of service and service quality required to meet current and future business requirements.

Category	Audit Criteria	Contents
Process	Evaluating wehter IT achieves Business Ojjectives for IT use	o Determine business purpose and requirements. o The processes exist and operate appropriately to meet current and future business requirements for IT use
	Allocating IT resources fit for Business purpose and requirements for IT use.	o Determine business purpose and requirements. o IT processes exist to provide and satisfy the current and ongoing needs of the organization's business, its purpose, and the processes operate appropriately future capability of IT.
Product	Business Performance	o Business service supported by IT exists and its usage is appropriate o Ensure effective, efficient, and acceptable use and delivery of IT
	IT services perfomance (or SLA report)	o IT services exist and its perfomance (SLA report) is appropriate. Ensure effective, efficient, and acceptable use and

		delivery of IT.

In case of Conformance, specific audit criteria would be:

Conformance Principle
IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.

Category	**Audit Criteria**	**Contents**
Process	Business Process comply with laws and regulations as appropriate for Information Systems,	o Ensure compliance. o Review the extent to which IT satisfies obligations (regulatory, legislation, common law, contractual), internal policies, standards and professional guidelines.
	Evaluation of IT conformance.	o Evaluate regularly the organization's internal conformance to its system for Governance of IT.
Product	The policies, procedures and guidelines	o Ensure those responsible establish regular and routine mechanisms for ensuring that the use of IT complies with relevant obligations (regulatory, legislation, common law, contractual), standards and guidelines for professionals. o Policies are established and enforced to enable the organization to meet its internal obligations in its use of IT. o IT staff follow relevant guidelines behaviour and development. o All actions relating to IT are ethical.
	IT conformance evaluation report	o Monitor IT compliance and conformance through appropriate reporting and audit practices, ensuring that reviews are timely, comprehensive, and suitable for the evaluation of the extent of satisfaction of the business. o Monitor IT activities, including disposal of assets and data, to ensure that environmental, privacy, strategic knowledge management, preservation of organizational memory (organizational intellectual property) and other relevant obligations are met.

In case of Human Factors, specific audit criteria would be:

Human Factors Principle
IT policies, practices and decisions demonstrate respect for Human Behaviour,

including the current and evolving needs of all the 'people in the process'.

Category	**Audit Criteria**	**Contents**
Process	IT Formulation Process for Human Behaviour	○ That IT activities take account of human behaviours and are appropriately considered.
	Formulation Process for the IT risks with human managed.	○ IT activities are consistent with identified human behaviour. ○ Risks, opportunities, issues and concerns may be identified and reported by anyone at any time.
Product	The policies and procedures	○ Policies and procedures are adequate. ○ The risks should be managed in accordance with published policies and procedures and escalated to there relevant decision makers.
	The education and training.	○ Exist education and training based on a consistent policy of an organization
	The report for human behaviour.	○ Reported about human behaviour. ○ Work practices are consistent with the appropriate use of IT

The primary role of audit is to provide assurance however, it can also include the drawing of conclusions and subsequent development and provision of various recommendations.

Assurance is an independent professional service that improves the quality of information for decision makers. One type of assurance is an attestation. This process includes the issuing of a written communication that expresses a conclusion about the reliability of a written assertion that is the responsibility of another party.

A principal type of non-assurance service is a consulting service.

IT auditors largely provide assurance to governing bodies that the use of IT in that organization is efficient, effective and acceptable. However, IT auditors may be asked by governing bodies to provide additional information about the non-conformity and/or poor performance on IT management systems. In those cases, an IT Auditor may provide a "recommendation" to a governing body. The major roles of the IT Audit function are depicted in Figure 1.

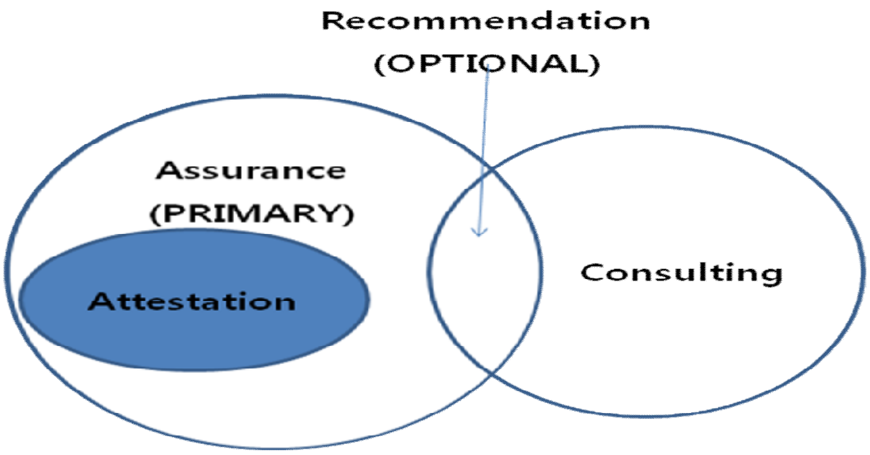

Figure 1 Major roles of IT Audit

5.3 Establishing the audit programme

5.3.1 Roles and responsibilities of the person managing the audit programme

The guidelines from ISO 19011:2011, Clause 5.3.1, apply.

5.3.2 Competence of the person managing the audit programme

The guidelines from ISO 19011:2011, Clause 5.3.2, apply.

5.3.3 Determining the extent of the audit programme

The guidelines from ISO 19011:2011, Clause 5.3.3, apply. In addition, the following specific guidance applies.

The extent of an audit programme can vary. Factors that can influence the extent of the audit programme include:

a) The size of the IT systems, including;
   1. The total number of IT personnel and relationships with third-party contractors working regularly at the location to be audited;
   2. The number of information systems (hardware and software);

b) The complexity of IT (including the number and criticality of IT processes, activities and/or products);

Consideration should be given in the audit programme to setting priorities based on IT risks and associated business risk areas that require more detailed examination.

5.3.4 Identifying and evaluating audit programme risks

The guidelines from ISO 19011:2011, Clause 5.3.4, apply.

5.3.5 Establishing procedures for the audit programme

The guidelines from ISO 19011:2011, Clause 5.3.5, apply.

5.3.6 Identifying audit programme resources

The guidelines from ISO 19011:2011, Clause 5.3.6, apply. In addition, the following specific guidance applies.

In particular, for all significant IT risks associated with environment and operation applicable to the auditee, auditors should be allocated sufficient time to verify the effectiveness of the corresponding IT related risk mitigation action.

5.4 Implementing the audit programme

5.4.1 General

The guidelines from ISO 19011:2011, Clause 5.4.1, apply.

5.4.2 Defining the objectives, scope and criteria for an individual audit

The guidelines from ISO 19011:2011, Clause 5.4.2, apply.

5.4.3 Selecting the audit methods

The guidelines from ISO 19011:2011, Clause 5.4.3, apply. In addition, the following IT specific guidance applies.

If a joint audit is conducted, particular attention should be paid to the disclosure of information during the audit. Agreement on this should be reached with all interested parties before the commencement of the audit..

5.4.4 Selecting the audit team members

The guidelines from ISO 19011:2011, Clause 5.4.4, apply. In addition, the following specific guidance applies.

The competence of the overall audit team should include:

a) Adequate knowledge and understanding of IT related risk management sufficient to evaluate the methods used by the auditee; and

b) Adequate knowledge and understanding of IT and IT related risk management that is sufficient to evaluate the overall effectiveness of the IT management system.

Where necessary, care should be taken that the auditors have obtained the necessary clearance to access audit evidence.

5.4.5 Assigning responsibility for an individual audit to the audit team leader

The guidelines from ISO 19011:2011, Clause 5.4.5, apply.

5.4.6 Managing the audit programme outcome

The guidelines from ISO 19011:2011, Clause 5.4.6, apply. In addition, the following specific guidance applies.

The person managing the IT audit programme should ensure that the following activities are performed:

- Distribution of IT audit reports to the governing body and/or external parties;
- Provision of recommendations with improvement of IT management systems.

5.4.7 Managing and maintaining audit programme records

The guidelines from ISO 19011:2011, Clause 5.4.7, apply.

5.5 Monitoring the audit programme

The guidelines from ISO 19011:2011, Clause 5.5 apply.

5.6 Reviewing and improving the audit programme

The guidelines from ISO 19011:2011, Clause 5.6 apply.

The guideline from 19011:2011, Clause 5.6 applies. In addition, the following specific guidance applies.

In order to monitor and improve the audit quality, ensure the inclusion of specific IT experts as part of the overall IT quality assurance programme.

6 Performing an IT Audit

6.1 General

The guidelines from ISO 19011:2011, Clause 6.1 apply.

6.2 Initiating the audit

6.2.1 General

The guidelines from ISO 19011:2011, Clause 6.2.1 apply.

6.2.2 Establishing initial contact with the auditee

The guidelines from ISO 19011:2011, Clause 6.2.2 apply.

6.2.3 Determining the feasibility of the audit

The guidelines from ISO 19011:2011, Clause 6.2.3, apply. In addition, the following specific guidance applies.

Before the audit commences, the audit team should request for any current and/or previous reviews undertaken and/or records pertaining to IT management systems. These reviews may contain confidential or sensitive information. If these reviews and/or records are unavailable then the audit team leader (or a person responsible for managing the audit programme) should determine whether the IT management systems can be adequately audited in the absence of those records and/or reviews. If the conclusion is that it is not possible to adequately audit without reviewing the identified records and/or reviews, then the auditor should ask the auditee that the audit cannot take place until appropriate access arrangements are granted. An alternative audit date could be proposed to or by the auditee.

6.3 Preparing audit activities

6.3.1 Performing document review in preparation for the audit

The guidelines from ISO 19011:2011, Clause 6.3.1 apply. The guideline from 19011:2011, Clause 6.3.1 applies. In addition, the following specific guidance applies.

Performing pre-study for preparation of the IT audit.

- Visit: to understand the auditee’s use of IT and to define skill and knowledge required for IT audit team.
- Interview: to understand the current IT environment and the associated IT operation.
- Data collection: to assist in a brief assessment of IT. It is important to predetermine what date needs to be collected for the audit. .

Note that this pre-study is not actual audit and collected information is not used for audit evidence at the conclusion of the audit.

6.3.2 Preparing the audit plan

The guidelines from ISO 19011:2011, Clause 6.3.2 apply. In addition, the following specific guidance applies.

When preparing the audit plan, evaluate the possibility of utilizing the automated tools to obtain an audit trail. This should be undertaken in advance of determining the audit methodologies, audit schedule and a composition of audit team and should also be undertaken in advance of any discussions with the auditee.

6.3.3 Assigning work to the audit team

The guidelines from ISO 19011:2011, Clause 6.3.3 apply.

6.3.4 Preparing work documents

The guidelines from ISO 19011:2011, Clause 6.3.4 apply.

6.4 Conducting the audit activities

6.4.1 General

The guidelines from ISO 19011:2011, Clause 6.4.1 apply.

6.4.2 Conducting the opening meeting

The guidelines from ISO 19011:2011, Clause 6.4.2 apply.

6.4.3 Performing document review while conducting the audit

The guidelines from ISO 19011:2011, Clause 6.4.3 apply. In addition, the following specific guidance applies.

Since documents for IT management systems are usually written with a certain methodology, it should be reviewed how these documents are prepared in terms of the procedures, techniques and guidance specified in the methodology. (e.g. Auditors should check that documents prepared by other management systems ((ISO/IEC 20000, ISO/IEC9001 or ISO/IEC27001), if relevant.)

In addition, auditors should confirm that the IT controls are related to the results of the risk assessment and risk treatment process, and can subsequently be traced back to the various objectives.

6.4.4 Communicating during the audit

The guidelines from ISO 19011:2011, Clause 6.4.4 apply.

6.4.5 Assigning roles and responsibilities of guides and observers

The guidelines from ISO 19011:2011, Clause 6.4.5 apply.

6.4.6 Collecting and verifying information

The guidelines from ISO 19011:2011, Clause 6.4.6 apply.

6.4.7 Generating audit findings

The guidelines from ISO 19011:2011, Clause 6.4.7, apply.

6.4.8 Preparing audit conclusions

The guidelines from ISO 19011:2011, Clause 6.4.8 apply.

6.4.9 Conducting the closing meeting

The guidelines from ISO 19011:2011, Clause 6.4.9 apply.

6.5 Preparing and distributing the audit report

6.5.1 Preparing the audit report

The guidelines from ISO 19011:2011, Clause 6.5.1 apply. In addition, the following specific guidance applies.

The recommendation should take account of and consider the types, complexity and size of resource required for implementing the recommendation. This contributes to realistic expectations and subsequent implementation timeframes being set.

6.5.2 Distributing the audit report

The guidelines from ISO 19011:2011, Clause 6.5.2 apply.

6.6 Completing the audit

The guidelines from ISO 19011:2011, Clause 6.6 apply.

6.7 Conducting audit follow-up

The guidelines from ISO 19011:2011, Clause 6.7 apply. In addition, the following specific guidance applies.

6.7.1 Establishing a plan to implement corrective measures

(1) Auditee should establish and submit a plan to implement the corrective measures specified by the audit report. The plan should include the following items for each corrective measure:
 -The methods for the implementation
 - The department/group/section responsible for the implementation
 - The deadline of the recommended implementation

(2) Implementation corrective plans should be established for both major and minor nonconformities.

(3) Recommended corrective measures can to be selected when determining such factors as cost and benefit of the implementation.

6.7.2 Performing follow-up audit.

Following the pre-agreed schedule, the auditee should implement the corrective measures and the audit team should perform a follow-up audit to review the adequacy of the corrections.

After the review, audit team may produce a final report to close the audit. If the corrective actions are found to be insufficient, an additional follow-up report should be prepared. The auditee should implement additional measures based on the follow-up report and re-obtain a review from the audit team.

7 Competence and evaluation of auditors

7.1 General

The guidelines from ISO 19011:2011, Clause 7.1 apply.

7.2 Determining auditor competence to fulfil the needs of the audit programme

The guidelines from ISO 19011:2011, Clause 7.2.1 apply. In addition, the following specific guidance applies.

In deciding the appropriate knowledge and skills, the following should be considered:

a) The complexity of the IT systems (e.g. criticality and/or continuity of operation) ;
b) The type(s) of business performed with the use of IT;
c) The extent and diversity of technology utilized in the implementation of the various components of the IT (e.g. the implemented controls, documentation and/or process control, or corrective/preventive action, etc.);
d) The number of IT systems and IT operational sites;
e) The extent of outsourcing and third party arrangements utilised;
f) The standards, legal requirements, and other requirements relevant to the audit programme.

7.2.2 Personal behaviour

The guidelines from ISO 19011:2011, Clause 7.2.2 apply.

7.2.3 Knowledge and skills

7.2.3.1 General

The guidelines from ISO 19011:2011, Clause 7.2.3.1 apply.

7.2.3.2 Generic knowledge and skills of management system auditors

The guidelines from ISO 19011:2011, Clause 7.2.3.2 apply.

7.2.3.3 Discipline and sector specific knowledge and skills of management system auditors

The guidelines from ISO 19011:2011, Clause 7.2.3.3 apply.

.

7.2.3.4 Generic knowledge and skills of an audit team leader

The guidelines from ISO 19011:2011, Clause 7.2.3.4 apply.

7.2.3.5 Knowledge and skills for auditing management systems addressing multiple disciplines

The guidelines from ISO 19011:2011, Clause 7.2.3.5 apply.

7.2.4 Achieving auditor competence

The guidelines from ISO 19011:2011, Clause 7.2.4 apply. In addition, the following specific guidance applies.

IT auditors should have the necessary knowledge and skills in IT, understand the associated mechanisms of IT management and governance of IT, and should understand the relevant business requirements and risks. The Auditors' work experience should also contribute to the development of their knowledge and skills in the IT domain.

7.2.5 Audit team leaders

The guidelines from ISO 19011:2011, Clause 7.2.5 apply.

7.3 Establishing the auditor evaluation criteria

The guidelines from ISO 19011:2011, Clause 7.3, apply.

7.4 Selecting the appropriate auditor evaluation method

The guidelines from ISO 19011:2011, Clause 7.4, apply.

7.5 Conducting auditor evaluation

The guidelines from ISO 19011:2011, Clause 7.5, apply.

7.6 Maintaining and improving auditor competence

The guidelines from ISO 19011:2011, Clause 7.6, apply.

Annex A

(Informative)

Practice Guidance for IT Auditing

The text below provides generic guidance on how to audit governance of IT as required by ISO/IEC 38500.

.

This guidance is primarily intended to be referenced and used by auditors who will perform IT audit, be they internal or external.

Optional additional standards can be used to guide the auditee or auditor. These are listed as “Relevant Standards” in the tables below. Auditors are reminded to base non-conformities on the audit criteria and the requirements of ISO/IEC 38500.

Table A.1 — IT Audit practice guidance

A1. Responsibility, **Individuals and groups within the organization understand and accept their Responsibilities in respect of both supply of, and demand for IT. Those with Responsibility for actions also have the delegated authority to perform those actions**.	
Process	
A1.1 The responsibilities Formulation process for current and future business objectives.	
Audit Criteria	• Determine current and future business objectives. • The responsibilities Formulation process exists for current and future business objectives. • Ensure effective, efficient, and acceptable use and delivery of IT
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Policy for IT governance exists. • Evaluate options for use of IT as per the business plan. • Roles and responsibilities are assigned to specific roles and changes are made as changes in the business and the IT environment are made. • IT governance policy, roles, and governance membership responsibilities are known and understood.
Example of Audit Evidence	• IT governance Policy • Framework of authorities, responsibilities and process roles • Roles and responsibilities for the use of IT.
Audit practice guide	• Ascertain that IT governance policy exists.
	• Review the organization chart and ascertain Formulation process to evaluate the options for assigning responsibilities in respect of the organization’s current and future use of IT . • etc

Process	
A1.2 IT responsibilities Formulation process for the organization's business objectives and performance.	
Audit Criteria	• Ensure the establishment and assignment of the appropriate IT responsibilities. • IT responsibilities are assigned to IT specialists who understand business values and processes.
Relevant Standards	• ISO/IEC 38500
Relevant controls	• For information system development, the governing body should define the roles and responsibility of the information systems department, and assign and delegate authority to perform its function. • **Receive the information to analysis IT responsibilities as followers** o business requirements o known limitations o approach to be taken for the management of risks • A defined review process exists.
Example of Audit Evidence	• Report of IT highlighting roles and responsibilities. • The minutes of the IT committee meeting
Audit practice guide	• Review of IT committee meeting and the Report of IT highlighting roles and responsibilities.
	• Ascertain to evaluate the report of the performance of those given responsibility in the governance of IT.
Product	
A1.3 The appropriate IT governance mechanisms.	
Audit Criteria	• The responsibility and authority of personnel should be clearly defined and separated; responsibilities should be in relation to both the supply of, and demand for IT.
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Evaluate the options for assigning responsibilities in respect of the organization's current and future use of IT. • IT responsibilities are assigned to IT specialists who understand business values and processes • The responsibility and authority of personnel should be clearly defined and separated. • Information systems are based on business strategy, the governing body has a specialized committee that defines the appropriate IS strategies, assign tasks, and manages the implementation of the optimization plan. • Clarify the purpose and objectives of the committee, that appropriate authorities and responsibilities have been allocated to the committee based on the overall optimization plan. • The committee should monitor all the activities concerning the information systems in the organization and implement necessary corrective measures. • The committee should adopt the technology guidelines to stay current with trends in information technologies. • The committee should report its activities to the management. • The committee should provide to the management the information necessary for strategic decision support. • Clarify the missions of the information system department and allocate appropriate authority and responsibilities to the department. • The information system department should consider reforming the

	organizational structure with separation of duty, specialization, authorization and outsourcing, based on the size and characteristics of the organization. • etc
Example of Audit Evidence	• The description of IT responsibilities. • Policy(s) and roles are approved by the Policy Authority. • Reports from IT specialists • Organizationalcharts (Computerization Committee,information department etc.) • Memorandum/meeting record of committees • etc
Audit practice guide	• Check the framework and roles of authorities, and that responsibilities are adequete. • Review Information of the framework and roles of authorities, responsibilities are cleare and well-known. • Review Organizational chart and ascertain to establish a specialized committee to define IS strategies and assign tasks and implement optimization plan.
	• Ascertain the committee report its activities to the management. • etc • Review the report from IT specialists about IT responsibilities • Review missions statement of the information system department and ascertain it's adequate. • etc
Product	
A1.4 The information that they need to meet their responsibilities and accountability.	
Audit Criteria	• Evaluate options for use of IT. • Ascertain the performance of those given responsibility in the governance of IT.
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Evaluate the roles and responsibilities of each member in accordance with changes in the business and the IT environment. • Ascertain the meeting reports for IT use or the Plan of IT use and ascertain that responsibilities and accountability of IT use is considered adequete. • Clarify missions of the committee and appropriate authorities and responsibilities are allocated to the committee based on the overall optimization plan. • The committee should monitor all the activities concerning the information systems in the organization and implement necessary corrective measures. • The committee should adopt the technology guidelines to stay current with trends in information technologies. • The committee should report its activities to management. • The committee should be aligned and contribute to the management of strategic decision support. • etc •
Example of Audit Evidence	• The plan of IT use • The report of IT use
Audit practice guide	• Verify roles and responsibilities of each member of personnel in accordance with changes in the business and the IT environment. •

	• Ascertain the meeting reports for IT use or the Plan of IT use and ascertain that responsibilities and accountability of IT use is considered adequate. • etc

A2. Strategy **The organization's business strategy takes into account the current and future capabilities of IT; the strategic plans for IT satisfy the current and ongoing needs of the organization's business strategy**.	
Process	
A2.1 Appropriate risk assessment Formulation Process.	
Audit Criteria	• Establishing an appropriate risk assessment • Ensure that IT use are subject to and evaluated against relevant international and national standards.
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Appropriate policies of risk assessment exist. • Systems are in place to gather materials and analyze information of internal, external risk. • etc •
Example of Audit Evidence	• Risk assesement policy • etc
Audit practice guide	• Review Risk assesement policy and ascertain it,is appropriate.
	• Ascertain that the Risk assessment process is applied for IT use. • etc
Process	
A. 2.2 Business Strategy Formulation Process	
Audit Criteria	• In establishing business strategy, do processes exist and do they operate appropriately to take into account the current and future capability of IT.
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Define the goals of the information systems overall optimization and ensure the alignment to business strategies. • Define principles for the use of IT and IT investment allocation. • Define the information system operating? model utilised for the organization. • Define policies on organizational structure and business process changes caused by introducing the new system. • Define policies on information security.
Example of Audit Evidence	• Principles for use of IT and IT investment allocation. • The goals of the information systems overall optimization. • The information system operating? model utilised for the organization.
Audit practice guide	• Review Principles for use of IT and IT investment allocation. • Ascertain steering committee approve for the optimization plan • Ascertain the goals of the information systems overall optimization and ensure the alignment to business strategies. . • Ascertain principles for use of IT and IT investment allocations are to meet business requirements. • Ascertain if the organizational information system model has been applied. • Ascertain policies on organizational structure and any business process changes caused by introducing the new system has been applied. • Ascertain to policies on information security

Process	
A. 2.3 IT Strategic Plan Formulation Process	
Audit Criteria	• In developing IT Strategic Plan processes exist to satisfy the current and ongoing needs of the organization's business strategy, and that the processes operate appropriately.
Relevant Standards	• ISO/IEC 38500
Relevant controls	• - Analysis of As-is business and Information systems • - Analysis of IT utilization opportunity to support business strategy • - Establishment of IT strategy • - Design of to-be IT model • - Development of IT strategy implementation plan
Example of Audit Evidence	• SOP for Strategic IT planning • Guideline for technology impact analysis • Interview agenda for executives, management and stakeholders • Method to evaluate priorities of IT strategy alternatives
Audit practice guide	• In order to audit whether the process for developing the IT Strategic Plan supporting business strategy are in place and implemented, it should be reviewed whether: o SOP for strategic IT planning is documented, communicated and maintained; o Method for identifying business improvement requirements exist; o Techniques and processes exist to support the investigating the potential of IT to support business improvement requirements; o Processes for reviewing alternatives for the target IT is in place; o Evaluation criteria in the selection of alternatives are established; o Methods to incorporate opinions and feedback of executives, management and stakeholders during the strategic IT planning process are considered; o Process are in place for measuring the performance of IT in implementing business strategy.

Product	
A. 2.4 Contents of Business Strategy	
Audit Criteria	• Business strategy exists and its contents are appropriate
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Ascertain if the Business strategy and its contents are appropriate and supported and approved by the steering committe.
Example of Audit Evidence	• Memorandum/meeting record of committee • Report of Risk assessment.
Audit practice guide	• Review the Business strategy risk assessment report and that its contents are appropriate

Product	
A. 2.5 Risk assessment report for It	
Audit Criteria	Risk assessment exists and its contents are appropriate.
Relevant controls	- Establish policies for Risk assessment - Ascertain risk assessmet is adqute. - Establish policies for ensuring business continuity of the information

	system. - Establish the business continuity plan by all stakeholders, and obtain approval of the head of the organization for the plan. - Ensure that policies for business continuity plan include employee training. - Ensure that all necessary personnel in the relevant departments are reformed of the business continuity plan. - Review the business continuity plan as necessary.
Example of Audit Evidence	・Risk assessment report ・BCP plan etc.
Audit practice guide	Review Risk assessment report and ascertain the plans for IT risk are framed by risk assessment.
	• Ascertain if the BCP plan is used to support the business • Review the business continuity plan as required. • Policies for ensuring business continuity of the information system are deemed adequate • Business continuity plan exists and is inclusive of all relevant stakeholders. Approval has been provided by the head of the organization • Business continuity planning policy includes employee training. • All necessary personnel in the relevant departments are informed and conversant with the business continuity plan.
Product	
A. 2.6 Contents of IT Strategic Plan	
Audit Criteria	• IT Strategic Plan exists and its contents are appropriate
Relevant Standards	• ISO/IEC 38500
Relevant controls	• - Analysis of As-is business and information • - IT utilization opportunity against business strategy • - IT strategy • - To-be IT model • - IT strategy implementation plan •
Example of Audit Evidence	• Busines strategy • Strategic IT plan • Results of Interviews with executives, management and stakeholoers • Results of IT alternatives evaluation • Results of current informaiton systems analysis •
Audit practice guide	• In order to audit whether IT strategic plan exists and its contents are appropriate, it should be reviewed whether: o Changes in both the internal and external environment are factors influencing the business strategy and that they are understood; o Business improvement activities and IT utilization opportunities selected for achieving business strategy are appropriate; o Improvement initiatives are identified through current information systems review; o Results of interview with executives, management and stakeholders are systematically reflected in improvement initiatives, to-be model, and IT strategy; o To-be model reflects specific requirements of the IT strategy; o Implementation priorities of IT strategic initiatives are appropriate to the evaluation criteria; o Gap between as-is and to-be models can be resolved by implementing strategic IT initiatives; o Feasibilities are assessed through the analysis of resource required and benefits expected for each strategic IT initiative; o KPI's are selected and results of measurement are provided in order to evaluate the contribution of strategic IT initiatives to supporting business strategy;

	o IT strategic plan is updated according to the changes in the environment; o Performance of current IT strategy is used as an input to the IT strategy planning process. o Operational performance of IT resource and systems adopted by IT strategy is regularly evaluated.
Product	
A. 2.6 Risk Assessment	
A. 2.6.1 Business Continuity Plan	
Audit Criteria	• To secure the business continuity of an organization, a business continuity plan specific to an information system should be established.
Relevant controls	• Establish policies for ensuring business continuity of the information system. • Establishment of the business continuity plan is inclusive of all relevant stakeholders. Approval has been provided by the head of the organization. • Ensure that policies for business continuity plans include employee training. • Ensure that all necessary personnel in the relevant departments are informed and conversant with the business continuity plan. • Review the business continuity plan as required. •
Example of Audit Evidence	• BCP plan • Policies for BCP plan
Audit practice guide	• Review BCP plan and ascertain the plans are framed by risk assessment.
	• Ascertain if the BCP plan is used to support the business • Review the business continuity plan as required. • Policies for ensuring business continuity of the information system are deemed adequate • Business continuity plan exists and is inclusive of all relevant stakeholders. Approval has been provided by the head of the organization • Business continuity planning policy includes employee training. • All necessary personnel in the relevant departments are informed and conversant with the business continuity plan.

A3.Acquisition IT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision making. There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.	
Process	
A3.1 Evaluate options for providing IT Formulation Process.	
Audit Criteria	• Evaluate the options in the provision of IT in support of approved proposals and that these options are balancing risks and value for money of proposed investments.
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Ensure that the IT investment plan is created in a manner consistent with corporate strategies. • Compare multiple IT investment plan alternatives based on impact, effects, risk, schedule and feasibility. • IT investment budgets are executed in line with approved processes. •
Example of Audit Evidence	• Busines strategy • Strategic IT investment plan
Audit practice guide	• Ascertain if the IT investment plan is aligned and in synch with the optimization plan : o The IT investment plan is created in a manner consistent with corporate strategies. o Compare multiple IT investment plan alternatives and that these are based on impact, effects, risk, schedule and feasibility. o IT investment budgets are being managed in line with approved processes. o etc
Process	
A3.2 Analysis of IT acquisitions Formulation Process.	
Audit Criteria	• Extend ongoing analysis of the Formulation Process and include the review of the supply arrangements (including both internal and external supply arrangements) to ensure that they support the business needs of the organization.
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Ongoing analysis of the Formulation Process - extend to support business needs as below o Establish the standard methodology for estimating the return on IT investments. o Assess financial performance of the entire (end to end / TCO) information system and individual projects, and take necessary actions to solve any problems. o Review whether IT investments have been properly executed or not.
Example of Audit Evidence	• IT investment policy • Report for IT investment • The minutes of commitee.
Audit practice guide	• Review the IT investment report and committee minutes to ascertain to the performance of IT. • Establish the standard methodology for estimating the return on IT investments.

	• Assess financial performance of the entire (end to end / TCO) information system and individual projects, and take necessary actions to solve any problems. • Review whether IT investments have been properly executed or not. • Etc
Product	
A3.3 IT investments plan	
Audit Criteria	• IT investments make provision for the required resourcing and associated capabilities for both the short and longer term.
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Ensure IT Investment Plan is appropriate. (Do we need to reference reviewing the capability plan / succession planning?) • Analysis required of the necessary capabilities for both the short term and the long term.
Example of Audit Evidence	• IT investment plans • Report on the result of IT investment. •
Audit practice guide	• Revew IT investment plans and ascertain to ensure required capabilities are provisioned for both the short and the longer term. • etc
Product	
A3.4 Policies on Information Asset Management	
Audit Criteria	• To manage information assets properly, information assets management policy and associated plans should be established.
Relevant controls	• Define policies of information asset management and establish appropriate controls. • Assess risks for information assets, and take appropriate measures to reduce those risks. • Consider efficient and effective use of information assets. • Consider productivity improvement through information asset sharing.
Example of Audit Evidence	• Policies on information asset management • Risk assessment for relevant asset policy • The minutes of commitee meeting.
Audit practice guide	• Review policies relating to information asset management to assess risks for information assets, and take appropriate measures to reduce those risks. • Review the minutes of committee meeting to evaluate asset risk. • etc

Product	
A3.5 Consignment or Entrustment of Business Plans	
Audit Criteria	• The policies for fulfilling a consignment or entrustment are described in the use of “External Resources” in the overall optimization plan. • To prepare consignment or entrustment business plan in concrete form, the consignment or entrustment business plan should be prepared, and approved by an authorised person.
Relevant controls	• Ensure the consignment or entrustment business plans are developed in accordance with the overall optimization plan, and obtain approval to those plans from the management. • Define the objectives, scopes, budget, and structure of the consignment or entrustment business. • Assess concrete effects and potential problems of the consignment or entrustment business make decisions based on the results of the assessments. •
Example of Audit Evidence	• Optimization plan • Consignment or entrustment business plans and policies • SLA’s
Audit practice guide	• Review optimization plan and ascertain develop consignment or entrustment business plans in accordance with the overall optimization plan, and obtain approval to those plans from the management. • Review optimization plan and ascertain that the objectives, scopes, budget, and structure of the consignment or entrustment business are made appropriately. • Ascertain to assess concrete effects and potential problems of the consignment or entrustment business make decisions based on the results of the assessments.
Product	
A3.6 Selection of the Service Provider of Consignment Business	
Audit Criteria	• Selection of a consignee should be based on the documented contractor / service provider plan for operations., • The criteria for selecting a consignee should be clarified.
Relevant controls	• Define selection criteria of service providers. • Present requirement specifications to candidate service providers. • Assess proposals submitted by candidate service providers. • Delegated authorities are published.
Example of Audit Evidence	• Consignment or entrustment business plans and policies • Selection criteria
Audit practice guide	• Service provider selection criteria and associated business requirements have been meet. • Ascertain if present requirement specifications to candidate service providers according to supply arrangements (including both internal and external supply arrangements) support the business needs of the organization. • Ascertain and assess proposals submitted by candidate service providers.

Product	
A3.7 Contracts	
Audit Criteria	• A contract with a consignee should be in accordance with the rules for a contract as a contractor or the rules for concluding a contract as a consignee.
Relevant controls	• Contracts are compliant with the consignment contract rules and/or the entrustment contract rules. • Define provisions concerning compliance. • Define whether to allow re-commission. • Define the holders of the intellectual property rights. • Define the special agreement and disclaimer clauses. • Define details of services and the sharing of responsibilities. • Re-examine contents of the contract in the event of additions to or changes in the contract. • Define policies for system audit.
Example of Audit Evidence	• Consignment or entrustment business plans and policies • Contract templates and/or models are in placel
Audit practice guide	• Review contract and if the following is described o Contracts are compliant with the consignment contract rules and/or the entrustment contract rules. o Define provisions concerning compliance. o Define whether to allow re-commission. o Define the holders of the intellectual property rights. o Define the special agreement and disclaimer clauses. o Define details of services and the sharing of responsibilities. o Re-examine contents of the contract in case of additions to or changes in the contract. o Define policies for system audit. •
Product	
A3.8 Consignment	
Audit Criteria	• To allow a consignee to perform subcontracted operations without excess or shortage, the contents of subcontracted operations performed by a consignee should be in agreement with the contents described in a subcontracting contract.
Relevant controls	• Assess consistencies between the actual consigned business and the contracted business. • Provide necessary specifications, data and other materials according to the contract. • Monitor progress of the consigned business, and take necessary measures against delay of the project. • Monitor the status of error prevention, fraud prevention and confidentiality protection at the consigned partners, and take measures as and when necessary. • Ensure that the acceptance of deliverables is carried out based on the consignment contract. • Ensure that the restitution and/or disposal of data and materials that are provided for the consignment are properly executed after completion of the consigned services. • Access and analyze results of the consigned services.

Example of Audit Evidence	• Consignment or entrustment business plans and policies • Contract • Actual business conduct • Acceptance criteria of deliverables • SLA
Audit practice guide	• Review contract and associated SLA's, and ascertain that the business requirements of users have been applied.
Product	
A3.9 Entrustment	
Audit Criteria	• The contents of entrusted business should be in agreement with the contents described in a contract.
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Ensure that the actual entrusted business is consistent with the contracted provisions. • Monitor progress of the entrusted business, and take measures against potential risks. • Implement a quality management process for deliverables. • Ensure that restitution and/or disposal of data, materials and other resources supplied from the contracted party are properly executed in accordance with the contract, after the completion of the contracted business.
Example of Audit Evidence	• Consignment or entrustment business plans and policies • Contract • Disposal of data, materials and other resources supplied from the contracted party • Quality control • SLA's.
Audit practice guide	• Review contract and SLA's and ascertain that Entrustment offer meets the requirements for IT use clearly. • etc
Product	
A3.10 The report of IT assets (systems and infrastructure)	
Audit Criteria	• IT assets (systems and infrastructure) are acquired in an appropriate manner, including the preparation of suitable documentation, while ensuring that required capabilities are provided.
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Ensure that IT assets are acquired in an appropriate manner. • Ensure that suitable documentation for IT assets is prepared • Ensure IT investment takes account of the required supporting capabilities needed for any acquisations.
Example of Audit Evidence	• Report of IT asset. • etc
Audit practice guide	• Revew Report of IT assets and ascertain the following: o IT assets are acquired in an appropriate manner. o Suitable documentation for IT assets is prepared o IT investment takes account of the required supporting capabilities needed for any acquisitions.

A4 Performance IT is fit for purpose in supporting the organization, providing the services, levels of service and service quality required to meet current and future business requirements.	
Process	
A4.1 Business Process is fit for Business purpose and requirements for IT use	
Audit Criteria	• Determine business purpose and requirements. • The business processes exist and operate appropriately to meet current and future business requirements for IT use
Relevant controls	• Determine business purpose and requirements. • IT services meet the requirements of the business.
Example of Audit Evidence	• IT governance Policy • The minutes of IT committee meeting. • Optimization plan
Audit practice guide	• Obtain IT governance Policy, optimization plan and IS development plan. • Revew the minutes of IT committee meeting with resepct the IS development plan and conform the IS development plan is aligned to the optimization plan and the risks of IT use.
	Ascertain that the IT committee meeting open timely. Please refer the note to this bullet point. What is the intent of this s tatement • • Ascertain that mechanisms exist to so as to ensure that IT are capable of support business processes with the required capability and capacity. • Ascertain the risks to continued operation of the business arising from any limitations associated with IT related activities. • Ascertain the existence of supporting IT processes that support the current and ongoing needs of the organization's business purpose, and the processes operate appropriately and provision for the necessary future IT capability.
Process	
A4.2 IT Process is fit for Business purpose and requirement.	
Audit Criteria	• Determine business purpose and requirements. • Determine the existence of supporting IT processes that support the current and ongoing needs of the organization's business purpose, and the processes operate appropriately and provision for the necessary future IT capability • IT assets are assigned and IT Process support the integrity, effectiveness, efficiency in the use of IT. • Risk of IT use is reviewed frequently.
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Mechanism exist to evaluate the risks, the integrity of information, and the protection of IT assets, including associated intellectual property and organizational memory. • Ascertain that mechanisms exist to ensure allocation of sufficient resources so that IT meets the needs of the organization, according to the agreed priorities and agreed budgets. • Ascertain the agreed priorities and budgetary constraints.

Example of Audit Evidence	• IT Operating Finance report • User satisfaction report . • Log reports • Analysis Report of IT use. (Do we need to define what this report is?)
Audit practice guide	• Ascertain the direction of IT is supported by IT Managers. • Ascertain that reports are monitored and the performance of IT use is improved.
Product	
A4.3 Business Performance	
Audit Criteria	• Business services exist and its usages are appropriate. • Ensure effective, efficient, and acceptable use and delivery of IT
Relevant controls	• Evaluate options for assuring effective, timely decisions with respect the use of IT and that it supports the overall business goals and direction. • Ensure the effectiveness and performance of the organization's system for Governance of IT is regularly evaluated.
Example of Audit Evidence	• IT governance policy • IT strategy plan • Report of IT use. • Meeting records with the users of IT / customenr satisfaction reports.
Audit practice guide	• Review IT strategy plan and evaluate options for assuring effective, timely decisions about the use of IT in support of business goals. • Review meeting records with the user to identify user requirement and that the effectiveness and performance of the organization's system for Governance of IT is regularly evaluated.
Product	
A4.4 IT requirements Analysis	
Audit Criteria	• For the use of IT, careful analysis on business requirements should be carried out.
Relevant controls	• Requirements are documented and completed in line with the relevant Project method. • Approval by the responsible personnel from the user department, the system development department, the operation department and the application maintenance department for the defined requirements based on the development plan. • Define target, scope and methodology for user requirement survey. • Analyze the present states of information systems with personnel who are familiar with the business process from the user department, the system development department, the operation department and the application maintenance department. • Ensure that user requirements are documented and confirmed by the user department. • Analyze potential risks in introducing the information system. • Ensure that affected business processes, management structures and rules/procedures are reviewed and assessed regarding the introduction of the information system. • Assess the effectiveness from both qualitative and quantitative perspectives when introducing the information system

	• Ensure that suitability with user requirements is assessed before implementing software packages.
Example of Audit Evidence	• Document of user requirement • Meeting records with users to identify user requirements • Records for assessment of user requirement • Optimization plan •
Audit practice guide	• Review Optimization plan and ascertain to perform analysis process. Not too sure I understand this. • etc
Process	
A4.5 Document Management	
Audit Criteria	• Top management shall provide evidence of its commitment to planning, establishing, implementing, operating, monitoring, reviewing, maintaining, and improving document management. • Keep the quality and importance of documents. • Documents life cycle management and check the quality of documents.
Relevant controls	• Approval for created documents from the appropriate stakeholders and responsible personnel in the information system department. • Define and comply with documentation rules. • Define the documentation plan. • Define the type, the objective and the method of creation of documentation. • Ensure that all documents are created in accordance with the documentation plan. • Approval for the contents of any modifications to documents from the appropriate stakeholders and the responsible personnel in the information department. • Update descriptions in documents and record the update history following any modification to the information system. • Ensure that document storage, duplication and destruction measures are taken in accordance with fraud prevention and confidentiality protection. •
Example of Audit Evidence	• Documentation rules • Records of documentation • Records of documentation history • Confidentiality of document and storage documentation.
Audit practice guide	• Review documentation rules. • Review the documentation records of that documentation management process exist. • etc
Process	
A4.6 Project Management	
Audit Objectives	• Perform planning, development, operation, and maintenance operations as planned, appropriate project management is performed. • To improve the management process, review and analyse the results and performance against a plan upon completion of an each process.
Relevant controls	• Define a project management approach and structure based on the project plan, and obtain approval from the appropriate stakeholders and the personnel responsible for planning, development, operations development and maintenance development. • Ensure that stakeholders and the personnel responsible in the planning department, the development, the operations department

	and the maintenance department are monitoring the progress of the project. • Ensure that the appropriate measures are taken against delays. • Analyze and assess project performance against the project plan at the end of each phase of the project, and obtain approval for the assessment result from the project manager. • Ensure that the assessment results are properly reflected in the plan for the next subsequent phase of the project. • Ensure that the assessment results are properly reflected in improvements to the approach and the structure of project management.
Example of Audit Evidence	• Project management policies and rules • Record of project management • Meeting record of project
Audit practice guide	• Ascertain that project management policies and rules exist. • Review project management records and ascertain that project management process exist. • Review project meeting records and ascertain the performance of projects etc
Process	
A4.7 Quality Management	
Audit Objectives	• A quality management plan should be required to maintain a level of quality worthy of the effort made to achieve organizational objectives in all life cycles of an information system and to perform quality management operations smoothly and effectively. • Verify that operations have been performed as planned and quality management objectives have been achieved, • The results of performance are analyzed and evaluated based on the quality management rules.
Relevant controls	• Develop a quality management plan according to quality criteria, and obtain approval of the plan from the appropriate stakeholders and the responsible personnel in the planning department, the development department, the operations department and the maintenance department. • Define the quality management plan methodology, systems and so on. • Analyze and assess quality performance against the quality management plan at the completion of each phase of the project, and obtain approval of the result from the project manager. • Ensure that the assessment results are properly reflected in improvements on quality management standards, approaches, and systems.
Example of Audit Evidence	• Quality management policies and rules • Project management records • Project meeting record s
Audit practice guide	• Ascertain quality management policies and rules exist. • Review project management records and ascertain quality management process exist. • etc

Product	
A4.8 Use of IT services and product.	
Audit Criteria	• IT services exist and its contents are appropriate. • Ensure integrity, effective, efficient, and acceptable use and delivery of IT.
Relevant controls	• IT supports the business, when required for business reasons, with correct and up-to-date data that is protected from loss or misuse. • Monitor the extent to which the policies, such as for data accuracy and the efficient use of IT, are followed properly. • Keep integrity, effective, efficient, and secure through all life cycle process.
Example of Audit Evidence	• The polcy and roles of IT use. • Business requirements • The perfomance report of IT through all life cycle process.
Audit practice guide	• Review Ascertain to offer IT service to support the business, when required for business reasons, with correct and up-to-date data that is protected from loss or misuse. • Monitor the extent to which the policies, such as for data accuracy and the efficient use of IT, are followed properly. • Ensure process maintain to keep integrity, effective, efficient, and secure through all life cycle process.
Product	
A4.9 IT Development Plans	
Audit Criteria	• IT development plan is developed in alignment with the optimization plan and business requirements. • Monitor the extent to which allocated resources and budgets are prioritised according to business objectives.
Relevant controls	• Approval for the development plan from the appropriate governing body. • Establish the development plan within the overall context of the optimization plan. • Ensure the development plan that specifyies objectives, targets processes, costs, and system development structurse and cost efficiency for investment. • Ensure the development plan includes education and training programs for stakeholders. • Ensure the development plan specifies the roles of the user department and of the information system development department. • Ensure the development plan indicates the cost calculation methodology for system development, operation and maintenance. • Ensure the development plan specifies conditions for defining system life cycle. • Ensure that the formulation and the system development methodology are defined based on a target scale and specific system requirements when designing the development plan. • Ensure that a feasibility study with alternatives is studied to achieve the objectives of the information system when designing the development plan.

Example of Audit Evidence	• Development plan • Management and governing body records for the development plan. • The system development methodology
Audit practice guide	• Review the IT development plan and ascertain that the plan is applied as follows: o Approval for the development plan from the appropriate governing body. o The development plan is consistent with the overall optimization plan. o The development plan specifies its objectives, targets processes, costs, and system development structurse and cost efficiency for investment. o The development plan includes education and training programs for stakeholders. o The development plan specifies the roles of the user department and of the information system development department. o The development plan indicates the cost calculation methodology for system development, operation and maintenance. o The development plan specifies conditions for defining system life cycle. o The formulation and the system development methodology are defined based on a target scale and specific system requirements when designing the development plan. o Ensure that a feasibility study with alternatives is studied to achieve the objectives of the information system when designing the development plan. o etc
Product	
A4.10 Change Management	
A4.10 Design and transition of new or changed services	
A4.10.1 Plan new or changed services	
Audit Objectives	• Determine business purpose and requirements. IT processes exist to satisfy the current and ongoing needs of the organization's business purpose, and the processes operate appropriately for future capability of IT. • New or changed services are planned to fulfil the service requirements. Planning for the new or changed services shall be agreed with the customer and interested parties.
Relevant Standards	• ISO/IEC 38500, ISO/IEC 20000-2, ISO/IEC 12207-1, ISO/IEC 15504-2
Relevant controls	• The existance of policy to initiate a new plan and/or change services and that it is aligned to the IT strategy. This needs to take into consideration the potential financial, organizational, and technical impact of delivering the new or changed services. It also takes into consideration the potential impact of the new or changed services on the IT management system. • Review the plan for the new or changed services. Plan should include or contain a reference to at least the following: o authorities and responsibilities for design, development and transition activities; o activities to be performed by the service provider and other parties including activities across interfaces from the service provider to other parties; o communication to interested parties;

	o human, technical, information and financial resources; o timescales for planned activities; o identification, assessment and management of risks; o dependencies on other services; o testing required for the new or changed services; o service acceptance criteria; • expected outcomes from delivering the new or changed services, expressed in measurable terms.
Example of Audit Evidence	• Policy to make a new plan or change services • Change management rules • Plan for new or changed services. • Review documentation • Tracking change management record and/or request/approval/actual changes/test/production
Audit practice guide	• Verify the new plan or changed services are made in accordance with the policy. Take into consideration the potential financial, organizational, and technical impact of delivering the new or changed services and consideration the potential impact of the new or changed services on the IT management system. • Inspect review memo's and the associated plan.. • Authorities and responsibilities for design, development and transition activities; • Activities to be performed by the service provider and other parties including activities across interfaces from the service provider to other parties; • Communication to interested parties; • Human, technical, information and financial resources; • Timescales for planned activities; • Identification, assessment and management of risks; • Dependencies on other services; • Testing required for the new or changed services; • Service acceptance criteria; • Expected outcomes from delivering the new or changed services, expressed in measurable terms. • etc.
Product	
A4.11 Implement Change Management services	
Audit Objectives	• Change management issues should be carried out in accordance with the change management rules so that changes can be made in a seamless and safe way.
Relevant controls	• Change management issues are rectified and implementation complies with the associated change management rules. • Ensure that the environment of other related systems is changed simultaneously when implementing change management issues. • Obtain approval of the results of change management issues from the appropriate stakeholders and the responsible personnel in the development department, the operation department and the maintenance department.
Example of Audit Evidence	• Change management rules • Tracking change management records and/or request/approval/actual changes/test/production
Audit practice guide	• Ascertain that Change management issues are rectified and implementation complies with the associated change management rules. • Ascertain that the environment of other related systems is changed simultaneously when implementing change management issues. • Ascertain that approval of the results of change management issues are obtain from the appropriate stakeholders and the responsible

	personnel in the development department, the operation department and the maintenance department.
Product	
A4.12 Disaster Recovery services	
A4.12.1 Risk analysis	
Audit Objectives	• To illustrate what actions are taken to protect information systems from a disaster (including acts of god / force majure???) or an act of terrorism, it is necessary to clarify the types of risks, including earthquake, flood, terrorism, etc.
Relevant controls	• Assess potential risks such as earthquakes and the range of impacts on the information system. • Analyze potential damage to the organization suffered from a shutdown of the information system and so on. • Assess the acceptable recovery time for each business processes and prioritize them.
Example of Audit Evidence	• contingency plan • record of risk analysis • risk treatment plan • disaster recovery plan
Audit practice guide	• Review contingency plan • Ascertain to Assess the acceptable recovery time for each business processes and prioritize them • etc
Product	
A4.13 Contingency Plan	
Audit Objectives	• A disaster contingency plan should be formulated by ensuring consistency with the business continuity plan so that appropriate actions can be taken quickly with the least confusion if a disaster occurs.
Relevant controls	• Develop contingency plans based on risk analysis and ensure that the plan is consistent with the business continuity plan. • Obtain approval for the contingency plan from the governing body of the organization. • Assess the feasibility of the contingency plan. • Define educational training policies for employees in the contingency plan. • Communicate and inform related departments of the contingency plan. • Update the contingency plan regularly and ensure that the plan is kept up to date.
Example of Audit Evidence	• Disaster recovery plan • Contingency plan • Record for training disaster recovery plan
Audit practice guide	• Review disaster recovery plan and contingency plan, and ascertain that they are made by appropriate risk analysis and kept up to date timely. • Ascertain training plan exit and practice with related member. • etc

Product	
A4.14 Backups	
Audit Objectives	• Recover an information system from failure in a reliable manner, it is also necessary to establish backup methods and procedures with recovery time goal.
Relevant controls	• Define methods and procedures for backing up the system, data and the necessary resources to meet the recovery objectives of the businesses. • Assess and confirm the backup methods and procedures by the responsible personnel in the operations department.
Example of Audit Evidence	• Backup plan • Record of backup and its results • Offsite storage of backup tapes
Audit practice guide	• Ascertain methods and procedures for backing up the system, data and the necessary resources to meet the recovery objectives of the business. • Confirm the backup methods and procedures are approved and understood by the responsible personnel in the operations department.
Product	
A4.15 Alternative Operations and Recovery	
Audit Objectives	• Alternative processing procedures should be established to continue operations until an information system is recovered from failure.
Relevant controls	• Define and assess alternative processing procedures and structures until resumption. This task should be conducted by the appropriate stakeholders and the responsible personnel in the operations department. • Define and assess recovery procedures and structures. This task should be done by the appropriate stakeholders and the responsible personnel in the operations department.
Example of Audit Evidence	• Backup recovery plan and test • Alternative processing recovery procedures
Audit practice guide	• Assess that alternative processing procedures and structures exist, are available until service resumes. This task should be conducted by the appropriate stakeholders and the responsible personnel in the operations department. • Assess that recovery procedures and structures exist. This task should be done by the appropriate stakeholders and the responsible personnel in the operations department.
Product	
A4.16 Systems Operation services	
A4.16.1 Operation Management Rules	
Audit Objectives	• Perform operations smoothly and efficiently, operations management rules and operational procedures are in place. A person in charge of supervising the operations should confirm and approve the process.

Relevant controls	• Responsible personnel from the operations department have approved the management rules and procedures. • Operation management rules are based on the operation management design. • Operational procedures are based on the operation management design and rules considering the target scale, periods and specific system requirements. • Ensure that responsible personnel are selected based on the operation management design and rules.
Example of Audit Evidence	• Operation rules • Acquisition of the operation document and requirement definitions.
Audit practice guide	• Operation management rules and procedures are approved by the responsible personnel and exist. • Operation management rules are based on the operation management design. • Operation procedures are based on the operation management design and rules considering the target scale, periods and specific system requirements. • That responsible personnel are selected based on the operation management design and rules.
Product	
A4.17 Operation Management services	
Audit Objectives	• An information system should be operated smoothly / seamlessly. • The operation of information system should be processed and completed as scheduled. • The system operations plan should be formulated..
Relevant controls	• Define the annual operation plan that has been approved by the responsible personnel. • Ensure that monthly and daily system operation plans are created from the annual operation plan. • Ensure that the operation activities comply with the operation management rules. • Ensure that job schedules are organized according to the priorities of the business processes. • Ensure that the system operation complies with the job schedules and operational instructions. • Ensure that exceptional operation of the system is handled based on the operation management rules. • Ensure that shift handovers are carried out in accordance with the operation management rules. • Ensure that job schedules are recorded with operation logs and the differentials from the original ones are analyzed. • Ensure that operational records are retained for a certain period in accordance with operation management rules. • Define a reporting system and procedures in proportion to the levels of impact of incidents or failures. • Ensure that all records of incidents or failures are retained and reported to the responsible personnel for operation (management). • Ensure that root causes of incidents or failures are investigated, and take proper actions to prevent reoccurrences. • Establish a support environment to help and assist users of the information system. • Provide users with information security education and training. • Establish a monitoring framework for system operations. • Ensure that operational efficiency is attained for the information system to improve performance and the utilization of resources.

Example of Audit Evidence	• Operation rules and procedures • The operation plan, document and requirement definitions • Operation report and log
Audit practice guide	• Ascertain the system operation plans are formulated. • Ascertain the system operation reports are formulated. • Review that the system operation plans are approved by management. • Review the system operation reports and ascertain the operations are smooth and monitor the extent to which the policies, such as for data accuracy and the efficient use of IT, are followed properly. • etc
Product	
A4.18 Managing Data	
Audit Objectives	• Prevent data-entry errors and to protect confidential data, it is necessary to document the rules for handling and managing data for operation. • A series of operations for data input to an information system shall be documented as a data input procedure. A data verification method and data approval method should also be established. • Abuse or leakage of data output should be prevented, and confidential data should be protected. To achieve this, a data output procedure and rules and data approval procedure should be established.
Relevant controls	• Define and ensure they comply with data control rules. • Ensure that access control and monitoring data (creation, changes, and deletion) are put in place effectively. • Ensure that data integrity is assured. • Ensure that data usage is recorded and analysed periodically. • Define the scope, method and timing of data backup according to business requirements, the data processing structure and data restoration. • Ensure that data delivery complies with data control rules. • Ensure that fraud prevention and confidentiality protection measures are used whenever data is exchanged. • Ensure that procedures for data retention, duplication and destruction are taken for error prevention, fraud prevention and confidentiality protection. • Ensure that data is protected from computer viruses. • Ensure that the intellectual property right of data is managed properly.
Example of Audit Evidence	• Data control rules (included input control rules and operational, output control rules.) • Data control report • Record of input data. • Record of output data
Audit practice guide	• Ascertain date control rules exit. • Review data control report and the data operations are adequate to keep accuracy, confidendential, with correct and up-to-date data that is protected from loss or misuse.
Product	
A4.19 Software Management services	
Audit Objectives	• Ensure that software is used properly and to prevent software from being abused, rules for handling and management of software should be established. (controls)

Relevant controls	• Define and comply with software control rules. • Ensure that access control and monitoring functions for software are put in place effectively. • Ensure that software usage information is stored and reviewed periodically. • Define the scope, method and timing of software backups according to business requirements and the data processing structure. • Ensure that software delivery is complies with software control rules. • Ensure that procedures for software data retention, duplication and destruction are taken for error prevention, fraud prevention and confidentiality protection. • Ensure that software is protected from computer viruses. • Ensure that the intellectual property right of software is managed properly. • Define policies for the utilization of free software (open source).
Example of Audit Evidence	• Software control rules • Software control report
Audit practice guide	• Ascertain operation procedures are run by software control rules. • Review software control report and ascertain software control perform appropriately. • etc
Product	
A4.20 Manage Hardware services	
Audit Objectives	• Promote the proper use of hardware, prevent hardware from failure, and to protect from natural disaster, hardware management rules and monitoring should be established.
Relevant controls	• Define and comply with hardware management rules. • Ensure that hardware is installed in an environment resilient to potential risks. • Ensure that periodical maintenance is provided for hardware. • Ensure that proper measures are taken for hardware failures and capacity. • Ensure that hardware usage is recorded and reviewed periodically. • Ensure that procedures for hardware retention, relocation and disposal are taken for error prevention, fraud prevention and confidentiality protection.
Example of Audit Evidence	• Hardware management rules. • Hardware management report.
Audit practice guide	• Ascertain operation procedures are run by hardware control rules. • Review hardware control report and ascertain hardware control perform appropriately.(include capacity ,incident) • etc
Product	
A4.21 Manage Network services	
Audit Objectives	• Operate the network properly and efficiently, network management rules should be established and monitored.

Relevant controls	• Define and comply with network management rules. • Ensure that access control and the monitoring functions for the network are put in place effectively. • Ensure that the network is periodically reviewed for monitoring logs. • Ensure that proper measures are taken against failures in the network. • Ensure that the network usage is periodically analyzed from stored records, capacity. • Define organization policies for services provided by network operators.
Example of Audit Evidence	• Network management rules • Network management report
Audit practice guide	• Ascertain operation procedures are run by network control rules. • Review network control report and ascertain network control perform appropriately.(include capacity ,incident)
Product	
A4.22 Manage Configuration services	
Audit Objectives	• Maintain the functions of an information system and achieve fast recovery in the event of failure, it is necessary to clarify software, hardware, and network configurations, installation parameters, support conditions, etc.
Relevant controls	• Ensure that the scope of software management, hardware management and network management is clearly defined. Ensure that a proper management level is provided. • Ensure that system configuration, vendors and support conditions for software, hardware and networks are clearly specified. • Ensure that the introduction and replacement of software, hardware and networks is decided before an assessment of its impact. • Ensure that the introduction and replacement of software, hardware and networks is planned systematically.
Example of Audit Evidence	• System configuration • Record of change managment
Audit practice guide	• Review system configuration and ascertin configiration management purocess are adqete or not. • etc
Product	
A4.23 Manage Facilities and Equipment services	
Audit Objectives	• Minimize the damage caused by suspension of the IS service or the outage of an Information System, buildings and related facilities should be established in an environment that allows an organization to avoid assumed risks properly.
Relevant controls	• Ensure that facilities are located in an environment resilient to potential risks. • Ensure that accesses to facilities and machine rooms are controlled for fraud prevention and protection of confidentiality. • Ensure that facilities are properly operated. • Ensure that maintenance of facilities is provided periodically. • Ensure that proper measures against failures are taken. • Ensure that the access logs to the facilities and machine rooms are recorded and reviewed periodically.

Example of Audit Evidence	• Facilities plan • Environment plan • Access logs
Audit practice guide	• Review facilities plan is met to Asset plan. • Ascertain that facilities are properly operated.etc
Product	
A4.24 Maintenance services	
A4.24.1 Maintenance Procedures and plan	
Audit Objectives	• Standardize maintenance operations and perform maintenance operations smoothly while ensuring reliability, maintenance rules and procedures should be established. • Clarify the scope of maintenance and the maintenance work. • A maintenance plan should be formulated based on the results of surveys and analyses.
Relevant controls	• Define the approval for maintenance rules and procedures from the person responsible for maintenance. • Define maintenance procedures according to the scale and necessary period of maintenance and specific system requirements. • Assess potential risks inherent in the maintenance, and develop necessary preventive measures. • Define the approval for maintenance plan from the personnel responsible for maintenance. • Examine and analyze the contents and influence of maintenance against change requests. • Define the objective, scope, methodologies, and schedule for the maintenance test plan.
Example of Audit Evidence	• Maintenance rules and procedures • Plan of maintenance • Record of approval for maintenance • Record of maintenance and procedures by the maintenance personnel
Audit practice guide	• Review plan of maintenance. • Ascertain maintenance procedures meet business requirements. • etc
A4.24.2 Maintenance Implementation	
Audit Objectives	• Prevent from errors, misconduct, performance degradation, etc., a system design document, program design document should be managed properly with an approval from interested parties
Relevant controls	• Ensure that any modifications of the system design documents and the program design documents are implemented according to the maintenance plan. Prior to the modification, obtain approval for any changes of documents from the personnel responsible for maintenance, together with the appropriate stakeholders. • Ensure that all program modifications are implemented according to the authorized maintenance procedures. Prior to modifications, changes should be approved by the personnel responsible for maintenance. • Verify that programming is written according to the modified program design documents.
Example of Audit Evidence	• Maintenance record • Record of maintenance – same thing as above?

Audit practice guide	• Review record of maintenance. • Ascertain modifications meet business requirements
A4.24.3 Maintenance Verification	
Audit Objectives	• Changed program has been tested properly and smoothly, a test should be conducted based on a maintenance test plan.
Relevant controls	• Ensure that tests of modified programs are performed in accordance with the maintenance test plan. • Ensure that any tests of modified programs are performed taking into account the range tests impacts. • Ensure that the user department of the system is involved in the tests for the modified program, and that the tests are performed in accordance with the user manuals. • Define the approval of the results of the tests of the modified programs from the appropriate stakeholder and personnel responsible for operations and maintenance. • Ensure that the results of the tests of the modified programs are properly recorded and stored.
Example of Audit Evidence	• Maintenance record • Record of approval for verification • Test record
Audit practice guide	• Review test record • Ascertain Maintenance is appropriate
Product	
A4.25 Promotion to Production services (is another word “migration”).	
Audit Objectives	• Perform the promotion (migration?) process correctly and smoothly, it is necessary to clarify the period, method, system, conditions and a promotion procedure.
Relevant controls	• Define promotion procedures taking into account of the promotion conditions. • Ensure that backups of the pre-modified program and data are created. • Ensure that the personnel responsible for operations and the maintenance department ensure that the modified system does not affect other information systems.
Example of Audit Evidence	• Promotion procedure and rules • Record of approval to move to production • Backup tapes for promotion
Audit practice guide	• Review promotion procedure and rules • Ascertain the appropriate promotion procedures exit
Product	
A4.26 Disposal of Old Information Systems services	
Audit Objectives	• Disposing an old information system smoothly and completely, an disposal plan should be prepared for potential risks of leakage of information.
Relevant controls	• Define the disposal plan of old information systems accounting for any risks that may be incurred. The plan is obtained approval for by the appropriate stakeholders and the responsible personnel in the operations and maintenance departments. • Decide the disposal measure and timing of disposal of old information

	systems, taking measures to prevent fraud and protect confidentiality.
Example of Audit Evidence	- Diposal rules and plan - Record of diposal of old information - Confirm disposal of information
Audit practice guide	- Review diposal rules and plan - Ascertain the diposal procedures are adequate.
Product	
A4.27 Information security management services	
Audit Criteria	- Implement physical, administrative and technical security controls in order to preserve confidentiality, integrity and accessibility of information assets.
Relevant Standards	- ISO/IEC 38500, ISO/IEC 20000-2, ISO/IEC 12207-1, ISO/IEC 15504-2
Relevant controls	- An information security policy with appropriate authority approve taking into consideration the service requirements, statutory and regulatory requirements, and contractual obligations. - Communicate the information security policy and the importance of conforming to the policy to appropriate - Personnel within the service provider, customer and suppliers; - Ensure that information security management objectives are established; - Define the approach to be taken for the management of information security risks and the criteria for accepting risks; - Ensure that information security risk assessments are conducted at planned intervals; - Ensure that internal information security audits are conducted; - Ensure that audit results are reviewed to identify opportunities for improvement - Operate appropriate information security controls to: o fulfill the requirements of the information security policy; o achieve information security management objectives; o manage risks related to information security. - Requests for change shall be assessed to identify: o new or changed information security risks; o potential impact on the existing information security policy and controls.
Example of Audit Evidence	- An information security policy - Information security risk assessments report
Audit practice guide	- These information security controls are documented and shall describe the risks to which the controls relate their operation and maintenance. - Review the effectiveness of information security controls. - Take necessary actions and report on the actions taken. - Identify external organizations that have a need to access, use or manage service provider's information or services. - Ensure to document, agree and implement information security controls with these external organizations. - Information security incidents should be managed using the incident management procedures, with a priority appropriate to the information security risks. - These information security controls shall be documented and should describe the risks to which the controls relate their operation and maintenance. - Review the effectiveness of information security controls. The service

	provider should take necessary actions and report on the actions taken. • Ensure to analys the types, volumes and impacts of information security incidents. Information security incidents shall be reported and reviewed to identify opportunities for improvement.

A5.Conformance IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.	
Process	
A5.1 Business Process to comply with laws and regulations for Information Systems,	
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Establish an organizational system (e.g. department) for IT satisfies obligations. • Exit internal policies, standards and professional guidelines.
Example of Audit Evidence	• Organizational chart • Internal policies, standards and professional guidelines.
Audit practice guide	• impacts of information security incidents. Information security incidents shall be reported and reviewed toidentify opportunities for improvement. • etc
Process	
A5.2 IT Formulation Process for conformance.	
Audit Criteria	• Evaluate regularly the organization's internal conformance to its system for Governance of IT
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Identify applicable laws and regulations to the organization, and inform and educate stakeholders. • Define the information ethics, and inform and educate related persons.
Example of Audit Evidence	• Organization chart • Report related laws and regulations to the organization, • Education plan
Audit practice guide	• Ascertain the formulation process exit. • Ascertain the training system exists.
Product	
A5.3 The mechanisms for ensuring that the use of IT complies with relevant obligations, standards and guidelines.	
Audit Criteria	• Ensure those responsible to establish regular and routine • mechanisms for ensuring that the use of IT complies with relevant obligations (regulatory, legislation, common law, contractual), standards and guidelines.for professional
Relevant Standards	• ISO/IEC 38500

Relevant controls	• Comply with laws and regulations for Information Systems, a department responsible for laws and regulations should be established in an organization. • Evaluate the organizatjon's internal Conformance to itssystem for Governance of IT.
Example of Audit Evidence	• Internal policies,Standards and professional guidelines.
Audit practice guide	• Ascertain regularlye valuate the extent tow hichITsatisfiesobligations • (regulatory,legislation,Commonlaw,contractua一).internalpo一 icies,Standards • andprofessionalguidelines. • Ascertain evaluate the organizatjon'sinternal Conformance to itssystem for Governance of IT.
Product	
A5.4 The policies, relevant guidelines for professional.	
Audit Criteria	• The policies are established and enforced to enable theorganization to meet its internal obligations in its use of IT. • IT staff follow relevant guidelines behavior and development. • All actions relating to IT be ethical.
Relevant controls	• ISO/IEC 38500
Example of Audit Evidence	• Policys • Gaidance • The report of investigations of knowledge of the policys and guidelines.
Audit practice guide	• Ascertain the policies and guidelines for IT use exist . • Review the report of investigations of knowledge of the policys and guidelines. • Ascertain IT staffs accept to meet their obligations by training and information is well-known. • etc
Product	
A5.5 The report that IT compliance and conformance through appropriate	
Audit Criteria	• Monitor IT compliance and conformance through appropriate • reporting and audit practices, ensuring that reviews are timely, comprehensive, and suitable for the evaluation of the extent of satisfaction of the business.
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Periodical or on going audit for IT complianse exit. • Ensure to obey roles and standards , guidelines.
Example of Audit Evidence	• Roles • Satnders • Gauidelines • Audit report • The report of investigations of satisfaction of the business.

Audit practice guide	• Review Audit report. • Review the report of investigations of satisfaction of the business. • Analysis IT compliance and conformance are suitable or not for the evaluation of the extent of satisfaction of the business. • etc.
Product	
A5.5 The report that environmental, privacy, strategic knowledge management,	
Audit Criteria	• Monitor IT activities, including disposal of assets and data, toensure that environmental, privacy, strategic knowledge management, preservation of organizational memory and other relevant obligations are met.
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Establish policies regarding processing of personal information, protection of intellectual property rights and for the provision of information disclosure. • Assess level of compliance with laws, regulations, and the information ethics, and take necessary actions for improvement.
Example of Audit Evidence	• Privacy policy • Privacy manegement report • property rights ledger
Audit practice guide	• Review the report of privacy, property rights. • Ascertain the improvement process exsit. • etc.

A6.Human Factors IT policies, practices and decisions demonstrate respect for Human Behaviour,including the current and evolving needs of all the ‘people in the process’.	
Process	
A6.1 IT Formulation Process for Human Behaviour	
Audit Criteria	• IT activities to ensure that human behaviours are identified and appropriately considered.
Relevant Standards	• ISO/IEC 38500
Relevant controls	• The human resource management policies exist. • Determine the necessary competence for personnel • Personnel performing work affecting conformity to service requirements are competent .
Example of Audit Evidence	• The human resource management policies • Report of committee for human behaviors.
Audit practice guide	• Ascertain The human resource management policies exsit. • Ascertain IT formulation process exsit.
Process	
A6.2 Formulation Process for the IT risks with human managed.	
Audit Criteria	• IT activities are consistent with identified humanbehaviour. • Risks, opportunities, issues and concerns may be identified and reported by anyone at any time.
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Ensure that its personnel are aware of how they contribute to the achievement of service management objectives and the fulfilment of service requirements. • Develop a career path program for each member of personnel, and review it in accordance with changes in the business and IT environment. • Personnel remain physically and mentally fit so that they are able to perform jobs (planning, development, operation, and maintenance operations) efficiently.
Example of Audit Evidence	• the minutes of committee • career path program • the report of Personnel remain physically and mentally fit
Audit practice guide	• Review the minutes of committee. • Review career path program • Review the report of Personnel remain physically and mentally fit • Ascertain Formulation Process for the IT risks with human managed exist.

Product	
A6.2 The policies and procedures	
Audit Criteria	• The policies and procedures are adequate. The risks should be managed in accordance with published policies and procedures and escalated to the relevant decision makers
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Evaluate IT activities to ensure that human behaviours are • Identified and appropriately. • Ensure these risks are managed In accordance with published policies and procedures and escalated to the relevant decision makers.
Example of Audit Evidence	• policies • procedures • the roles of escalation of relevant decision make
Audit practice guide	• Ascertain policies and procedures are exsit. • Ascertain to assess IT risk form human Behaviour
Product	
A6.3 The education and training.	
Audit Criteria	• Exist education and training based on a consistent policy of an organization
Relevant Standards	• ISO/IEC 38500
Relevant controls	• Develop and update the educational training plans and curriculums in accordance with the human resource management policies. • Ensure that the educational training plans and curriculums are prepared on the basis of the improvement of technological skills, the acquisition of business knowledge, the audit of information security of the information system, and so on. • Provide educational training chances to each member of personnel periodically and effectively, based on the educational training plans and curriculums.
Example of Audit Evidence	• Educational training plans and curriculums • Record of educational training
Audit practice guide	• Ascertain the educational training plans and curriculums in accordance with the human resource management policies. • etc
Product	
A6.4 The report for humanbehaviour.	
Audit Criteria	• Reported about humanbehaviour. • The work practices to ensure that they are consistent with • the appropriate use of IT.
Relevant Standards	• ISO/IEC 38500

Relevant controls	• Maintain appropriate records of education, training, skills and experience. • Ensure that the work environment is properly managed in accordance with healthcare considerations. • Carry out regular medical examinations and prepare mental healthcare programs.
Example of Audit Evidence	• The report of Human Behaviour • sample of career path program • healthcare programs.
Audit practice guide	• Review healthcare programs. • Ascertain to monitor work practices to ensure that they are consistent with • The appropriate use of IT • etc

Bibliography

[1] ISO/IEC 38500:2008, *Corporate Governance of Information technology – a standard for corporate governance of information technology*

[2] ISO/IEC TR38502:201x*, *Corporate Governance of Information technology – Framework and Model*

[3] ISO/IEC 19011: 2011(E), *Guidelines for auditing management systems*

[4] ISO/IEC 17021:2006, Conformity assessment. Requirements for bodies providing audit and certification of management systems

[5] ISO/IEC 12207:2008, *Systems and software engineering -- Software life cycle processes*

[6] ISO/IEC 15504-2:2003*, Information technology -- Process assessment -- Part 2: Performing an assessment*

[7] ISO/IEC 20000-2:2005, *Information technology -- Service management -- Part 2: Code of practice*

[8] ISO 31000:2009, *Risk management - Principles and guidelines*

[9] ISO Guide 73:2009, *Risk management - Vocabulary*

[10] ISO/IEC 27007:2012, *Information technology – Security techniques – Guidelines for information security management systems auditing*

[11] ITGI, Information Security Governance framework: 2009

[12] COBIT® 4.1 Control Objectives for Information and related Technology, ©1996-2007 All rights reserved. Used with permission. The IT Governance Institute®, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008, USA.
http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx