Information System Audit Directives

Office of the Auditor General
Anamnagar, Kathmandu, Nepal
2023

Information System Audit Directives

Office of the Auditor General
Anamnagar, Kathmandu, Nepal
2023

Foreword

It is my immense pleasure to release the Information System Audit Directives of the Office of the Auditor General of Nepal. This directives will be applicable in undertaking respective financial, compliance, performance audits of the entities as per the Audit Act, 2075.

This directives provides a clear picture of methods and approaches to audit that the audit staff is required to comply with in imparting their duties. It has been built around the prevailing Audit Act, Nepal Government Auditing Standards (NGASs), and office policies that require conducting a high-quality audit. Since NGASs are based on INTOSAI framework for Professional Pronouncement (IFPP), this directives seeks to incorporate the Nepal audit practices at par with the international best practices.

This directives provides guidance and direction in all phases of the audit from pre-panning to follow-up including planning, execution, reporting and follow-up of information system audits with necessary annexures which encourages professional judgment where it requires. The directives does not override the legal requirements and conditions of NGASs. Likely, it shall not limit the professionalism of the officials entrusted with the responsibility of conducting audits.

Our knowledge, skill, and experience with auditing practices continue to evolve, and so will this directives. This directives is expected to be updated for the continuous improvement of audit practices to meet legal provisions, audit standards, and practices to address emerging risks.

My special thanks to all staffs who prepared the directives and provided their valuable feedback and comments to make this directives implementable which, I do hope, will be of use to conduct audits efficiently and effectively.

May 15, 2023

Tankamani Sharma, Dangal
Auditor General

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Full form
ACL	Audit Command Language
ASOSAI	Asian Organization of Supreme Audit Institutions
BAI	Build Acquire Implement
BCP	Business Continuity Planning
BPR	Business Process Reengineering
CAATs	Computer-assisted audit tools
CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
COTS	Commercial-off-the-shelf
DFID	Department of International Development
DLD	Detailed Level Design
DRP	Disaster Recovery Plan
DSS	Decision Support System
EDP	Electronic data processing
FCGO	Financial Comptroller General Office
GEA	Government Enterprise Architecture
GUID	INTOSAI Guidance
HLD	High Level Design
HR	Human Resource
ICQ	Internal Control Questionnaire
ICT	Information and Communication Technologies
IDEA	Interactive Data Extraction and Analysis
IDI	INTOSAI Development Initiative
IFPP	INTOSAI Framework of Professional Pronouncements
INTOSAI	International Organization of Supreme Audit Institutions
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISQC	International Standard on Quality Control
ISSAIs	International Standards of Supreme Audit Institutions
ITIL	Information Technology Infrastructure Library
KPIs	Key Performance Indicators
LAN	Local Area Network
LLD	Low Level Design
MIS	Management Information System
NAMS	Nepal Audit Management System
NPC	National Planning Commission
OAGN	Office of the Auditor General of Nepal
OLTP	Online Transactional Processing
PAC	Public Accounts Committee
PFMA	Public Financial Management and Accountability
PoC	Proof of Concept

Abbreviation	Full form
QAR	Quality Assurance Review
QCA	Quality Control and Assurance
QoS	Quality of Service
RDBMS	Relational Database Management Systems
RFP	Request for Proposal
RPOs	Recovery Point Objectives
RTOs	Recovery Time Objectives
SAI	Supreme Audit Institution
SDLC	Software Development Life Cycle
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SOD	Separation of Duties
SRS	System Requirement Specification
TOGAF	The Open Group Architecture Framework
UAT	User Acceptance Testing
UPS	Uninterruptible Power Supply
URS	User Requirement Specification
VPN	Virtual Private Network
WAN	Wide Area Network
WGITA	Working Group on Information Technology Audit

Background

1. Overview

OAGN is the Supreme Audit Institution (SAI) of Nepal and as part of its audit mandate conducts audit of a number of entities at all levels of the government (federal, provincial and local). In fact, OAGN has an audit environment in which major auditees including the FCGO (which processes 90% of all government accounting information) use computer based financial management and accounting systems[1] such as TSA (Treasury Single Account), FMIS (Financial Management Information System), etc. These systems commonly referred to as Information Systems (IS) or Information Technology (IT) Systems[2] are used for conducting financial transactions and generating financial reports, statements and other information. These system capture, store, process, retrieve, deliver and utilize data for communicating a wide variety of information for informed decision making at various levels of government organizations. Hence, especially from financial audit perspective, it becomes imperative for OAGN to derive an assurance on the appropriateness of these IT System and the associated controls before concluding the audits.

Additionally, government and other public sector entities in Nepal have been increasingly adopting Information and Communication Technologies (ICT) in order to enhance effectiveness and efficiency in their functioning and delivery of various public services. Since the delivery mode of public services is rapidly transitioning from physical to electronic, governments are now functioning as digital platforms for providing services to the citizens, as well as infrastructure for other IT-driven information systems[3]. This transition to electronic processing has triggered a significant change in the environment in which SAIs work and hence impacts the way in which OAGN conducts its audit. Additionally, with increasing investments and reliance on IT systems by government entities, there is also a need to adopt a focused approach and methodology for carrying out independent audits of critical IT systems, to provide assurance that adequate measures have been designed and are operated (by entities) to minimize the exposure to various risks arising from usage of IT systems such as:

- *data integrity*: The property that data meet with a priority expectation of quality and that the data can be relied on.
- *confidentiality*: Preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information.
- *availability*: Ensuring timely and reliable access to and use of information
- *reliability*: Refers to the degree of consistency of a system or the ability of a system (or component) to perform its required function under stated conditions.
- *compliance*: Adherence to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies[4]

Even when the audited organisation has implemented some risk-reduction measures, an independent audit is required to provide assurance that adequate controls (General Computer Controls[5] and Application Controls[6]) have been designed and are operated to minimize the exposure to various risks[7].

---

[1] OAGN IT Strategic Plan 2016-20
[2] The terms IT (Information Technology) and IS (Information Systems) are interchangeably used in this manual.
[3] GUID 5100 para 1.4
[4] ISACA Glossary
[5] General IS Controls are not specific to any individual transaction stream or application and are controls over the processes in an IT implementation which support the development, implementation and operation of an IT System. They would typically involve IT Governance, Organisation and Structure, Physical and Environmental Controls, IT operation, IS Security, and Business Continuity.
[6] Application Controls are controls specific to an IT System and involve mapping of business rules into the application thus providing for Input, Processing, Output and Master Data controls.
[7] WGITA-IDI handbook on IT Audit for SAIs

OAGN has been making efforts on developing appropriate capacity to conduct IS audits in Nepal. OAGN has been conducting IS audits that are currently managed by "Information Technology and Special Audit Directorate" under the Performance Audit Division. In past, OAGN has also taken support from international donor agencies such as DfID for sourcing of IS audit experts (e.g. under PFMA-2 [Public Financial Management and Accountability]) for providing technical assistance to OAGN IS auditors in IS audits. Additionally, in OAGN's IT Strategic Plan 2016-20, 'building capacity in information technology auditing' is one of the objectives under IT strategic goal 3: "Establish capabilities in auditing in information technology environments and using IT based audit tools", which establishes OAGN's strategic focus on IT audits.

To further support OAGN in its efforts to mainstream IS audit, this IT manual has been prepared, with an aim to establish general principles, approach and methodology for conducting IS audits. The IS audit manual of OAGN is based on the ISSAI framework and also derives from the IT audit handbook prepared jointly by the INTOSAI Working Group on IT Audit (WGITA) and the INTOSAI Development Initiative (IDI).

2. Objective of the IS audit directives

The objective of the IS audit directives is to provide guidance to OAGN auditors on how to conduct audits related to the specific subject matter of Information Systems or where the audit of information systems may be part of a larger audit engagement which may be Financial, Compliance or Performance audit. The directives covers all phases of the IS audit lifecycle viz. planning, conducting, reporting and follow-up. This directives, shall also be applicable to auditors, conducting IS audit on behalf of OAGN.

3. Scope for individual initiative and professional judgement

It should be recognized that no guidance or policy or manual of general application could suit all circumstances. Therefore, the auditors are required to exercise their professional judgment in using this manual. If an approach, method, process, or procedures is found inappropriate for a specific auditee and a more suitable and practical alternative can be used, then the alternative way should be used after obtaining the approval from the Assistant Auditor General (Performance Audit division) or appropriate authority in charge of the assignment. The approved departure from IS audit manual shall also be documented.

4. Structure of the directives

The IS audit directives of OAGN, is structured along the following chapters:

- **Introduction**: This section contains definition of IS audit, applicable policy framework, objectives of IS audit in context of financial audit, compliance audit and performance audit, applicability of IS audit at OAGN, brief on IT general and application controls, general requirements of IS audit and overview of the IS audit process.

- **Planning IS audit**: This section describes steps in IS audit planning covering strategic IS audit planning, annual IS audit planning and auditee level planning. This chapter contains details for selection of IT systems for IS audit, preliminary risk assessment of IT controls and preparation of IT audit plan.

- **Conducting IS audit**: This section contains steps and techniques for conducting IS audit to gather sufficient and appropriate audit evidence against the audit criteria in line with the audit objectives. This section also contains guidance on usage of CAATs for conducting audit procedures.

- **Reporting on IS audit**: This section contains the types of IS audit reports and considerations for reporting issues of IS audits. It also contains format of IS audit report and key considerations for IS auditors, while preparing the IS audit reports.

- **Audit Follow-up**: This section describes the audit follow-up in context of IS audit.

- **Annexures**: This section contains sample questionnaires, data collection forms, sample data tests for application controls, usage of CAATs for audit procedures, and audit matrices for conducting audit of IT controls (general and application controls).

5. Regarding future updates to the directives

This directives shall be appropriately updated as and when there are changes in the applicable IS audit standards or guidelines issued by, INTOSAI IFPP.

1. Introduction

1.1. Definition of Information Systems

Information Systems can be defined as a combination of strategic, managerial and operational activities involved in gathering, processing, storing, distributing and using information and its related technologies. The complexity of such an Information System may range from a simple book in which entries for receipt and payment of money are maintained manually, to a more complex IT-driven system such as a system for tax assessment, in which all processes — collection of data (e.g. tax returns filed through online web portal), storage on servers, processing of assessment (based on programming using taxation rules) and communication of tax demand, refund and acknowledgement (real time or at prescribed intervals) — are automated. Information Technology comprises the hardware, software, communication and other facilities used to input, store, process, transmit and output data in whatever form. (**GUID 5100 para 3.1**)

1.2. Definition of Audit of Information Systems

"Audit of Information Systems may be defined as the examination of controls related to IT-driven information systems, in order to identify instances of deviation from criteria, which have in turn been identified based on the type of audit engagement - i.e. Financial Audit, Compliance Audit or Performance Audit". (**GUID 5100 para 3.2**)

"IS audit is the process of deriving assurance on whether the development, implementation and maintenance of IT systems meets business goals, safeguards information assets and maintains data integrity. In other words, IS audit is an examination of implementation of IT systems and IT controls to ensure that they meet the organization's business needs without compromising security, privacy, cost, and other critical business elements". (**WGITA – IDI handbook on IS audit for Supreme Audit Institutions**[8])

1.3. Applicable international principles, standards and guidelines[9]

a. Section 22 of INTOSAI-P 1 "The Lima declaration", on audit of electronic data processing facilities mentions that:

"The considerable funds spent on electronic data processing facilities also calls for appropriate auditing. Such audits shall be systems-based and cover aspects such as planning for requirements; economical use of data processing equipment; use of staff with appropriate expertise, preferably from within the administration of the audited organisation; prevention of misuse; and the usefulness of the information produced"

b. INTOSAI guidance GUID 5100: Guidance on Audit of Information Systems, 2019

- The GUID 5100 contains guidance for auditors that may be used to conduct Performance and / or Compliance audits related to the specific subject matter of Information Systems or where the audit of information systems may be part of a larger audit engagement which may be Financial, Compliance or

[8] The INTOSAI Working Group on IT Audit (WGITA) and the INTOSAI Development Initiative (IDI) jointly worked on producing an updated Handbook on IT Audit with a view to provide SAI auditors with standards and universally recognized good practices on IT Audit. This Handbook provides a comprehensive explanation of the major areas that IT auditors may be required to look into while conducting IT audits. This handbook was endorsed by the XXI INCOSAI held in Beijing, China in October 2013 and was published in February 2014. The WGITA/IDI Handbook follows the general auditing principles as laid down under the International Standards for Supreme Audit Institutions (ISSAI).

[9] Source: ISSAI.org as on Shrawan 1, 2077

Performance audit. It contains procedures that can be applied by auditors to the Planning, Conducting, Reporting and Follow Up stages of the audit process[10].

- The GUID is also intended to provide the foundation for development of future GUIDs in the 5100-5109 series on the subject area of the audit of Information Systems, within IFPP.
- The framework laid out in this GUID is consistent with the Fundamental Principles of Public Sector Auditing (ISSAI 100), Fundamental Principles of Financial Auditing (ISSAI 200), Performance Audit Principles (ISSAI 300) and Compliance Audit Principles (ISSAI 400)[11].
- ISSAI 100, 200, 300 and 400 lay down the basic precepts of auditing as related to Financial Audit, Performance Audit and Compliance Audit. These ISSAIs relate to general principles, procedures, standards, and expectations of an auditor. They are equally applicable to audits of Information Systems too[12].
- GUID 5100 provides further guidance on how any audit of Information Systems could be addressed by using financial/performance/compliance auditing and hence, *does not* contain any further requirements for the conducting the IS audit.

1.4. OAGN's legal mandate for IS audit

The Office of the auditor general of Nepal (SAI Nepal) receives its mandate from the constitution - Article 241(1) and the Audit Act 2075. As per constitution and audit act, SAI Nepal is empowered to conduct audits of all government agencies including the legislative bodies, judicial bodies, security agencies at all three tiers of government, fully state owned enterprises and the other entities as prescribed by the law in ***such a manner*** as prescribed in law with due considerations given to the aspect of regularity, economy, efficiency, effectiveness and propriety thereof. Since, IS audit becomes relevant in context of financial audit, compliance audit and performance audit, it comes under the mandate of OAGN, as none of the above audits would be complete, without auditing controls of the underlying IT systems.

1.5. IT controls

A **control** is the combination of methods, policies, and procedures that ensure protection of the organisation's assets, accuracy and reliability of its records, and operational adherence to management standards. In an IT context, controls are divided into two categories: IT general controls and IT application controls.

[10] For specific audit of Public Debt Information Systems (PDIS) refer to GUID 5259. It contains audit matrices for testing of application controls specific to PDIS. Auditors shall refer to these guidelines, in addition to OAGN IS audit manual, for audit of public debt information system.
[11] GUID 5100 para 1.2
[12] GUID 5100 para 2.1

The **IT General Controls** are the foundation of the IT control structure. These are concerned with the general environment in which the IT systems are developed, operated, managed and maintained. General IT controls establish a framework of overall control for the IT activities and provide assurance that the overall control objectives are satisfied. General controls are implemented using a number of tools such as policy, guidance and procedures as well as putting in place an appropriate management structure, including that for management of the organisation's IT systems. Examples of general controls include the development and implementation of an IS Strategy and an IS Security Policy, setting up of an IT steering committee, or an IT wing or department, organisation of IS staff to separate conflicting duties, and planning for disaster prevention and recovery. A list of IT domains, audit areas which generally fall under IT General controls is presented below:

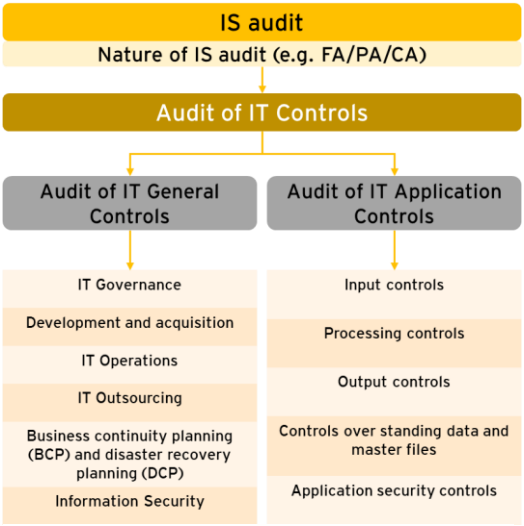


Figure 1: IT general and application controls

Table 1: IT General controls[13]

S/N	IT Domain	Audit Area/s
1.	IT Governance	▸ Business needs identification, direction and monitoring ▸ IT strategy and planning ▸ Organizational structure, standards, policies and processes ▸ Internal control (IT risk management and compliance mechanisms) ▸ Investment decisions (development and acquisition of solutions) ▸ IT Operations ▸ People and resources
2.	Development and acquisition	▸ Requirement development and management ▸ Project management and control ▸ Quality assurance and testing ▸ Solicitation[14] ▸ Configuration management
3.	IT Operations	▸ IT service continuity management ▸ Information Security Management ▸ Capacity management ▸ Problem and incident management ▸ Change management ▸ Service level agreements (SLA)
4.	Outsourcing	▸ Outsourcing policy ▸ Solicitation ▸ Vendor/ contract management ▸ Service level agreements (SLA)

[13]The domains and audit areas should be taken only as a guidance. Auditors shall use their judgement and knowledge in selecting the IT domains and areas to be audited under an IS audit. Auditors should keep themselves abreast with latest auditing standards and guidelines, in the field of IS audit such as INTOSAI auditing standards, international standards of professional IT Audit organizations such as Information System Audit and Control Association (ISACA).

[14] Solicitation is the process of documenting the requirements of the business and collecting other reference materials that will assist the vendor in providing the IT solution.

S/N	IT Domain	Audit Area/s
		▶ Benefit realization ▶ Security
5.	Business continuity plan (BCP) and disaster recovery plan (DCP)	▶ Business continuity Policy, Plan and organisation ▶ Establishment of business continuity function ▶ Business Impact assessment and risk management ▶ Preventive and environmental controls ▶ Disaster recovery Plan ▶ Testing ▶ Security ▶ Back-up and data recovery for outsourced services
6.	Information Security[15]	▶ Information security environment ▶ Risk assessment ▶ Security Policy ▶ Organisation of IT security ▶ Communications & operations management ▶ Asset management ▶ Human resources security ▶ Physical and environmental security ▶ Access controls ▶ IT systems acquisition, development and maintenance ▶ IT security incident management ▶ Business continuity management ▶ Compliance (with legal, environmental, and information quality, and fiduciary and security requirements)

IT Application Controls are specific controls unique to each computerized application. They apply to application segments, functionalities and relate to the transactions carried out in the system and existing data. Application controls include data input validation, encryption of data to be transmitted, processing controls, output controls, etc. For example, one of the input (application) control for a treasury system is that while creating a bill in the system, system shouldn't allow user to raise an advance bill against the regular/contingent bill budget head, or the system shouldn't take bill amount, if the total expenditure under the head, for the office, exceeds the budgeted amount. Similarly, there are processing (application) controls, such as in case of vendor payments, the deductions should be as per rates in the relevant policy. List of Audit areas under application controls are presented below[16].

[15] As on Shrawan 1, 2077, Guidelines on Information Systems' Security Audit, including Cyber Security (Earlier ISSAI 5310) are in development, under the heading "Consolidating and aligning guidance on IT audit with ISSAI 100". Working title: Guidelines on Information Systems' Security Audit, including Cyber Security (Earlier ISSAI 5310).

[16] Though test procedures and checklists for audit of application controls are presented in annexures, it is not realistically possible to provide these details for every possible scenario of application/s testing. Hence, IT auditors should be aware of the control concepts as presented in table above and develop audit tests and checklists depending on the audit objective and application being audited.

Table 2: IT application controls

IT Application controls		
S/N	**Audit Area/s**	**Some examples of application controls**
1.	**Input controls**	▶ Data entry/field checks (e.g. validation of entered credit card numbers), ▶ Source documents management (e.g. preparation and retention procedures) ▶ Error handling mechanisms (error messages, suspense files) ▶ Data entry authorisation rules (e.g. segregation of duties)
2.	**Processing controls**	▶ Business rules mapping ▶ Integrity and completeness checks, report of out-of-balance conditions ▶ Automated calculations ▶ Input reconciliations
3.	**Output controls**	▶ Completeness and accuracy validations, reconciliation ▶ Output review and tracking ▶ Review and follow-up of application-generated exception reports ▶ Output labeling, handling, retention and distribution procedures
4.	**Application security controls**	▶ Traceability mechanisms (audit trails, log review, use of unique identifiers) ▶ Logical access control to functionalities and application data ▶ Stored data protection
5.	**Controls over standing data and master files**	▶ Procedures for physical and logical access to master/standing data files ▶ Periodic reconciliation with independently held records ▶ Audit trails of transactions done on master data files

IT general controls ensure appropriate development and implementation of applications, as well as program, data files and of computer operations[17]. Hence, design and implementation of IT general controls may impact the effectiveness of the application controls and influence the extent to which the application controls can be relied upon by the management to manage risks. If general controls are weak, they severely diminish the reliability of controls associated with individual IT applications. This is very useful for auditors, since based on testing of IT general controls, they can decide on the extent of testing required for application controls. Most common IT general controls that enhance application controls are[18]:

- Logical access control over infrastructure, applications and data
- System development life cycle controls
- Program change management controls
- Physical access controls over the data centre
- System and data back-up and recovery controls
- Computer operations controls.

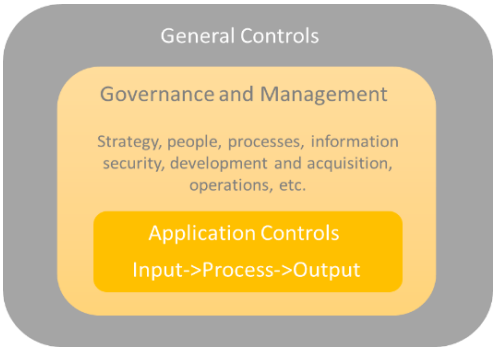


Figure 2: Relationship between IT general and application controls

[17] ISACA, IS Auditing Guidelines-Applications Systems Review
[18] WGITA – IDI handbook on IT audit for Supreme Audit Institutions

In addition to IT general controls and application controls there are certain addition areas/topics that might be of interest to the auditors. Since, there are many emerging areas in IT, the OAGN IS auditors should be aware of these and should well equipped to conduct audits of these areas, in case the need arises. These areas can be audited using the approaches and techniques mentioned in this manual. Depending on the objective of the IS audit and areas being audited, IS auditors shall develop additional questions/issues dealing with these areas.

Table 3: Addition topics for IS audit

S/N	Topic	Audit Area/s
1.	Website/portals[19]	▶ User experience ▶ Security, privacy ▶ Response time ▶ Outsourcing related issues
2.	Mobile computing	▶ Wireless security, privacy, encryption ▶ User experience ▶ Specific policies regarding mobile computing in the organisation ▶ Risks of using personal devices to access corporate data and services ▶ Risks of unauthorized access to the data that reside on the device ▶ Increased risks of damage or theft of corporate devices
3.	Computer forensics	▶ Evidence (data, access, log) retention for analysis ▶ Capture and preserve data as close to the breach as possible ▶ Data collection standards for possible law enforcement use ▶ Minimally invasive data capture process without disruption to business operations ▶ Identification of attackers if possible.
4.	Electronic Government, electronic Governance and mobile Governance	▶ Same as regular IS audit (general and application controls)
5.	Electronic commerce (e-commerce)	▶ Availability ▶ Transactions security (Public Key Infrastructures) ▶ Scalability of the solution ▶ User experience and, mostly important ▶ The business process undertaken by the e-commerce strategy.

1.6. Objectives of IS audit

The objective of IS audits is to ensure that the IT resources allow organizational goals to be achieved effectively and use resources efficiently or to look at the value proposition the IT system is expected to deliver. The objective of IS audit also depends on the *type of audit* undertaken by the OAGN viz. financial, compliance and performance audits. Hence, the IS audit can be audit of a comprehensive IT systems or of specific domains e.g. IT governance, development and acquisition, IT operations, outsourcing, application controls, IS security,

[19] Auditors may refer to policy and guidelines published by Ministry of Communication and Information Technology for design/development of websites and management. Refer to https://nitc.gov.np/document/

business continuity, etc. based on the type of larger audit it is part of. The objectives of IS audit in context of financial audit, compliance audit and performance audit, are[20]:

Table 4: Objectives of IS audit in context of FA, CA and PA

	In context of Financial Audit (FA)	In context of Compliance Audit (CA)	In context of Performance Audit (PA)
Objectives of IS audit	To evaluate the relevant general controls[21] and application controls[22] which have an impact on *reliability* of data from information systems, which in turn have an impact on the financial statements of the audited entity	To draw assurance on compliance of the processes of the information systems with the laws, policies and standards applicable to the audited entity.	To draw assurance that IT resources allow organizational goals to be achieved efficiently and effectively, and that the relevant general controls and application controls are effective in prevention, detection and correction of instances of excess, extravagance and inefficiency in the use and management of information systems.

Further illustration of objectives of IS audit, with examples, in context of Financial Audit, Compliance Audit and Performance Audit, with examples, is presented below.

Objective of IS audit in context of Financial Audit:

Objective of Financial audit is to determine whether an entity's financial information is presented in accordance with the applicable financial reporting and regulatory framework. In case, an IT system is involved in preparation of financial statements, it is imperative that the system should have all requirements for preparation of the financial reports. E.g. system should be able to capture financial information, apply regulatory framework requirements, process the information, and present it in required format. These issues are related to application controls of input, processing and output in addition to master data and application security. Application controls are dependent on adequate support from IT General controls and IT governance. Hence, Financial Auditors should therefore derive an assurance on the appropriateness of the IT System and its associated controls before concluding their audit. The assurance on the IT system should be derived through an IS audit of the system looking at all aspects of IT Governance, IT General Controls, and IT Application Controls.

The way this can be done is either through incorporating issues of IS audit in the Financial Audit plan/programme (of entity and offices) or through a full-fledged IS audit, to derive assurance on the IT system. Once an assurance is derived through a full-fledged IS audit, it may not be essential to conduct an IS audit during every financial audit through the same system if there is an assurance that no change and no compromise of the system has happened during the period since last IS audit.

Objective of IS audit in context of Compliance Audit:

[20] GUID 5100 para 5.2

[21] General Controls are manual or automated procedures which aim to ensure confidentiality, integrity and availability of information in the physical environment within which information systems are developed, maintained and operated.

[22] Application Controls are IT dependent manual or automated procedures within an information system that affects the processing of transactions, and may relate to validation of input data, accurate processing of data, delivery of output data and controls related to integrity of master data.

Objective of Compliance audit is to assess whether a particular subject matter is in compliance with applicable authorities identified as "criteria". Example: for the subject matter "procurement of medical equipment within health department", in case an IT system is in place for procurement, it should comply with the applicable laws and regulations, as well as standards and guidelines adopted by the entity. The evaluation of compliance in respect of IT Governance will involve assurance on the mechanisms to ensure that the governance functions are being carried out and monitored periodically, that the internal control mechanism is working effectively and that all IS policies are being implemented as envisaged. The evaluation of compliance in respect of IT General Controls will involve assessment of the existence of the controls with adequate monitoring and risk mitigation mechanisms being in place and adherence to the prescribed standards and performance parameters in the entity. The evaluation of IT Application Controls will involve the assessment of existence of mapping of business processes and rules into the IT system and input, process and output controls related to data validation, completeness, correctness, and reliability of processes.

Objective of IS audit in context of Performance Audit:

Performance auditing is an independent, objective, and reliable examination of whether government undertakings, **systems**, operations, programmes, activities or entities are operating in accordance with the principles of economy, efficiency, and effectiveness and whether there is room for improvement. IS auditors shall examine the IT systems implemented with respect to the criteria of economy, efficiency, and effectiveness and value to the citizen.

a. ***Economy***: Examination of economy in context of implementation of IT system would essentially involve minimizing the costs of resources throughout the life cycle of the IT System, i.e. from the system acquisition to system implementation and regular operation. Costs can be minimized through market discovery which may be hampered due to inefficient user requirement definition or improper sourcing. Also, instead of outsourcing IT services they could have been managed internally by the entity. Thus, IS auditors could highlight the limitations of the entity or the process of acquisition as the case may be.

b. ***Efficiency***: Inefficiencies may be pointed out by IS auditors if there are duplication of any processes, undue idling of any process, unnecessary checks built into the system, etc.

c. ***Effectiveness***: Examining the effectiveness in respect of implementation of IT Systems would involve establishing if it has met its objectives, which inter alia should meet the entity's overall goals and objectives.

PA additionally contributes to accountability and transparency and focusses on areas that can add value add to citizens and have greatest potential for improvement. Hence, PA approach to IS audit, may promote good governance using IT systems and lead to system improvement through identification of issues during system acquisition, development, implementation and operation.

1.7. Scope of IS audit

Scope of the IS audit decides the *extent* of audit scrutiny, the coverage of IT systems and their functionalities, IT processes to be audited, locations[23] of IT systems to be covered, and the time period[24] of audit analysis.

Scope of IS audit shall be decided based on the objectives of the audit and the preliminary risk assessment of the entity/ IT system. As part of risk assessment of the entity/IT system, the IS auditor would be required to assess the policies and procedures that guide the overall IT environment of the audited entity, ensuring that the corresponding controls and enforcement mechanisms are in place. This shall help auditors in identifying the IS audit domains and areas, that shall be included in the 'Scope' and the extent of audit scrutiny (audit analysis methods) required.

Based on preliminary risk assessment (during planning), the **scope of an IS Audit** may be drawn from any or all of the following domains[25] of the audited entity, that would be relevant to the IS audit objectives[26]:

1) Organizational Policy on IT[27]
2) Organizational Governance Structure on the subject of IT
3) General controls provided in the business area being automated
4) Asset Management
5) Development, Acquisition and Maintenance of Information Systems, including mapping of business processes and associated programming logic
6) IT Operations Management
7) Physical Environment Management
8) Human Resources Management
9) Communications Management
10) Information Security Management[28]
11) Statutory Compliance Management
12) Business Continuity and Disaster Recovery Management
13) Application Controls Management

1.8. Application of IS audit at OAGN

This section contains the modality of IS audit to be followed at OAGN.

1.8.1. IS audit in context of Performance audit or Compliance audit

a. **Compliance Audit**: For example, one of the topics for Compliance Audit could be " *To verify that Department of Roads has planned, conducted and monitored the process of procurement of road construction projects as required under Procurement Act*". In this case, if a procurement IT system is involved for procurement of goods and services, then IS audit can be taken as part of the compliance audit. As discussed in section on "objectives of IS audit", the objectives of IS audit shall be derived from the objective of the compliance audit

[23] Location would include the back-end servers (application or data or otherwise), user locations, networks in a generic manner and would also determine the physical locations to be covered in a distributed network across buildings, or cities, as applicable.
[24] Time period for audit analysis is XX years for defining the scope of the IS Audit engagement, that is relevant to the aims defined for the audit engagement. This will enable IT auditors to draw suitable conclusions on the audits conducted.
[25] A majority of the domains described have been adapted from ISO/IEC 27001
[26] GUID 5100 para 5.3
[27] Including aspects of Strategic Management
[28] Including Cyber Security

which in this case will be "compliance of procurement system with the applicable laws and regulations, as well as standards and guidelines adopted by the entity". Auditors shall accordingly select the relevant IS audit domains (Scoping) for audit and frame the criteria for conducting the IS audit in line with overall compliance audit objectives.

b. **Performance Audit**: In another example, from Performance Audit perspective, "*Examination of economy in context of implementation of a new IT system such as 'Company Registration System'*" could be one of the subject matter/topic. Auditors shall keep in mind that in this case objective of IS audit is "to check if the costs of resources throughout the life cycle of the IT System, i.e. from the system acquisition to system implementation and regular operation, are minimized or not". Hence, auditors shall accordingly focus on the relevant IS audit domains (scope) such as system acquisition, development, implementation, outsourcing, and operation for audit and frame the criteria for conducting the IS audit in line with the overall performance audit objectives.

Depending on the type of audit engagement, Compliance Audit manual or Performance Audit guidelines, shall be applicable for the audit. However, IS auditors shall refer to the IS audit manual for procedures on scoping and preparation of audit matrices for audit of *relevant IT domains and areas*. In such cases, the Audit team shall be composed of members that collectively have the competence to conduct IS Audit engagements to achieve the intended audit objectives, i.e. a mix of IS auditors and auditors (from other directorates, as applicable) with expertise in the select subject matter and conducting PA and CA.

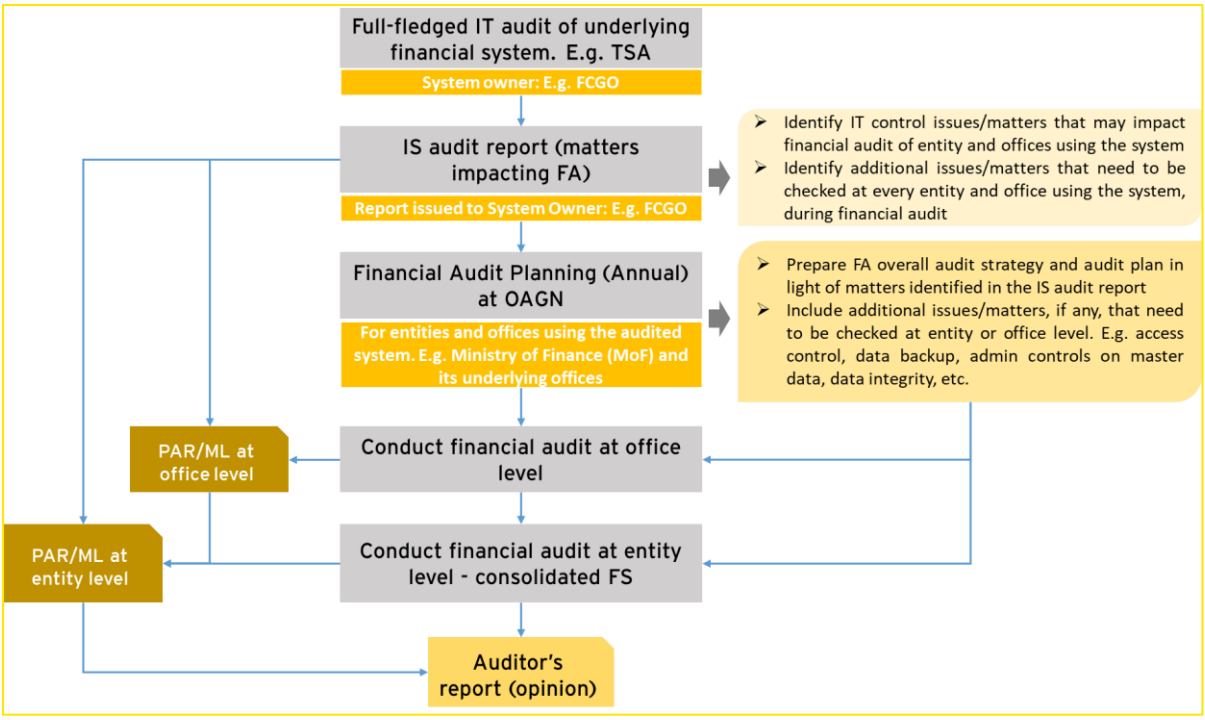
1.8.2. IS audit in context of Financial Audit

GUID 5100 states that IS audit could also be conducted as part of a larger audit engagement such as Financial Audit, however, in context of Nepal, since majority of the entities use common systems for financial management and accounting (e.g. FMIS, TSA), once an assurance is derived through a full-fledged IS audit, it may not be essential to conduct a full-fledged IS audit for financial audit of all entities/offices using the using the same system. In this case, once an IS audit of IT system is conducted the matters concerning the IT controls shall be reported in the IS audit report by the IS auditors. The impact of the matters reported, shall be evaluated by the financial auditors, during Annual Audit Planning, based on IS audit report and consultations with the IS auditors.

IS audit of relevant financial & accounting system should be conducted before the Financial Audit of entities and offices using the system. i.e. for the purpose of FA planning starting from April/May of a year, the IT audit of the relevant system/s should be finished by March of the same year. This will ensure that financial auditors take into account, matters identified from IS audit of relevant System, for financial audit planning of entities and offices. The findings of IS audit report may impact the overall audit strategy, audit plan, procedures for test of controls and other tests for financial audit of offices/entities , which may in turn affect the opinion expressed by the Financial Auditors in the Auditor's report. These considerations of IT control assessment in the FA process have been covered in the FA manual and related guides[29].

Figure 3: IT audit in context of Financial Audits

[29] E.g. AP 1 Overall Audit Strategy in FA manual, Financial Accountability Guide (review of control structure)



For the purpose of full-fledged audit of applications/systems from FA perspective, IS auditors, shall focus on relevant IS audit issues of IT governance, access controls, change management controls, other relevant application security controls and application controls such as[30]:

Table 5: Illustrative list of IT audit domains and issues for audit of financial systems in context of FA

IT domain	Key issues/areas to be focused
IT general controls: Design and implementation of IT general controls may impact the effectiveness of the application controls and hence influence the extent to which the application controls can be relied upon by the management to manage risks.	
IT governance	➢ Mechanism/s in place for identifying and defining requirements of the IT system ➢ IT strategy or policy in place to guide operations of the IT functions including documentation of the same ➢ Mechanism in place for managing IT risks (in terms of policy, plan, resources, etc.) ➢ Presence of dedicated IT structure for management of IT system with defined roles and responsibilities for IT staff ➢ Mechanism/s in place to ensure compliance to applicable policies and procedures
IT operations	➢ Mechanism/s in place for defining service level agreements between the IT team and the users of the system (such as line ministries) and ensuring compliance to SLAs ➢ Procedures for monitoring and evaluation of SLAs based on feedback from the users

[30] For details audit analysis methods for various IT domains, refer to the illustrative audit matrices presented in the Annexures. Also, the actual scope of audit shall be based on the preliminary risk assessment of the IT control risks as presented in this manual.

IT domain	Key issues/areas to be focused
	➢ Presence of relevant documentation on problem and incident management, SLA contract, etc. ➢ ***Program Change management:*** ○ Documented change management policy covering: Request for change- authentication- acceptance- prioritization - change design -testing change- implementation- documentation ○ Change controls in place (e.g. approvals, documentation of record, etc.) ○ Other program change management controls, as applicable
Business continuity and disaster recovery	➢ Policy or plan for business continuity and disaster recovery including documentation ➢ Presence of appropriate team for managing BCP and DRP activities ➢ Control measures in place to prevent impact of disasters on financial data, IT system operations and users ➢ Mechanism in place for data backup, etc. to handle emergency situations[31] ➢ Environmental control mechanism in place at the back-up site ➢ Security of data, application, hardware, and data center during back-up disaster recovery procedures
Information security	• Policy, guidelines, etc. on information security risk assessment • Quality of such policy and guidelines • Risk mitigation practices in place • Mechanism/s in place for protecting confidential data • Organisation of IT security with defined roles and responsibilities • Controls over network operations • Controls over communication (internal and external) • Asset management (hardware and software) policies in place • Matters of training of staff on Information security aspects • Measures for *physical security* in place, including unauthorized access to the system • ***Access controls:*** ○ Access control policy in place; is it clear, efficient and effective? ○ Access control mechanism is place[32] ○ **Privileges management**: Safety and effectiveness of process for granting and revoking access control to full-time employees, part-time employees, vendors, etc.
IT Application controls: These controls are specific to a system and cover matters of data input validation, data security, processing controls, output controls, etc. In context of financial systems, these will largely be related to checking validations for input of financial details, processing of financial transactions as per defined	

[31] E.g. Data backup and other security protocols and safeguard details are to be maintained by users of FCGO's system/s, in OAGN form number 903: Data Backup authentication form. Auditors shall check if the forms are being maintained and verify the correctness of information captured in the forms.

[32] E.g. OAGN form number 901: Electronic system user description, change and postponement request form and OAGN form number 902: Electronic system user details, changes and suspension records are to be maintained by users of FCGO's system/s.

IT domain	Key issues/areas to be focused
rules, generation of outputs correctly and as per requirements of financial reporting, application security and controls over system master data.	
Input controls	• Input validation controls (capturing financial data in the system) • In case data is recorded from external systems, what the adequacy of controls to ensure data integrity? • Error handling procedure in the system, during incorrect data entry or failure to input data • Protocols for data entry authorisation, documented policy, etc.
Processing controls	• Mapping of relevant financial business processes rules and requirements in the system. E.g. rules for % deduction on vendor bills, allowances and deductions of salary bills, etc. • Integrity of transactions and data processed in the application • Compliance to relevant financial rules and procedures
Output controls	• Controls to ensure completeness and accuracy of outputs in forms of financial reports or statements[33] • Mechanism in place for protection and distribution of outputs • Mechanism in place to check accuracy of outputs through reconciliation with other sources (such as outputs from other systems) • Controls in place to prevent tampering with output by unauthorized users.
Application security	• Provision of audit trails for capturing edits, overrides, authorisation logs, etc. • Correctness and adequacy of audit trails maintained in the system • Protection of application data against misuse (as discussed under information security)
Control over standing data or master files	• Mechanisms in place to ensure integrity of master data/files such as CoA/budget heads, master data on budget, supplier vendor data, etc. • Access control mechanisms over master data

Once a full-fledged IS audit of the common underlying systems is conducted, it might not be necessary to conduct a full-fledged IS audit of the same system every year, unless significant changes [34] were made in the system since the last IT audit. However, there might still be certain matters/issues that need to be checked, for establishing assurance of IT controls, before concluding the financial audit of entities and offices using the system/s. These matters/issues form the scope of the IS audit and shall largely be decided based on:

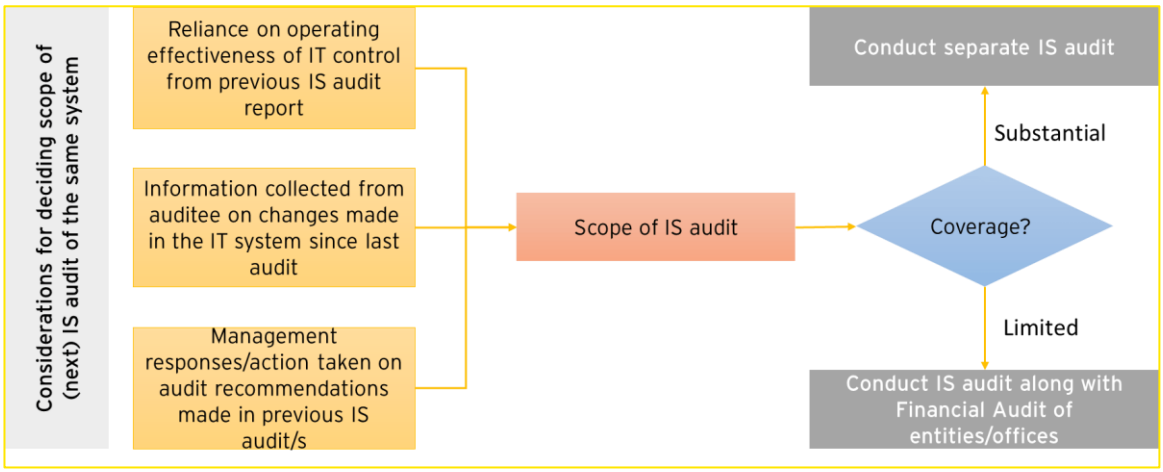
- Changes made to the IT system, since last audit, that might have an impact on the financial reports, and financial information generated from the system. Auditors shall gather this information from the system owner (during annual audit planning) and accordingly assess the nature of changes done and identify IT audit issues on which these changes might have an impact on.

[33] Financial statements are applicable at entity level whereas financial reports/information is applicable at the underlying offices. This financial information captured and processed at office level, acts as an input for consolidated financial statement at the entity level.

[34] Significant changes are the changes in the underlying system that may lead to control environment deficiencies, in turn leading to risk of material misstatements in financial reports or information generated from the system (Refer to Financial Audit manual for further details).

- Additionally, from previous IS audit, auditors will already have information on extent to which they can rely on the operating effectiveness of the IT controls. Also, during annual audit planning stage, Auditors collect information on auditee/IT system and conduct assessments to get an idea about the extent to which IT controls can be relied upon.
- Additionally, there could be certain matters identified during the previous IS audit of the system that are yet to be resolved by the auditee (follow-up). These matters need to be considered while deciding the scope of IS audit, as these issues will still have impact on the financial audit of entities and offices.

Figure 4: Considerations for deciding scope of next IS audit of the same system



- Considering the above inputs, Auditors shall decide on the scope of the IT audit. In case the scope of IT audit turns out be substantial, then auditors shall conduct a separate IS audit as per the process described above.
- However, if scope of IT audit is limited, the IT audit issues can be checked during the financial audit of entities/offices. The audit team in this case shall be a mix of IT auditors and financial auditors. IS auditors shall communicate the findings of IS audit to the financial auditors, who will in turn evaluate the impact of IS audit findings on the financial audit process and auditor's report.
- Depending of the scope of IS audit as discussed earlier, the matters related to IT controls that may need to be checked at the entities/offices, using the system could be:
  - Access control at user location including privilege management
  - Disaster recovery and backup procedures at user location[35]
  - Relevant IT application controls
  - Other matters/issues identified by the auditor during planning stage

For financial audit of SoEs, in case there are underlying financial or accounting systems in place, the auditors shall follow the following key steps (similar to FA of other entities):

1. Since the system is likely to be a standalone system, IT controls issues will be checked during the financial audit itself.
2. In parallel to planning the FA, auditors shall also plan for audit of relevant IT issues as discussed earlier

[35] Financial data recorded and processed at user location, has to be either synced to a central server or backed up on a regular basis to avoid loss of financial data in case of a disaster. Auditors need to check if the controls for data backup and recovery are in place at the user location. Usually in web-based application, data is automatically stored at a central data server maintained by the "system owner" and backed up on a backup server as per their backup policy.

3. Auditors shall conduct Test IT controls to derive assurance on the appropriateness of the IT System
4. In case control weaknesses are identified, auditors shall perform substantive testing
5. Auditors shall also complete other procedures for financial audit as per SoE guide
6. Auditors shall assess the impact of identified IT control weaknesses on reporting of financial audit issues and on opinion to be expressed in the auditor's report.

1.8.3. Separate IS audit

As mentioned above, separate IS audits can be undertaken for deriving an assurance on the appropriateness of the IT System and its associated controls especially for financial management IT systems that are being used to manage financial data and prepare financial statements of the entities.

Separate IS audit may also be undertaken with following objectives[36]:

a. Review of the controls of the IT systems to gain assurance about their adequacy and effectiveness

b. Evaluation of the processes involved in the *operations* of a given area such as a payroll system, or financial accounting system

c. Evaluation of the performance[37] of a system and its security, for example, a railway reservation system

d. Examination of the system development process and the procedures to ensure:
- Controls are identified and developed into the new system;
- Controls exist to manage the project and development project decisions are transparent;
- Predetermined standards are set (and followed);
- Development specifications make sense and are cost effective;
- That future technology improvements are considered;
- Systems are robust and reliable, secure from unwanted interference and auditable; and
- The development objectives are clear and achievable.

e. Additional areas/topics that might be of interest to auditors such as websites/portals, e-Governance software, etc.

In such cases, audit procedures from planning to follow-up stage, mentioned in the IS audit manual, shall be followed.

Note: In case, as a result of the IS audit, certain issues related FA, CA, or PA are encountered by the IS auditors, the same need to be highlighted to concerned audit directorate in OAGN. Conversely, in case if any issues are encountered (by auditors from other directorates) during FA, CA, or PA that need attention from IS audit perspective, they need to be highlighted to the "Information Technology and Special Audit Directorate" under the Performance Audit Division. In both cases, consultation between different directorates on issues is required. This will ensure that respective directorates, take into account, relevant issues, while planning their audits.

1.9. General requirements for IS audit

This section contains general requirements for IS audit related to audit documentation, supervision and review.

[36] WGITA/IDI IT audit handbook

[37] E.G. average response time, user satisfaction score, error rates, availability, load management, request rate/traffic, etc.

1.9.1. Audit documentation

Audit documentation is the record of the audit work performed and the audit evidence supporting audit findings/observations and conclusions. Preservation of the audit results and the audit evidence is to be ensured by IS auditors such that they conform to the requirements of reliability, completeness, sufficiency, and correctness. It is also important for IS auditors to ensure that the audit process is preserved to enable subsequent verification of the audit analysis procedures. Audit documentation shall be retained and protected from any modification and unauthorised deletion in NAMS. The period of retention will be as per OAGN's IT policy (7 years), after which the audit documentation shall be archived as per the archival policy of OAGN.

Documentation includes a record of:

- The planning and preparation of the audit scope and objectives
- The audit plan/programmes
- The evidence collected on the basis of which conclusions are arrived at
- All working papers including general files pertaining to the study of organisation and system
- Points discussed in interviews clearly stating the topic of discussion, person interviewed, position and designation, time and place
- Observations as the auditor observed the performance of work. The observations shall include the place and time, the reason for the observation and the people involved
- Reports and data obtained from the system directly by the auditor or provided by the audited staff. The IS auditor should ensure that these reports carry the source of the report, the date and time and the conditions covered
- At various points in the documentation, the auditor shall add their comments and clarifications on the concerns, doubts and need for additional information. The auditor should return to these comments later and add remarks and references on how and where these were resolved
- Where the audit work is reviewed by a peer or a superior, the remarks arising out of the review should also be recorded in the documentation
- The draft and final reports of the audit should form part of the audit documentation.

1.9.2. Supervision and review

- The work of audit staff should be properly supervised during the audit, and documented work should be reviewed by a senior member of the audit staff such as supervisor or team leader. The senior member of the audit staff (such as Director/Team Leader) should also provide necessary guidance, training and a mentoring role during the conduct of audit, which will be crucial in this new area of IS audit.

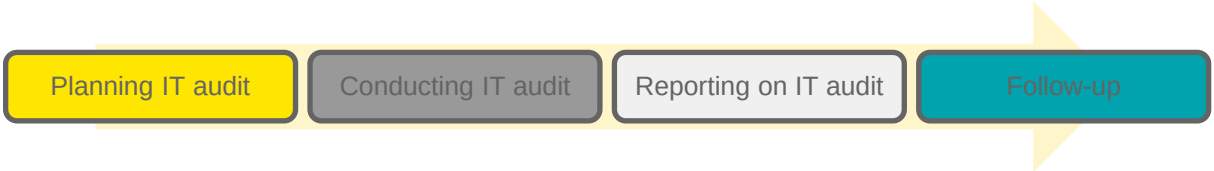
- The Audit Director/Team Leader should ensure that the proper audit documentation exists, contains appropriate and sufficient evidence, and is complete and easily retrievable.

- Working papers should be prepared in sufficient detail to enable an experienced auditor with no previous connection with the audit to ascertain what work has been performed to support the findings and conclusions.

- The overall review process should be done by the Assistant Auditor General (AAG) in-charge of IT Audit directorate, to ensure that all conclusions made are consistent with each other, are relevant, logical, constructive and supportive.

1.10. Overview of IS audit process

The IS audit process covers planning, conducting, reporting[38] and follow-up stages.



- **Planning stage** primarily includes identification of system/application to be audited, definition of audit objectives and audit scope, preliminary understanding of "understanding of the system, controls and risks associated", development of entity audit plan and arranging/identifying resources for audit. In planning phase, IS auditors shall gain an understanding of the auditee's environment including, its structure and operations. They also need to understand the operations of entity that are performed using IT systems, associated controls and related inherent and control risks. The auditor need to conduct a preliminary risk assessment to evaluate the overall IT control environment at the auditee. Based on the result of risk assessment, auditors shall form the extent of procedures to be used for conducting the audit.

- **Conducting stage** involves test of controls, substantive testing, collection and evaluation of evidences. In this phase, IS auditors verify and test if IT controls are operating effectively. As discussed in planning phase, IT auditors will already have information on control policies, procedures and objectives and would have designed their audit plan accordingly. Auditors shall check effectiveness of general and application IT controls to help ensure that the IT system maintains the confidentiality, integrity, availability and reliability of critical computer processed data.

- **During Reporting phase**, IS auditors draw conclusions on the findings, and develop IS audit report to communicate the objectives of the audit, the audit scope, methodology adopted, findings, conclusions and recommendations, to the auditee's management.

- **Follow-up** involves following up with the auditee on recommendations made in the IS audit report, presenting unresolved findings to the legislature (PAC) and planning follow-up IS audits for audit of unresolved findings, as applicable.

[38] The ASOSAI IT Audit methodology uses the same top-down, risk-oriented approach in the evaluation of IT controls.

2. Planning IS audit

The IS audit planning has three stages of planning, viz. Strategic IS audit Planning, Annual IS audit Planning (Macro planning) and Entity level planning (Micro planning). Strategic IS audit Planning is a long-term planning (3 to 5 years) where IS audit targets and objectives for the audit are determined by OAGN. It can also contain new and emerging areas to audit with respect to IT and may also contain new methods of systems development (such as agile programming), acquisition or other emerging technologies (such as cloud computing) in public sector. In essence, Strategic IS audit Plan will provide the *tone and direction* for IS audits of OAGN. Strategic Audit plan shall also identify the IS audit universe to the extent possible.

Annual Audit Planning process shall prioritize and select suitable topics/IT systems for audits during a year from the audit universe by applying a risk-based approach.

Once the topics are finalized, next steps will be preparation of detailed audit plans for the selected entities/IT systems and logistical planning.

Each stage of planning is explained in detail in the following sections.

2.1. Strategic IS audit Planning

Strategic IS audit plan addresses matters such as:

- Goals and long-term objectives of IS audit and Key Performance Indicators;
- How to re-orient audit techniques and methods to meet the changing requirements in Nepal;
- Human and infrastructure requirements related to IS audit
- Training needs of OAGN staff for undertaking IS audits

OAGN shall assess its environment through surveys, interaction with the audited entities, assessment of direction and development of technological solutions and their adoption by the audited entities, and any other legal or mandatory requirements. The Strategic IS audit Plan shall form part of OAGN's IT Strategic plan[39], and will be covered under IS audit related strategic goal/s. As mentioned earlier, the Strategic IS audit Plan will set a direction in terms of objectives of IS audit, key areas of focus, professional capacity development of OAGN staff and identification of other requirements for conducting IS audit.

Additionally, identification of audit universe at this stage would also be done. OAGN shall identify universe of IT system for audit, based on its goals and long-term objectives, and priorities of auditing in response to the assessment of its environment. IS systems to be audited from perspective of financial audits, can also be included in the IT audit universe.

For example: OAGN conducts financial audit of entities, to determine whether an entity's financial information is presented in accordance with the applicable financial reporting and regulatory framework. However, auditees of OAGN, both at national and subnational level, maintain various IT systems, such as BMIS (Budget Management Information System), FMIS (Financial Management Information System), RMIS (Revenue Management Information System), SuTRA (Sub-National Treasury Regulatory Application), to manage their financial transactions and information. These IT systems are used to map the requirements for preparation of financial statements, i.e. capture of financial information, application of framework requirements, processing of the

[39] Current OAGN's IT Strategic Plan is for 2016-2020

information, and presentation in the required format. Financial Auditors should therefore derive an assurance on the appropriateness of the IT System and its associated controls before concluding their financial audit. The assurance on the IT system should be derived through an IS audit of the system looking at all aspects of IT Governance, IT General Controls, and IT Application Controls, as discussed in earlier sections. Since Financial Audit is one the key mandate of OAGN, the IS audit universe of OAGN, shall contain relevant financial management IT systems.

Table 6: Sample IT audit universe for IS audits

S/N	IT system	System Owner/ Entity	Key System Users
1.	BMIS - Budget Management Information System	Ministry of Finance (MoF)	Program and Budget Implementation Division of MoF
2.	LMBIS - Line Ministry Budget Information System	Ministry of Finance	Budget executing agencies
3.	AMIS - Aid Management Information System	Ministry of Finance	International Economic Cooperation Coordination Division (IECCD) of MoF
4.	FMIS - Financial Management Information System	Financial Comptroller General Office (FCGO)	FCGO, DTCOs (District Treasury Controller Office), planning division chiefs and accounts chiefs of ministries and other central entities.
5.	TSA - Treasury Single Account	FCGO	Paying offices of central ministries, FCGO, MoF, National Planning Commission (NPC) and other GoN' agencies users
6.	RMIS - Revenue Management Information System	FCGO	Agency banks, Inland Revenue offices, DTCOs, FCGO, Nepal Rastra Bank (NRB)
7.	CGAS - Computerized Government Accounting System	FCGO	FCGO
8.	PAIS - Public Assets Information System	FCGO	Paying offices at districts, DTCOs
9.	Debt Management System	FCGO	MoF
10.	Pension Management System	FCGO	Pension Management Office (PMO), banks, DTCOs, NRB
11.	SuTRA - Sub-National Treasury Regulatory Application	PEFA (Public Expenditure and Financial Accountability)	State and local governments
12.	TABUCS - Transaction based Accounting and Budget Control System	Ministry of Health and Population (MoHP)	MoHP
13.	FMIS - Financial Management Information System	Department of Road (DoR)	DoR
14.	MARS - Municipal Administrative and Revenue Management System	Ministry of Federal Affairs and General Administration	Local governments
15.	National Electronic Government Procurement System	Public Procurement Monitoring Office (PPMO)	All Ministries, Departments and Agencies (MDAs) of Government of Nepal.

Since majority of the systems are centrally managed by a few organizations such as FCGO, MoF, PPMO, etc. IS auditors shall cover the 'system owner'/entity in the IS audits. However, during IS audit planning, in case auditors

come across certain control issues[40] that might have to be checked at the other locations (offices/users), auditors shall include them (locations) in the scope of IS audit. However, a single IS audit report will be issued to the system owner/entity.

Additional IT systems may be in use at national and subnational government levels and other IT systems may be procured or implemented by the government entities in future. Also, audit of some IT systems may be of requested by governmental bodies, legislature, PAC or oversight bodies. Hence, the IS audit universe shall be re-visited annually and updated, if required. There will be a periodic (annual) review and update of the Strategic IS audit Plan of the OAGN to address its goals of ensuring transparency, accountability and contribution to good governance. Please note that IT systems/entities will be selected from this audit universe during the Annual Audit Planning at OAGN.

2.2. Annual IS audit Planning

Annual IS audit planning will be conducted as part of OAGN's Annual Audit Planning. Annual IS audit planning involves translating the long-term IS audit strategic plan into a yearly audit plan. This stage involves selection of the IT system/s and entities to be audited during a financial year based on priority of IS audit topics.

The methodology for selection of IS audits, presented in this manual shall be used for finalizing audits from the IS audit universe. This methodology adopts a risk-based approach toward prioritizing of IS audit topics and selection. As mentioned earlier, in addition to the risk-based approach to select audit topics, OAGN may be required to take on audits by requests by oversight bodies (Parliament, etc.) or the executive or other public bodies. Based on auditor's judgement, such topics can also be included in the annual IS audit planning.

After selection of IS audit topics, in the Annual Audit Plan of OAGN, following details should be mentioned:

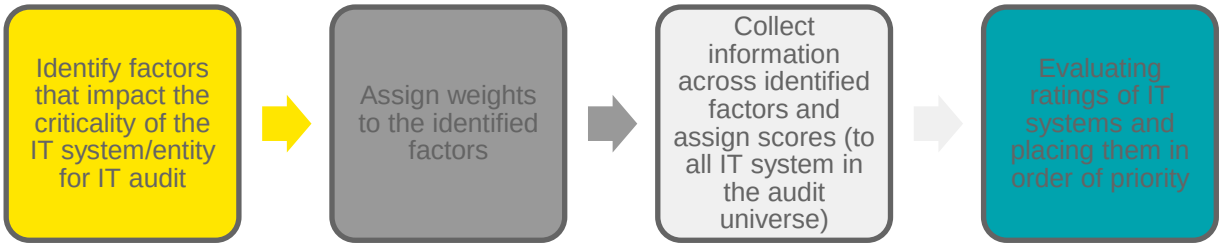
- Brief of methodology used for selection of IT audits
- Priority score of IT systems based on risk-based planning
- IT systems selected for audit,
- Overall objective of IS audit (as discussed in section 1.8) for each selected IT system
- Brief description of IT system, and auditee[41]
- High level resource requirements (estimates), and
- Tentative timelines (start date and end date of each IS audit)

Selection of IS audits

Following are the steps in risk-based approach for selection of entities/IT systems for IS audits:

Figure 5: Steps in risk-based audit planning for IS audits

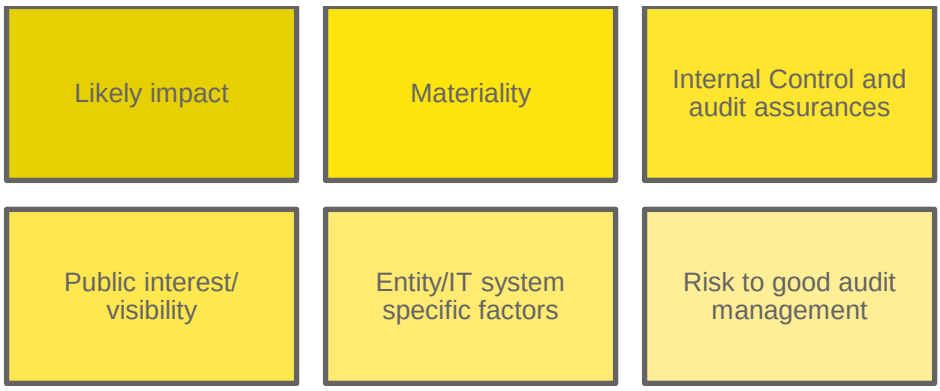
[40] For example: It may happen that system owners has granted administrator privileges to some of the underlying user offices, which in turn can create and maintain new user records. In such case, auditors need to check if access controls are in place at the user offices that are given administrator rights/privileges.
[41] System owner and user offices, as applicable



These steps are explained in detailed in following sections.

2.2.1. Factors impacting criticality of the IT systems

Figure 6: Factors impacting criticality of the IT systems for audit (for selection)



Factor 1 - Likely impact of Audit: It is important to consider the impact, that the audit of IT system, is likely to have. OAGN should assess potential value addition and whether something new and useful can be said or not by conducting the IS audit. The potential impact on entity to be audited, in terms of making recommendations on potential IT audit issues, can also be considered by the auditors while scoring IT systems on this factor. Auditors shall also consider, if the audit topic meets the goals and objectives of IS audits as defined in Strategic IS audit plan or focusses on a 'new areas' of IS audit.

Factor 2 - Materiality: Materiality shall be based on the judgement of the IS auditors considering qualitative as well as quantitative aspects. A matter can be judged material if knowledge of it would be likely to influence the decisions of the intended users/auditee. There are two aspects to materiality:

- **Quantitative aspects**: This relates to the 'amount' or 'value' or 'budget' of investment made in the IT system and the annual cost of operation and maintenance (O&M) of the system. Higher the investment and annual running cost, higher will be the criticality of the system on this factor. Additionally, mode of financing also impacts the criticality of the system. E.g. A system financed through external borrowings (e.g. donor agencies) will be considered more critical than a system financed through entity's own budget, since in former case, entity has an obligations towards the borrower, to show intended benefits of funded program.

- **Qualitative aspects**: This is based on the judgement of the auditor, on the potential contribution of auditing in broader scenario of administration and/or management. Various factors that can be considered for deciding materiality, by the auditors are presented below.

a) ***Complexity of the IT system***: Some IT systems are more complex than others and hence may carry higher priority of audit for OAGN. E.g. TSA is used across multiple paying offices of central ministries, FCGO, MoF, National Planning Commission (NPC) and other GoN' agencies users, across multiple locations in Nepal. The system is in use by multiple offices, has a large user base, is interfaced with other systems such as BMIS, FMIS, is used for all kinds of government payments, and is a web based OLTP system. This system also

processes larger volume of data for both receipts and payments, on a daily basis. Hence, due to inherent complexity of this IT system it carries higher priority over a batch processing systems or a data consolidating system or a support system. In addition, batch processing systems or data consolidation systems may be relatively less vulnerable to risks as compared to online transaction processing systems such as TSA. E.g. risk of downtime for an online payment system, that processes real-time transactions, is higher than a system used for batch processing at certain intervals of the day.

b) ***Nature of services provided by the IT system***: Systems that are used for business-critical services as Public Financial Management (PFM) including budgeting, payments, receipts, accounting carry higher priority over systems that are used for support functions such as human resources management, procurement, payroll, etc. Hence, auditors shall ideally focus on IT systems that are used for carrying our business-critical functions of the entities.

c) ***Reliance of entity on IT system***: The extent of reliance of the entity on the IT system also determines the criticality of the IT system. The extent of reliance means to what extent does the entity uses the functionality of the IT system for carrying out its functions. E.g. in some cases, the outputs of IT system may directly be used for business-critical operations such as revenue generation. RMIS and other tax collection system that have direct access to payers, are used for collection of money on behalf of the government and also have inbuilt accounting functionality. On the other hand, there might be a system which is only used for accounting of receipts, based on data entered by the users which they received from other sources such as banks. In this case the reliance of entity on the system, for carrying out its functions will be lower, since manual intervention is required on outputs generated from the system. Hence, higher the reliance of entity/ies on IT system, for their operations, higher will be the system criticality.

d) ***Sensitivity of data***: Systems dealing with sensitive data, need to have better general and application controls to ensure privacy of user data and hence carry higher priority for audits. This is largely applicable for IT systems that store data on citizens/public such as tax-payer data or vendor specific data. In such cases, issues of access controls need to be checked to ensure if system has sufficient controls to protect sensitive data.

- Auditors may also consider other aspects of materiality based on their judgement.

Factor 3 - Internal control and audit assurances on IT system/Entity: This factor takes into account audit history of the IT system, which helps auditors in prioritizing systems that have not been audited recently or have several critical or recurring observations made by the auditors in past audits. The systems that haven't been audited in recent years carry higher priority over systems that have been recently audited by OAGN (e.g. last year). It may also happen, that several issues relating to IT systems were made in the previous audits carried out by OAGN and many of the issues are yet unresolved by the entity. Additionally, there could be system specific issues identified in the audit reports for audits carried by external agencies (hired by the entity). In all such cases, higher priority for audit will be given to the IT system in question. Auditors shall also give higher preference to IT systems for which a third-party IT audit certification is not performed by the entity.

Factor 4 - Public interest/visibility[42]: Some IT systems may be of interest for the legislature and public due one or the other reasons. Hence operations of these systems carry more importance to the government and the public. E.g. some IT systems may be accessed by the public to access data or information/reports such as tax collection systems. Public may also directly conduct transactions on such-systems. Additionally, certain systems may also be of potential interest to OAGN stakeholders such as press/media, general public, parliament, NGOs, etc. The systems processing data of public interest carry risks of failure of business, erosion of credibility of the organization or financial loss to the entity, in case wrongful data is processed. Hence, such systems carry higher priority for audits.

[42] Though public interest is one of the factors, however, it is important that selection of topics for auditing take place without any form of outside pressure, maintaining the OAGN's independence.

Factor 5 - Entity/IT system specific aspects: There are several other factors relating to IT governance mechanisms, policies, procedures, that should be in place at entity for managing the IT operations, system development, acquisition and outsourcing, IS security, etc. Lack or absence of such mechanisms, policies or procedures pose a number of risk to the entity's operations that are carried out in the system. E.g. whether, entity has a dedicated IT team or resources for managing IT operations. Following areas can be considered for evaluating priority of IT system, on this factor.

- **Level of computerization at entity**: Higher the level of computerization at an entity, higher will be the criticality of the IT system for audit. The reason being, that in case of higher computerization, it is expected that entity has sufficient general controls to ensure proper functioning of the IT systems to meets business goals, safeguards information assets and maintains data integrity.
- **System development and management (including data):** IT System under consideration could have been developed and implemented by an external agency or in-house or by a government agency. Similarly, after system may be maintained by the entity or outsourced and managed by external agencies. From the perspective of OAGN, system that is developed and managed externally, or hosted on outsourced facilities, shall carry higher priority of audits, since in that case, system operations and entity specific data is exposed to higher risks.
- **System operation**: Systems with higher years of operation are more likely to more mature and stable than the systems with lower years of operation. Hence systems with lower years of operation may be susceptible to more control weaknesses and carry more priority.
- **Change management**: Some systems may be frequently updated compared to other systems and may have been modified/upgraded in the recent years. In case a system is regularly modified it is imperative for the entity to have a documented change management policy in place. System updates may often impact the existing controls and functionality and hence such frequently updated systems have higher priority for IS audit.
- **Dedicated IT staff**: System with higher (number of) dedicated IT staff, have higher priority, since in such cases, the entity should have IT governance mechanism in place to manage the IT staff. Also, in such cases, entity is spending higher resources on management of IT systems and hence, appropriate general controls are to be in place to ensure that the entity achieves business goals with the given resources.
- **Other entity specific factors**: There are other entity specific factors that determine the priority of IT systems for audit. E.g. does an entity have an approved IT Policy in place, does an entity has a documented disaster recovery plan and business continuity plan, does the entity has an approved IT security policy, does the entity has system specific documentation such as technical design documents (High level and detailed design), testing documentation, and installation guides and user manuals. Higher priority is to be given to IT systems owned by entities that do not have such policy/documents in place, as they are more susceptible to risks.

Factor 6 - Risk to good audit management: Auditor shall assess potential risks in undertaking the audit considering the complexity of IT system, entity's operation and available skill and knowledge of the IS auditors. Auditor shall assess, if the audit topic is auditable or not considering availability of sufficient information to undertake the audit, accessibility of audit location and availability of skilled team to cover the audit.

2.2.2. Assigning weightage to the factors

Once, the factors impacting criticality of the IT systems have been identified and selected, next step is to assign weightage to these factors. Auditors shall use their judgement while assigning weightage to the factors based on overall significance of the factor towards criticality of IT systems for IT audit. OAGN may also consult select entities in finalizing weightages of these factors. The sum of weights of all factors should be 100%. Recommended weights for various factors are presented below.

Table 7: Weights for factors that impact criticality of the IT systems

S/N	Factors impacting criticality of the IT systems	Assigned Weightage
1.	**Likely impact**	20%
2.	**Materiality**	20%
3.	**Internal Control and audit assurances**	15%
4.	**Public interest/visibility**	10%
5.	**Entity/IT system specific factors**	20%
6.	**Risk to good audit management**	15%
Total		**100%**

2.2.3. Compiling information on IT systems and arriving at weighted scores

Next step is to compile information for all IT systems/entities in the audit universe and assign scores to them across all (six) factors. The assessment of criticality of IT systems is *largely* based on subjective assessment of the risk parameters or factors. However, Auditors may ask several questions while giving scores to IT systems across all factors. A list of questions, that auditors can ask, while collecting information on the above factors is presented in the Annex 1: Questions for assessing criticality of IT systems - Topic selection.

Based on the information collected, scores will be assigned to the 'factors' for all IT systems in the audit universe, and total (weighted) score shall be derived for each of the IT system. Maximum score for any of the factors can be 10 and minimum score 0. Maximum Total (Weighted) score could be 10 for any of the IT system/Topic.

Table 8: An illustration of matrix for selection of IT systems/topics for audit

Factor impacting criticality of IT systems	Weightage	Scoring					
		Topic 1		**Topic 2**		**Topic 3**	
		Assigned	Weighted	Assigned	Weighted	Assigned	Weighted
Likely impact	20%	7	1.4	10	2	5	1.0
Materiality	20%	5	1	10	2	5	1.0
Internal Control and audit assurances	15%	10	1.5	10	1.5	10	1.5
Public interest/visibility	10%	0	0	8	0.8	10	1.0
Entity/IT system specific factors	20%	10	2	8	1.6	5	1.0
Risk to good audit management	15%	5	0.75	8	1.2	10	1.5
Total scores	100%	37	**6.65**	54	**9.1**	45	**7**
Overall Rank	-	3		1		2	

2.2.4. Placing systems in order of priority for audits

After weighted scores for IT systems is arrived at, they shall be placed in order of priority based on their overall rank. This risk-based classification, ensures that OAGN undertakes IS audit of critical/priority IT systems during a year, considering the resource requirements, associated risks, and OAGN's strategic focus. OAGN shall be able to achieve goals and objectives for IS audit mention in its strategic IS audit plan.

Additionally, a suitable range (of score) can be selected for classifying IT systems as high, medium or low risk, based on their total scores (illustrated below). This classification can be used for selection of IT systems on a cyclical basis. E.g. Systems with 'low risk' category can be audited once in three years and systems with medium risk category can be audited once in every 2 years. This classification can also be used for deciding % of IT systems under each category to be audit in the current year. E.g. 100% for high risk category, 50% of medium and 33% of low risk. However, it should be noted that OAGN shall decide on the number of IS audits to be undertaken during a year depending on its strategic priorities, available resources and audit mandate. An illustration of risk categorization of IT systems based on their weighted scores is presented below.

Table 9: Illustration of risk categorization of IT systems based on their weighted scores

Weighted score	Risk category
More than 8 but less than or equal to 10	High
More than 5 but less than or equal to 8	Medium
Less than or equal to 5	Low

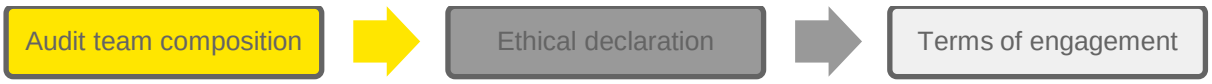
2.3. Entity level planning

Entity level planning involves development of a detailed IS audit plan for audit IT system of the selected entity, beginning with outlining the audit objectives. The objectives and scope of the audit determines the IS audit work.

However, for designing an audit plan for the entity, auditors need to understand the entity and its IT environment and assess the risk associated with the IT system for identifying the audit issues to be included in the audit matrices. The results of this assessment provides the basis for determining the extent and type of subsequent testing required during conducting IS audit. Please note that planning is an iterative process and it may happen that while conducting audit, IS audit auditors come across evidence or information that may require reevaluating their earlier conclusions and other planning decisions that were made based on those conclusions. Hence, auditors shall update the audit plan accordingly.

2.3.1. Pre-planning activities

There are certain activities that need to be performed before the activities for preparation of entity level plan (audit plan) can be undertaken.



2.3.1.1. Audit team composition

After selection of topics for IS audit, audit team shall be composed to perform the entity level planning, audit execution, and subsequent audit procedures.

Audit team shall be composed of members that collectively have the competence to conduct IS Audit engagements to achieve the intended audit objectives. The necessary knowledge, skills and competence, required for IS audits, shall be acquired through a combination of training, recruitment and engagement of external resources, per the strategic plan of the OAGN[43].

IS audit team shall collectively have capacity to[44]:

- Understand the technical elements of an IT-driven information system, including all relevant instances of the application in use, so as to be able to access and use the IT infrastructure for the audit process
- Understand extant rules, regulations and the environment in which the IT-driven information systems of the audited entity are operating
- Understand the mapping of business processes into the programming logic for information system of the audited entity
- Apply both business and IT knowledge to evaluate the risk of manual override of a system program or configuration that would allow exceptional processing of transactions
- Evaluate the design and test the operating effectiveness of application controls in relevant information systems
- Understand the audit methodology, including relevant auditing standards and guidelines applicable to the OAGN

[43] Ref: GUID 5100 - para 5.6 and 5.7
[44] GUID 5100 - para 5.8

- Understand the IT performance/ compliance criteria against which the audit findings are to be compared, including frameworks for IS management, such as COBIT, ITIL, TOGAF[45]
- Understand IS techniques to collect the audit evidence from automated systems
- Understand IS Audit Tools to collect, analyse, and reproduce the results of such analysis or re-perform the audited functions
- Access and use IS Infrastructure to capture and retain audit evidence
- Access and use IS Audit Tools to analyse the collected evidence

In case the IS audit is undertaken in context of other audit engagements (CA or PA or FA), the whole team shall work in an integrated manner to achieve the overall audit objective. To achieve effective integration, following points need to be taken care of[46]:

a) Comprehensively documenting the work to be performed by the IS auditors;
b) Formulating a *protocol for sharing of information* between the IS auditors and other auditors;
c) Identifying which information systems and control objectives are within scope of the IS audit;

"Information Technology and Special Audit Directorate" under the Performance Audit Division, shall be entrusted with the responsibility of conducting all IS Audit engagements for the OAGN, and interact with other directorates at the OAGN who have legacy knowledge of the audited entity, in order to quickly get an understanding of the entity's functions and related business processes. This audit directorate shall be the central group with IT specialists who assist other audit directorates in the OAGN to conduct the IS audits or deploying IT specialists as per requirement of the audit. Moving forward, as the number of IS audits undertaken by OAGN increases, OAGN may establish a dedicated IS Audit group or function with IS audit specialists. Additionally, since technology is becoming more embedded in audits, OAGN will focus on developing appropriate IS audit skills of more auditors and plan for building capacity of all auditors on basic IT audit skills.

Engaging external resources:

As per the requirement of IS audit, OAGN may engage external resources such as IT consultants, contractors, specialists and experts to conduct IS Audit, in cases of resource or skillset constraints. It shall be ensured that such external resources are adequately trained and sensitized to the guidelines for professional conduct (Code of Ethics) and on processes and products of IS Audit applicable to the OAGN, and that their work is adequately monitored through a documented contract or a service-level agreement and appropriate involvement from staff of the OAGN in the planning, conducting, reporting and follow-up stages of the audit, is ensured. OAGN shall therefore need skilled and knowledgeable team members in-house to monitor the work of external resources and enforce adherence to guidelines and service level agreements. It is also important to clearly establish **terms of the audit** with external resources and their roles and responsibilities.

2.3.1.2. Signing ethical declaration

All the members of the audit team shall comply with the ethical codes and need to give compliance declaration in the manner prescribed in OAGN Code of Ethics.

[45] The Open Group Architecture Framework (TOGAF) is an enterprise architecture methodology that offers a high-level framework for enterprise software development
[46] Ref: GUID 5100 para 5.5

2.3.1.3. Terms of engagement

Auditors should ensure that the terms of the audit have been clearly established even when audits may be required by statute or initiated by OAGN. In all cases the auditor, the auditee's management, those charged with governance and others as applicable should reach a common formal understanding of the terms of the audit and their respective roles and responsibilities. Important information may include the subject, scope and objectives of the audit, access to data, the report that will result from the audit, the audit process, contact persons, and the roles and responsibilities of the different parties to the engagement[47].

Terms of engagement can be issued to the auditee in form of an engagement letter communicating the IT system to be audited, objective of the audit, tentative time period of the audit, offices or programs to be included in audit, roles and responsibilities of the auditee' management, support required from auditee's management in audit process, and requesting access to auditee's systems, records, documents, offices, etc. as required for audit. It should be ensured that due cooperation and support of the audited entity is sought in completing the audit, including access to records and information, and provisions made to get any electronic data in the format necessary to allow analysis.

2.3.2. Planning activities

This section details the activities to be undertaken for preparation of audit plan for the entity/IT system to be audited.

2.3.2.1. Understanding the auditee's environment and its Information system

It should be noted that as per ISSAI Fundamental Principles of Public Sector Auditing: "auditors should obtain an understanding of the nature of the entity/programme ***to be*** audited". This includes an understanding of **internal controls**, as well as objectives, operations, regulatory environment, ***systems***, and business processes involved. Even in small entities where information systems and business processes relevant to financial reporting are less sophisticated, their role may be significant. The role of the auditor is to understand the potential business and IT risks facing the audited entity, and in turn to assess whether the deployed controls are adequate to meet the control objectives.

The prerequisite to developing the audit plan is to have a clear understanding of audited entity, its Information Systems and related activities. The information collected and understanding developed for the IT system, provides data for risk assessment, that forms the basis for planning (scoping) the audit.

Note: It should be noted that, a preliminary understanding of the auditee's environment and IT system, to some extent, would already have been gathered during the Annual Audit Planning stage. Additional, understanding to develop the audit plan will be gathered during "Entity level planning" stage. During this planning phase, auditors need to focus only on the relevant IS audit domains, and areas, which affect the objective of the overall audit engagement.

In general, IS auditor shall gather information on the following aspects of the entity/IT system to be audited:

[47] ISSAI 100.44

1) Organizational function and operating environment

This covers a general understanding of business processes and functions of the entity and how the IT system support these processes and functions. Auditors shall seek to understand:

- Entity's business and functions and its strategic goals and objectives
- Major types of transactions and assets involved in achieving business goals and objectives
- The extent to which IT systems are used to process and control such transactions and business processes
- Critical business units inside the entity that conduct business and their geographical spread
- Regulatory framework in which the entity carries out its business and operates its IT system
- Major spending programs related to IT systems
- Type of risks faced by entity across its business, IT systems, critical business units, involved in conducting business

This understanding helps the auditors to further narrow down the scope of the audit in line with the audit objective and also develop a holistic view to planning such audits.

A note on regulatory framework in which entity operates its IT system:

Auditor shall have an understanding of various policy and guidelines issued by Ministry of Communication and Information Technology, Department of Information Technology, that are application to IT systems in Nepal. Accordingly, auditors shall identify the policy and guidelines that are applicable to the entity. This will ensure that auditors include aspects of compliance of IT systems with relevant regulatory framework of Nepal, in the entity audit plan. A few of the examples such policy and guidelines[48] are:

- Electronic Transactions Rules-2064: Auditee shall comply with the requirements of electronic record, their certification, verification of digital signature and other security aspects of electronic signatures and records.
- Government Websites Design/Development and Management Guidelines-2068
- Nepal GEA SOA Development Lifecycles v2.0: Development lifecycle applicable to project teams engaged in the design, development and implementation of web services in Nepal.
- Nepal GEA Security Architecture v2.0
- Nepal GEA Infrastructure Architecture v2.0
- Other applicable policy guidelines for requirement analysis for IT Systems for Government entities in Nepal and design consideration guidelines covering data architecture, application architecture, integration architecture, security architecture and infrastructure architecture.

Note: Please note that, this activity will have to be undertaken in detail, in case nature of IS audit is undertaken as a subject matter for compliance audit or objective of IS audit is to check compliance of system development, acquisition and operation procedures with the applicable regulatory framework in Nepal.

2) Organization structure

This includes an understanding of entity's hierarchy and structure and more importantly understanding of structure of IT unit, if any. Auditor shall seek to understand:

- Organizational levels, and segregation of duties within the entity and the IT unit
- Human resource policies and management practices
- Separation of duties between the IS audit and other functional units in the entity

This understanding helps the auditors to establish line of audit enquiry and provides valuable inputs into supervisory controls and controls over access to IT system and hardware.

3) Criticality of the IT system

[48] Source: https://nitc.gov.np/document/

Aspects of criticality of IT system are covered in the Annual Audit Planning. The aim is to identify business critical functions of the entity that are supported by IT systems. This understanding helps the auditors in scope and extent of IS audit largely in terms of functionalities of IT systems to be audited. This helps auditors to identify mission critical system functionalities, failure of which would have serious impact on the entity. Auditors shall also obtain and understanding of business process flows through the system. This can be done by document study of relevant manuals, interviews with key personnel (both business users and technical users) and observation of procedures to understand how the systems supports the business of the entity.

4) Nature of hardware and software used

A typical application forming the core of an IT System in a computerised organisation, will have a combination of database management system with specific databases, application software(s) mapping the business rules in the system through specific modules, and front end user interface(s) supported by network application software if there is a networked environment. The databases and applications software reside on servers, which are essentially high capacity computers capable of hosting large and multiple databases and applications. The servers could be specific to different user requirements such as data servers, application servers, internet servers, and proxy servers[49]. Hence, auditors should collection information on the nature of hardware and software in use at the auditee.

Some aspects of "nature of hardware and software used" are covered in the Annual Audit Planning. The aim is to develop a detail understanding of vulnerabilities faced by hardware and software being used. This would involve taking a stock of hardware and software used, evaluating hardware acquisition and maintenance procedures, method of procurement of software (in-house or commercial off the shelf), operating systems, database management systems, network systems, network and system architecture, connectivity related technology, etc. This assessment would help the auditors in scoping of IS audit in terms of coverage and also resource allocation. Sample forms for collection of information on IT software and hardware have been presented in the annexures.

The information that is required for understanding auditee's environment and IT systems, can be gathered from:

- NAMS (database from external systems)
- Interviewing key personnel of the auditee (virtual interviews are also an option)
- Reviewing relevant material available, including, auditee's annual report, independent audit reports, policy documents, IT strategy, auditee's strategic plan or other material
- Questionnaire/ data collection forms
- Policies and procedures, application-specific user manuals, documentation on IT outsourcing contracts, functional design documents, vendor-supplied technical reference manuals, and list of reports (standard and customised). This will help in understanding of the environment in which the system operates and identifying the business risks from control failure.

The *extent* of knowledge of the organisation and its processes required by the IS auditor are largely determined by the nature of the organisation and level of detail in which audit work is being performed. Knowledge of the organisation should include the business, financial and inherent risks facing the organisation and its IT Systems. It should also include the extent to which the organisation relies on outsourcing to meet its objectives and to

[49] WGITA/IDI IT Audit handbook

what extent the entire business process has been mapped in an IT environment[50]. The auditor should use this information in identifying potential problems, formulating the objectives and scope of work, performing the work and considering actions of management for which the IS auditor should be alert[51].

Based on the understanding developed of the Information System and the audited entity, IS auditors may decide on their approach for IS audits. IS audit would eventually involve audit of General and/or Application Controls.

2.3.2.2. Risk assessment

Through understanding of the audited entity and the information system, auditors should conduct an assessment of risks that affect the IT system. Risk assessment helps auditors in designing audit plan that contains the **scope** of the audit. Risk assessment basically helps in deciding the:

- Priority IS audit domains, audit areas/sub-areas, and likely risks/issues associated with the audit areas that need to be checked during the audit
- Objectives of checking the potential audit issues under selected audit areas
- Type of analysis methods (nature of testing), required for checking the audit issues
- Extent of testing required, and
- Resourcing, scheduling of audits

Auditors need to assess what risks affect the IT system and the severity of impact on the entity's business. These risks can be differentiated as inherent risks, control risks and detection risks. These risks combined represent the Audit Risk.

As per GUID 5100 para 5.11

For carrying out risk assessment for IS Audit engagements, the principles laid down in ISSAIs 100, 200, 300 and 400 may be used by auditors in addition to those used in conduct of specific subject matter of IS Audit (as mentioned below).

[50] Organisations changing over from a manual to a computerised environment would normally conduct a Business Process Reengineering (BPR) exercise. It may be possible that some of the business processes are being carried out manually along with the IT Systems. These particular scenarios would present specific interest areas for IT Auditors.

[51] WGITA/IDI IT Audit handbook

1) Inherent Risk

- It consists of the probability that certain features of the IT driven information systems of an audited entity, by their very nature, may result in an adverse impact on the delivery of the function mandated to be carried out by the entity.
- For example, an information system of an auditee which is required to make information available for all members of the public, carries the inherent performance (load) risk that beyond an anticipated peak user limit, the information system may fail to respond, and the information would not be available to any user. While the audited entity may adopt controls to mitigate inherent risks, in many cases, the entity may have to simply tolerate the existence of such risks, within an acceptable risk level.
- Another example is that inherent risk associated with application security of a web-based IT system. By nature, the security risks associated with a web-application are usually high, since, multiple user groups access the information in the application over internet.
- Inherent Risk shall be assessed, before the influence of Control or Detection Risk is considered by the Auditors.

2) Control Risk

- It consists of the probability that IT general and application controls that have been adopted by the auditee may fail to mitigate the adverse impact that they were designed in response to. At the planning stage it would suffice for the auditor to form a *general* opinion on the nature and adequacy of the controls deployed in an IT system and also areas where the controls are weak and vulnerable. This forms the basis of the extent, the areas, and the depth of testing required.
- For example, an information system of an entity which is required to ensure that access to confidential data is restricted to authorized personnel may adopt the control of requiring the presentation of a username and password by personnel attempting to gain access. The Control Risk in this situation is that the username and password are not adequately secure and can be guessed by unauthorized personnel through repeated attempts, resulting in loss of confidentiality and potential adverse impact on the entity. An entity that insists on use of secure, non-trivial passwords which have a combination of alphabets, numbers and special symbols, and ensures that the information system prevents access to the username beyond a certain number of failed attempts to gain access would have a *lower* Control Risk than one that does not have these features.
- Another example is that the control risk associated with manual reviews of computer logs can be high because activities requiring investigation are often easily missed owing to the volume of logged information. The control risk associated with computerised data validation procedures is ordinarily low because the processes are consistently applied.
- Since, actual test of controls can only be done in the execution phase, the objective of the risk assessment in planning phase is to conduct a **preliminary assessment of the adequacy of controls** based on discussions with the management, a preliminary survey of the application, questionnaires and available documentation.
- The level of control *awareness* in the auditee organization and existence or non-existence of control standards are also key indicators for preliminary control assessment that auditors need to factor in risk assessment.
- Control risk assessment also help in fine-tuning audit objectives and scope and nature of analysis required during audit execution.
- The extent of internal controls[52] present in the organization (auditee) would also determine the risk levels of the IT system and the extent of substantive testing required. Higher the extent of internal controls in an organization, lower is the extent of substantive testing required.

Elements of controls that should be considered when evaluating control strength are classified as Preventive, Detective and Corrective with the following characteristics:

Table 10: Elements of controls to be considered for evaluating control strength

[52] Policies, procedures, practices and organizational structures put in place to reduce risks are referred to as internal controls

Preventive	Detective	Corrective
• Detect problems before they occur • Monitor both operations and inputs • Attempt to predict potential problems before they occur and make adjustments • Prevent an error, omission or malicious act from occurring	• Controls that detect and report the occurrence of an error, omission or malicious act	• Minimise the impact of a threat • Resolve problems discovered by detective controls • Identify the cause of a problem • Correct errors arising from a problem • Modify the processing systems to minimize future occurrence of the problem

An illustration to conduct the preliminary assessment of the adequacy of IT controls is presented in subsequent sections.

3) Detection Risk

- It consists of the probability that the absence, failure or inadequacy of IT controls adopted by an entity, which may have a potentially adverse impact on the entity, are *not* detected by the auditor. Detection risk is the risk that the IS auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors.
- For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high because logs for the whole period of the audit are usually not available at the time of the audit. On the other hand, the detection risk associated with identification of lack of disaster recovery plans is ordinarily low since existence is easily verified in form of available documentation (policy).

Audit Risk

Based on the assessment of inherent, control and detection risks, auditors shall arrive at the overall audit risk. This will give auditors an idea about the extent to which controls can be relied upon during testing. Auditor shall be able to identify controls that are most likely to be effective and therefore should be tested to determine if they are in fact operating effectively (during audit execution). The higher the assessment of inherent and control risk the *more* audit evidence the IS auditor should normally obtain from the performance of substantive audit procedures. This approach helps auditors to plan audit tests better, since auditors can avoid expending resources on testing controls that clearly are **not** effective. An illustration to calculate audit risk is presented in the figure below.

Figure 7: Audit risk

Audit Risk = Inherent Risk X Control Risk X Detection Risk		
Inherent risk can be	**Control risk can be**	**Detection risk can be**
• High • Medium • Low	• No or weak control (High) • Decent control (Medium) • Strong control (Low)	• High (Detection of control risk requires substantial time input of auditor) • Medium • Low

IS auditor shall use professional judgement in completing the risk analysis across IS audit areas and domain. An illustration of calculation of Audit Risk of IT Governance domain and related issues is presented below.

Table 11: Risk assessment for audit planning (Illustrative)

IS audit Domain	Audit areas	Issue	Inherent risk	Control risk	Detection risk	Audit Risk	Remarks, risks, etc.
IT Governance	01 Business needs identification, direction and monitoring	IT requirements	High	High	Medium	High	
		Leadership	Medium	Low	Low	Low	
		IT investments	High	Medium	Medium	High	
	02 IT strategy and planning	Quality of IT strategy	High	Low	Low	Medium	
		Risk management	High	Medium	Medium	High	
	03 Organizational structures, standards, policies, and procedures	Structure of the IT organisation	Medium	Medium	Low	Medium	
		Policy and procedures	High	Low	Low	Low	
	04 People and resources	HR and logistics	Low	Low	Low	Low	
	05 Risk assessment and compliance mechanisms	Mechanism	High	Medium	Medium	Medium	

While deciding audit risk, auditor shall also consider materiality, since not all issues are likely to be material.

Materiality

The materiality of an IS Audit ***issue*** shall be decided under the overall framework for deciding materiality in OAGN. The perspective of materiality shall vary depending on the nature of the IS Audit engagement. Materiality for public sector Financial, Performance and Compliance Audits, from which the IS Audit engagement would be drawn, have been described in respective manuals/guide[53].

Example: IT access control

It is qualitatively material if unauthorised persons/entities have access to the IT-systems. For example, for the HR / payroll system, it is crucial that only those who are processing the information have access. If unauthorised persons have access, even though it is read-only access, and the persons cannot manipulate the information, there will be a breach of confidentiality. Another example is if unauthorised persons get access to classified information, for example to the database of the Ministry of Defence or Ministry of External Affairs that can be misused when/if it falls into the wrong hands, which may have serious implications for the nation.

The IS auditor should determine whether any IT general deficiency (issue) could potentially become material. The significance of such deficient IT general controls should be evaluated in relation to their effect on application controls, i.e., whether the associated application controls are also ineffective. If the application deficiency is caused by the IT general control, then they are material. For example, if an application-based tax calculation is materially wrong and was caused by poor change controls to tax tables, a management decision not to correct an IT general control deficiency and its associated reflection on the control environment could become material when aggregated with other control deficiencies affecting the control environment[54].

A stepwise illustration of control risk assessment

Step 1: Select potential audit areas to be considered for risk assessment based on overall audit objective

As discussed earlier, there are many objectives of conducting an IS audit. Once an IT system and an objective of conducting IS audit is decided in the Annual Audit Plan of OAGN, auditors can select potential audit domains and

[53] Ref: GUID 5100 para 5.13

[54] Materiality Concepts for Auditing Information, ISACA Guidelines (G6)

areas that may have to be audited to meet the overall audit objectives. For example, in case the audit objective is review of system security then following audit areas can be considered for risk assessment:

- IT security Policy
- Risk assessment of IT security infrastructure
- Organization of IT security
- Communications and operations management
- Asset management
- Human resources security
- Physical and environmental security
- Access control
- IT systems acquisition, development and maintenance
- IT security incident management
- Business continuity management
- Compliance

Step 2: Understanding of expected controls that should be in place

For each IS audit area there are certain expected controls, absence of which may lead to potential issues/risks. Auditor shall have an understanding of controls that should be in place to manage risks affecting the system and the likely impact on business in case controls are ineffective (control objectives) . An illustrative list of expected controls across various IS audit areas is ***annexed*** this manual for reference of the auditor. However, IS auditors are expected to have this understanding from their prior work experience, education qualification and trainings[55]. As mentioned earlier, audit team composed for audit shall have the necessary skills and competence to conduct the IS audit.

Step 3: Preliminary assessment of the adequacy of controls

The role of the auditor is to understand the potential business and IT risks facing the audited entity and in turn to assess whether the deployed controls are adequate to meet the control objectives. Based on *discussions with the management, survey of the application, questionnaires and available documentation,* auditor shall conduct a preliminary assessment of adequacy of controls across the select IS audit areas. Based on information collected and auditor's judgement, additional IS audit domains, and areas shall be included for risk assessment, to ensure that audit objectives are met. Auditors shall assess if the suitable mechanisms are in place for managing control risks. An illustration of such control risks is presented below.

Table 12: Illustration for preliminary assessment of adequacy of controls

IT domain	Audit area	IT issues/ sub-areas	Preliminary assessment of adequacy of IT controls
IT Governance	01 Business needs identification, direction and monitoring	IT requirements defined.	▶ Low (not well defined) ▶ Medium ▶ High (well defined)
	01 Business needs identification, direction and monitoring	Leadership	▶ Low (No IT steering committee) ▶ Medium ▶ High (IT steering committee involved in decision making

[55] In addition to annexures, auditors may refer to IT audit handbook by INTOSAI Working Group on IT Audit (WGITA) and INTOSAI Development Initiative (IDI) for further details on risk associated with various IT domains and areas.

IT domain	Audit area	IT issues/ sub-areas	Preliminary assessment of adequacy of IT controls
	01 Business needs identification, direction and monitoring	IT investments	▶ Low (no disciplined approach) ▶ Medium ▶ High (Disciplined approach)
	02 IT strategy and planning	Quality of IT strategy	▶ Low ▶ Medium ▶ High
	02 IT strategy and planning	Risk management	▶ Low ▶ Medium ▶ High
	03 Organizational structures, standards, policies, and procedures	Structure of the IT organisation	▶ Low ▶ Medium ▶ High
	03 Organizational structures, standards, policies, and procedures	Policy and procedures	▶ Low ▶ Medium ▶ High
	04 People and resources	HR and logistics	▶ Low ▶ Medium ▶ High
	05 Risk assessment and compliance mechanisms	Mechanism	▶ Low ▶ Medium ▶ High

**The same process has to be applied for all probable IT audit domains and areas under the purview of audit to ensure that the objective/s of overall audit is/are met.*

It should be noted that before arriving at the conclusion of control risk, auditor shall consider that there might be a pay off between the costs and the risks, which are acceptable to the auditee's management. For example, the management might consciously decide that offsite storage is not required in view of low risks, that are acceptable to the business. Hence, it is important for auditors to study the management perspective and laid down policy before audit comes to a conclusion of acceptable and unacceptable risks.

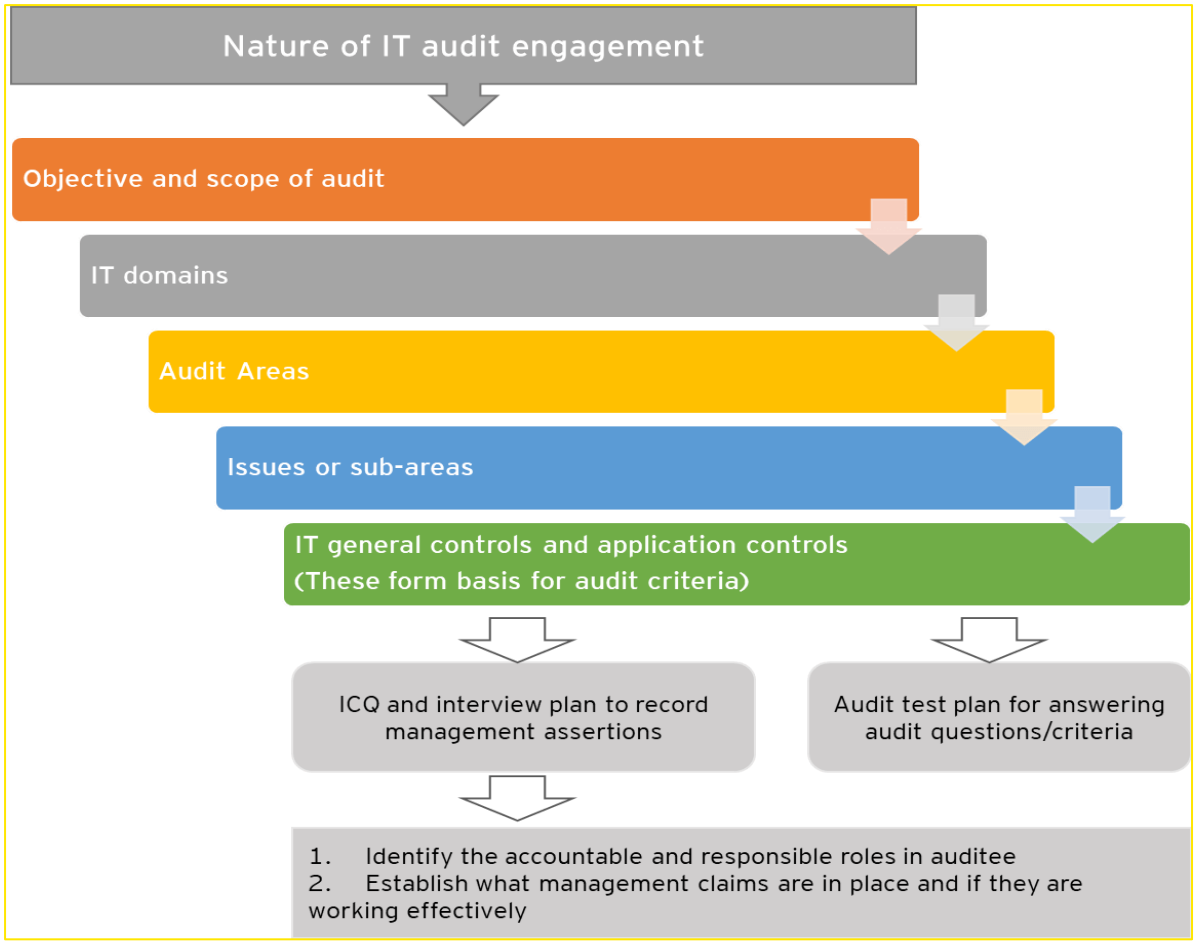
Based on the risk assessment, detailed audit objectives for audit of various IS audit areas/sub-areas are decided. It also helps in deciding nature, scope and extent of testing required. These aspects are covered in the Audit Plan.

2.3.2.3. Audit Plan

Audit plan is the scoping of the IS audit, based on the risk assessment as described above, which includes deciding the extent of audit scrutiny, the coverage of IT systems and their functionalities, IT processes to be audited, locations of IT systems to be covered, and the time period to be covered. It will be, essentially, setting or delineating the boundaries of the audit. The scoping is based on the risk assessment explained in previous section, where auditors shall identify the potential auditable areas. As mentioned earlier, the higher the assessment of inherent and control risk the more audit evidence the IS auditor should normally obtain from the performance of substantive audit procedures.

Scoping is performed through **IT domain cascade.** Through risk assessment, specific domain or a combination of domains, along with most critical audit areas and issues are identified, for including in the audit plan. This is based on understanding of risks associated with entity/IT system and preliminary assessment of adequacy of controls, in place to mitigate the risks. A diagram showing the mechanics of developing an audit plan is presented below.

Figure 8: Audit plan (mechanics): Scoping[56]



As discussed in section 1.7, the scope of audit will involve focusing on specific domains of the IT system which would be of relevance to the IS audit Objective. These domains would generally suffice for any IT System. However, as the field of IT is ever changing, IS auditors should not preclude possibilities of newer areas to be brought under scope of their audits, if found relevant[57]. Please note that, a comprehensive IS audit would involve examination *of all* the IT Domains.

Scope of audit depends upon the risk profile of the IT system being audited as well as the resources available with OAGN. If the risks are higher, the scope may have to be narrow but extensive in coverage within the scope of IS audit.

Based on understanding of entity/IT system and risk assessment, auditors, identify domains, areas and issues to be included in the audit plan. The criteria is based on the auditors' understanding of what measures should be in place for addressing the issues. Auditors shall record this information in related *audit matrices* (annexed) which they shall use as a work base for the audit and should extend as necessary.

[56] Based on WGITA/IDI IT audit handbook
[57] Chapter 9, Additional topics of interest, WGITA-IDI Handbook on Information Technology Audits for Supreme Audit Institutions.

An illustration of risk-based *selection* of IS audit domains, areas and issues is presented below. Auditors shall analyze, validate and optimize each selection and based on their relative importance include them in the IS audit plan.

Table 13: Audit planning (scoping): Domain, areas and issues- Illustration

IS audit Domain	Audit areas	Issue	Overall Risk	Include in audit?	Remarks, risks, etc.
IT Governance	01 Business needs identification, direction and monitoring	IT requirements	High	Yes	
		Leadership	Low	No	
		IT investments	High	Yes	
	02 IT strategy and planning	Quality of IT strategy	Medium	Yes	
		Risk management	High	Yes	
	03 Organizational structures, standards, policies, and procedures	Structure of the IT organisation	Medium	No	
		Policy and procedures	Low	No	
	04 People and resources	HR and logistics	Low	No	
	05 Risk assessment and compliance mechanisms	Mechanism	Medium	Yes	

Formal techniques, such as risk analysis or problem assessments, possible sources of evidence, auditability and significance of the issue considered, that can help in the planning process, can be recorded in the remark's column.

Audit matrix

Based on the analysis performed in earlier sections, audit matrices covering all the relevant issues for audit as per audit objective and scope of audit, shall be designed. An 'Audit Matrix' outlines important Audit issues, criteria etc. under different IS audit Areas, information required (potential evidence or sources for evidence) and method for analysis/testing for collecting audit evidence. This acts as a *guidance/base* for auditors for conducting the audit and testing the controls that the auditee has put in place to manage an acceptable level of risk associated with a domain and area and mitigate such risks. Audit matrix is used to collected evidence/findings during conducting IS audit.

This matrix should be prepared at the planning stage, though the contents can be updated during IS audit process, if necessary. Auditors can make necessary modifications to the audit matrix format as well, if they deem it necessary (e.g. to include substantive tests that may be required based on test of IT controls). Following format for an audit matrix shall be used for this purpose.

Table 14: Template for audit matrix

IS audit Domain: <<From audit objective and scoping>>
Audit area: <<Select based on scoping>>

Audit objective: <Objective of auditing the selected audit area>>	
Audit issue: <Based on risk assessment/scoping>>	
Criteria: << Assessment will be done against the criteria; expected controls to mitigate or manage risks associated with audit area and issue/sub-area >>	
Information required: <<for assessment against the criteria/ audit evidences/ sources of evidence>>	**Analysis method/s:** <<Enter method of analysis such as interview, analysis of documents or physical evidence, statistical analysis, focus groups discussions, etc. and tests as required for collected of audit evidences>>

A list of suggested audit matrices, for various IS audit domains is presented in the Annexures[58].

Logistical planning

During planning, it is also important to decide aspects of resource resourcing (including budget), planning and scheduling of audit.

For each of the audit issue, work will be assigned to the auditor/s from the audit team. Work shall be allocated to the auditor/s from the audit team based on their expertise and work experience. The number of man-days for which auditors are to be engaged shall be estimated and start date and end date for audit of audit areas shall also be assigned.

Location/s where the issue has to be checked by the auditor shall also be selected during this stage. It may happen that the IT system being audited is used by many offices/locations. In such cases, audit examinations should be spread over suitably, so that audit conclusions become more representative.

Audit of <XX> IT system for <<YY> Auditee										
Fiscal year:										
Start date of Audit:						End date of Audit:				
IT Domain	Audit Area	Audit objective	Audit Issue	Audit Criteria	Information required	Analysis methods	Assigned to	Location	Start date	End date

Contents of the Audit Plan

Audit plan shall largely include the following topics:

Contents of the Audit Plan
a) Introduction
b) Background on IT system and current status
c) Objectives of the (planned) IS Audit

[58] As per WGITA/IDI IT audit handbook

Contents of the Audit Plan
d) The need for IT audit of XXX system <<Justification for selection of IT system for IS audit. Please note that this justification can be arrived from the priority assessment conducted during Annual Audit Planning, as part of process for "selection of IS audit topics". >>
e) Policy and legal provisions applicable to operation of IT system
f) Other applicable provisions related to IT environment of entity
g) Auditee information: a. Brief description of organization goals, structure, regulatory env., IT systems, operations, etc. b. Major activities carried by the auditee using IT system c. Any observations for entity from previous or current audits d. Any other information relevant to the IS audit (such as PAC interest, issues highlighted by public, etc.)
h) **Brief of approach and methodology to be adopted for audit** <<planning, conducting, reporting and follow-up>>
i) Scope of audit a. Risk assessment conducted for scoping of audit b. Results of risk assessment <<Audit domain, areas and issues to be included in audit along with their risk scores>>
j) Brief of audit to be conducted a. For identified issues/questions, what is the objective and criteria? b. Brief of audit analysis/test methods/ sample selection for conducting audit c. Brief of information required for audit analysis
k) **Expected results/outcome of audit** <<As per the audit objective>>
l) **Audit team** <<including sub-contractors, if applicable>>
m) **Work allocation** << including sub-contractors, if applicable>>
a. Tasks assigned to each of the team member, along with tentative effort required b. Total man-days required for audit <<tentative>>
n) Audit Scheduling a. Audit period <<start date, end-date>> b. Day-wise tentative schedule of audit <<with day-wise key activities>> c. Scheduling of work of each team member for the audit period <<Activity to day mapping for each team member>>
o) **Estimated costs of audit** <<including operation expenditures and payment to sub-contractors>>
p) Budgetary provision/approval for IS audit <<As applicable>>
q) **Disclosures** on compliance to code of ethics, finalized terms of reference, supervision and review roles, etc., as applicable
r) Preparer, reviewer and approver comments and sign-off.
s) **Annexures (Audit matrices)**

Further guidelines for preparing audit plan

1. **Domains, audit areas, objectives and issues:** As discussed earlier, the auditable issues (scoping) should be identified based on the risk assessment of entity and its IT environment. Additionally, the overall audit objective also plays an integral role in defining the scope of the IS audit. E.g.
   - IS audit can be conducted in context of financial audit or compliance audit. In that case, the scope of IS audit, would largely depend on the objective of the overall financial or compliance audit, as discussed in earlier sections.
   - IS audit can also be conducted for assessment of entity's actions in procuring or developing new IT systems. In this case appropriate IT domains such as IT Governance and Development and acquisition, etc. shall be included in the scope of audit.
   - IS audit can also be conducted for a full performance audit of critical IT systems. Hence, scoping shall accordingly focus on relevant domains, areas and issues for audit.

However, In all the cases, auditable issues may arise from both the IT related and other IT governance issues.

2. **Criteria**: IS auditors should also identify evaluation criteria that should be measurable, reliable and consistent with the audit objectives/ issues being investigated by the IS auditor at this stage.

3. **Sources of information**: To satisfy the criteria, adequate information or evidence needs to be identified and collected in a manner that can be preserved for future reference to support audit conclusions. The collection of information may require specific tools and techniques. Different tools and techniques need to be identified and utilised, especially during the substantive testing stage .The analysis methods also are typical to the IS environment and need to be suitably utilised to derive relevant and meaningful conclusions. The typical sources of information in an organisation having IT Systems can be:
   - The flow diagrams including system flow diagram, data flow diagram, process flow diagram, etc.
   - System development documents such as the User Requirement Specification (URS) document[59], and System Requirement Specification (SRS).
   - Electronic data[60].
   - Other information available in the organisation related to its functions, control and monitoring systems etc. such as forms, budgetary information, different reports including reports from previous audits, external audits, internal reviews etc.
   - Policy, procedures, and other guidance.
   - The users of the system
   - The audited entities will also have their own combination of hardware, operating system, database management systems, application software and network software. IS auditors should be able to gather information from these sources to carry out their analysis (sample data collection formats annexed).

4. **Selection of Analysis methods/s**: Depending upon the objective of the audit, Auditors may be concerned with the design, implementation and/or operating effectiveness of controls. Where the Auditor is concerned with the design of the control, an interview or inspection of documented business rules may be sufficient. Where the Auditor is concerned with the implementation of controls, inquiry may not be sufficient, and it may be necessary to conduct a walkthrough or perform data analysis to substantiate that the control as designed has been implemented. Finally, if the Auditor is concerned with the operating effectiveness of the control, (s)he may be required to test a sample of transactions to demonstrate that the control has operated effectively throughout the relevant period[61].

5. **Testing strategy for test of application controls**: While testing application controls the auditors need to:

a) Identify the significant application components and the flow of information through the system and gain a detailed understanding of the application by reviewing the available documentation and interviewing appropriate personnel. Since a full-fledged ERP systems may contain many modules covering various

---

[59] URS – User Requirement Specification Document contains requirements that show the functions of the organisation that the IT system is supposed to carry out and the end user operability desired. This is the stage where a complete and clear delineation of user's requirements should be specified by the users. A deficient user requirement specification may ultimately lead to development of a deficient system. This is a good starting point for the IT Auditor.

[60] Electronic data would include structured data where the most common ones are Relational Database Management Systems (RDBMS) that are capable of handling large volumes of data such as Oracle, IBM DB2, Microsoft SQL Server, Sybase, and Teradata.

[61] GUID 5100 para 6.7

processes, the auditor may limit the scope of the modules and functionalities to be tested based on objective and scope of the audit. Hence, only relevant business processes in the IT system shall be studied.

For example:
A usual Integrated Financial Management system has many modules such as budget management, expenditure management, revenue management, accounting, cash and bank management, treasury, procurement, human resource management, cadre management, project sanctions, audit, etc. Hence, if the objective of IS audit is to check compliance of IT system with procurement laws, then auditor may limit the scope of audit to procurement module and only linkages with other modules of master data, budgeting, expenditure, projects and accounting. In this case, audit of other modules such as HR, cadre, revenue, etc. and even complete audit of linked modules is not required.

b) Understand the application control risks and their impact by reviewing the criticality of the business process that the application segment is affecting.
c) Develop a testing strategy to identify the control strengths and weaknesses and evaluating the impact of the weaknesses.

For developing a *testing strategy* auditors shall study related documentation such as the functional design specifications, change management documentation since the first deployment or the last audit, user manuals, vendor-supplied technical reference manuals, etc. The testing strategy would also depend on factors like assets at risk, the time in existence of the application in support of the business, quality of internal controls, sensitivity of transactions, significant business process changes resulting in changes in the application, and previous audit results, if any.

For example:
For assessing Segregation of Duties (SoD) and input authorization, it would be important to review job descriptions for various user roles and match them to privileges assigned to roles in the system. Also review authorization procedures and confirm existence of action logs of user accounts having administrator privileges in the system. Audit trail or system logs can also be checked for evidence of managerial review and deviations, if any.

3. Conducting IS audit

In case IS audit is part of a larger audit viz. Compliance Audit or Performance Audit or Financial Audit, it shall be conducted as per the process described in respective manuals/guidelines. However, audit steps to be followed, specifically in context of an IS audit (issues) are presented in this section.

3.1. Authorization letter

OAGN shall issue audit authorization letter for the audit team, addressed to the auditee. The authorization letter shall include the following:

- Tentative date audit shall commence
- Details of field audit team

In addition, the authorization letter shall include request to the auditee to provide the audit team with:

- Access to all information that is relevant to the audit of IT system, including access to records and information
- Additional information that auditor may request from for the purpose of the audit; and
- Unrestricted access to persons and IT system/s within the auditee for the purpose of obtaining sufficient and appropriate audit evidence.

As per GUID 5100 para 6.2

Specifically, for an IS Audit, Auditors may solicit due cooperation and support of the audited entity in completing the audit, including *access* to records and information. Auditors may identify mode of access to electronic data in the format necessary to allow analysis, in consultation with the audited entity. The mode of access to data would be SAI specific.

3.2. Entry meeting

The entry meeting shall be conducted at the beginning of audit as a formal audit commencement meeting. The entry meeting shall be an opportunity for auditors to apprise the auditee management of the broad objectives of the audit, proposed timelines for audit, key audit areas to be undertaken for audit, and communicating any other areas of concern based on previous audit findings. It shall also be an opportunity for OAGN auditors to fine tune the objectives of audit, based on management concerns and perceptions regarding the IT system. This shall allow clarification of certain issues and underlying business concerns, if any, and help the audit to be conducted smoothly besides appraising the entity of the data, information and documents that will be required by the audit team. The audit entry meeting can also be used as a platform to discuss and communicate with the management and those charged with governance, the terms and conditions of the audit engagement. In summary, the Entry meeting is conducted to achieve the following purposes:

- introduce members of the audit team to auditee's management;
- determine appropriate persons within the auditee, with whom to communicate;
- determine the matters that need to be communicated:
  - responsibilities of the auditee management and the auditor team, as it has been agreed in the engagement letter and included in the audit authorization letter;
  - planned objective, scope and timing of the audit; and
  - auditor independence;
- establish the communication process (the process, form, timing and adequacy). It is essential the effective communication throughout the audit process be established.

Minutes of the entry meeting shall be documented as part of audit documentation.

3.3. Evidence collection

Audit evidence is the collection of data, records, documents, and information by the IS auditors to substantiate their observations to the relevant stakeholder(s), at the relevant time period (at the time of audit or subsequently), sufficiently, reliably, and correctly. The IS auditor shall gather appropriate and sufficient audit evidence and analyse the same to ensure that the audit objectives are adequately addressed. Please note that methods for collecting evidence (analysis methods), and information sources are decided while planning the audit in audit matrices and can be updated during the audit based on further information available to auditors.

Audit evidence can be collected using an appropriate combination of the many techniques such as Interview, Questionnaire, Observation, Walk Through, Flow charts, Data Capture and Analysis, Verification, Re-computation, Reprocessing, and Third-party confirmation[62].

The types of audit evidence, could largely be in form of:

- Observed process and existence of physical items
- Documentary audit evidence including electronic audit evidence (e.g. electronic records)
- Data Analysis/tests (including analysis from CAATs e.g. from IDEA)

3.3.1. Methods for collection of audit evidences

a. **Physical evidence**: Physical evidence is obtained by observing and should be corroborated by the auditee, particularly in case it is crucial for the audit findings. Physical verification is also important in case physical access controls are been checked for unauthorized access to computers, terminals, and also for visual verification of safety equipment at computer centers.

b. **Interviews**: Interviews can be used for both qualitative and quantitative information collection during evidence collection. Auditors can interview various user groups such as system analyst and programmers, data entry staff, users of the IT systems, and operation staff. For interviews it is important that the auditors should take care of the following points:
   - Ensure that information that is to be collected from interviews is not available elsewhere
   - Ensure that objective of the interview is clear, and questions are prepared accordingly. General information can be asked during the beginning of the interview and specific information afterwards.
   - Ensure that right interviewees are identified, and they are available on the scheduled date and time
   - Ensure that after each interview, the information collected is recorded. Care should be taken to separate facts from opinions and also determine how the information can be used to meet the audit objectives.
   - MoM of each interview shall also be signed off by the interviewees.

c. **Questionnaires**: Questionnaires can also be used to collect information from a large set of respondents such as application users. Questionnaires can be used to access system effectiveness based on user responses and also for identifying system weaknesses, that could be further looked into. While preparing questionnaires, auditors shall ensure that:
   - Questions are specific with close ended answers
   - Questions are clear and instructions, if required, for answering the questions are also mentioned
   - Language of questions should be as per the target respondents. E.g. questions to IT administrators may be technical in nature whereas questions to users, should be in simple language.
   - Questions shouldn't be ambiguous, leading, presumptuous, hypothetical or un-professional.

[62] Ref: GUID 5100 para 6.5

d. **Flowcharts**: Flowcharts are typically used to visually represent a process, associated controls and identify control weakness in the process. Auditors should be well versed in techniques for preparing and evaluating flowcharts. Flowcharts, act as an important tool for visually communicating to the auditee, control weakness in the IT processes or getting confirmation from auditee on the identified control weaknesses.

e. **Electronic data**: Electronic data can also be received from the entity to form audit evidences. Auditors shall ensure that the electronic evidence collected and documented is sufficient, reliable and accurate to sustain the audit observations. Such electronic evidence may consist of data files, user logs, analytical models, Management Information Systems (MIS) Reports, etc. and shall be appropriately gathered and stored in a manner such that they are available for drawing assurance on the accuracy and validity of the audit process. The evidence gathered during an IS audit shall have necessary timestamps and details containing steps of data analysis carried out, so that there is clarity on when the evidence was created, stored and last modified, to mitigate the risk of subsequent changes[63].

   In case of receiving data dumps[64] from the audited entity, Auditors shall ensure that each data dump is accompanied by a letter from the audited entity. Such a forwarding letter shall specify[65]:

   - The source (through reference to time stamp of generation of the data dump/ hash number for the data dump) of the data for the purposes of ensuring integrity of data, authentication[66] and non-repudiation[67]
   - The parameters of extraction used to create the data dump, i.e. queries used/ reports run.
   - If such a forwarding letter from the audited entity is not received, internal documents may be generated by the Auditors noting important information such as the date on which the data was handed over, from what file the data dump was created, and whether the data was from the production environment or from some other environment, etc.

f. **Third party reports**: Evidence can be collected from third party audit reports also. In case of examination of technical Reports prepared by third party auditors on technology specific subject matters, Auditors shall adopt appropriate procedures to draw assurance on compliance, financial or performance aspects of such Reports. If, as a result of such procedures, reliance is placed on the contents of such Reports, the fact of reliance shall be suitably disclosed in the audit report[68].

g. **Analytical procedures**: Analytical procedures can be used for checking if certain transactions in the IT system appear reasonable or not and whether they require testing. Various analytics methods such as regression, trend analysis, etc. can be used for identifying transactions or accounts that need further verification or investigation and also areas which don't. Hence, Analytical procedures shall be performed early in the audit to optimize audit work.

Understanding of the IT System and database in the organisation is clearly an essential step before data extraction (for analysis). IS auditors should decide on the appropriateness of the use of one or more of the above techniques and ensure that they are satisfied with the integrity and usefulness of the technique. The use of any of the techniques should not impact the integrity of application system and its data at the audited entity. Data gathering techniques should be based on risk assessment carried out by the audit team, as well as the time and resources available for the audit.

---

[63] GUID 5100, para 6.12
[64] Data dump is defined as a large amount of data transferred from one system or location to another
[65] Ref: GUID 5100 para 6.4
[66] Authentication is defined as the act of verifying the identity of a user- ISACA Glossary of Terms
[67] Non-repudiation is defined as the assurance that a party cannot later deny originating data; provision of proof of the integrity and origin of the data and can be verified by a third party. A digital signature can provide non-repudiation – ISACA Glossary of Terms
[68] GUID 5100 para 6.14

3.3.2. Test of IT controls

Auditors shall conduct procedures[69] to examine the reliability and sufficiency of IT controls (general and application). This can be done through methods of collecting audit evidences mentioned above or through specific tests such as compliance tests. Based on the test of controls, auditors shall decide priority areas to be undertaken for substantive testing of the IT controls. Various methods for test of IT controls, across IT audit domains and areas, are presented in the Annexures as part of audit matrices (analysis methods).

Depending on the scope of audit, as discussed in planning stage, test of IT controls, may include examination that[70]:

- IS Policy has been defined, adopted and communicated
- IS Governance structure is in place and is functional
- Inventory of IS assets has been periodically carried out and requirements for augmentation, replacement and removal have been identified
- Processes for sharing of infrastructure and common services for information systems with other public entities are in place and functional
- Processes for development, acquisition and maintenance of Information Systems have been defined, adopted and communicated (including that of change management)
- Processes for IT Operations (in-sourcing, out-sourcing, service agreements) have been defined, adopted and communicated
- Measures to ensure physical security and intended physical working conditions have been adopted.
- Measures for training and sensitization of human resources to ensure confidentiality, integrity and availability of information as well as compliance with the IS Policy and Governance structure requirements, have been adopted
- Measures to ensure confidentiality, integrity and availability of various communication modes and channels have been adopted
- Measures for Information Security Management have been adopted Measures for Statutory Compliance Management have been adopted
- Measures for Business Continuity and Disaster Recovery Management have been adopted
- **Application Controls** adopted within each information system are adequate and reliable. For this auditors need to have an understanding of the business process, mapping of the business process onto the IT system and the associated IT application controls. Such an assessment shall include the identification of significant application components, identification of the criticality of the application to the entity, review of available documentation, interview of personnel, understanding of application control risks and their impact on the entity, and development of tests to examine the adequacy and reliability of such application controls.

The assessment of general and application controls shall therefore cover the audited entity's Policies, Processes, People and Systems, in line with the IS Audit objectives[71].

---

[69] Before performing procedures, auditors should ensure that they have an understanding of the system architecture, and the underlying data and its sources. This understanding should have been developed from the planning stage, based on which required audit tools and techniques for audit analysis have been selected in the audit matrix. Auditors shall also have understanding of general IT controls and business processes, mapping of business processes onto the IT system and the associated IT application controls. In case, there is a change in understanding during conducting IT audit, the required audit tools and techniques may be revisited. This would also lead to decision on substantive testing of the IT system and its controls.

[70] GUID 5100 para 6.5

[71] GUID 5100 para 6.6

Compliance tests[72] are concerned with testing the transactions (in application) for compliance with rules and regulations of the entity and provide auditors with evidence about presence/absence of internal controls. Compliance tests can be used to test the existence and effectiveness of a defined process, which may include a trail of documentary or automated evidence. Some examples of compliance tests as they relate to the IT environment include:

- Determining whether passwords are changed periodically (as per password policy)
- Determining whether system logs are reviewed
- Determining whether program changes are authorized
- Determining whether controls are functioning as prescribed
- Determining whether a disaster recovery plan was tested

Results of compliance tests also determine the *extent* to which substantive tests may be carried out. Strong controls revealed in the compliance tests can limit the substantive tests and vice versa.

Auditors shall also consider how the evidence about the general controls impacts the nature, timing and extent of evidence required to obtain assurance about the operation of application controls. If the Auditor has obtained sufficient and appropriate audit evidence regarding the effectiveness of the general controls that support the logical access of personnel to IT systems and change management within the production environment, (s)he may be able to conclude on the operating effectiveness of automated application control procedures. This can be done by testing a smaller sample of transactions because the effectiveness of the general IT environment provides evidence to the auditor on the effectiveness of the application control in the relevant period. In case of manual application control procedures, Auditors may have to test a sample size appropriate to the confidence level selected[73].

3.3.3. Sampling

Audit sampling is the testing of selected items within a population to obtain and evaluate evidence about some characteristic of that population, in order to form a conclusion concerning the population. Auditing in an IT environment may facilitate the analysis of 100 percent of a population, especially at the preliminary assessment stage. However, for carrying out Substantive Testing, samples may be necessary since audit *efficiency* relies on obtaining the minimum audit evidence, sufficient to form the audit opinion.

Auditors may not always be in a position to examine all instances, transactions or modules or IT systems, given resource constraints and the cost-benefit trade-offs of the audit exercise. In such a situation, based on *materiality* considerations, auditors shall adopt audit sampling for detailed examination, to draw reasonable audit conclusions. Auditors may use CAATs (e.g. IDEA) for carrying out different types of sampling, and determine an appropriate sample size, depending on the underlying Inherent and Control Risks. Audit samples[74] are drawn in order to provide the auditor with a reasonable basis on which to draw conclusions about the entire population of data, on the basis of conclusions drawn from the application of audit procedures and analysis to the audit sample. Auditors may consider the purpose of the audit procedure and the characteristics of the population from which the sample will be drawn and determine a sample size sufficient to reduce sampling risk[75] within an

---

[72] Tests of control designed to obtain audit evidence on both the effectiveness of the controls and their operation during the audit period (ISACA Glossary)
[73] GUID 5100 para 6.8
[74] ISSAI 2530, Financial Audit, Audit Sampling, Sections 6 to 9
[75] Sampling risk is the chance that the sample will not be representative of the population it is drawn from. A false positive error occurs when the auditor believes a control is working or an account balance is correct when in fact the control is not working, or the account balance is incorrect. A false negative occurs when the auditor

acceptable level. When doing IS audit within the scope of Financial Audit, procedures for sample selection defined in Financial Audit manual shall be used[76].

It is important that the items selected should be representative, in order to be able to form a conclusion on the entire population. For example, projecting results of tests applied on only those items having a specific feature, such as high value items only, on the whole population, would give skewed results.

Statistical and non-statistical sampling

Two general approaches to audit sampling are **statistical sampling** and **non-statistical sampling.** Non-statistical sampling is based on auditors' judgement of material and risky items/transactions. In this case, auditor shall decide, the method of sampling[77], the sample size (how many number of items to be examined from the entire population) and which items to be selection (sample selection)[78]. Under non-statistical sampling, there are two primary methods: **Attribute sampling** and **Variable sampling.**

- **Attribute sampling** is generally used in compliance testing situations and deals with the presence or absence of the attribute and provides conclusions that are expressed in rates of incidence. E.g. all procurements above XX amount not having an approved PO (as required by procurement law). It should be used when the question of "how many" is important and to determine the characteristics or "attributes" of a population.
- **Variable sampling** is generally applied in substantive testing situations and deals with population characteristics that vary and provides conclusions related to deviations from the norm. It is used to answer the question "how much" and applied to populations that usually consist of monetary values such as NPR. E.g. Variable sampling can be used to predict the average salary paid to employees belonging to the same salary band or average value of suppliers' bills paid by an office during a month, or average collections made by a tax collection office in a day/month.

Statistical sampling is a method of selecting a portion of a population, by means of mathematical calculations and probabilities, for the purpose of making scientifically and mathematically sound inferences regarding the characteristics of the entire population[79]. Statistical sampling may be used in different auditing situations. There are different ways in which a statistical sample can be selected. The most frequently used method is random selection where each item in the population has an equal chance of selection. Simple random sampling ensures that every number of the population has an equal chance of selection. It is useful for testing internal controls. For example, the auditor may decide that if there are errors above a certain threshold the control systems are inefficient. The sample could be selected using random numbers through computers. CAATs software such as IDEA can also be used for sample selection. Once the sample is selected, identified audit tests are to be applied on the sample.

3.3.4. Substantive testing

Based on assessment of IT controls and compliance tests, Auditors shall identify priority areas for Substantive Testing, which involves detailed testing of the IT controls by employing various Computer Aided Audit Techniques (CAATs) such as IDEA for *enquiry, extraction and analysis of data*. During substantive testing the tests are designed to substantiate the assertions as per audit objectives. Substantive tests provide auditors with

---

believes a control is not working or an account balance is incorrect when in fact the control is working, or the account balance is correct.

[76] Ref: GUID 5100 para 6.11

[77] Random, systematic, cluster or stratified sampling.

[78] For further guidance on sampling, IS auditors may refer to Information Technology Sampling Guidelines (Guidelines 2208) created by ISACA.

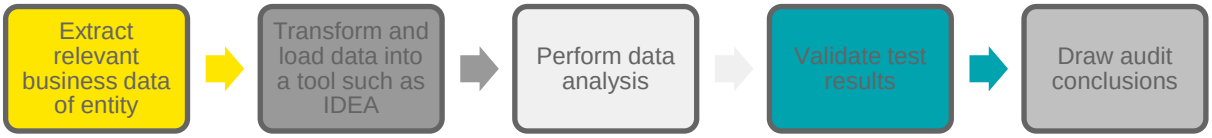
[79] ISACA Glossary

evidence about the validity and propriety of the transactions and balances. Auditors use substantive tests to test for monetary errors directly affecting financial statement balances. Auditors shall design and execute substantive testing in order to substantiate the audit objectives. Some examples of substantive tests as they relate to the IT environment include:

- Conducting system availability analysis
- Performing system storage media analysis
- Conducting system outage analysis
- Comparing computer inventory as per book vis-à-vis actual count
- Reconciling account balances

Auditors can use CAATs such as IDEA software to execute various IS audit techniques such as such as User Log Analysis, Exception Reporting, Field Wise Totalling, File Comparison, Stratification, Sampling, Duplicate Checks, Gap Detection, Ageing, Virtual Field Calculations etc. Advantages of use of CAATs/IDEA include analysis of large volumes of data, repeatability of tests on different data sets and with different criteria and automated documentation of audit tests and results with timestamps[80]. Typical steps in substantive testing of adequacy of application controls are:

Figure 9: Steps in substantive testing using CAATs/IDEA



Data analysis: Most analysis can be executed straight from a working data file. Some analysis may require transformations of the raw data, subsets, or specific input data to comply with statistical software such as IDEA. IT systems use many different data types and representations (numeric, string, alpha, etc). The IS auditor should be cognisant of these and use the appropriate tools for analysis. The auditor can use CAATs/IDEA to carry out the information analysis. Other tools such as Microsoft Excel, Microsoft Access, Power BI, etc. also provide the facility to import as well as analyse data. Any of the following techniques can be used by the IS auditor for data analysis:

a. Obtaining a copy of data (data dump) from the audited entity and running analysis on data analysis software (e.g. IDEA). Special care is to be taken to convert copy of data into a format that is readable in the analytics software.
b. Performing tests in the IT system, by use of test data. The premise is that it is possible to generalize about overall reliability of a programme if it is reliable for a set of specific tests. Care should be taken that the testing doesn't affect the integrity of the entity's system or its data.

For further information on techniques for data analysis process, please refer to Annexure 5 – Data Analysis Techniques and usage of CAATs**.** Usage of CAATs for performing audit procedures, is also discussed in subsequent section.

3.3.5. Usage of CAATs for performing audit procedures

CAATs (such as IDEA) can be used for performing multiple audit procedures, such as:

- for testing details of transactions and final balances in the IT system. E.g. CAATs can be used to recalculate, tax deductions made on a vendor bill for payment and check if it matches with the system (e.g. TSA) records.

[80] GUID 5100 para 6.10

Similarly, other calculations, made by the systems can be checked in the CAATs. This is called parallel simulation.

- for identifying, significant fluctuations or inconsistencies in the financial transactions. This can be done by designing analytical procedures. E.g. An analytical procedure can be defined for checking payments to the same vendor in a select period of time, that are XX% higher than the average payment made to the vendors in the prior periods. Other example could be, checking total amount of advances made to an employee and if it exceeds the policy criteria and checking if the advances were settled within policy guided time period.
- for preliminary risk assessment during planning stage. Since, IDEA will run on the data collected from external systems such as LMBIS, TSA, BMIS, SuTRA, etc. in NAMS, it can be used to identify potential control weaknesses based on analysis of the transactions. This will help auditors in design of audit plan for the auditee.
- testing general controls such as testing the setup of configuration of the operating system on which the system runs or access procedures to program libraries
- creating sampling programs to extract data for substantive audit testing.
- testing application controls for example by replicating a business rules in CAATs and checking if the output is same as in the application.
- CAATs can also be used to validate programmes/systems through techniques such as program code review, program code comparison, parallel simulation, tracing programs, etc.

Similarly, IS auditors can design various audit procedures while analysing data through CAATs/IDEA depending on the type of system being audited. For example, while auditing a payroll system, IS auditors can use CAATs to check: if duplicate employee names, address, phone number, etc. exists in the personnel records, or check if salary is paid to employee which has left the organization, or compare salary paid to employee against the approved salary band for that designation, or check if deductions and allowances are as per the allowable rules, or reconcile payments made to all employees under an office with the total salary charged by that office against the salary head for a particular month, etc. Similarly, while auditing an inventory system, auditors can check if invoices were raised against an approved PO, or match invoice and PO amounts, or compare deviation between actual and standard costs, or conduct high value item analysis, or select a sample of stock for reconciliation, or test duplicate records of the same item, etc.

Usage of CAATs has many advantages over manual examination such as:

- Easier sample selection from large volume of data
- Substantive testing and analysis of large volumes of data can be done within a short span of time and with less effort
- Tests can be repeated easily on different files/data
- Flexible and complex tests can be done with change in parameters
- Automated Documentation of audit tests and results
- More efficient deployment of audit resources

However, since usage of CAATs requires appropriate skillset and effort, there are some factors which should be considered before using CAATs for IS audit, such as:

- Does the use of CAATs provide additional value to audit?
- Are the tests going to be repeated in other/future audits of the same auditee or other auditees whose nature of business and operations are similar?
- Are the transactions processed on-line and/or real-time?
- Will the use of other audit techniques entail higher costs and extra time?

In order to use CAATs to audit a particular area, the auditor should plan in detail. It is important to understand and obtain information/details about tables/files relationships, database dictionary/triggers, record layout, control totals, data size/format, and system documentation, before commencing a CAATs enabled audit. It is also important to include auditors skilled in usage of CAATs in the audit team. For further information on usage of CAATs for application program review and data analysis, refer to Annexure 5 – Data Analysis Techniques and usage of CAATs.

3.3.6. Documentation of specific items tested

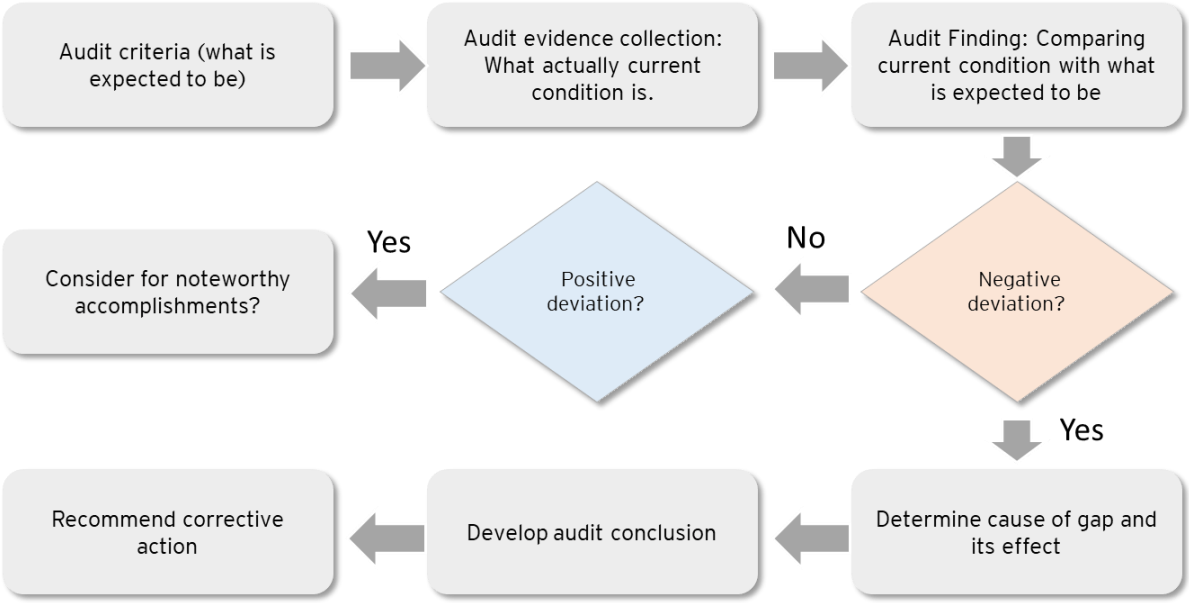
The auditor should record the identifying characteristics of the specific items tested. This demonstrates the accountability of the audit team for its work and facilitates the investigation of exceptions or inconsistencies. Identifying characteristics to be documented will depend on the nature of the audit procedure and the subject matter. For example,

- a detailed test of system generated purchase orders may require documenting the selected transactions by their dates and unique purchase order numbers.
- whereas, for a procedure requiring selection or review of all items over a specific amount from a given population, the auditor may record the scope of the procedure and identify the population, e.g. all receipts above NPR 50,000.
- for a procedure requiring inquiries of specific entity personnel, the documentation may include the dates of the inquiries and the names and job designations of the entity personnel preferably in form of Minutes of the Meeting.
- for an observation procedure, the documentation may identify the process or subject matter being observed, the relevant individuals and what they were responsible for, and when the observation was carried out.

3.4. Evidence evaluation

The process for evaluating audit evidence and arriving at conclusions and forming recommendations is presented in the figure below.

Figure 10: Audit findings, conclusions and recommendations



3.4.1. Audit findings

After collection of evidence, the observed conditions are to be compared against the audit criteria, mentioned in the audit matrices, to arrive at audit findings. The steps involved are:

- Based on evidence collected, auditor should assess, if the current situation falls short of the audit criteria
- Auditor shall also find the cause of such deviation of current situation from criteria. This will help in identifying the corrective action
- Auditor shall also judge the consequence of current condition falling short of the criteria. The same shall be reported in the audit report (impact). The consequence shall be reasonable and logical.
- Based on the evaluation of audit evidence and discussions with the auditee, auditor shall prepare the draft recommendations for improving the condition.

The audit team and the audit director (Team leader) shall ensure that appropriate evidence on non-adherence to criteria is collected, documented and discussed with the appropriate levels of auditee's management.

Table 15: Recording audit findings

Domain: IT Governance				
Audit area: Strategy and planning				
Issue	**Criteria**	**Audit finding**	**Link to evidence**	**Relevant**
Risk management	Risk management policy <<From audit matrix>>	<<As per evidence collected>>Current condition, Cause, Consequence	Documents, information, acts/rules, electronic data, result of tests/audit analysis.	Yes/No

As findings, auditors shall report on the effectiveness of design, implementation and operations of controls as per the audit objective. They shall also mention details of tests performed for collection of audit evidences and arriving at audit findings.

3.4.2. Audit conclusions and recommendations

Audit findings, conclusion and recommendations must be based on audit evidence. In formulating the audit conclusion or report, the IS auditor should have regard to the materiality of the matter in the context of the nature of the audit or audited entity[81]. IS auditors should frame conclusions on the audit findings based on the audit objectives. The conclusions should be relevant, logical and unbiased. Sweeping conclusions regarding absence of controls and risks thereon should be avoided, when they are not supported by substantive testing. For e.g. "absence of IT Policy may lead to haphazard IT development in an organization and it may lead to mismatch between hardware procurement and software development" cannot be an audit conclusion even if audit discovers that an organization does not have an IT Policy. Audit should further examine whether it has actually led to haphazard development and whether such development can be ascribed to lack of IT policy and if so, in what way.

IS auditors should report recommendations when the potential for significant improvement in operations and performance is substantiated by the reported findings. Auditors should also report the status of uncorrected significant findings and recommendations from prior audits that affect the objectives of the current audit. Constructive recommendations can encourage improvements. Recommendations are most constructive when they are directed at resolving the cause of identified problems, are action-oriented and specific, are addressed to parties that have the authority to act, are feasible, and, to the extent practical, are cost-effective. For balanced reporting, noteworthy accomplishments may be reported on.

It is important that the conclusions are tested against evidence collected and discussed with the auditee in the "exit meeting" to get inputs and validate its correctness and completeness.

3.5. Exit meeting

Exit meeting is conducted to ensure that the audit findings and recommendations are discussed and agreed with management and, where relevant, those charged with governance. Exit meeting also reduces the risks of misunderstanding between the management and the auditor at a later stage on issues reflected in the draft IS audit report. Exit conferences also help in finalizing recommendations which are practical and feasible, based on discussions with the auditee. The significant findings are communicated to the auditee management during the exit meeting. Before communicating findings to the auditee management, they have to be reviewed by the Team Leader and AAG in-charge of the IS audit directorate.

As part of audit documentation, the auditor and management should maintain the minutes of the exit meeting detailing the discussions of the auditor's report (first draft) and the specific audit findings, and the decisions reached on findings, and recommendations, as applicable.

[81] Derived from ISSAI 100 para 54

4. Reporting on IS audit

4.1. Reporting considerations for IS audit

This section described reporting considerations for IS audit depending on the type of IS audit undertaken by OAGN.

Table 16: Reporting considerations for IS audit

Type of IS audit engagement	Reporting procedures
Separate IS audit	IS audit report shall be issued to the auditee as per the procedures described in IS audit manual
IS audit in context of FA	IS audit report will be shared internally with the financial auditors (other applicable directorates) of OAGN. In the IS audit report, IS auditors shall mention how the results of the IS audit work may be relevant for the Financial Audit. The findings of the IS audit report (weaknesses in IT control environment) will act as an input for other directorates for planning, conducting and reporting the financial audits. As discussed earlier, the results of IS audit may impact the overall audit strategy, audit plan and procedures for test of controls for FA, which in turn may impact the opinion presented by auditors in the final Auditor's report.
IS audit as a subject matter for CA or PA	Reporting requirements will be as per the CA or PA reporting requirements, since the overall objective of IS audit, in this case, will be derived from the subject matter of CA or PA.

As per GUID para 7.1

Since an IS Audit engagement would be either a Financial Audit (ISSAI 200), Performance Audit (ISSAI 300) or Compliance Audit (ISSAI 400), Auditors may consider the reporting requirements accordingly. This would be SAI specific. Similarly, each SAI may have its own reporting thresholds based on materiality of the audit findings. Likewise, an Auditor, while reporting upon an IS Audit engagement may consider the statutory and internal limitations on disclosure of financial and technical information.

As per GUID para 6.15

The ISSAIs provide that the auditors should establish effective communication throughout the audit process and keep the audited entity informed of all matters relating to the audit (cf. ISSAI 100 paragraph 43). In audits that involve IS Audit work the result of the IS Audit may in some cases, be communicated to the entity through the means of a separate letter. In these cases, it may be important to explain how the result of the audit work relates to other communications which are part of the same financial, performance or compliance audit and how the results of the IS audit work may be relevant for the resulting SAI audit report.

4.2. Types of IS audit Report

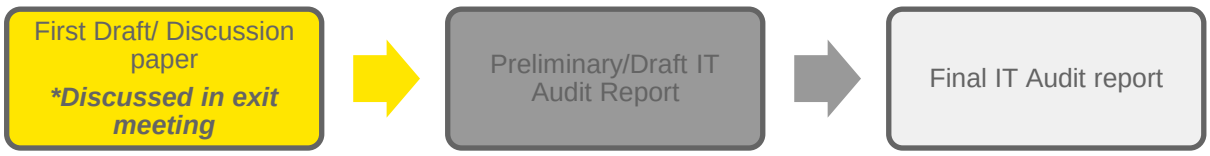
For IS audit, the significant findings need to be communicated to auditee (management) during the exit meeting in form of a **first draft or discussion paper**. The first draft needs to be reviewed by the Team leader or equivalent authority and AAG before it can be presented in the exit meeting. Auditors should also report the status of

uncorrected significant findings and recommendations from prior audits that affect the objectives of the current audit.

After the exit meeting, a formal **Preliminary Audit Report/ draft IS audit report**, will be issued to the auditee. This report shall also include recommendations made by the auditor to resolve the audit findings/observations. The report shall be reviewed by the Team leader/Audit Director and AAG in-charge of the IS audit Directorate.

Auditee management shall then respond to (the findings) in the Draft IT audit report, after which **Final IS audit report** will be prepared by the OAGN. It is the final audit report that may be accessed by the legislature and can be published for access by the public.

Figure 11: Types of report



1) **First draft or discussion paper**: The reporting process begins with the discussion of the first draft (discussion paper). This draft shall be sent to the auditee prior to the exit meeting. The draft is then discussed in the exit meeting with the auditee management. This allows any inflammatory wording, factual errors and/or inconsistencies to be identified, corrected or eliminated at an early stage. Once the auditee and the auditor have discussed the contents of the draft audit report, the auditor shall make the necessary amendments and prepare the Preliminary/Draft IS audit Report.

2) **Preliminary/draft IS audit Report**: This report is the formal draft given to the auditee so that they can respond to the observations raised in the report. It is prepared based on the exit meeting. It has to be issued to the auditee within <3 days> of the exit meeting. After its issuance, it is the duty of management to formally address all the findings in the Preliminary/draft IS audit Report.

3) **Final Audit Report**: When auditee's comments are received, the auditor then prepares a response indicating the audit position. This is achieved by putting together the auditor's comments and the auditee's (Management) response in one report, which is the Final Audit Report. The auditor should review each response received to determine that timely corrective action and adequate detail have been provided for each finding of the report.

Auditee's management is expected to provide their response to OAGN within <35 days> of issuance of Preliminary/draft IS audit report to them, subject to extension granted, if any (by the OAGN). In case auditee fails to respond within the set timelines, the same issues need to be incorporated in the final report, mentioning that no management response was received.

4.3. Considerations while preparing the IS audit report

- Auditors shall be aware of the need to limit the use of technical jargon, and of the sensitivity of the information presented (e.g. passwords, usernames, ID, and personal information), in the report. Despite the technical nature of an IS Audit, Auditors shall ensure that the report is fully understandable by senior management of the audited entity, the stakeholders, and the general public. Auditors shall incorporate an

appropriately detailed glossary of terms in Reports, which cross references the definition of an acronym or a term with a scenario-based explanation of how this operates in a controlled environment[82].

- Auditors shall consider the potential negative impact of the report once the IS Audit report is published. For example, if the IS Audit report detects some security risks in the information system of an audited entity and the same are reported before necessary controls to mitigate the risks have been adopted, the vulnerability of the information system may be exposed to the public. In such a scenario, Auditors shall consider options such as reporting only after the necessary controls have been adopted, or not reporting the exact security risk in full, in order to avoid potential adverse impact on the audited entity[83].

- By their nature the audit reports tend to contain significant criticisms, but in order to be constructive they should also address future remedial action by incorporating statements by the audited entity or by the auditor, including conclusions or recommendation[84].

- In case IS auditors and the auditee unit disagree about a particular recommendation or audit comment, the Audit Report may state both positions and the reasons for the disagreement as an appendix. Alternatively, the auditee's views may be presented in the body of the report or in a cover letter.

4.4. Structure of the IS audit report

The format for contents for the IS audit report is presented below.

- **List of Acronyms, Glossary**
- **Executive summary**
- **Introduction**
  - **Description of IT system to be audited**
  - **Audit objectives and scope**
  - **Applicable Policy and legal provisions**
  - **Audit methodology (***used in order to complete the audit***)**
- **Summary of findings**
  - **For each audit domain**
    - **For each audit area under an audit domain**
      - **Criteria**
      - **Audit observation/findings <<***shortfalls against criteria***>>**
      - **Impact of finding<<***based on conclusions made from consequence of shortfalls***>>**
      - **Recommendation (s)**
      - **Management response <<***Auditee's response addressing the findings or recommendations: to be updated based on management response***>>**
      - **Auditor's final position on Audit <<** *Incorporated in Final Audit Report, based on management response***>>**
- **Noteworthy accomplishment <<***if any***>>**
- **Limitation of the audit**
- **Annexure/s <<***Supporting documents, flowcharts, follow-up action plan for auditee, etc***.>>**

[82] Based on GUID 5100 para 7.2
[83] Based on GUID 5100 para 7.3
[84] ISSAI 100 para 55

4.4.1. A note on introduction

a) A brief introduction to the IS audit being taken up would be the starting point of the report. The report must briefly give details of the system highlighting application and operating software environment and hardware resources required to run the system. The criticality of the system must be assessed and mentioned, as many of the audit observations gain their seriousness from the criticality of the system. If the data flow is complex, a flow chart may be annexed to the report.

b) Knowledge of the objectives of the audit, as well as of the audit scope and methodology for achieving the objectives, is needed by readers to understand the purpose of the audit, judge the merits of the audit work and what is reported, and understand significant limitations. In reporting the audit's objectives, auditors should explain the aspects of performance examined. To avoid misunderstanding in cases where the objectives are particularly limited, it may be necessary to state areas that were *not audited*. In reporting the scope of the audit, auditors should describe the depth and coverage of work conducted to accomplish the audit's objectives. The applicable dates of coverage of audit shall also be mentioned. Auditors should, as applicable, explain the relationship between the universe and what was audited; identify organizations, geographic locations, hardware and software used and the period covered; report the types and sources of evidence; and explain any quality or other problems associated with the evidences.

c) To report the methodology used, auditors should clearly explain the evidence gathering and analysis techniques used. This explanation should identify any significant assumptions made in conducting the audit; describe any comparative techniques applied; describe the criteria used; and when sampling significantly supports auditors' findings, describe the sample design and state why it was chosen.

4.4.2. A note on summary of findings

a) As discussed earlier in the report, IS audit is carried out across IT domains which have various IS audit areas. There are objectives of auditing various IS audit areas against which the auditors shall report the significant findings. A suggestive list of various audit areas, objectives and criteria to assess the audit objectives is presented in the Annexures. In reporting the findings, auditors should include sufficient, competent, and relevant information to promote adequate understanding of the matters reported and to provide convincing but fair presentations in proper perspective. Auditors should also report appropriate background information that readers need to understand the findings.

b) Auditors should report conclusions as called for by the audit objectives. The strength of the auditors' conclusions depends on the persuasiveness of the evidence supporting the findings and the logic used to formulate the conclusions. As mentioned earlier, sweeping conclusions regarding absence of controls and risks thereon may be avoided, when they are not supported by substantive testing. The report should be able to logically link the various observations. For example, poor security controls resulting in unauthorized transactions which are found out by using CAATs (e.g. IDEA), would more clearly show the overall deficiencies in the IT environment than all these being reported separately.

c) Auditors should report recommendations when the potential for significant improvement in operations and performance is substantiated by the reported findings. Recommendations to effect compliance with laws and regulations and improve management controls should also be made when significant instances of noncompliance are noted or significant weaknesses in controls are found. Auditors should also report the status of uncorrected significant findings and recommendations from prior audits that affect the objectives of the current audit.

d) Constructive recommendations can encourage improvements. Recommendations are most constructive when they are directed at resolving the cause of identified problems, are action oriented and specific, are addressed to parties that have the authority to act, are feasible, and, to the extent practical, are cost-effective.

e) In reporting significant instances of non-compliance, auditors should place their findings in perspective. To give the reader a basis for judging the prevalence and consequences of non-compliance, the instances of non-compliance should be related to the universe or the number of cases examined and quantified in financial terms.

4.4.3. Noteworthy Accomplishments

Noteworthy management accomplishments identified during the audit, which were within the scope of the audit, can be included in the audit report along with deficiencies. Such information provides a fairer presentation of the situation by providing appropriate balance to the report.

4.4.4. A note on limitation of the audit

Limitations to the IS audit should also be pointed out in the report. The typical limitations could be inadequate access to data and information, lack of adequate documentation of the computerisation process, leading the IS auditor to devise their own methods of investigation and analysis to derive conclusions. Auditors should also report significant constraints imposed on the audit approach by data limitations or scope impairments. Any other limitation faced by the IS auditor should be pointed out in the report appropriately. Example of few of the limitations could be:

- if the data used for audit analysis was not from production environment, it should be so mentioned as a limitation.
- Similarly, if there is only production environment and audit could not test dummy data to evaluate input controls comprehensively, it should be mentioned as a limitation.

Please note that**,** no such information about a system should be mentioned in the body of the audit report which might help outsiders to break into the system. Such information, such as table name, path, table structure etc., can only be treated as audit evidence but the reporting has to be carefully monitored. This is particularly true of any network system or a web-based ERP systems.

5. Audit Follow-up

Unless follow-up is put in practice, auditors cannot gauge whether the desired impact of audit has been effective or not. Therefore, a follow-up is one of the important components of the audit process, and that audit process cannot be complete without it. Further, even management and those charged with governance may not be motivated to take action if there is no follow-up system in OAGN.

- In case audit engagement on Information Systems is drawn from one or more of the main types of Audit such as compliance audit and performance audit, auditors shall consider the follow up requirements for such Audit engagements to be on par with those for mentioned Financial Audit, Performance Audit and Compliance Audit manuals/guidelines[85].

- For IS audits, auditors shall follow-up on observations and recommendations to ensure the issues that have been identified have been resolved by the auditee. Follow-up focuses on whether the auditee has adequately addressed the matters raised, including any wider implications. Insufficient or unsatisfactory actions by the auditee may call for a response from the auditor that shall be recorded in the final audit report.

- Follow up starts with issue of Preliminary/draft IS audit report to the audited entity. Findings included in the draft IS audit report have to be settled and responded back within 35 days of issuance. Auditee may seek extension from OAGN on valid grounds based on which OAGN may extend the response time by <one> month. However, follow-up in OAGN is a continuous process, until the outstanding audit findings are resolved based on appropriate action taken by management or those charged with governance[86].

- For ensuring that OAGN received management responses on observations raised in the IS audit report, the IS auditors should have follow-ups[87] with the agency management at the highest level and document their responses. If these efforts fail, adequate evidence about efforts made should be kept on record and mentioned in the report about these efforts.

- Unsettled findings should be recorded in the Final Audit Report that may be presented to PAC (Public Accounts Committee) for further follow-up. Legislative committees such as Public Accounts Committee(s), play an active role in the review and follow-up of the audit reports tabled in the legislature. Therefore, there are two levels of follow-up of audit findings and recommendations, i.e. one at the Public Accounts Committee/legislative level for issues reported in annual report and another at OAGN level.

- Auditors shall include the uncorrected significant findings and recommendations from the IS audits in next audit of the IT system. Especially in case of IS audit of financial systems, if matters identified during earlier IS audit are still pending and have continuous impact on auditing - those matters need to be considered in the follow-up audit. The follow-up IS audit can be planned as a separate IS audit or as part of financial audit of entities and offices. Please note that, systems which carry significant unresolved audit findings from previous audits, automatically carry higher priority during Annual Audit Planning as per the criteria for "selection of IS audit topics".

This page is intentionally left blank.

---

[85] Ref: GUID 5100 para 8.1

[86] Even after issuance of Final Audit Report, "open" or "unresolved" observations will be available in NAMS for OAGN auditors. Hence, they can be tracked till closure.

[87] NAMS also has follow-up functionality to track auditee's response. Moreover, communications to auditee can also be sent by OAGN through NAMS.

Annexures

Annex 1: Questions for assessing criticality of IT systems - Topic selection

Table 17: Illustrative questions for assessing criticality of IT system for "Topic selection"

S/N	Sample questions	Responses
Likely impact of Audit		
1.	Has the area been previously audited by OAGN or is it a new area? E.g. systems can be used for providing healthcare services, education services, law& order services, etc. Also, systems may be used at sub-national level or local level such as Municipal Accounting Software. Similarly, some systems may have been developed using new technologies or standards. OAGN shall evaluate whether such audits have been conducted in past and if no how much value addition can be brought in by auditing such systems.	
2.	What is the potential impact, on entity to be audited, in terms of identifying weaknesses and making recommendations ?	
Materiality		
3.	What is the amount of investment made in the IT system for procurement?	
4.	What is the annual cost of operation and maintenance of the IT system?	
5.	What was the mode of financing the systems – from entity's budget, or internal borrowings or external borrowings? **Priority for audit to be given to systems finances from external borrowings.*	
6.	Complexity of the IT system: ▸ What are the numbers of entities/offices using the system? ▸ What are the number of users across locations, using the system? ▸ What is the number of PCs/desktops that are used for running the system? ▸ Is the system interfaces/integrated to external systems? ▸ Is it a batch processing, or online transaction processing system? ▸ What is the volume of data, including offline data, in the system? ▸ On what type of network does the system operate? – public network/online/web, or extranet/VPN/WAN, or intranet/internal LAN, or desktop-based application with no network.	
7.	Nature of services provided by the IT system: ▸ Is the system used for critical business functions or system is used for support function such as office information systems, HR systems? E.g. TSA is a used for receipt and expenditure accounting that is a critical business functions for FGCO. Similarly, excise department, may have a systems for collection of revenue which a critical business function.	
8.	Reliance of entity on IT system: ▸ Does the entity completely rely on an IT system to perform its business operations or partially rely or may not rely at all. ○ Does Entity uses outputs of IT system directly to perform business-critical operations or revenue generation	

S/N	Sample questions	Responses
	○ Or, outputs of IT system are not directly used, but manually processed or checked before performing business critical operations ○ Or, extent of reliance on IT systems for performing business operations is very low ○ Or, IT system are not used for business-critical functions	
9.	Sensitivity of data: ▶ Does the system record public/citizen data or data related to any other third party, that may be considered private or sensitive data? ▶ Can general public perform online transactions on the system?	
10.	Any other aspects of materiality?	
Internal control and audit assurances on IT system/Entity		
11.	How recently, was the system audited (IS audit) by OAGN?	
12.	Were there any significant audit findings, in the previous IS audit, that need to be checked again?	
13.	Are there any unresolved issues/matters that were reported in previous IS audits?	
14.	Are there any significant issues/matters (related to IT system) from any other audit/s conducted by OAGN or an external agency?	
15.	Has a third-party certification of system been done?	
Public interest/visibility		
16.	What is the level of potential interest to OAGN stakeholders such as press, general public, parliament, NGOs, etc.	
17.	Does public uses system data/information through internet or any other means in form of report or otherwise?	
18.	To what extent wrongful data impact public interest? ▶ Failure of business, public lawsuits ▶ Loss of credibility and negative image of the organization ▶ Financial loss to the entity e.g. potential loss of revenue	
Entity/IT system specific aspects		
19.	Level of computerization at entity: ▶ What is the level of computerisation at entity? ○ Almost all business processes are computerized? ○ Some of the business processes are computerised while others are manual? ○ There is very low level of computerisation, and most processes are manual?	
20.	System development and management (including data): ▶ Was the system developed with in-house capacity, or by a government agency or a private agency or a mix? ▶ System is currently managed by entity with in-house capacity, a government agency or private agency or outsourced?	
21.	System operation:	

S/N	Sample questions	Responses
	▶ Since, how many years is the system is operational?	
22.	Change management: ▶ How frequently is system updated? ▶ Is there a documented and approved change management policy?	
23.	Dedicated IT staff: ▶ Does the entity have dedicated IT staff for managing the system? ▶ Does the entity ○ has a Chief Information Officer (CIO) or equivalent position in charge of activities related to IT or, ○ a Senior official in charge of activities related to IT in addition to their responsibilities, or ○ doesn't have any designated staff to manage activities related to IT	
24.	Other entity specific factors: ▶ Does the entity has an approved IT policy? ▶ Does the entity has a documented disaster recovery and Business Continuity Plan? ▶ Does the entity has an approved IT security Policy? ▶ Does the entity has system specific documentation such as HLD, LLD, Testing documentation, installation guides, user manuals?	
Risk to good audit management		
25.	Does audit team have required competency and expertise to complete audit?	
26.	Is sufficient information available to plan and conduct the IS audit?	
27.	Is the location of audit accessible?	

Annex 2: Information required for understanding the auditee and IT system

During planning stage, auditor has to gain a preliminary understanding of auditee's environment and IT system. For this auditor has to collect information from various sources. In the table below is mentioned an illustrative list of information required for this purpose. Auditors may update the list, for an audit engagement, as required.

Table 18: An illustrative list of information required for understanding the auditee & IT system

S/N	Information required
1.	Brief background of the organization
2.	Organizational chart
3.	Personnel policy
4.	Regulations and laws that affect the organization (for example, Income Tax Act)
5.	List of applications and their details
6.	Network and application architecture, including client-server architecture
7.	Organizational structure of the IT department with job descriptions
8.	IT department's responsibilities with reference to the specific application
9.	Cost associated with the system
10.	Project management reports
11.	Details of hardware (Annex 3)
12.	Details of software (Annex 2 including whether developed in-house etc.)
13.	Database details
14.	Data Flow Diagram, Data Dictionary, Table listings
15.	If it is an RDBMS, details of relationships between the tables and database triggers
16.	Details of interfaces with other systems
17.	Systems manual, User manual and Operations manual
18.	Performance analysis reports
19.	List of users with permissions
20.	Test data and test results
21.	Security set up for the system
22.	Previous audit reports
23.	Internal audit reports
24.	User feedback about the system
25.	Peer review reports

Annex 3: Details of IT Software

During planning stage, information shall be collected on the IT system to be audited. The following template shall be used for collecting information on the IT software.

Table 19: Form for collecting information on the IT software (Illustrative)

Name of the auditee:
Date of information collection:
Head of department (auditee)
Contact details of auditee:

S/N	Required Information	Response
1.	Name of IT application and category of IT application (Financial management system, Accounting system, HR/Personnel management systems, Decision Support System, Inventory/stock, Engineering/Manufacturing, Payroll, e-governance, etc.)	
2.	Does the system affect the financial and accounting processes of the organization (Yes/No)	
3.	Broad functional areas covered in the IT application:	
4.	Has the application system been developed in house or by outsourcing? If outsourced, please mention the contracted amount:	
5.	System developer or provider (Name and contact)	
6.	Is it a COTS or Bespoke solution?	
7.	System managed by (Name and contact; could be internally managed or by external agency)	
8.	Developed duration (start date/end date)	
9.	Date of operation:	
10.	Estimated number of people engaged in operation of the system:	
11.	Estimated number of users of the system:	
12.	Location/s of IT systems installation (Implemented districts, offices, etc.):	
13.	Category of IT systems: (Mainframe based or Web-based or EDI or File server system or client server system, others (specify)	
14.	Source code (Availability (yes/no) and developed on which platform)	
15.	Software and version of software used for:	
	▸ Operating system/s	
	▸ Network software	
	▸ Communication software	
	▸ Database Management System (DBMS)/ Relational Database Management system (RDBMS)	
	▸ Front end tool	
	▸ Programming language/s	
	▸ Any other	
16.	Is the system used for business-critical operations or otherwise? How much does the entity relies on the system for its business-critical operations?	
17.	Database Server	
18.	Back-up Server	
19.	E-mail Server	
20.	Server existed place	

S/N	Required Information	Response
	▶ Exists at Center	
	▶ Exists at District	
21.	Software Test Condition (UAT results, third part tested?)	
22.	Networking	
23.	What is the average volume of transactional data generated on a monthly basis in terms of storage space?	
24.	Does system has functionality to provide audit trail of all transactions processed?	
25.	Is system documentation available? (user manual, system design documents, others (specify)	
26.	Is there any system in place to make modifications to the application being used on a regular basis to support the function? (Yes/No)	
27.	Does the system transmit/receive data to/from other organizations? (Mention systems it transmits or receives data from)	
28.	Any other details, please specify: _____	
In case of systems that are under development		
29.	What is the current stage of software development? (Requirement gathering, Functional design, Technical Design (HLD, DLD), Development, testing, pilot, parallel run, implementation/deployment, etc.)	
30.	What is the projected cost for IT system?	
31.	What is the target date of completion?	
32.	Is system development on schedule as per project plan, or ahead or delayed?	

Annex 4: Details of IT Hardware

The following template may be used for collection information on hardware and assessment of IT related physical infrastructure condition. The requirements of items under IT infrastructure shall be updated as per the requirement of the audit engagement.

Table 20: Form for collecting information on IT hardware (Illustrative)

Name of the auditee:
Date of information collection:
Head of department (auditee)
Contact details of auditee:

S/N	IT Infrastructure	Quantity (No)		Usage Status			Remarks, if any
		As per record	Physically existed	Running	To be repaired	Useless	
Details of hardware items (with specifications):							
1.	Printer						
2.	Telephone						
3.	Alterative power back-up						
4.	Scanner machine						
5.	Digital camera						
6.	Photocopy machine						
7.	Fax machine						
8.	Overhead projector						
9.	UPS						
10.	Number of terminals/PCs with specification (e.g. Pentium IV capacity computer and 1024 x 768 pixel capacity screen)						
11.	Internet machinery having at least 512 kbps capacity						
12.	Windows, Linus or MAC operating system having capacity of Windows XP or above						
13.	Internet browser such as- Internet Explorer 8+, Firefox 28+, Google chrome 3+ , safari 5.0+ etc.						

S/N	IT Infrastructure	Quantity (No)		Usage Status			Remarks, if any
		As per record	Physically existed	Running	To be repaired	Useless	
14.	Other technology and machineries specified by system manager (PPMO)						
Details of networking hardware (with specifications)							
15.	Routers						
16.	Switches						
17.	Modems						
18.	Network Interface Controller						
19.	Terminal adapters						
20.	Others (specify)						
21.	Are more than one IT Application(s) running on the same Hardware? If Yes, specify the name(s) of these IT Application(s)						
22.	Please mention, any other matter regarding physical infrastructure condition: _____						

Annex 5: Data analysis techniques and usage of CAATs

This section contains data analysis procedures, and techniques for using CAATs for:

- Validating application programs/systems
- Analyzing data files
- Performing other data analysis techniques

Data analysis process

1) Extracting relevant entity business data:

Understand the data structure by obtaining and studying data definition documents from the audited entity. If read-only access on the system is granted by the audited entity, then data stored in tables relevant for the audit exercise can be extracted by querying the database if the skillset exists. Otherwise, the entity can be requested for providing a copy of the relevant source data. Data can be received in the form of a database dump that contains a record of the table structure and/or the data from a database and is usually in the form of a list of SQL statements. IS auditors may have to create similar environment (compatible versions of common database applications, operating systems, hardware etc.) as at the audited entity to import/analyse data from the copy of extracted data dumps. In many cases this represents the most important aspect of application control testing since extracting data correctly sets the stage for the success of subsequent processes. IS auditors may also be required to convert data from one form to another to facilitate better reading and analysis.

2) Transforming and loading data:

CAATs tools allow importing of data from multiple databases into a spreadsheet format and assist in transforming, formatting of data for further analysis. It is important for the auditor to undertake some pre-formatting of the source data to make the analysis exercise easier.

3) Performing data analysis

The main steps involved in analysing business data of the audited entity to draw assurance on the quality of application controls are common to any form of data analytics. Key Considerations in Data analysis are to:

- Identify the purpose of the analysis;
- Understand the sample(s) under study;
- Understand the instruments being used to collect data;
- Be cognizant of data layouts and formats[88]; and
- Establish a unique identifier if matching or merging is necessary.
- IS auditors need to plan the:
    - Statement of research questions / Objectives
    - Methods used to answer research questions
    - Criteria for evaluation
    - Evidence
    - Analysis
    - Conclusion
- File restructuring procedures (syntax creation, adding new variables as needed)
- Data cleaning procedures (e.g. removing outliers)

[88] Layout would mean understanding of different databases, tables within, coding pattern utilized and relationships between table and databases. Understanding of different database models will be helpful in this regard.

Most analyses can be executed straight from a working data file. Some analysis may require transformations of the raw data, subsets, or specific input data to comply with statistical software or tools that the auditor may use

Techniques for examining integrity of application programs are:

a. ***Use of test data:*** Analysis with test data is done in situations where the quality of program is intended to be tested. The premise is that it is possible to generalize about overall reliability of a program if it is reliable for a set of specific tests. Use of Test data involves Designing of Test Data and Creating of Test Data before running the program with the test data. Often this technique is deployed at the application testing stage by the developer itself, before an application or changes to it is migrated into production (i.e. live transactional operation). While auditing a recently deployed IT system or change management process, the auditor may review the procedures undertaken in the testing phase.

b. ***Code comparison:*** Developers use code comparison techniques which involve comparison of the Source Code of a program or changes to it with standard design methodologies for the particular programming language with the intent of discovering bugs, security breaches or violations of programming conventions. These are mostly developers' tools and not often used by IS auditors. For code samples selected by independent security test teams, the auditors' role would be to determine that the code was tested for security and that the results were documented and reported, and that violations and vulnerabilities detected were appropriately remediated. However, auditors with appropriate skillsets may resort to code comparison in relation to change management or initial commissioning of an application program, if the scope provides for it.

c. ***Test of data integrity:*** Data integrity testing is a set of substantive tests that examines accuracy, completeness, consistency and authorization of data available in the system. These tests will indicate weakness in input or processing controls. The data integrity tests help identify the robustness of relational integrity by checking validation routines that were built into the application during the design of input condition constraints and data characteristics at the table definition stage of database design.

Techniques for data analysis using CAATs

d. ***Sampling:*** Sampling techniques are useful to derive suitable conclusions based on statistically sufficient checks on limited data. There are two primary methods of sampling used by IS auditors. These are Attribute sampling and Variable sampling. Attribute sampling is generally used in compliance testing situations and deals with the presence or absence of the attribute and provides conclusions that are expressed in rates of incidence. Variable sampling is generally applied in substantive testing situations and deals with population characteristics that vary and provides conclusions related to deviations from the norm. For testing validations and other input controls in a system which deals with large set of data, the auditor may find it useful to draw a random sample of transaction records stored in the system database.

   Most data analysis applications including spreadsheet applications provides for easy functions to select a particular data element (field/ column/ row) and the related data cells and create random subsets of the chosen data set by using algorithms based on random number seeds, or simple formulae.

e. ***Summarization and stratification***: These two techniques help profiling data before any test of controls are undertaken. Summarizing data helps totaling of transactions in terms of defined attributes that helps the auditor gain an overall understanding of the transactions. For example, totaling the payments made by vendor types provides a useful insight on the high value vendor payments. A very useful function available in spreadsheet and CAATs is the pivot table. It helps generating summary information from large database in a very short span of time.

Stratification of data prepares a frequency distribution of the data in terms of defined bins or intervals. It can give the auditor important information about the nature of the data and can also help us identify the areas where detailed tests should be conducted.

f. ***Conditional queries***: The technique of data extraction based on conditional queries is useful to conduct a number of checks on the quality of application controls that include testing of completeness, of integrity, of correct mapping of business rules. IS auditors need to have detailed domain knowledge of the business rules of the entity to design meaningful conditional queries to verify whether business rules are properly mapped into the application.

- **Test of inputs controls:** For example, in an IT system which may support a particular Government funded education / welfare program it is important to create permanent beneficiary records in the form of master data tables in the database. A test of input controls in this case is to extract a sample of master records stored in the master table and check if the data capture for related attributes (unique Ids, names, addresses, location IDs) have blanks, meaningless values, duplicates, etc. Evidence of any of these errors would indicate deficiencies in data descriptions during table design.

- **Test of processing controls:** or testing of processing controls a specific substantive test may be to find out whether a particular business rule is properly mapped into the IT system which is used to do the business processing. For example, in a system used by the tax department, the test could be to ensure that the conditions for grant of tax rebate are mapped into the system. In this case, an extraction of records could be made from the sample tax dataset with a condition that simulates the business rule as per law. Any output of this extraction exercise that is non-compliant to the business condition may indicate improper processing control or non-mapping of the business rule. Such non mapping leads to repeated errors that could result in material impact on the finances of the entity.

Other data analysis techniques

g. **Identifying duplicates:** A common test of relational data integrity in a database is to examine the existence of duplicates where none should logically exist, in terms of the defined business rules of the entity. For example, in a tax or a social security database, the relevant identity is defined to be unique as per law. Evidence of duplicates in this data field would indicate improper validations vis-à-vis inputs to standing data resulting in an operational or financial risk to the audited entity. The analysis tools provide for simple functionality to detect duplicate keys. These can be found even in transactional tables that could enhance the risk of duplicate payments.

IS auditors need to evaluate the need for such tests, depending upon the application control being tested within the process. For example, if the auditor is reviewing financial controls within applications for payables processing the chances of the system generated purchase order number being duplicated would be quite improbable. However, if the auditor needs to test for controls on submission of duplicate vendor bills (an external input), which is a non-system generated input, this test can be deployed.

h. ***Gap analysis***: The objective of deploying this technique is to ascertain completeness and to test for gaps in a numerical data field which is expected to have sequential numbering. In MS Excel this is found by serially sorting values in the data field in question, adding a calculated field based on the sequential logic, and then filtering for rows where exceptions occur. The CAATs/audit tools use a simple gap detection feature where the field in question needs to be defined for identification of gaps. To use the duplicate or gap detection functionalities, the auditor does not require much querying experience.

i. ***Working with multiple files***: The source database often contains large number of transaction and master tables to fulfil the need of normalization of data. While working with imported datasets it is often useful to add together particular fields into one data table with the use of a matching key (field). Database management systems allow joining of multiple files with the help of 'joining' function. Use of matching

functions or conditional queries on joined tables help the auditor assess the referential integrity between data tables or even between separate related business applications used by the entity.

For example, if an entity registers prospective suppliers on a web portal and uses a separate procurement application for raising purchase orders, the business rules should necessitate that the supplier database is linked to the procurement database. Joining tables from these two separate databases by means of matching vendor names or vendor IDs would help establish the adequacy of the interface between the two related business applications.

Annex 6: Audit matrix for audit of IT Governance

IS audit Domain: IT Governance	
Audit area: Business needs Identification, Direction and Monitoring	
Audit objective: Assess whether the organisation's leadership effectively directs, evaluates and monitors IT use in the organisation in order to fulfil the organisation's mission.	
Audit issue 1: Defining IT requirements: How does the organisation identify and approve business and IT requirements?	
Criteria: The organisation has a plan on how it identifies emerging business or IT needs and the Steering Committee approving requirements has sufficient information to make their decisions.	
Information required: ▸ Requirements management process ▸ Steering committee charter and operating principles including approval and rejection thresholds ▸ List of approved and rejected requirement	**Analysis method/s:** ▸ Review of documents to ensure that new business requirements are identified and analysed according to the organisation's requirements management process. ▸ Review of approved or rejected requirements to ensure that these are in accordance with accepted operating principles. ▸ Interview management or others responsible for approving projects to ensure that they take into account the IT organisation's capabilities, skills, resources, and training, and the ability of the users to utilise the new tools and methods or procedures.
Audit issue 2: Leadership: How does the leadership direct and monitor the performance of business and IT objectives on a periodic basis?	
Criteria: Performance measures are established, and the steering or equivalent high-level committee conducts periodic reviews and meetings and takes appropriate action, or there is a reporting system to management that informs them of the status of key performance measures.	
Information required: ▸ Performance measures for business and IT ▸ Periodic reports about project status ▸ Minutes from periodic reviews ▸ List of action items and their status etc.	**Analysis method/s:** ▸ Review sample management decision or memos to ensure that they are clear, well substantiated, and unambiguous. ▸ Review performance measures to ensure that they cover both business and IT systems. ▸ Review project status reports (or other documentation that has the status of the project (meeting minutes, emails, etc.)) to ensure that it contains cost, schedule and performance indicators and variations from plan. ▸ Review management actions items to ensure that they are assigned and tracked to closure and include lessons learned.
Audit issue 3: IT Investments How does the organisation manage IT investments?	
Criteria: Performance measures are established, and the steering or equivalent high-level committee conducts periodic reviews and meetings and takes appropriate action, or there is a reporting system to management that informs them of the status of key performance measures.	

Information required:	Analysis method/s:
▶ Investment management plan and procedures ▶ Portfolio of IT projects ▶ Sample cost benefit analysis reports ▶ List of approved and rejected or deferred projects ▶ Project status reports for approved projects ▶ Sample post project evaluation reports	▶ Interview management to determine the organisation's investment management procedures. ▶ Review portfolio to assess whether projects have been prioritised according to approved criteria. ▶ Review status reports to see they provide cost and schedule tracking ▶ Review cost benefit analysis reports to assess that they are complete, reflect actual conditions and do not overstate the benefits or understate cost or schedule (utilise specialist services of economists or cost experts as needed). ▶ For projects in trouble, determine whether their methodology was suitable to the type of project and properly applied, and whether QA has been involved during the life cycle. ▶ Interview management to determine whether any projects have been terminated due to underachieving benefits or performance. ▶ Interview management to determine how the organisation makes decisions on building vs. acquiring (buying) solutions (for example, based on capability, skills, cost, risk, etc.).

IS audit Domain: IT Governance	
Audit area: IT Strategy	
Audit objective: Confirm whether there is an IT strategy in place, including an IT plan and the processes for the strategy's development, approval, and implementation and maintenance which is aligned with the organisation's strategies and objectives. The risks and resources while accomplishing IT objectives are effectively managed.	
Audit issue 4: Quality of IT strategy Does the organisation have an IT strategy that serves to guide its IT functions?	
Criteria: An organisational-level IT strategic plan exists, it translates business objectives into IT goals and requirements, addresses the needed IT resources to support the business, and it is reviewed and updated periodically.	
Information required: ▶ IT Strategic Plan, or equivalent document ▶ Meeting minutes from IT and Organisation's Steering committee meetings.	**Analysis method/s:** ▶ Review of document. ▶ Interview business owners to determine if their needs are met by the IT organisation. ▶ Review periodic IT Committee and Organisational Steering Committee meeting minutes to ensure that business owners are represented and that strategic IT decisions are made at the Steering Committee level. ▶ Review the IT Strategy or interview management to determine resources' requirements and how they are determined and

	approved, who approves appropriate acquisition of tools and other resources (staff, contractors, skill via training, etc.).
Audit issue 5: Risk management How does the organisation manage their risks?	
Criteria: The organisation has a risk management policy and plan and has assigned sufficient resources to identify and manage risks.	
Information required: ▶ Risk management plan ▶ List of risks (including IT) and mitigation strategies ▶ Minutes of periodic risk assessment or other meeting if available.	**Analysis method/s:** ▶ Review risk management plan or other document to ensure that risk management responsibilities are clearly and unambiguously assigned. ▶ Review of documents to determine whether IT risks are part of the overall governance risk and compliance (GRC) framework. ▶ Review meeting minutes to ensure that new risks are added and analysed as appropriate. ▶ Interview personnel responsible for risk management to determine whether the risks to be mitigated have appropriate cost estimates, and resources are allocated. ▶ Interview management or review minutes of meeting to determine that leadership is aware of both IT and other risks and monitors their status on a periodic basis.

IS audit Domain: IT Governance	
Audit area: Organizational structures, policy and procedures	
Audit objective: Ensure that there are organisational structures, policy, and procedures in place that enable the organisation to meet its mandate for business goals.	
Audit issue 6: Does the structure of the IT organisation enable it to meet its IT Goals and business needs?	
Criteria: The IT Organisation is positioned at a sufficiently high level within the organisation and its roles and responsibilities are clearly defined including those of the Chief Information Officer (CIO) or equivalent.	
Information required: ▶ Overall organisation chart ▶ IT Organisational chart.	**Analysis method/s:** ▶ Review organisational charts to determine that the IT organisation is positioned at a strategic level (for example, there is a CIO who reports to or is a member of the Steering Committee). ▶ Review the IT organisation chart to determine that it is aligned to support the business (has a help desk, data base managers, maintenance personnel or contactors who help and facilitate IT operations).
Audit issue 7: Policy and procedures Has the organisation approved and is it using appropriate policies and procedures to guide its business and IT operations?	
Criteria: The organisation documents, approves, and communicates appropriate policies and procedures to guide the business and IT operations in order to meet its mandate.	

Information required: Organisational policies regarding: ▶ Human Resources including hiring and termination security, document retention, contracting and/or outsourcing, software development and/or acquisition, etc. ▶ Procedures for the selected policy areas ▶ Emails or other ways policy is communicated to appropriate users and stakeholders ▶ QA reports to management reporting on periodic policy and procedures compliance and other issues ▶ Request changes to policy and or periodic review and results.	**Analysis method/s:** ▶ Review policies to ensure they are approved and current. ▶ For example, review the Human Resources policy to determine that skill requirements are defined, and training is identified for new and other staff. ▶ Review initial and refresher training materials or other internal processes through which these policies and procedures are communicated within the organisation. ▶ Interview members of the quality assurance or other group that is responsible for enforcing policies to see what they do to ensure compliance. ▶ Interview QA or compliance staff to determine how and when they report their results to senior management. ▶ Interview personnel responsible for compliance of policies and procedures to determine how often they report the results to senior management and how they solicit input on non-compliance anonymously or independently. ▶ Interview managers and users to understand their perception and attitude to the analysed policies and procedures. In case of frequent opinion: "Procedures are to complex" ask what and how they could be simplified. ▶ Review policy change control history to determine that policies are updated periodically or as needed. ▶ Review QA reports to ensure that they contain any policy or procedure compliance issues as appropriate. ▶ Review emails or other mechanisms (physical mail, training, etc.) to ensure that policies are distributed to appropriate users and stakeholders when updated or on an as-needed basis. ▶ Review policies to determine adequacy by looking for (as an example): ○ Scope of policy and mandate. ○ Definition of roles and responsibilities. ○ Required resources and tools. ○ Linkage to procedures. ○ Rules to deal with non-compliance.

IS audit Domain: IT Governance
Audit area: People and resources
Audit objective: To assess whether sufficiently qualified/trained personnel are employed and that they have access to suitable resources that enable the organisation to meet its business goals.
Audit issue 8: HR and logistics How does the organisation deal with meeting current and future people and resource requirements?

Criteria: The organisation should have a plan to meet its current and future requirements for meeting business needs.	
Information required: ▶ Organisational policies regarding: ○ Human Resources & Training ○ IT Strategy or Strategic Plan ○ Hiring & Training Plans.	**Analysis method/s:** ▶ Review policies to ensure they are approved and current. ▶ Review policies to ensure they require various groups (IT, quality assurance (QA), Business Users) to identify their current and future needs for personnel and resources. ▶ Review hiring and training plans to ensure that they reflect identified needs. ▶ For example, review the Human Resources policy to determine that skill requirements are defined, and training is identified for new and other staff. ▶ Interview HR or business managers to assess how they ensure critical positions are staffed during contingencies or extended absences. ▶ Review initial and refresher training materials or other internal processes through which these policies and procedures are communicated within the organisation. ▶ Review the IT Strategic plan to ensure that it contains people and resource requirements for current and future needs.

IS audit Domain: IT Governance	
Audit area: Risk assessment and compliance mechanisms	
Audit objective: To assess whether the organization has a system of measures and procedures to determine whether the organisation's activities are and remain consistent with the approved plans.	
Audit issue 9: Mechanism How does the organisation ensure that it has an adequate and working compliance mechanism to ensure all policies and procedures are being followed?	
Criteria: The organisation has a mechanism (via a QA group, internal audit, or spot check, etc.) to ensure that all policies and procedures are being followed.	
Information required: ▶ Organisational policies & procedures(Security, SDLC, Training, etc.) ▶ Organisation Chart ▶ Quality Assurance Plan ▶ Reports from compliance teams or groups ▶ Steering Committee Minutes	**Analysis method/s:** ▶ Select a sample of policies and organisational procedures to assess compliance. ▶ Interview management to determine who is responsible for ensuring compliance to the (audit selected) policies and associated procedures. ▶ Interview team or group responsible for compliance of above to determine how they accomplish their duties. ▶ Review reports from various compliance groups to see what they found, what actions they have taken and reported to management. ▶ Review steering committee minutes to see if high level compliance issues are discussed at this or at other meetings.

	▶ Interview author(s) to determine reason for update to existing policies or procedures. ▶ Review past non-compliance issues and resolutions. ▶ Review training or other dissemination mechanisms (email, memo, notice) to see if non-compliance issues were addressed.

Annex 7: Audit matrix for audit of Development and Acquisition

IS audit Domain: Development and Acquisition	
Audit area: Requirements development and Management	
Audit objective: Assess how the organisation identifies, prioritizes and manages their requirements for IT systems.	
Audit issue 1: How does the organisation identify user requirements for IT systems?	
Criteria: The organisation has a plan or procedures on how to collect, review, and catalog requirements for new or added functionality	
Information required: ▸ Requirements' management plan or procedure ▸ Sample user submitted requirements ▸ Sample initial review	**Analysis method/s:** ▸ Review the requirements' management plan or procedures to ensure users, stakeholders, or other relevant users are involved in identifying requirements. ▸ In a major functionality enhancement development, user consultation and prototype development can be implemented in parallel. The information interchange between the business process owners and vendor/ IT organisation needs to be looked into. ▸ Review sample requirements to ensure that there is an initial review, and that similar or duplicate requirements are grouped.
Audit issue 2: How does the organisation analyse, prioritise, and manage user requirements?	
Criteria: The organisation analyses, prioritises, and manages requirements to ensure that user needs are met in an optimum and cost-effective manner	
Information required: ▸ List of requirements ▸ Sample analysis of ▸ requirements ▸ Requirements traceability matrix ▸ Criteria for priority of requirements	**Analysis method/s:** ▸ Review requirements to determine that they include author, date, priority, cost, risk, and other elements. ▸ Review analysis of requirements or comments on requirements by business owners or stakeholders to determine that all views are solicited and summarised for appropriate analysis (accept, defer, reject, etc.) taken. ▸ Review traceability matrix to determine that approved requirements are assigned to either development or acquisition projects and are tracked to closure when implemented. ▸ Review criteria for requirements priority to assess whether they include elements such as cost, business need, emergency issues, and new mandates.

IS audit Domain: Development and Acquisition

Audit area: Project Management and Control	
Audit objective: Assess how the organisation manages and controls the development or acquisition of approved IT projects.	
Audit issue 3: How does the organisation plan for the development or acquisition of IT projects?	
Criteria: The organisation has a project management plan or equivalent for each approved project that guides its execution	
Information required: ▸ Project management plan or equivalent	**Analysis method/s:** ▸ Review the requirements' management plan or equivalent to ensure that it contains the project description, scope, cost, schedule, risks, management structure and that it identifies stakeholders (internal or external). ▸ Review the plan to ensure that it has been approved by senior management and incorporates comments by stakeholder. ▸ Review the project's organisational chart to determine the roles of individuals who are responsible for quality assurance or testing, development, and installation of the system on organisations IT infrastructure, support group, etc. ▸ For acquisition projects, ensure that the plan or equivalent list of those who will be responsible for oversight of the contractor exists and review approvals given by responsible persons. ▸ Interview project managers to determine which SDLC method is being used for the development of the project.
Audit issue 4: How does the organisation control IT projects?	
Criteria: The organisation controls and tracks projects to ensure they meet their cost, schedule, and performance requirements.	
Information required: ▸ Project cost and schedule baselines ▸ Project status reports ▸ Contractor status reports, SLA ▸ Results of reviews ▸ Action items	**Analysis method/s:** ▸ Compare project cost and schedule baselines with project status reports to assess deviations. ▸ Interview project manager / review reports to determine whether appropriate corrective action was taken for major deviations. ▸ Interview project management team and review minutes of meetings with contractor to assess the frequency and effectiveness of monitoring the outsourced project activities. ▸ Review contractor SLA or contract to ensure that they are following the terms of the contract, for example, look for contractors conducting periodic reviews, providing status reports, tracking action items, conducting risk management activities in accordance to the contract. Interview contract officer at the organisation to determine how it manages the contractor if SLAs are not available.

IS audit Domain: Development and Acquisition	
Audit area: Quality Assurance and Testing	
Audit objective: Assess how the organisation ensures that IT projects under development or acquisition meet their quality goals.	
Audit issue 5: Does the organisation have a quality assurance organisation and are their roles and responsibilities defined?	
Criteria: An established procedure for conducting quality assurance activities.	
Information required: ▸ Quality assurance policy or plan ▸ Quality assurance procedures ▸ Roles and responsibilities of the Quality Assurance group or individual(s) ▸ Quality assurance reports ▸ Project adopted SDLC	**Analysis method/s:** ▸ Review the quality assurance policy and/or plan to determine what group or individuals is responsible for conducting quality assurance activities for the project (for example, the Quality Assurance group should review documents to ensure they accurately reflect the requirements, review user manuals to ensure they are legible and do not contain missing elements or steps). ▸ Review the quality assurance procedures or interview quality assurance personnel to determine what activities they conduct (observe peer reviews, sit in on design or other reviews, etc.). ▸ Review reports from the quality assurance organisation to determine what they observed (whether the project team is following its project management plan, and the adopted SDLC and associated reviews etc.) to whom are issues reported.
Audit issue 6: How does the organisation plan for and conduct testing on IT systems?	
Criteria: The organisation conducts test on IT systems and based on the results accepts or rejects the system.	
Information required: ▸ Test plan ▸ Test schedule ▸ Test results ▸ Accept or reject criteria	**Analysis method/s:** ▸ Review test plans. ▸ Compare project cost and schedule baselines with project status reports to assess deviations, if any. ▸ Interview project manager / review reports to determine whether appropriate corrective action was taken for major deviations. ▸ Interview project management team and review minutes of meetings with contractor to assess the frequency and effectiveness of monitoring the outsourced project activities. ▸ Review contractor SLA or contract to ensure that they are following the terms of the contract, for example look for contractors conducting periodic reviews, providing status reports, tracking action items, conducting risk management activities in accordance to the contract. Interview contract officer at the organisation to determine how it manages the contractor if SLAs are not available.

IS audit Domain: Development and Acquisition

Audit area: Solicitation	
Audit objective: Assess how the organisation ensures that solicitation activities (set of tasks such as firming up the needs document, framing RFP, evaluating proposals, conducting pre-bid clarifications, designing and floating tender, evaluation, etc. leading up to the award contract) are conducted in accordance with its adopted solicitation plan or procedure.	
Audit issue 7: What is the plan or procedure for the conduct of solicitation activities?	
Criteria: Solicitation activities including vendor selection are conducted in accordance with the organisation's solicitation plan	
Information required: ▶ Solicitation plan or procedure ▶ Solicitation package ▶ User review of requirements ▶ User review of solicitation package ▶ Applicable laws that govern the conduct of solicitation.	**Analysis method/s:** ▶ Review the solicitation plan to ensure it covers areas such as user involvement, getting bids on a competitive basis, conducting market research prior to contract on areas as applicable, and that vendor selection is based on objective criteria. ▶ Interview key contracting personnel to assess how they ensure that the solicitation package is complete (for example, by getting users, stakeholders, experts as appropriate to review it). ▶ Interview users or business owners to ensure that they were consulted during the generation of requirements or approved the technical requirements of the solicitation and / or the final bid package. ▶ Interview contracting officer(s) to assess how they ensure that the solicitation process follows applicable laws and regulations.
Audit issue 8: What criteria does the organisation use in selecting a vendor?	
Criteria: The organisation uses objective and published criteria for vendor selection for each.	
Information required: ▶ Vendor selection criteria ▶ Vendors scoring matrix or equivalent.	**Analysis method/s:** ▶ Review the vendor selection criteria to ensure that it reflects the intent of the solicitation (for example, on a software contract, vendor selection should not include parameters not critical to the organisation). ▶ Interview key stakeholders to assess if they agree with the selection criteria. ▶ Review vendor scoring matrix or equivalent to confirm it is consistent with the selection criteria.

IS audit Domain: Development and Acquisition
Audit area: Configuration management
Audit objective: Assess how the organisation manages configurations of work products related to development and acquisition.
Audit issue 9: What policy does the organisation use for configuration management?
Criteria: Configuration management activities are conducted according to the organisational policy or procedure.

Information required: ▶ Configuration management policy or procedures or equivalent.	**Analysis method/s:** ▶ Review the configuration management policy for adequacy by looking for (as an example): ▶ Scope of policy and mandate ▶ Definition of roles and responsibilities ▶ Required resources and tools ▶ Linkage to procedures ▶ Rules to deal with non-compliance. ▶ Interview personnel responsible for configuration management if there is no policy to assess how they ensure that their duties are uniformly carried out for the organisation.
Audit issue 10: What group or individual(s) are responsible for authorising changes and for final installation into the production environment?	
Criteria: Only authorized and approved changes should be introduced into the production environment.	
Information required: ▶ Group or individual responsible for authorising changes ▶ Process for approval and introducing approved and tested changes to the production environment.	**Analysis method/s:** ▶ Ensure that a group exists that authorises changes to the work product(s). The group could be the change control board or equivalent that reviews and approves changes. ▶ Interview personnel responsible for authorising introducing new software to the production environment to ensure that software has been tested (including regression testing with other systems if needed) meets the acceptance criteria, has appropriate documentation, and includes user training (if appropriate) prior to being introduced for business. ▶ Interview personnel responsible for authorising changes to the production system to determine how they control and prevent unauthorised changes to the system (for example, by controlling access to the production system, separating the production and development environments, etc.).

Annex 8: Audit matrix for audit of IT Operations

IS audit Domain: IT Operations	
Audit area: Service Management	
Audit objective: To assess whether the IT organisation is actively monitoring IT operations against agreed-to internal Service Level Agreement or contract.	
Audit issue 1: Key parameters What baseline service metrics are covered by the internal SLA between the business and the IT organisation?	
Criteria: SLA Best practices – allocation of responsibilities between the business process owners and the IT support group, documented network management business objectives, service offerings and metrics, definition for problem types, help desk responsibilities.	
Information required: ▶ Entity's internal SLA between business owners and IT organisation. ○ Help desk responsibilities ○ Service reports generated ○ User/ application response time.	**Analysis method/s:** ▶ Review the SLA to find whether it contains appropriate elements – detailed and measurable service level objectives, systems and services covered, quality of service (QoS), services not covered, application level support and troubleshooting, system availability, help desk hours, response and resolution time dependent on severity classification of a problem, throughput, maintenance schedules etc. ▶ Check whether data back-up and recovery practices are consistent with the entity's BCP standards. ▶ Check if the Business Process Owners have signed on the agreement. ▶ Interview sample of users to understand the level of awareness.
Audit issue 2: Compliance What mechanisms are in place to ensure that the SLA is adhered to consistently?	
Criteria: SLA implemented, monitored and amended where necessary.	
Information required: ▶ The SLA parameters ▶ Reporting timelines ▶ Charts or graphs that show the success or failure of how these agreements are met over time ▶ Periodic meeting documents that reviews the analysis of the baseline and trends ▶ Operational parameters: defect rates, help desk requests, other communication trails, response time, Time to implement new functionality, change documentation, serviced locations and incentive and	**Analysis method/s:** ▶ Review the reports that the IT Organisation generates daily or over any other time interval. Check if all the indicators agreed upon are being monitored through the reports/trend graphs etc. ▶ Review reports to examine what metrics are measured and reported to the management periodically. ▶ Review documents to check whether the helpdesk activity reports are considered by the management and compared to resolution requests, and critical issues are noted for buying decisions and for periodic review of the SLA itself. ▶ Interview IT organisation personnel and examine the nature of supervision of help desk personnel, the monitoring tools used, the support task prioritisation, gathering of baseline for network and application, data on response time, frequency of back-ups, testing of backed up data to verify compliance with SLA requirements.

penalty clauses (especially important if IT support services are outsourced)	▶ Check what actions are taken by the IT unit, or in the case of an outsourced IT support group – by the organisation's management – if operational parameters are not in agreement with SLA requirements.
Audit issue 3: Effectiveness Does the management of IT services ensure satisfaction of business users and help meet business objectives of the organisation?	
Criteria: Achievement of performance metrics that are aligned to business needs and goals.	
Information required: ▶ Help desk reports minutes of meetings between business stakeholders and IT organisation ▶ Agenda items for SLA review cycles.	**Analysis method/s:** ▶ Interview a sample of business users (at various levels) or conduct a satisfaction survey about the quality of services by the help desk and IT support group. ▶ Review help desk reports to check whether a significant proportion of critical service issues were prevented before being reported by users. ▶ Check whether the resolution time for reported issues was less than the parameters set in the SLA. ▶ Check whether SLA parameters were being reviewed by management periodically and examine QoS issues.
IS audit Domain: IT Operations	
Audit area: Capacity Management	
Audit objective: Assess whether the IT organisation is ensuring that the system capacity and performance meets current and future business needs.	
Audit issue 4: Agreement on parameters Is there a documented agreement between the business and IT organisation that is used as the basis for selecting operational parameters for IT operations?	
Criteria: IT governance – track and monitor strategy implementation in terms of measurable metrics.	
Information required: ▶ Internal SLA, or other form of agreement ▶ IT operational parameters – processing resource availability, average system login time, % downtime, average system response time, etc.	**Analysis method/s:** ▶ Review the agreement or operating guidance that the IT group is using. Ensure that it is has been reviewed and signed by the relevant business users or senior executive management. ▶ Compare performance baseline parameters (viz. network resource availability, host response time) set by IT organisation with the Operating guidance set by Business process owners to verify that the IT organisation follows the operating guidance.
Audit issue 5: Monitoring Does the IT organisation collect and review system performance data on a real time/periodic basis for better alignment with business needs?	
Criteria: Best practices by system/network administrators including performance base lining, collection of traffic and configuration information, system resource availability, observe traffic stats and trends, what-if analyses, and use of tools to pinpoint causes of performance deterioration.	
Information required:	**Analysis method/s:**

▶ Reports, action items, help desk response time, and other metrics.	▶ Use Compliance issue in SLA matrix. Pay special attention to all elements having impact on capacity, i.e. compare actual capacity metrics to the SLA requirements, etc.
Audit issue 6: Performance data analysis Is the performance data analysed and tuned for efficiency gains and avoidance of capacity constraints? If needed, has the IT organisation planned for and acquired additional resources to meet business needs? Does the IT organisation hire, train, or contract for staff as the business needs change?	
Criteria: Parameters set in the agreement/operation guide, best practices in performance tuning (memory, optimisation of network response time, OS, I/O; efficient design of database schema, scheduling tasks according to priority and resource requirement, upgrade or tuning procedures set up to handle capacity issues on both a reactive and long-term basis).	
Information required: ▶ Reports, actions, status reports, performance metric graphs ▶ Minutes of meeting at the apex IT organisation level.	**Analysis method/s:** ▶ Review the reports that the IT Organisation generates daily or at other chosen time frame, look to see if it generates and analyses trend data, identifies bottlenecks to look for action items, and exception reporting for capacity issues. Compare to SLA requirements. ▶ Compare reports/trend patterns to verify procedural actions taken in response to the reports. ▶ Review minutes of meetings and find whether IT staffing issues, capacity problems and any additional resource needs are discussed and highlighted at the right time.

IS audit Domain: IT Operations	
Audit area: Problem and Incident Management	
Audit objective: To evaluate the effectiveness of organisation's problem and incident management policies and procedures.	
Audit issue 7: Policy awareness Is there a documented incident response policy and are the business users aware of it?	
Criteria: Best practices in incident response.	
Information required: ▶ Entity's incident response policy ▶ Guidelines for communicating with outside parties regarding incidents.	**Analysis method/s:** ▶ Review the policy to find whether it contains appropriate stages – preparation, detection and analysis, containment and eradication, post-incident activity. Does type of activity depend on high incidence or level of incidents? ▶ Verify whether the policy assigns responsibility, scope and reporting requirements. ▶ Review the actual procedures by which the business users are made aware of the policy, and the nature of communication between the incidents response team and the business stakeholders.

	▶ Interview a sample of business users across the organisation to get an assurance about the awareness of the incident response plan.
Audit issue 8: Skills set and resources Is there an adequately skilled incident response team with proper tools, resources and higher management support to handle incidents?	
Criteria: Incidents response best practices, guidelines, as laid down in SLA	
Information required: ▶ Incident response policy and plan ▶ Charter of the incident response team, composition and expertise ▶ SLA ▶ Incident response awareness training, upgrade strategy for skillsets of IT staff ▶ List of logging tools and applications used for network monitoring and usage.	**Analysis method/s:** ▶ Look at whether the team has a charter to investigate incidents. ▶ Look for expertise in networks, operating systems, and security in the team members and how they conduct their work. ▶ Review the service desk procedures to check whether escalation procedures are laid down for incidents that cannot be resolved immediately in accordance to risk categories defined in the SLA. ▶ Review what actions have been taken in response to past incidents. ▶ Review case report(s) to check whether appropriate personnel were involved in investigating incidents. ▶ Check what incident management tools are being used – are they relevant for the organisation's needs? ▶ Verify whether the organisation has established logging standards and procedures to ensure that adequate information is collected by logs and security software and that the data is reviewed regularly.
Audit issue 9: Effectiveness of response Does the incidence response strategy result in effective response to incidents?	
Criteria: Incidents response best practices (COBIT 5 DSS domain, ITIL on Service support)	
Information required: ▶ Incident response action items, forms logs, etc. ▶ Periodic security awareness training ▶ Incident handling procedures – guidelines for prioritising incidents ▶ Case reports and action taken.	**Analysis method/s:** ▶ Check if an incident response/handling priority is assigned to each asset or service. ▶ Verify whether procedures provide for the capture and analysis of volatile[89] and static data in a timely manner. ▶ Verify whether the response team periodically makes users aware of policies and procedures regarding appropriate use of networks, systems, external media and applications. ▶ Review documents to find whether post-incident activities such as refresher training has been given to user groups to avoid costly recurrence of significant incidents. ▶ Look for whether source of incident was identified. Look for action taken. (Procedure change, reprimand, training, etc.).

[89] Volatile data are data that are overwritten or changed over time, where a snapshot cannot be obtained without capturing the information interactively, or by regularly scheduled data extracts

	▶ Check whether the incident response team records all resolved incidents in detail and review the information for possible update in the knowledge base.

IS audit Domain: IT Operations	
Audit area: Change Management	
Audit objective: Assess whether the entity has implemented a standardised procedure for controlling all changes to the core IT systems and applications.	
Audit issue 10: Policy Does the organisation have an approved Change management policy that contains the appropriate controls throughout the change cycle?	
Criteria: Best practices in change controls: Request for change- authentication- acceptance- prioritisation - change design -testing change- implementation- documentation	
Information required: ▶ Change management policy and procedures, process flow diagrams ▶ Change control board charter ▶ Timeline of policy review ▶ Change documentation: Change request, Change control testing procedures, quality assurance plan, test plan & procedures ▶ Change Management software reports and logs ▶ Minutes of meeting of the change control board ▶ Change management summary reports considered by the management.	**Analysis method/s:** ▶ Refer to general requirements for policy and procedures in IT Governance section. ▶ Review the change management policy document to verify whether procedures for initiation, review and approval of change are laid out along with mapping of responsibility for these tasks. ▶ Review the change control board charter to identify the allocation of responsibilities and responsibility levels. ▶ Interview personnel observe actual practices and review documents to obtain assurance that change management procedures are followed: ask to see a change, trace change to operational environment, see that requisite procedures – e.g. management review and prioritisation – were followed, look for approvals and documentation. ▶ Look to see if internal QA has done an audit. Review if adequate review of logs and reports are done by the management where a change management software is used. ▶ Ensure that the access to production source library (e.g. Source code, configurations) is limited to CM staff, and the IT organisation is preventing unauthorised changes to the operational environment. ▶ Review documents observe practices to ensure that business users are associated during testing of changes to ensure correctness. ▶ Ensure that program changes have appropriate sign-off by relevant business stakeholder before moving into production.
Audit issue 11: Fallback procedures How does the IT organisation ensure that the organisation can revert back to a previous version if needed?	

Criteria: Change Management best practices – documentation on procedures and responsibilities for recovery of affected areas due to undesirable change impact.	
Information required: ▶ Change management procedures ▶ Documentation on change tests and implementation ▶ Recovery documentation and configuration change logs ▶ Back-up and restore procedures	**Analysis method/s:** ▶ Review documentation, interview business users to find if unintended impacts of functionality changes/ enhancements have been addressed on priority, in line with business interests.
Audit issue 12: Emergency changes Are emergency changes controlled adequately when established change management procedures for defining, authorising, testing and documenting of changes cannot be followed?	
Criteria: Are there approved guidelines for emergency changes?	
Information required: ▶ Emergency change control procedures ▶ Documentation of emergency changes that have been made during the audited period	**Analysis method/s:** ▶ Review the change management procedures to identify whether they contain a dedicated section and set of procedures to control emergency changes to the system. ▶ Ask for an example of an emergency change. Compare against documented procedure. Look for what testing was done prior to introduction into production environment. If documented procedure does not exist, ask how it knows what to do and who approves such changes. ▶ Examine whether emergency changes are approved by an appropriate member of the management before moving into production.
Audit issue 13: Change closure and documentation Are there appropriate processes followed for the update of associated systems and user documentation after a change is implemented?	
Criteria: Change management best practices (e.g. COBIT 5-BAI domain, ITIL on Service support).	
Information required: ▶ Process documentation of functionalities affected by change ▶ Established procedures for documentation.	**Analysis method/s:** ▶ Review documents to ensure comprehensiveness and consistency of changes implemented. Did operational procedures, configuration information, application documentation, help screens and training materials follow the same change management procedure, and were they considered to be an integral part of the change. ▶ Examine whether there is an appropriate retention period for change documentation and pre- and post-change system and user documentation. ▶ Examine what mechanisms exist to update business processes for changes in hardware or software to ensure that new or improved functionality is used.

Annex 9: Audit matrix for audit of IT Outsourcing

IS audit Domain: IT Outsourcing	
Audit area: Outsourcing Policy	
Audit objective: To assess whether the agency has an adequate policy on outsourcing.	
Audit issue 1: Key elements of outsourcing Policy Does the organisation have a policy on outsourcing?	
Criteria: Organisational policy on outsourcing	
Information required: ▸ Policy Document ▸ Approval process for outsourcing of a function/ service ▸ List of outsourced functions/ services ▸ List of outsourced functions/ services with partial outsourcing ▸ Mode of service by the service provider ▸ Cost-benefit analysis on outsourcing of a function/ service ▸ List of outsourced service providers with locations ▸ Approval related documents for outsourced functions/ services ▸ Strategy to ensure continuity in case of takeover of the service provider by another organisation ▸ Information on any takeover of the service provider ▸ Monitoring documents/ reports.	**Analysis method/s:** ▸ Review policy to ensure it is approved. ▸ Review policy to check (for example) it contains information about organisation assets that can be outsourced or not, identifies the list of services/ functions that it may outsource. ▸ Review acquisition or outsourcing approval documents to ensure senior management are involved in the approval. ▸ Document review to assess that the organisation has identified the risks associated with respect to different modes of outsourcing and locations of outsourced service provider. ▸ Document review to verify whether the organisation is aware of risks associated with possibility of takeover of the service provider. ▸ Document review to verify whether the organisation has ensured that the business continuity, data rights, security, ownership and cost are embedded in the service agreement covering the case of takeover. ▸ Document review to assess that the policy includes identification of monitoring parameters for the outsourced functions and requires them to be included in the outsource agreement.

IS audit Domain: IT Outsourcing
Audit area: Solicitation
Audit objective: To assess whether the agency has a policy on how to manage solicitation.
Audit issue 2: Policy and Process of solicitation ▸ Does the organisation have a policy on acquisition? ▸ Does the organisation have a definite process for identification and selection of the service provider? ▸ Does the organisation have a process to ensure inclusion of user requirements into the Service Level Requirements/ contractual requirements? ▸ Are the related decisions taken at appropriate levels?

Criteria: Provisions of organisation policy on Outsourcing and policy on IT services procurement dealing with solicitation and acquisition.	
Information required: ▶ Acquisition or equivalent Policy ▶ List of laws regulating the acquisition and outsourcing ▶ Selection process for identification and selection of a service provider ▶ List of outsourced functions/ services along with the service provider ▶ User requirements for the contracted or outsourced service ▶ Contract/ Service Level Agreement ▶ Approval related documents for selection of service provider.	**Analysis method/s:** ▶ Document review to assess that the organisation has a policy on solicitation or acquisition. ▶ Review policy to ensure it contains provisions for data requests from sub-contractors if the prime contractor has included sub-contractors as part of the proposal. ▶ Document review to assess that the policy on solicitation and acquisition complies to the laws on outsourcing and acquisition (review that it references to provides links to applicable laws and regulations) ▶ Review of selection process for compliance to the policy for each a sampling of contracts or outsourced service (review that the selection process is transparent, has objective criteria, the selection team is comprised of personnel who understand the requirements, is represented by contractual and legal personnel, and consult with users as appropriate for clarification). ▶ Ensure that the contractual requirements have been approved by users and relevant stakeholders. ▶ Meet with the contractual office to ensure that an appropriate level of management approved the solicitation and contract.

IS audit Domain: IT Outsourcing	
Audit area: Vendor or contractor monitoring	
Audit objective: To assess whether the organisation is managing the contractor or vendor and takes appropriate action when performance or quality deviates from established baselines.	
Audit issue 3: Vendor management ▶ Is there a contract with the service provider? ▶ Are Service Levels identified and agreed through a Service Level Agreement? ▶ Is there a monitoring arrangement (for services) with the service provider? ▶ Are the service levels ensured through this arrangement? ▶ Is appropriate action taken when service level agreement provisions are not met?	
Criteria: Provisions/ parameters defined in Service Level Agreement and the follow up actions by the organisation.	
Information required: ▶ Contract/ Service Level Agreement ▶ Approved schedules, baselines, cost and other technical parameters that define the product or service being acquired or outsourced	**Analysis method/s:** ▶ Document review to assess if a service level agreement has been established. ▶ Review of monitoring reports submitted by the contractor to ensure that they contain elements that are in the contract or ▶ SLA (cost, schedule, performance, risk, status, issues, and status of past action items or tasks).

▶ Monitoring documents/ reports / meeting minutes of reviews conducted, action items, direction to vendor (task orders, statement of work, etc.) ▶ Impact assessment of deviations ▶ Action items or direction to vendor ▶ Action taken reports on deviations from service levels.	▶ Review of monitoring reports to identify service deficiency/ deviation and assessment of impact due to the deficiencies/ deviations. ▶ Review of notices and action-taken reports for action taken to be commensurate with impact on business and contractual provisions.

IS audit Domain: IT Outsourcing	
Audit area: Data Rights	
Audit objective: To assess whether the organisation's data protection requirements are identified, and that they are part of the contractual requirements.	
Audit issue 4: Data protection and management of data ▶ Are the data protection and access rights built into the service contract? ▶ Is the data defined appropriately to cover the transaction data as well as the programs/ software supporting the data, as the case may be? ▶ Is there a mechanism to ensure that the data protection and security requirements as per the Service Level Agreement are being adopted and implemented by the service provider?	
Criteria: Organisation's data protection and access rights requirements are levied on the contractor as appropriate.	
Information required: ▶ Organisation's Data Protection and access rights requirements ▶ Definition of data (for protection and access rights) ▶ Contract with the service provider ▶ List of data access records from the service provider ▶ Reports of third-party audits or self audits with recommendations and follow up on them ▶ Monitoring reports ▶ Correspondence with the service provider on the subject ▶ Incident handling reports ▶ Non-disclosure agreement with the outsourced agency ▶ List of information disclosed by the outsourced agency to third party / unrelated party(s).	**Analysis method/s:** ▶ Document review on adequacy of data protection and access rights requirements/ definition of data. ▶ Document review of the contract with service provider to check for incorporation of Data Protection and access rights requirements. ▶ Document review of third party/ self audit reports. ▶ Document review of the monitoring reports, correspondence and incident handling reports to assess the follow-up activities by the organisation. ▶ Review of the non-disclosure agreement to verify that all relevant information is covered. ▶ Verify if the disclosure of information by outsourced agency is authorized.

IS audit Domain: IT Outsourcing

Audit area: Overseas Service Provider	
Audit objective: To determine if the organisation has strategy on contracting services to overseas vendors.	
Audit issue 5: Management of vendor who is overseas Whether the organisation understands the issues involved in outsourcing to overseas agencies while outsourcing to overseas agencies?	
Criteria: Provisions of outsourcing policy related to outsourcing to overseas agencies. Laws of land regulating business with overseas agencies.	
Information required: ▶ List of laws and regulations related to outsourcing services ▶ Information on any in-country presence of the service provider ▶ List of foreign offices of the organisation ▶ List of laws and regulations regulating the service provider in their country ▶ Bilateral agreement between the country of organisation and the service provider facilitating outsourcing agreements ▶ Reports on vendor's past performance on delivery times and quality issues in ▶ Cost benefit analysis of indigenous and overseas service provider ▶ Outsourcing contract and Service Level Agreement ▶ Information on escrow amount/ financial guarantee related to performance ▶ List of deviations from the Service Level Agreement and outsourcing contract ▶ Monitoring and follow up reports on action taken on deviations by the service provider.	**Analysis method/s:** ▶ Document Review to assess that the organisation has identified risks related to outsourcing to overseas service provider. ▶ Document review to assess the cost benefit analysis addressed the risks related to outsourcing to overseas service provider. ▶ Document review to assess that adequate background check on the service provider has been carried out. ▶ Document review to assess that a robust system is in place to ensure performance on Service ▶ Level Agreement and outsourcing contract. ▶ Document review to assess that any deviations from Service Level Agreement and the contract are followed up in a timely manner ensuring minimum downtime and loss to the organisation.

IS audit Domain: IT Outsourcing
Audit area: Retaining business knowledge/ ownership of business process
Audit objective: To assess whether the agency retains business knowledge and ownership of business process(es).
Audit issue 6: Policy on ownership of business knowledge and processes ▶ Is the business process ownership well delineated and documented? ▶ Is it ensured that the loss of business knowledge due to outsourcing does not occur? ▶ Is there capacity to conduct the outsourced services in house? ▶ •Can business continuity be ensured if the vendor was unable to provide services at any point/ in future?

Criteria: Organisation retain business knowledge and are able to continue operations in-house for mission critical function if contractors or vendors are unable to provide the service. Retention of business process ownership. Retention of business knowledge. Performance vis a vis business continuity with respect to the service provider failing to provide service at any point.	
Information required: ▶ Identification of business processes, and critical skills that need to be retained in-house ▶ Documentation of business processes ▶ Detailed system design document of outsourced service with the organisation ▶ List of training of staff on the business processes, system design, data, application software ▶ Incident reports/ correspondence related to stoppage of service/ dispute with the service provider, including those related to ownership of system/ data ▶ Meeting minutes with contractor.	**Analysis method/s:** ▶ Document review to assess that the ownership of the process, data and application software is retained by the organisation through adequate provisions in the contract. ▶ Document review to assess that the business knowledge in terms of data, application software, system design are well documented and that the staff is updated with these periodically through training etc. ▶ Document review to assess that the organisation and its staff are involved in any system updates carried out by the outsourced agency and the detailed system update documentation is provided to the organisation. ▶ Document review to assess that there are no incidents or disputes with the service provider with respect to ownership of system and data. ▶ Review meeting minutes with the contractor to ensure that if there are any high-level risks, they are jointly managed and tracked to ensure continuity of operations.

IS audit Domain: IT Outsourcing	
Audit area: Cost control and management	
Audit objective: To assess whether the organisation has ensured most economical cost through the life cycle of the outsourced contract.	
Audit issue 7: Cost benefit assessment ▶ Have all the costs (including future costs) for outsourcing been identified? ▶ Has due cost-benefit analysis been carried out and best option been chosen? ▶ Are there specific responsibilities on the organisation in the outsourcing, and do they have critical cost elements/ impacts built in? ▶ Are additional costs or escalated costs being charged to the agency?	
Criteria: The cost benefit analysis is realistic and is the basis on which the programme is managed and controlled.	
Information required: ▶ Initial cost benefit analysis ▶ Estimated cost of outsourced contract ▶ Selection process of the service provider vis a vis cost element	**Analysis method/s:** ▶ Document review to assess that all costs have been identified by the organisation, reviewed and approved by relevant stakeholders. ▶ Document review of the selection and approval process.

▶ Approval process documents related to selection ▶ Instances of additional costs/ escalation of costs by the service provider ▶ Service Level Agreement and contract ▶ Monitoring reports with respect to specific function/ activity for which escalation / addition of cost is being sought ▶ Action documents on requests for additional costs/ escalation of costs by service provider.	▶ Document review to assess that all costs are reflected in the contract and that there are no hidden costs including any future costs. ▶ Review that all costs are subject to cost-benefit analysis before commitment by the organisation. ▶ Review and comparison of estimated vs. actual expenditures on the contract. ▶ Review of expenditure vis a vis the available budget. ▶ Review of the performance of service provider on specific activity/ function for which change in cost is sought through monitoring reports and assess the need for such change. ▶ Review of action by organisation on additional costs/ escalation of costs by service provider.

IS audit Domain: IT Outsourcing	
Audit area: Service Level agreement	
Audit objective: To assess whether the agency has developed the Service Level Agreement detailing all its requirements and is actively monitoring the vendor against the agreement	
Audit issue 8: Adequacy of service Level agreement ▶ Is a service level agreement agreed to between the organisation and the service provider? ▶ Is the service level agreement detailed enough to identify all roles and responsibilities between the organisation and the service provider? ▶ Is the service level agreement implemented diligently? ▶ Does the organisation have a mechanism to monitor the implementation of the service level agreement? ▶ •Is there a mechanism available to address exceptions to the service level agreement?	
Criteria: The service level agreement is the basis for monitoring and controlling the contractor or vendor against technical and other requirements.	
Information required: ▶ Service level agreement or contract ▶ Technical and other requirements (list of services that will be performed by the vendor) ▶ List of responsibilities of organisation and vendor ▶ Baselines for the services that will be measured, measurement period, duration, location, and reporting timelines (defect rates, response time, help desk staffing hours, etc.) ▶ Periodic vendor performance status reports.	**Analysis method/s:** ▶ Document review to assess that all user requirements are translated to service level requirements. ▶ Document review to assess that the roles and responsibilities of the organisation and the service provider are clearly identified and delineated. ▶ Document review to assess that the parameters for performance levels are clearly identified and included in the service level agreement. ▶ Document review to assess that the service level monitoring mechanism is established and agreed to between the organisation and service provider. ▶ Review vendors status reports to assess that the parameters in the SLA are being reported on by the contractor and reviewed by appropriate personnel within the organisation.

	▶ Assessment of compliance to SLA technical parameters and baselines. ▶ Verify the action taken by the organisation for deviations from service level agreement.

IS audit Domain: IT Outsourcing	
Audit area: Security	
Audit objective: To assess whether the security requirements are addressed in outsourcing and being complied with.	
Audit issue 9: Response to security requirements ▶ Have the security requirements been identified by the organisation with respect to outsourcing? ▶ Is there a mechanism ensuring that the security requirements of the organisation are addressed by the service provider? ▶ Does the organisation have a mechanism to monitor compliance to security requirements by the service provider?	
Criteria: The organisation's pertinent security requirements are levied on the contractor as appropriate.	
Information required: ▶ Organisation security policy ▶ Outsourcing Contract ▶ Service Level Agreement ▶ Inventory of data, application software and hardware with the service provider ▶ Inventory of back up data files and application software with the service provider ▶ Access control logs of the data files, application software as well as hardware at the outsourced location ▶ Security plan for the back-up site and disaster recovery site ▶ Monitoring reports with respect to security issues ▶ Correspondence between organisation and service provider with respect to security issues.	**Analysis method/s:** ▶ Document review to assess that the security requirements have been identified by the organisation and built into the outsourcing contract or SLA. ▶ Verify if the organisation has the inventory of data files, application software. ▶ Verify that the organisation monitors/ is aware that status of data files, application software and hardware are preserved during the back up and data recovery process carried out by the outsourced agency. ▶ Verify if the organisation has assurance on authorization of any change in data, application software and hardware by the outsourced agency. ▶ Verify if the organisation has an assurance on the access to the data, application software and hardware at the outsourced location through study of access logs (physical and logical). ▶ Verify if the organisation has assurance on security mechanisms put in place by the service provider. ▶ Verify if the organisation receives regular reports and acts on the information in the monitoring reports.

IS audit Domain: IT Outsourcing
Audit area: Back-up and disaster recovery for outsourced services
Audit objective: To assess whether outsourced services adhere to business continuity and disaster recovery plans as required in the contract or service level agreement.

Audit issue 10: Backup and recovery Procedures Is the vendor meeting the requirements of the contract or SLA for BCP and DRP?	
Criteria: Contractual or service level agreement for BCP and DRP at the vendor.	
Information required: ▶ Contract or SLA ▶ Internal Audit or third-party certification of BCP and DRP readiness of the vendor ▶ Periodic reports of BCP / DRP testing or updates.	**Analysis method/s:** ▶ Review contract or SLA to ensure that the vendor is required to ensure BCP and DRP on the outsourced data, applications and services. ▶ Review contract or SLA to ensure that the vendor is to provide independent or internal audit reports that confirm that BCP/DRP activities are in place and that the vendor tests their procedures periodically. ▶ Review submitted reports from the vendor to ensure that testing has been conducted in accordance with the conditions of the contract and /or SLA. ▶ Review periodic reports to ensure that the procedures have been updated if needed

Annex 10: Audit matrix for audit of BCP/DRP

IS audit Domain: Business Continuity Plan and Disaster Recovery Plan	
Audit area: Business continuity Policy	
Audit objective: To assess whether there is an effective business continuity policy in the organisation.	
Audit issue 1: Policy Does the organisation have a contingency plan and policy for business continuity?	
Criteria: The organisation has a published/ approved and adopted contingency plan and has a policy in place that comprehensively covers all areas of contingency operations and clearly identifies training requirements and testing schedules.	
Information required: ▶ Business Continuity Policy Document ▶ IT Policy Document ▶ Approval process for adoption of business policy objectives ▶ Correspondence and minutes of meetings related to business continuity	**Analysis method/s:** ▶ Document review for assessing that the policy is consistent with the organisation's overall IT policies. ▶ Document review to assess that the policy addresses requirements of business continuity by defining organisation's contingency objectives, organisational framework and responsibilities for contingency planning. ▶ Review or interview personnel to determine how often the policy is updated if conditions change. ▶ Review policy to determine who approved it and when was it last distributed / interview a sample of business users to assess if the policy has been sufficiently communicated within the organisation.
IS audit Domain: Business Continuity Plan and Disaster Recovery Plan	
Audit area: Organisation of business continuity function	
Audit objective: To assess whether an adequate business continuity team is in place.	
Audit issue 2: Business continuity function Is there a business continuity team or equivalent function in place?	
Criteria: Coverage of all critical areas of the organisation in the team. Roles and responsibility requirements for the team members.	
Information required: ▶ Organisation chart of organisation ▶ Organisation chart of business continuity team ▶ Role/ responsibility description of the business continuity team members ▶ Correspondence / meeting minutes on issues of business continuity	**Analysis method/s:** ▶ Document review / Interview relevant staff to assess that all critical areas of organisation are represented in the business continuity team or equivalent ▶ Document review to assess that there is adequate ownership and assignment of business continuity responsibility on the senior management. For example, has the management identified the level and urgency of recovery, and is this reflected in the policy? ▶ Document review to assess that all critical departments have assigned team members for disaster recovery and their roles are clearly laid out. ▶ Interview a sample staff in business continuity team / equivalent to assess that they are aware of their roles for business continuity for each critical business unit/department.

▶ Business continuity plan	

IS audit Domain: Business Continuity Plan and Disaster Recovery Plan	
Audit area: Business Impact Assessment	
Audit objective: To assess whether the business impact assessment and risk assessment have been completed and a risk management system is in place.	
Audit issue 3: Risk assessment Have business impact analysis and risk assessments been carried out and critical data, application software, operations and resources been identified and prioritised?	
Criteria: Enterprise Risk Management framework or equivalent Business Continuity Policy or equivalent Completion of the Business Impact Assessment and identification of critical data, application software, operations and resources.	
Information required: ▶ Risk Assessment report(s) ▶ Business impact assessment report(s) ▶ List of critical data, application software, operations and resources for each function ▶ List of residual risks ▶ List of related stakeholders ▶ Review report(s) on risk and business impact assessment ▶ Enterprise risk assessment policy/ framework ▶ Minutes of meetings on risk assessment and business impact assessment.	**Analysis method/s:** ▶ Document review to assess that the risk assessment was carried out, probable threats and their impacts are identified. ▶ Document review to assess that all functional areas were considered in the risk assessment and impact assessment. ▶ Document review to assess that the impact analysis evaluated the impact of any disruption in relation to time and other related resources and systems. ▶ Document review to assess that the decision on residual risks were taken at appropriate level. ▶ Document review to assess that the organisation has determined RTOs (Recovery Time Objectives) and RPOs (Recovery Point Objectives) for each critical application. ▶ Document review to assess that the RTOs and RPOs are practical and reasonable for each application and line of business or function. ▶ Document review to assess that the senior management involvement/ approval. ▶ Document review to assess that relevant stakeholders were involved in risk identification and impact assessment.
Audit issue 4: Risk management Is a risk management process (including mitigation and tracking, etc.) in place and have emergency processing priorities been established?	
Criteria: Coverage of the risk management process vis a vis risk assessment and business impact assessment. Risks and emergencies are promptly addressed as per organisation's agreed parameters.	
Information required: ▶ Risk Management process document ▶ Risk Assessment and Business Impact Assessment Report(s)	**Analysis method/s:** ▶ Document review to assess that the risk management process addresses all high priority items.

▶ List of all relevant personnel, members of the BCP team with roles and responsibilities ▶ List of prioritized items for emergency process ▶ List of residual risks identified ▶ List of instances of emergency process being invoked ▶ Emergency process/ response reports.	▶ Interview and document review to assess that all relevant personnel, including senior management are aware of their role and responsibilities and carry them out. ▶ Document review to assess that the residual risks do not have material impact on the organisation. ▶ Document review and observation to assess that the emergency instances are adequately handled. ▶ Document review to assess impact of the emergency. ▶ Review meeting minutes or list of risks to determine that risks have been assigned, mitigation activities defined, and that risks are tracked periodically, and status updated.

IS audit Domain: Business Continuity Plan and Disaster Recovery Plan	
Audit area: Disaster Recovery Plan	
Audit objective: To assess whether the Business Continuity Plan includes back-up and recovery plans for hardware, data, application software and data centre (recovery) and has been suitably implemented?	
Audit issue 5: Back-up Procedures Have the data and program back-up procedures been devised and implemented effectively?	
Criteria: Established criticality of applications and functions as per Organisation's Business Impact Assessment. Determined periodicity of back-ups. Documented back-up and recovery plans.	
Information required: ▶ Back up plans and procedures for the hardware, data, application software ▶ Back-up logs/ Version logs ▶ Roles and responsibilities for back-up ▶ List of storage locations and periodicity ▶ Retention schedule ▶ Security arrangement for back-up site ▶ Disaster logs ▶ Roles and responsibilities for recovery activities ▶ Training records of responsible personnel ▶ Impact assessment of disasters ▶ Report on disaster recovery activities.	**Analysis method/s:** ▶ Document review to assess that the back-up plan includes all critical hardware, data, application software. ▶ Document review to assess that detailed back-up procedures have been devised. ▶ Document review to assess that the back-up plan is adequately implemented. ▶ Analysis of logs to assess the back-up is taken at determined timelines and are retained for the specified time period. ▶ Verify that the right version of back up is available. ▶ Document review to assess the adequacy of back-up location and the mode of transport of back up files etc. to the back-up location. ▶ Verify that the security, logical or physical is adequate for the back-up site. ▶ Verify that the back-up files can be used for recovery. ▶ Document review to assess that back-up procedures are implemented minimising loss of time and resources. ▶ Document review to assess that detailed recovery procedure has been devised and includes resetting of system parameters, installation of patches, establishing the configuration settings, availability of the system documentation and operating procedures,

	reinstallation of application and system software, availability of most recent backup, and testing of system. ▶ Document review to assess that recovery procedures are implemented minimising loss of time and resources. ▶ Document review/ Interview staff to assess that the relevant staff have been trained on the back-up and recovery procedures.

IS audit Domain: Business Continuity Plan and Disaster Recovery Plan	
Audit area: Environment Control	
Audit objective: To assess whether the organisation has suitable environment control at back-up sites.	
Audit issue 6: Control mechanisms Has an environment control mechanism been devised and put in place at the back-up site?	
Criteria: Environment control parameters in the environment control mechanism.	
Information required: ▶ Environment Control programme ▶ List of probable environment hazards identified during risk assessment with locations (risk assessment document) ▶ List of environment mitigating steps undertaken.	**Analysis method/s:** ▶ Document Review , observation, walk through of procedures to assess that: ○ Un-interrupted power supply is available. ○ Adequate fire protection system is put in place. ○ Humidity, temperature and voltage are controlled within limits. ○ Adequate flood protection system is put in place. ○ Environment controls are as per the regulations. ○ Environment control measures are conveyed to and adhered to by all concerned staff.

IS audit Domain: Business Continuity Plan and Disaster Recovery Plan	
Audit area: Documentation	
Audit objective: The business continuity plan is adequately documented to conduct effective interim business activities and recovery procedures after a business interruption.	
Audit issue 7: Documented plans for backup and recovery procedures, roles and responsibilities Does the organisation have a documented disaster recovery plan that is readily available for back-up and recovery?	
Criteria: Availability and currency (newness) of the business continuity and disaster recovery plan	
Information required: ▶ Business continuity plan ▶ Disaster recovery plan ▶ Version/ currency of business continuity and disaster recovery plan ▶ Distribution list of business continuity and disaster	**Analysis method/s:** ▶ Document review to assess the currency of the business continuity plan. ▶ Document review to assess the currency of the disaster recovery plan ▶ Verify if the latest version of business continuity plan and the disaster recovery plan are communicated to all concerned. ▶ Determine if the business continuity and disaster recovery plan documents are available at off-site to be available in case of a disaster.

recovery plans to all concerned. ▶ OAGN form: Data Backup authentication form	▶ Verify that roles and responsibilities of back-up and disaster recovery team/ related staff are clearly listed out. ▶ Interview a sample of staff to assess whether disaster recovery procedures are known and understood.

IS audit Domain: Business Continuity Plan and Disaster Recovery Plan	
Audit area: Testing the BCP/DRP	
Audit objective: To assess whether the business continuity disaster recovery procedures have been tested.	
Audit issue 8: Trials Has the organisation tested its BC and DR procedures, and what changes (if any) have been made as a result of the test?	
Criteria: The organisation should test its documented BCP and DRP procedures via drills or mock-ups to ensure that they work in actual conditions. Personnel involved in ensuring continuity should be aware of their roles.	
Information required: ▶ BC and DR procedures & Test procedures ▶ List of items for which business continuity/ disaster recovery plan has to be tested ▶ Frequency of testing of business continuity plan and disaster recovery plan ▶ List of tests conducted ▶ List of test criteria like RTOs and RPOs etc. ▶ List of testing methods employed ▶ Test results & actions taken or test recommendations ▶ Follow up action on test results.	**Analysis method/s:** ▶ Document review to assess whether all relevant items are covered for testing. ▶ Document review to assess whether the tests are conducted are right intervals, in time. ▶ Document review to assess that the tests were conducted against identified criteria. ▶ Document review to assess that the tests were conducted using appropriate testing methods. ▶ Document review to assess that the recommendations are conveyed to appropriate authorities for follow-up. ▶ Document review to assess that the test recommendations are adequately followed up and the business continuity plan or the disaster recovery plan are adequately updated.

IS audit Domain: Business Continuity Plan and Disaster Recovery Plan
Audit area: Security
Audit objective: To assess whether business continuity plan and disaster recovery plan ensure security of data, application software, hardware and data center.
Audit issue 9: Efficiency of security Indicators To determine whether the data, application software, hardware and data centre are secured appropriately during the back-up disaster recovery procedures?

Criteria: Security baselines for the organisation like procedures laid down in the IT security policy and disaster recovery plans	
Information required: ▶ Inventory of data, application software and hardware ▶ Inventory of back-up data files and application software ▶ Access control logs of the data files, application software as well as hardware ▶ Security plan for the back-up site and disaster recovery site.	**Analysis method/s:** ▶ Verify if the number and status of data files, application software and hardware are preserved during the back-up and data recovery process. ▶ Verify if the data, application software and hardware have undergone any change during the process of back-up or disaster recovery through study of control totals on number of records and size of files related to data and application software. ▶ Verify if there has been any breach of security through examination of access control logs (physical and logical).

IS audit Domain: Business Continuity Plan and Disaster Recovery Plan	
Audit area: Back-up and disaster recovery for outsourced services	
Audit objective: To assess whether outsourced services adhere to business continuity and disaster recovery plans.	
Audit issue 10: To determine whether the outsourced service provider ensures adoption of the organisation's business continuity plan and disaster recovery plan.	
Criteria: Backup and disaster recovery Procedures for outsourced services, service agreements	
Information required: ▶ Inventory of data, application software and hardware of the organisation with the outsourced agency ▶ Inventory of back-up data files and application software of the organisation with the outsourced agency ▶ Access control logs of the data files, application software as well as hardware with the outsourced agency ▶ Test results of back-up plan and disaster recovery plan at the outsourced agency ▶ Security plan for the back-up site and disaster recovery site at the outsourced agency site ▶ Strategy to ensure continuity in case of takeover of the service provider by another organisation ▶ Information on any takeover of the service provider	**Analysis method/s:** ▶ Verify if the organisation verifies if the number and status of data files, application software and hardware are preserved during the back-up and data recovery process at the outsourced agency. ▶ Verify if the organisation verifies if the data, application software and hardware have undergone any change during the process of back-up or disaster recovery through study of control totals on number of records and size of files related to data and application software at the outsourced agency. ▶ Verify if the organisation verifies if there has been any breach of security through examination of access control logs (physical and logical). ▶ Verify if the organisation verifies that the testing of back-up and disaster recovery is ensured at the outsourced agency. ▶ Verify whether the organisation is aware of the risks associated with possibility of takeover of the service provider. ▶ Verify whether the organisation has ensured that the Business Continuity is embedded in the service agreement.

Annex 11: Audit matrix for audit of Information Security

IS audit Domain: Information Security	
Audit area: Risk assessment	
Audit objective: To ensure that all risks associated with information security have been identified and an appropriate risk mitigation strategy is put in place.	
Audit issue 1: Assessment mechanism Does the organisation has an effective and well-documented information security risk assessment mechanism?	
Criteria: Internal policy, procedures or regulations reflect organisation's preparedness to manage critical risks	
Information required: ▶ IS Security Policy ▶ Formal procedures of risks management ▶ System configuration documentation.	**Analysis method/s:** ▶ Analyse risk management policy, risk assessment documents and interview top management and operational level to: ○ understand the real role of the organisation in risk assessment procedures. ○ identify who are involved in assessing risks. ○ find out the mechanism's operational costs. ○ verify whether risk assessment is performed and documented on a regular basis, or whenever the conditions change. ○ check if the current system configuration is documented, including links to other systems. ○ check if the documentation contain descriptions of key risks for the organisation's system, business, and infrastructure? ▶ In the case of lack of the formal procedures and documents on risk assessment, do not underestimate controls that are embedded within the operation procedures of the organisation – verify if the compensatory control mechanism embedded within operations is effective. This can be seen by walk through of a sample of operations, etc.
Audit issue 2: Coverage Does the risk assessment cover all important internal and external risks? Are possible effects and impact of Information Security breaches assessed?	
Criteria: All the significant risks are identified and assessed properly (best practices in risk assessment[90]).	
Information required: ▶ Documented Risk Assessments ▶ Risk register ▶ Incident handling reports.	**Analysis method/s:** ▶ Review documents to check if the risk assessment performed by the audited organisation was based on sufficiently comprehensive information. Check whether data and reports were obtained from the organisation's incident management system. (Support your analysis with results of Analysis Methods of IT Operations focused on Incident Management system, esp. if the information security incident handling

[90] ISO 27005 information security risk management, ISACA Risk IT Framework, COSO Enterprise Risk Management Framework.

	forms a system separated from a general incident management system.) ▶ Validation Test 1: Security audit trails: Determine if security audit trails capture user identification (ID), type of event, data and time, success or failure indication, origination of event, and the identity or the name of the affected object ▶ Interview relevant personnel to verify whether there is a standard re-assessment of risk whenever the organisation plans to roll out new information systems, upgrades, and new versions. ▶ Check the risk assessment design for completeness, relevancy, timeliness and measurability. ▶ Check if consequences of infrastructure inoperability is considered while assigning risk categories. Verify documents to see if a business impact analysis is done for the consequences of critical information becoming unavailable, corrupted, inappropriately compromised or lost. ▶ Review incidence response reports and earlier risk documents/ registers to examine whether the risk assessment methodology has been effective in the past
Audit issue 3: Mitigation Are significant risks mitigated in effective and efficient way?	
Criteria: Adequate risk mitigation practices are in place.	
Information required: ▶ Problem/incident handling reports ▶ Periodic activity reports.	**Analysis method/s:** ▶ Review incident handling reports and check whether appropriate procedures were in place to prevent, detect and control security risks identified in the risk assessment document. ▶ In organisations that do not follow a well-defined risk assessment mechanism, determine what compensatory control exist. Analyse if any serious security incidents occurred in relation to risks that might have been mitigated better with a properly working risk assessment mechanism, vis-à-vis existing compensatory controls. ▶ Take into account that problem/incident reports may be incomplete in some cases. Nevertheless, important events may be reflected directly or indirectly in other documents, as e.g. annual activity reports or other periodic reports.

IS audit Domain: Information Security
Audit area: Information Security Policy
Audit objective: To assess whether there is adequate strategic direction and support for information security in terms of a security policy, its coverage, organisation-wide awareness and compliance.

Audit issue 4: Information security Policy Does the organisation possess an Information Security Policy? Is it properly implemented and documented? Does it form a consistent and robust IT security plan?	
Criteria: The organisation's information security policy covers all operational risks and is able to reasonably protect all business-critical information assets from loss, damage or abuse[91].	
Information required: ▶ IT Strategy ▶ Legal acts defining information security requirements ▶ Formal and written information security policy ▶ Organisation structure and its job description ▶ Contractual arrangements with external party's IT Security Plan.	**Analysis method/s:** ▶ Check the document to examine whether IT Strategy adequately highlights the critical role of Information Security. Also refer and use the IT Governance matrix for IT Strategy. In the absence of a written IT strategy, interview top management, middle level management and staff to see what their understanding of the strategic role of Information security is. ▶ Assess compliance of the organisation's IT Strategy and Information Security Policy external compliance requirements ▶ Compare policy goals and security procedures to determine the effectiveness of integration of information security requirements into the IT security plan (charter, framework, manual etc.). Verify whether it is regularly reviewed at appropriate management levels. ▶ Examine coverage of the IT security plan and check whether it considers IT tactical plans, data classification, technology standards, security and control policies and risk management. ▶ Check if the IT security plan identifies: Roles and responsibilities (board, executive management, line management, staff members and all users of the enterprise IT infrastructure), Staffing requirements, Security awareness and training; Enforcement practices; and the need for investments in required security resources. ▶ Review and analyse the charter to verify that it refers to the organisational risk appetite relative to information security, and that the charter clearly includes scope and objectives of the security management function. ▶ Check security incident reports and follow-up documents to find what actions the organisation takes when individuals violate the security policy. ▶ Check the incident reports to identify the number of Information Security breaches by employees or external parties in given period to assess effectiveness of the policy.
Audit issue 5: Confidentiality Has the organisation confidentiality requirements or non-disclosure agreements that appropriately reflect the need for protecting information? Do the policies secure information in the organisation's relation with external parties?	
Criteria: The organisation's information security policy is able to protect all confidential information related to internal stakeholders and third parties	

[91] See ISO 27000 series Information Security Management System and other internal policy, procedures or applicable regulations

Information required:	Analysis method/s:
▶ External and internal regulations concerning confidential and classified information. ▶ E.g., Non-disclosure clauses for employees. ▶ Contractual arrangements with external parties ▶ Information security policy ▶ IT Security Plan.	▶ Check procedural measures taken by the organisation to comply with the confidentiality requirements. ▶ Where access to confidentiality breach cases are restricted to special law procedures and specialised agencies only, base your opinion on their reports and recommendations to the organisation's management – if available. ▶ Review contractual arrangements with external parties or contractors. Do they involve granting and invoking access, processing, communicating or managing organisational information assets? ▶ Check whether the contractual terms and obligations define the security restrictions and obligations that control how contractors will use organisation's assets and access information systems and services. ▶ Check whether any information security breaches were committed by contractors. Check management action on such breaches.

IS audit Domain: Information Security	
Audit area: Organization of IT security	
Audit objective: To ensure the secure operation of IT processing facilities.	
Audit issue 6: Structure Does the auditee have clear organisation of IT security? Are security roles and responsibilities defined with regard to information security policy?	
Criteria: Documented and clear IT roles and responsibilities relating to Information Security Policy[92]	
Information required: ▶ IT Organisation structure ▶ Internal regulations related to IS security ▶ Job descriptions ▶ Minutes of relevant bodies' meetings.	**Analysis method/s:** ▶ Determine if the responsibility for IT security is formally and clearly stated. ▶ Check whether a process exists to prioritise proposed security initiatives, including required levels of policies, standards and procedures. ▶ Check how senior management maintains an appropriate level of interest in information security within the organisation.
Audit issue 7: Coordination How does the organisation coordinate information security activities from different parts of organisation?	
Criteria: No responsibility conflicts, disharmony nor "no-man's land" in Information Security activities[93]	
Information required: ▶ Legal requirements concerning classified information ▶ Organisation structure	**Analysis method/s:** ▶ Check documents observe practices and interview personnel to verify whether there are inherent conflicts/ overlaps/ gaps between security procedures followed by employees in different departments/ units.

[92] See ISO 27000 series
[93] See ISO 27000 series Information Security Management System

▶ Internal regulations related to IS security ▶ Minutes of meeting of IT security committee ▶ Failure reports.	▶ Check operational workflow procedures to identify if some information is transmitted to external parties out of control of responsible units/employees. ▶ Check if higher level managers are aware of coordination problems and whether they supervise inspections and coordinating activities. ▶ Review processes to check whether there is any established procedure for management to authorize new information processing facilities.

IS audit Domain: Information Security	
Audit area: Communication and Operations management	
Audit objective: To ensure that internal and external communication is secure.	
Audit issue 8: Policy and procedures Are policy and procedures adequate for safe and efficient internal and external communication?	
Criteria: The policy and procedures form stable management environment for internal and external communication[94]	
Information required: ▶ Formal and written policy for communications and IT operations ▶ Documentations of operational procedures.	**Analysis method/s:** ▶ Check whether the policies and procedures of the organisation embrace communication with citizens, mass media, and external organisations. ▶ Verify how the organisation documents its operating procedures and makes them available to all users. Interview a sample set of users at different levels to examine whether the procedures for data handling are well known by employees. ▶ Check how often the communication and data handling procedures are reviewed and updated.
Audit issue 9: Network control How does the organisation manage and control information in the network?	
Criteria: Network operations are managed and performed in safe and effective way	
Information required: ▶ Information restriction policy ▶ Network Admin Logs/Registers ▶ Results of the logs analysis ▶ User Acceptance Test Report ▶ Service Level Agreement(s)	**Analysis method/s:** ▶ Check what tools are used for network monitoring and analysis. verify whether users and IT systems of the audited organisation are protected against spam. ▶ Check whether Intrusion Detection System configurations and logs are analysed by appropriate personnel to ensure security of information from hacking attacks and malware intrusions. Verify whether the attacks (failed and effective ones) are analyzed and reported. ▶ Check the statistics of spam, hacking and malware attacks. ▶ Inquire how the organisation provides secure transmission of transactions passing over public networks. E.g. Circulating/ notifying operating procedures to users for online transactions.

[94] See following standards: ISO-27002, S15-IT Control (ISACA Standard), COBIT

▶ Information available to the public or found in the web pages.	▶ Review policies to verify whether data transmission outside the organisation requires an encrypted format prior to transmission. ▶ Inquire whether information security policies have been implemented in accordance to the sensitivity classification of organisation's data (e.g., confidential, sensitive). ▶ Through enquiry determine whether the client utilises cryptography for sensitive information processing. ▶ If so, conduct a validation testing. **Control validation Testing Procedures** Validation Test 1: Operating effectiveness of cryptographic controls: Determine: ○ the existence of processes for the key management life cycle. ○ key destruction. ○ segregation of duties for the authorized key custodians
Audit issue 10: Configuration management Are the IT resource settings/ applications under appropriate configuration control?	
Criteria: Clear and well-managed configuration system that supports Information Security in communication and operations.	
Information required: ▶ Policy and procedures referring to configuration matters in operations area ▶ Configuration lists/ library.	**Analysis method/s:** ▶ Review role matrices to determine who is responsible for administering the configuration, and what the scope of the configuration control in operations is. ▶ Check how it is registered, controlled and updated. ▶ Verify if any problems occurred in the past because of configuration discrepancies. If so, interview managers to check what procedures have been implemented to configuration changes

IS audit Domain: Information Security	
Audit area: Assets Management	
Audit objective: To encourage appropriate protection of IT assets.	
Audit issue 11: Assets management Does organisation have an appropriate asset management system that supports its Information Security?	
Criteria: Ensuring appropriate protection of information assets (Ref: ISO 2700 series Information Security Management System, COBIT, and other internal policy, procedures or regulations applied).	
Information required: ▶ Asset management policy ▶ Asset Classification ▶ Information classification ▶ Asset disposal procedures ▶ Financial audit reports (if they refer to assets and inventories).	**Analysis method/s:** ▶ Review policy to check if there is an acceptable use policy for IT hardware and software (Example, laptops may be used for personal use if it does not interfere with official business). ▶ Check whether the asset database is up to date. ▶ Check inventory records to verify whether assets are categorised in terms of value, sensitivity, or other categories. ▶ Review procedures for assets disposal and the level of supervision mandated. Check the authorization requirement for any disposal or re-

	use of equipment. Inquire persons and check provisions that ensure data is erased prior to disposal or re-use of equipment.

IS audit Domain: Information Security	
Audit area: Human Resources Security	
Audit objective: To ensure that all employees (including contractors and any user of sensitive data) are qualified for data handling and understand their roles and responsibilities, and that access is removed once employment/ contract is terminated.	
Audit issue 12: Staff awareness and responsibility Are employees aware of their roles and responsibilities with respect to their duties and security responsibilities?	
Criteria: Professionally trained staff in guarding information security	
Information required: ▸ HR Policy and recruitment procedures ▸ Information Security policy and procedures ▸ Competency Standard for IT Personnel ▸ Individual assessment reports ▸ Security incident reports (including violation of code of ethics or code of conduct) ▸ Security Awareness Campaign ▸ User Management ▸ Roles and Responsibilities.	**Analysis method/s[95]:** ▸ Inspect hiring documentation for a representative sample of IT staff members to evaluate whether background checks have been completed and evaluated. ▸ Inspect selection criteria for performance of security clearance background checks. ▸ The role of each position must be clear. Supervision activities should be run to check adherence to management policies and procedures, the code of ethics, and professional practices. ▸ Check if roles that are critical for Information Security are clearly defined and documented. Employees and third parties assigned such roles should know their responsibilities with respect to protecting the organisational information assets, including electronic data, IS infrastructures, and documents. Review for appropriate definition of critical roles, for which security clearance checks are required. This should apply to employees, contractors and vendors. ▸ Check for appropriate Segregation of Duties between IT security management and Operations. ▸ Check if the policy of IT personnel placement, transfer and rotation, as well as employee termination is clear to reduce dependence on the individual. Verify what knowledge transfer mechanisms are followed.
Audit issue 13: Training Is training in Information Security procedures effective in enhancing staff's professional skills in guarding the same ?	
Criteria: Conduct, Scope and Periodicity of Organisational Training for Information Security.	
Information required: ▸ Training schedule	**Analysis method/s:**

[95] Human resources vis-à-vis Information Security is one of key topics in other sections including IT Governance, and portions of this Audit Matrix such as Information Security Policy (awareness, responsibility, top-down information flow, sanctions) and/or Access Control (individual user rights)

▶ Results of ending tests ▶ Evaluation of training effectiveness.	▶ Assess the training effectiveness measurement process, if any, to confirm that the critical IT security training and awareness requirements are included. ▶ Inspect IT security training programme content for completeness and appropriateness. Inspect delivery mechanisms to determine whether the information is delivered to all users of IT resources, including consultants, contractors, and temporary staff members and, where applicable, customers and suppliers. ▶ Inspect training programme content to determine if all internal control frameworks and security requirements are included based on the organisation's security policies and internal controls (e.g., impact of non-adherence to security requirements, appropriate use of company resources and facilities, incident handling, employee responsibility for information security). ▶ Inquire whether and confirm that training materials and programmes have been reviewed regularly for adequacy. ▶ Inspect the policy for determining training requirements. Confirm that the training policy ensures that the organisation's critical requirements are reflected in training and awareness programmes. ▶ Interview staff to assess whether they have undergone the organisational training and whether responsibilities in maintaining information security and confidentiality are clearly understood by them.

IS audit Domain: Information Security	
Audit area: Physical Security	
Audit objective: To prevent theft or damage of IT hardware, unauthorized access, and copying or viewing of sensitive information.	
Audit issue 14: Premises safety Are the buildings and grounds of the organisation secured against physical and environmental risks?	
Criteria: Ensure that physical and environmental security stays in compliance with the safety requirements and sensitivity classification of IT assets.	
Information required: ▶ Network diagram ▶ Site Security Plan ▶ Periodical physical testing report ▶ Reports by relevant services (e.g. Fire dept).	**Analysis method/s:** ▶ Analyse what the audited organisation's primary physical security controls are. Check if they match the up-to-date risk analysis. ▶ Review location and physical precautionary measures for key elements of IT infrastructure. Check what environmental controls are in place (fire extinguisher, alarm, power systems, etc.). ▶ Verify if recommendations by relevant services (esp. firemen, housing inspection, disaster prevention) been implemented. ▶ For security plans relating to disasters, refer to BCP and DRP matrices.
Audit issue 15: Physical access Are the buildings and grounds of the organisation secured against physical and environmental risks?	

Criteria: Security measures are put in place by the organisation to ensure no unauthorised physical access to critical IT facilities (server rooms, data storage etc.)	
Information required: ▶ Layout of IT hardware installation ▶ Site Security Plan ▶ Devices configuration ▶ Periodical physical testing report ▶ Incident reports.	**Analysis method/s:** ▶ Review security instructions, network diagram and related documents and check how the organisation controls access to sensitive areas of its premises. ▶ Review and observe the in/out traffic and how the physical security system works. ▶ Determine what means are used. Obtain policies and procedures as they relate to facility security (gates, badges, turnstiles, guards, barriers, key and card reader access etc.) and determine if those procedures account for proper identification and authentication. ▶ Check who maintains and controls the allocations of access control to the sensitive locations. Find if the level of management is sufficient for Information Security. ▶ Find if access to secure areas /secure rooms/ server locations is restricted. ▶ Select a sample of users/employees and determine if their access to facilities is appropriate, based upon their job responsibilities. ▶ Verify if incidents are reported to an incidents/problems management system. Find if they are analysed and lessons learnt.
Audit issue 16: Intrusion defense. Whether the organisation has a policy on intrusion detection and follows it	
Criteria: Procedure to combat intrusions as laid down in Organization's Internal Security Policy	
Information required: ▶ Site Security Plan ▶ Devices configuration ▶ Incident reports.	**Analysis method/s:** ▶ Inquire how the organisation's security unit knows that an intrusion has occurred to secure locations. ▶ Check instructions to find out the Process for handling an intrusion to a secure space or building. ▶ Check incident reports to identify whether intrusion was detected early. ▶ Check if the organisation have a clear desk or clean screen policy to prevent unauthorised access.

IS audit Domain: Information Security	
Audit area: Access control	
Audit objective: To ensure that only authorized users have access to relevant information	
Audit issue 17: Access policy Does the organisation have clear and efficient policy on access control?	
Criteria: The Access Policy gives sound basis for control of relevant information distribution.	
Information required: ▶ Access Policy and procedures ▶ List of users	**Analysis method/s:** ▶ Analyse Access Policy and procedures to ensure that employee duties and areas of responsibility are separated in order to reduce opportunities for unauthorised access and privilege approval.

▶ Access control list/ matrix.	▶ Validation Test: Operating effectiveness of authorization of user access to the LAN (not separate testing of user access to applications should be done in conjunction with application reviews). Select a sample of user and system accounts to determine existence (access control software maybe used) of the following: ○ clearly defined requested role and/or privileges mapped to job functions. ○ business justification for access. ○ data owner and management authorization (i.e. signatures/ written approvals). ○ Business/risk justification and management approval for non-standard requests. ○ Access requested is commensurate with job function/role and required segregation of duties.
Audit issue 18: Privileges management. Is process for granting and revoking access control to employees and contractors safe and effective?	
Criteria: The Information Security function monitors user account management operations on a timely basis and reports the operating efficiency and effectiveness.	
Information required: ▶ Access control procedures ▶ Sample of employees' transfers and terminations.	**Analysis method/s:** ▶ Check procedures to determine how often the various accesses and privileges that employees or users have in the organisation are reviewed. ▶ Check how the privileges that are granted to an employee are confirmed (examples include asking the supervisor, area manager, group, etc.) ▶ Interview sample of users and check instructions to verify how the users are informed about their responsibility for protecting sensitive information or assets when the access is granted to them. ▶ Determine whether the organisation's security practices require users and system processes to be uniquely identifiable and systems to be configured to enforce authentication before access is granted, and that such control mechanisms are utilised for controlling logical access across all users, system processes and IT resources. ▶ Analyse other than password privileges, e.g. how it is checked that a user does indeed have sufficient access and privileges to the requested resource? (Examples include access from secure location, hardware tokens or fingerprint readers, etc.) ▶ Validation Test 1: Operating effectiveness of transfers and terminations: Obtain from HR a sample of employee transfers and terminations and, through review of system account profiles and/or CAATs (e.g. ACL, IDEA) determine if access has been appropriately altered and/or revoked in a timely manner. ▶ Validation Test 2: Password management: Verify that the quality requirements for passwords are defined and enforced by the network management system and/or operating

	systems based on local requirements/ organisation policy or best practice.

For audit issues related to security, please refer to audit matrices of IT Operations, IT outsourcing, BCP/DRP.

Vulnerability assessment and Penetration testing (VAPT)

Key definitions, purpose and scope of VAPT[96]

Vulnerability assessment and penetration testing are both security services that focus on identifying vulnerabilities in the network, server and system infrastructure.

1) A **Vulnerability Assessment** is a rapid automated review of network devices, servers and systems to identify key vulnerabilities and configuration issues that an attacker may be able to take advantage off. It's generally conducted within the network on internal devices and due to its low footprint can be carried out as often as every day.

Vulnerability Assessment answers the question "What are the issues on my network?"

2) A **Penetration Test** is an in-depth expert-driven activity focused on identifying various possible routes an attacker could use to break into the network. In-addition with the vulnerabilities it also identifies the potential damage and further internal compromise an attacker could carry out once they are past the perimeter.

Penetration Testing answers the question "What can a motivated attacker do?

VAPT together helps IS Security Auditors in finding flaws that exist in the system and risks associated with those flaws.

VAPT is usually carried out by professional organizations providing services in areas of IS security audits. The first step of VAPT is usually defining the scope of the audit and depends on the organization, it's industry and compliance standards. The output of VAPT usually contains a technical report explaining each issue identified, step-by-step POCs (Proof of Concepts) for each issue, code and configuration examples to fix the issue and reference links for further detail.

Vulnerability Assessment & Penetration Testing (VAPT) are largely mandated across various industries and sectors. There are a wide range of compliance standards that require such audits to be carried out periodically. Some of the well-known international standards are:

- ISO 27002 / ISO 27001
- PCI DSS – Payment Card Industry Data Security Standard
- SOX – Sarbans-Oxley Act
- HIPAA – Health Insurance Portability and Accountability Act
- TRAI – Telecom Regulatory Authority of India
- DOT – Department of Telecommunication
- CERT-In – Cyber Emergency Response Team of India
- GLBA – The Gramm–Leach–Bliley Act
- FISMA – The Federal Information Security Management Act
- NIST – National Institute of Standards and Technology
- SAS 70 – Statement on Auditing Standards
- COBIT – Control Objectives for Information and Related Technology

[96] Source: https://vapt.in/

Only in case the auditee under consideration is mandated to carry out VAPT (in Nepal), and objective of overall audit requires audit of Information Security aspects of the application, IS auditors shall check whether:

- the entity has undertaken vulnerability scanning and penetration testing of the network and systems in scope to provide assurance over the security of their IT environment.
- the entity follows up on matters from the penetration testing and takes appropriate actions to resolve or mitigate against risks and vulnerabilities.

Method for audit analysis for IS auditors:

- Enquire of management what security standard and operational system compliance has been carried out. In particular ascertain whether a VAPT (penetration test) has been performed by a qualified penetration tester.
- External testing should include:
    - systems that provide services on the internet (such as email servers and web servers)
    - systems to prevent unauthorised access from the internet into the organisation (such as firewalls)
    - systems to allow staff and contractors to connect into the organisation remotely (such as a Virtual Private Network)
    - if the organisation uses third-party suppliers and they have access to and from the organisation's systems from their own office locations this should also be considered as an external connection and tested
- Internal testing should include vulnerability scanning and manual analysis of the internal network. At a minimum it should include:
    - desktop and server build and configuration
    - network management security
    - patching at operating system, application and firmware level
    - configuration of remote access solutions (including solutions for managed devices and Bring Your Own Device if allowed)
    - build and configuration of laptops and other mobile devices such as phones and tablets used for remote access
- Review findings and assess significant issues and follow up activities.

Annex 12: Audit matrix for audit of Application controls

IS audit Domain: Application Controls	
Audit area: Input controls	
Audit objective: To assess whether valid data is being entered into the application by authorised personnel.	
Audit issue 1: Validation of inputs Does the application have adequate input validation controls?	
Criteria: Several good practices provide basis for criteria of good input validation controls, e.g. validation rules are comprehensive, documented and implemented into the application entry interfaces; different methods and interfaces for data entry are documented; invalid data is properly rejected by the application; the validation criteria is updated in a timely, appropriate and authorized manner; there are compensating controls such as logs and authorisation rules in case of the possibility of overriding input controls; and there are proper controls and documentation for the application interfaces.	
Information required: ▶ Business requirements and rules ▶ Data input types ▶ Legal and external compliance requirements ▶ Structure of data interfaces with other applications ▶ System flow diagrams ▶ User manuals ▶ Validation rules	**Analysis method/s:** ▶ Analyze business rules, requirements, application documentation and inquire business process owners to determine which validation rules should be assured in the business process being assessed. Check if these validation rules were proper designed and documented. Verify whether the validation controls for data input are being enforced: observing application users into real action; running the application in a testing environment and testing different interfaces for data entry; and analysing data records stored in the database through the use of CAATs. ▶ Obtain functional description for each class of input and design information on transaction data entry. Inspect the functionality and design for the presence of timely and complete checks and error messages. If possible, observe transaction data entry. ▶ Assess whether validation criteria and parameters on input data match business rules and enforce rejection of unmatched input types. In case of online processing systems, verify that invalid data is rejected or edited on entry and test the logic checks/calculation checks performed. Database operatives (such as *, =, or, select) should be disallowed as valid input, as they can be used to disrupt or retrieve information from the database. ▶ Inquire managers about whether validation criteria and parameters on input data are periodically reviewed, confirmed and updated in a timely, appropriate and authorized manner. Assurance could be obtained through documentation review, code analysis or interviews. ▶ Inquire and check documentation in order to verify the possibility of overriding input data control validations and controls. Verify if the override actions are being properly logged and reviewed for appropriateness. Check whether authority to override is restricted to only supervisory staff and to a limited number of situations. Inspect error corrections, entry overrides and other documents to verify that the procedures are followed.

	▶ Determine which interfaces exist with the application. These interfaces could be in the form of real-time data transmission or periodic transmission of data files via batch processes. Review system flow diagrams and system code and interview the application developers or administrator to obtain information on interfaces and controls over them. E.g.: Control totals from interface transmissions. E.g., Hash[97]
Audit issue 2: Is management of source documents, data collection and entry adequate?	
Criteria: Data preparation procedures are documented and understood by users; there is appropriate logging and records of the source documents received until their disposal; there is assignment of unique and sequential numbers to each transaction and original source documents are retained for the time required by legal standards or policies.	
Information required: ▶ Classes of source documents ▶ Entity's criteria for timeliness, completeness and accuracy of source documents ▶ Data preparation procedures ▶ Data interfaces with other applications ▶ Document retention policies ▶ System flow diagrams	**Analysis method/s:** ▶ Inspect and observe creation and documentation of data preparation procedures and inquire whether and confirm that procedures are understood, and the correct source media are used. ▶ Assess whether the Data Processing group (DP) or equivalent group maintains a log of all the user departments' source documents received and their final disposal. Verify the existence of a system of reconciliation of record counts with user department groups. ▶ Verify that all source documents include standard components, contain proper documentation (e.g., timeliness, predetermined input codes, default values) and are authorized by management. ▶ Inspect whether critical source documents are pre-numbered and how out-of-sequence numbers are identified and taken into account. Identify and review out-of-sequence numbers, gaps and duplicates using automated tools (CAATs). ▶ Verify if there is assignment of unique and sequential numbers to each transaction preventing duplication. ▶ Enquire responsible personnel about retention policies. Verify how these policies are ensured. A sample of system records might be checked against its source documents.
Audit issue 3: Does the application have adequate procedures for error handling?	
Criteria: There is a system of clear and compact error messages communicating the problems so that immediate corrective action can be taken for each type of error. Errors are corrected or appropriately overridden before processing transactions. Logs are reviewed periodically, and necessary corrective action is taken.	
Information required: ▶ Error types and messages ▶ Log review procedures	**Analysis method/s:** ▶ Discuss the application's error and exception handling with the developer and/or administrator. Inquire whether and confirm that

[97] A method for ensuring the accuracy of processed data. It is a total of several fields of data in a file, including fields not normally used in calculations, such as account number. At various stages in the processing, the hash total is recalculated and compared with the original. If any data has been lost or changed, a mismatch signals an error

▶ Policies and procedures for dealing with rejected data ▶ Suspense file review procedures	policies and procedures exist for handling transactions that fail edit and validation checks. ▶ Verify whether the system provides error messages for every type of error (field level or transaction level) not meeting the edit validation. ▶ Verify how the application behaves if data is rejected by the input controls. Check whether the data items are recorded or if they are automatically written in a suspense file. Check if the automated suspense file includes codes indicating error types, date and time of entry and identify the person entering data. Evaluate if there are procedures for reviewing and correcting data in the suspense file before processing it again. Assess whether an escalation procedure is in place when error rates are too high and corrective action is taken. ▶ Ask managers about the existence of procedures for periodically reviewing the log. Verify whether the procedures include the initiation of corrective measures. Obtain evidence – either documental or digital – that the log is being periodically reviewed.
Audit issue 4: How data entry authorization into the application is being managed?	
Criteria: Authorization levels for transactions were established and are enforced by proper controls; there is proper segregate of duties for data entry; and there are compensating controls in place for those cases in which segregation of duties is not possible.	
Information required: ▶ Legal and external compliance requirements ▶ Business requirements and rules ▶ User manuals ▶ OAGN form 901: Electronic system user description, change and postponement request form ▶ OAGN form 902: Electronic system user details, changes and suspension records	**Analysis method/s:** ▶ Inquire whether and confirm that the design of the system provides for the use of preapproved authorization lists. Verify, through inspection of authorization lists, that authorization levels are properly defined for each group of transactions. ▶ Assess whether authorization rules for data input, editing, acceptance, rejection and override for major classes of transactions are well designed and documented. ▶ Observe that authorization levels are properly applied running the application in a testing environment. Verify, through the use of CAATs or embedded audit modules, that the authorization records present in the database are compliant to the authorization rules defined. ▶ Determine if a separation of duties (SOD) table exists, and review for adequate separation of key duties/ job functions and permitted transactions, then, look into list of users and user-specific access privileges. Assess whether segregation of duties ensures that the person keying the data is not also responsible for verification of document. Verify the adoption of compensating controls in cases which SOD was not feasible.

IS audit Domain: Application Controls
Audit area: Processing controls

Audit objective: To assess whether the application ensures data integrity, validity and reliability throughout the transaction processing cycle.	
Audit issue 5: Are the business processes rules and requirements properly mapped into the application?	
Criteria: Application transactions run accordingly to the expected behavior.	
Information required: ▶ Application documentation ▶ Business rules and requirements ▶ Data flow chart ▶ Highly critical transactions list ▶ Source code	**Analysis method/s:** ▶ Identify the executable programs in the application from a study of the data flow chart and match them with defined and established business process rules. ▶ Review the application documentation to verify that it is applicable and suitable for the task. Where appropriate for critical transactions, review the code to confirm that controls in the tools and applications operate as designed. Reprocess a representative sample to verify that automated tools operate as intended. ▶ For highly critical transactions, set up a test system that operates like the live system. Process transactions in the test system to ensure that valid transactions are processed appropriately and in a timely fashion.
Audit issue 6: Do the application controls ensure the integrity and completeness of its transactions?	
Criteria: The application does correctly identify transactional errors. Data integrity is maintained even during unexpected interruptions to transaction processing. There is an adequate mechanism for handling processing errors, review of suspense files and clearance.	
Information required: ▶ Application design documentation ▶ Business rules and requirements ▶ Out-of-balance reports ▶ Reconciliations ▶ Report review procedures ▶ Suspense files	**Analysis method/s:** ▶ Assess whether the application has adequate validity checks in place to ensure processing integrity. Inspect the functionality and design for the presence of sequence and duplication errors, referential integrity checks, control, and hash totals. ▶ Inspect reconciliations and other documents to verify whether input counts are coherent with output counts to ensure completeness of data processing. Trace transactions through the process to verify that reconciliations effectively determine whether file totals match or the out-of-balance condition is reported. Inquire whether control files are used to record transaction counts and monetary values, and that the values are compared after posting. ▶ Verify that reports are generated identifying out-of-balance conditions and that the reports are reviewed, approved and distributed to the appropriate personnel. ▶ Take a sample of data input transactions. Use appropriate automated analysis and search tools to identify cases where errors were identified erroneously and cases where errors were not detected. ▶ Inquire whether and confirm that utilities are used, where possible, to automatically maintain the integrity of data during unexpected interruptions in data processing. Inspect the audit trail and other documents, plans, policies and procedures to verify that system capabilities are effectively designed to automatically maintain data integrity.

	▶ Inspect the functional description and design information on transaction data entry to verify whether transactions failing validation routines are posted to suspense files. Verify that suspense files are correctly and consistently produced and that users are informed of transactions posted to suspense accounts. For a sample of transaction systems, verify that suspense accounts and suspense files for transactions failing validation routines contain only recent errors. Confirm that older failing transactions have been appropriately remediated.

IS audit Domain: Application Controls	
Audit area: Output controls	
Audit objective: Assess whether application assures that output information is complete and accurate before further use and that it is properly protected.	
Audit issue 7: Does the application have controls to ensure completeness and accuracy of its output?	
Criteria: Procedures have been designed to ensure that the completeness and accuracy of application output are validated prior to the output being used for subsequent processing, including use in end-user processing; tracking of application output is properly enabled; output is reviewed for reasonableness and accuracy; and completeness and accuracy controls are effective.	
Information required: ▶ Completeness and accuracy controls ▶ Methods for balancing and reconciliation ▶ List of electronic outputs /reports ▶ Sample of electronic output	**Analysis method/s:** ▶ Obtain a list of all electronic outputs that are reused in end-user applications. Verify that the electronic output is tested for completeness and accuracy before the output is reused and reprocessed. ▶ Examine the balancing and reconciliation of output as established by documented methods. ▶ Select a representative sample of electronic output and trace selected documents through the process to ensure that completeness and accuracy are verified before other operations are performed. ▶ Re-perform completeness and accuracy tests to validate that they are effective. ▶ Examine if each output product contains processing program name or number; title or description; processing period covered; username and location; date and time prepared; and security classification. ▶ Select a representative sample of output reports and test the reasonableness and accuracy of the output. Verify that potential errors are reported and centrally logged.
Audit issue 8: Is the output data properly protected?	
Criteria: Output is handled in line with the applicable confidentiality classification; distribution of outputs/ reports are appropriately controlled.	
Information required: ▶ Output handling and retention procedures	**Analysis method/s:** ▶ Review output handling and retention procedures for privacy and security. Assess whether procedures have been defined that require

▶ Information classification policies	the logging of potential errors and their resolution prior to distribution of the reports. Examine the system of reconciliation of output batch control totals with input batch control totals before release of reports establishing data integrity. ▶ Check if there are documented procedures for labeling sensitive application output and, where required, sending sensitive output to special access-controlled output devices. Review the distribution methods of sensitive information and verify that the mechanisms correctly enforce pre-established access rights.

IS audit Domain: Application Controls	
Audit area: Application security	
Audit objective: Assess whether application's information is properly secured against misuse.	
Audit issue 9: Do the traceability mechanisms of the application are sufficient for its purpose?	
Criteria: There are audit trails that capture edits, overrides, and authorization logs to critical transactions; the audit trails are periodically reviewed to monitor unusual activity; the audit trail is adequately maintained and protected; and unique and sequential numbers or identifiers are assigned to every transaction.	
Information required: ▶ Audit trail structure and documentation ▶ Override policies ▶ Review procedures ▶ System flowcharts	**Analysis method/s:** ▶ Obtain documentation and assess the design, implementation, access and review of audit trails. Inspect the audit trail structure and other documents to verify that the audit trail is designed effectively. Inquire who can disable or delete the audit trails. ▶ Inspect the audit trail, other documents, plans, policies and procedures to verify that adjustments, overrides and high-value transactions are designed effectively to be promptly reviewed in detail. ▶ Inspect the audit trail, transactions (or batches), reviews and other documents; trace transactions through the process and, where possible, use automated evidence collection, including sample data, embedded audit modules or CAATs, to verify that periodic review and maintenance of the audit trail effectively detects unusual activity and supervisor reviews are effective. ▶ Inquire how the access to the audit trail is restricted. Examine access rights and access logs to the audit trail files. Verify whether only restrict and authorized personnel have access to the audit trail. Assess if the audit trail is protected against privileged modifications. ▶ Verify, where possible, using automated evidence collection, if unique identifiers are being assigned to each transaction.
Audit issue 10: Is the application data properly protected??	
For physical and logical access control refer to Annexure on Information Security. For disaster recovery planning refer to Annexure on BCP/DRP	

IS audit Domain: Application Controls

Audit area: Controls over standing data and master files	
Audit objective: Are there sufficient Master/Standing Data File controls for ensuring integrity and accuracy of Master Files and Standing Data.	
Audit issue 9: Are there sufficient controls on access to master/standing data file and amendments?	
Criteria: ▶ There is controlled and restricted physical and logical access to master/standing data files. ▶ Any changes to master/standing data files is properly authorized, reviewed and documented ▶ Guidelines on creation, approval, update of master/standing files exists ▶ Integrity of master and standing data files is verified periodically.	
Information required: ▶ Relevant guidelines on management of master/standing data files ▶ Structure for Master/standing data setup. E.g. database structure, functional setup in system	**Analysis method/s:** ▶ Obtain documentation and assess if clear guidelines on creation, review, approval, updating, or any other transaction on master data, exists. ▶ Test sampled master data/standing data files transactions to ensure that guidelines have been followed ▶ Check if the audit trails of transactions done on master data files exists and whether proper procedure for review and approval have been followed. ▶ Check the integrity of master and standing files by checking, control totals and periodic reconciliation with independently held records. ▶ Check procedures for physical and logical access to master/standing data files and whether there is any scope of uncontrolled or unrestricted access.

महालेखापरीक्षकको कार्यालय
Office of the Auditor General
बबरमहल, काठमाडौं, नेपाल
Babar Mahal, Kathmandu, Nepal
नीति योजना तथा जनशक्ति विकास महानिर्देशनालय

पत्र संख्या २०७७।७८ च नं ०३

मिति २०७७।४।१६

विषय **नेपाल सरकारी लेखापरीक्षण मानकको कार्यान्वयन सम्बन्धमा**

श्री सबै विभागहरु

श्री सबै महानिर्देशनालयहरु

श्री सबै निर्देशनालयहरु

महालेखापरीक्षकको कार्यालय ।

उपरोक्त सम्बन्धमा लेखापरीक्षण ऐन, २०७५ को दफा २९ ले दिएको अधिकार प्रयोग गरी महालेखापरीक्षकले गर्ने लेखापरीक्षणलाई वस्तुपरक, विश्वसनीय र भरपर्दो बनाई लेखापरीक्षणको गुणस्तर अभिबृद्दि गर्न साविकमा स्वीकृत भएका सरकारी लेखापरीक्षण मानदण्ड एवं सरकारी लेखापरीक्षण नीति मानदण्ड खारेज गरी सर्वोच्च लेखापरीक्षण संस्थाहरुको अन्तर्राष्ट्रिय संगठनले जारी गरेका अन्तर्राष्ट्रिय लेखापरीक्षण मान (INTOSAI Framework for Professional Pronouncements, IFPP) मा आधारित "नेपाल सरकारी लेखापरीक्षण मान" (Nepal Government Auditing Standards, NGAS) २०७७।४।१६ मा स्वीकृत गरिएको छ । अत कार्यालयबाट यस वर्षदेखि लेखापरीक्षण गर्दा तपसीलका नेपाल सरकारी लेखापरीक्षण मानको कार्यान्वयन गर्नु हुन अनुरोध छ ।

तपसील

NGAS नम्बर	नेपाल सरकारी लेखापरीक्षणमानको नाम
INTOSAI-P 1	The Lima Declaration
INTOSAI-P 10	Mexico Declaration on SAI Independence
INTOSAI-P 12	The Value and Benefits of Supreme Audit Institutions- making a difference in a life of citizens
INTOSAI-P 20	Principles of Transparency and Accountability
ISSAI 100	Fundamental Principles of Public-Sector Auditing
ISSAI 130	Code of Ethics
ISSAI 140	Quality Control for SAIs
ISSAI 200-299	FInancial Audit Principles
ISSAI 300-399	Performance Audit Principles
ISSAI 400-499	Compliance Audit Principles
ISSAI 2000-2899	Financial Audit Standards
ISSAI 3000-3899	Performance Audit Standards
ISSAI 4000-4899	Compliance Audit Standards

जानकारीको लागि

माननीय महालेखापरीक्षकज्यू ।

भवदीय

(घनश्याम पराजुली)
नायव महालेखा परीक्षक

Phone: 4258174, 4266034, 4255707, A.G. Fax: 977-1-4268309, Fax: 977-1-4262798, Post Box: 13328
email: aag.mgmt@oagnep.gov.np Web Page: www.oagnep.gov.np