ISSAI 5300

The International Standards of Supreme Audit Institutions, or ISSAIs, are issued by INTOSAI, the International Organisation of Supreme Audit Institutions. For more information visit *www.issai.org*

INTOSAI

Guidelines on IT Audit

June 2016

PSC-Secretariat
Rigsrevisionen • Landgreven 4 • P.O. Box 9009 • 1022 Copenhagen K • Denmark
Tel.:+45 3392 8400 • Fax:+45 3311 0415 •E-mail: info@rigsrevisionen.dk

INTOSAI

EXPERIENTIA MUTUA
OMNIBUS PRODEST

INTOSAI General Secretariat – RECHNUNGSHOF
(Austrian Court of Audit)
DAMPFSCHIFFSTRASSE 2
A-1033 VIENNA
AUSTRIA
Tel.: ++43 (1) 711 71 • Fax: ++43 (1) 718 09 69

E-MAIL: intosai@rechnungshof.gv.at;
WORLD WIDE WEB: http://www.intosai.org

Table of Contents

PREFACE

Series 5300-5399 of ISSAIs has been allocated to the Guidelines on Information Technology Audit under the ISSAI framework. ISSAI 5300, the first ISSAI in the 5300 series, is an overarching, general principles ISSAI on the fundamentals of IT Audit. It addresses the general principles, approach and methodology to conduct IT Audits.

The ISSAI 5300 also intends to act as a guide for SAIs to conduct IT Audits, develop IT Audit capacity and utilize limited IT Audit resources to provide an assurance to the audited entities, government and the people of a country on integrity, reliability and value for money on IT implementations.

The ISSAI 5300 has been developed within the framework of ISSAIs by conducting a review of the existing standards related to IT Audits/ Information Systems Audits, standards regarding information systems, national and international auditing standards, in particular the existing ISSAIs. Another key feature of the ISSAI 5300 is that it ensures that the basic nature inherent in IT Audits is appropriately linked/embedded with different forms of audit identified at the level 3 ISSAIs.

Further, being a level 4 guidance, the material in this ISSAI has been divided into two categories: **Requirements** – which are essential for conducting a good quality IT Audit; followed by **Explanations** – which explain the requirements in more general terms. This has been done to ensure that the ISSAI retains its primary function of providing general supportive guidance as is intended under the ISSAI framework.

The ISSAI 5300 also takes into consideration the levels of maturity of Information Systems in government sector and the maturity level of IT Audits in different SAIs.

The ISSAI is structured around the following major sub-themes:

1. Framework for IT Audits
2. General Requirements specifically pertaining to IT Audits
3. Requirements specific to IT Audit Process
4. IT Audit Techniques and Tools
5. The Reporting Requirements of IT Audits.

There is a separate Annexure devoted to Data Analytics.

The ISSAI lays the foundation for development of future ISSAIs in the 5300-5399 series and/or subject specific guides by dealing with specific topics of relevance to the INTOSAI community in the area of IT Audits.

A project team comprising Brazil, India (Project Lead), Indonesia, Japan, Poland, and the US drafted the ISSAI.

A. FRAMEWORK FOR IT AUDIT

1. Authority and Scope of ISSAI 5300

1.1 ISSAI 5300 provides the overarching framework for conducting IT Audits within the framework of ISSAIs.

1.2 The framework laid out in this ISSAI is consistent with the Fundamental Principles of Public Sector Auditing (ISSAI 100), Fundamental Principles of Financial Auditing (ISSAI 200), Fundamental Principles of Performance Auditing (ISSAI 300) and Fundamental Principles of Compliance Auditing (ISSAI 400).

1.3 The ISSAI provides requirements for the professional practice of IT Auditing followed by explanations to enhance the clarity and readability of the framework.

1.4 Requirements contain information necessary for high quality IT audit work. They make clear to the auditors of what is expected of them and to the stakeholders of what they can expect from the IT Audit conducted by a SAI.

1.5 Explanations describe in more detail what a requirement means or is intended to cover.

1.6 This ISSAI has been prepared by a Project Team comprising Japan, Poland, Indonesia, India, the US and Brazil.

2. Introduction to IT Audits

2.1 Government entities have increasingly adopted Information and Communication Technologies (ICT) to conduct their functions and deliver various services. Such ICT based systems are commonly, also, referred to as Information Systems (IS) or Information Technology (IT) Systems.

2.2 Supreme Audit Institutions (SAIs) are mandated to audit the Government and their entities as per their respective audit mandate.[1]

2.3 SAIs, thus, promote the efficiency, accountability, effectiveness and transparency of public administration[2].

2.4 The continuous development of Information and Communication Technology has made it possible to capture, store, process and deliver information electronically. This transition to electronic processing has triggered a significant change in the environment in which SAIs work. Moreover, the government expenditure on IT is growing. Therefore, it becomes imperative for an SAI to develop appropriate capacity to conduct IT Audits.

3. Definition of IT Audit

3.1 The IT Audits are defined as:

*"*An examination and review of IT systems and related controls to gain assurance or identify violations of the principles of legality, efficiency, economy and effectiveness of the IT system and related controls*."*

[1] ISSAI 1, The LIMA Declaration
[2] United Nations General Assembly Resolution A/66/209

3.2 IT Audit[3] is, thus, a broad term that pervades Financial Audits[4] (to assess the correctness and compliance to other assertions of an organization's financial statements), Compliance Audits[5] (evaluation of internal controls), and Performance Audits[6] (to assess whether the IT Systems meet the needs of the users and do not subject the entity to unnecessary risk). There may however be instances where some audits can be devoted only to the IT component of a system.

4. Mandate for IT Audits

4.1 The mandate of SAI for IT audit shall be derived from the overall mandate provided to the SAI to conduct audits.[7] Some SAIs may also have specific mandate for conducting IT Audits or audit of IT systems.

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

4.3 The specific mandate, if provided, should address jurisdiction of audit for auditing IT Systems, which are utilised by the entity to fulfil its functional objectives. It should also provide for timely, unfettered, direct and free access to all necessary documents and information from the entity[8], both manual and electronic, whether the function or any of its part is insourced or outsourced.

4.4 The mandate for SAI to conduct IT Audits should conform to the principles under ISSAIs of levels 1 and 2.

B. GENERAL REQUIREMENTS SPECIFICALLY PERTAINING TO IT AUDIT

5. Risk based audit approach to IT Audit

Requirement:

The IT Auditor shall consider the IT Audit risks when the auditor takes a risk based audit approach.

The IT Audits should be conducted based on a risk based audit approach

Explanation:

5.1 Risk based audit approach involves identification of risk elements[9] in the entity being assessed along with their potential impact and thus identifying priority area to be audited.

5.2 Risks, while auditing an entity, involve Inherent risks, Control Risks, and Detection Risks. The risk elements are identified addressing the three risks. Together the three risks comprise what is called the Audit Risk.

---

[3] IT audit is also referred to as IS Audit, Systems audit, Information audit, information security audit, computer assurance reviews, IT assurance, etc.
[4] ISSAI 200 Fundamental Principles of Financial Auditing
[5] ISSAI 400 Fundamental Principles of Compliance Auditing
[6] ISSAI 300 Fundamental Principles of Performance Auditing
[7] Principle 3, ISSAI 10 – Mexico Declaration on SAI Independence and ISSAI 100 – Fundamental Principles of Public Sector Auditing
[8] Unrestricted Access to records; Principle 4, ISSAI 10 – Mexico Declaration on SAI independence
[9] Risk elements would be related to areas like IT Governance, System design and development, Out(In)sourcing, Operations, IT Security, Monitoring and Control.

5.3 Inherent Risks are the risks built into the system which can have an impact on the delivery of the function mandated to be carried out by the entity. Anonymity of users is an inherent risk of an IT System, especially in a networked environment. The organizations should put in place control measures to address inherent risks. In some cases, the entity may even accept the risks as such, without any counter measures to address the risks, where their impact is assessed to be not material and thus, within the acceptable level of risk.

5.4 Control risks are the risks where the control measures have the possibility of failure. In such cases, material errors are possible and should be identified immediately. IT systems invariably address these through Application controls[10] and General controls[11]. It is the robustness of these controls which ensure the delivery of function being carried out by the organization/ IT System. Failure or compromise of these controls presents a situation of Control Risks.

5.5 Detection risks in conduct of IT Audits are the risks of non-detection of absence or failure of IT and related controls and the associated compromise in the functioning of the IT System.

5.6 There are many risk assessment approaches and methodologies available from which the SAI may choose from. These range from simple classifications of risk profile of IT Systems as high, medium and low, based on the judgement of IT auditors of an SAI, to complex and, apparently, scientific calculations to provide a numeric risk rating of the IT systems.[12]

6. Materiality

Requirement:

SAI shall consider materiality at all stages of the IT audit process.

Explanation:

6.1 IT Auditors should consider materiality throughout the (IT) audit process. Materiality considerations affect decisions concerning the nature, timing and extent of audit procedures and the evaluation of audit results. Considerations may include stakeholder concerns, public interest, regulatory requirements and consequences for society.[13]

6.2 Materiality concerns all aspects of such audits, such as the selection of topics, definition of criteria, evaluation of evidence and documentation and management of the risks of producing inappropriate or low – impact audit findings or reports.

6.3 The materiality of an IT Audit issue should be decided under the overall framework for deciding materiality in an SAI. The perspective of materiality would vary depending on the nature of

[10] Application Controls are the controls inbuilt into an individual application or a group of related applications comprising an IT application system. They are input controls, processing controls, output controls and master data controls which are applicable at the input, process and output stages of the IT system.

[11] General Controls are controls on the related systems and processes supporting the IT application system. These pertain to areas like the business case for the IT system, system design and development, acquisitions, outsourcing/ insourcing, operations (apart from application controls), human resource management, IT security, monitoring etc. The general controls and the application controls are intricately associated while assuring the successful implementation of an IT system. If general controls are weak, they severely diminish the reliability of controls associated with individual IT applications.

[12] WGITA-IDI Handbook on IT Audits for Supreme Audit Institutions

[13] ISSAI 100 – Fundamental Principles of Public Sector Auditing – Para 41

IT audit. Materiality for public sector financial, performance and compliance auditing, of which IT audit is a part, are discussed in ISSAIs 200, 300 and 400[14].

6.4 Materiality and Risk

Risk assessment used in IT auditing is intricately linked to the materiality requirements of the concerned audits. Materiality of a non-compliance is assessed based on the capacity to influence decisions by intended users. When the inherent risks are high, the occurrence of a small noncompliance may be material because of the possibility of accumulating nature of the impact of such noncompliance. When control risks are high (thereby meaning absence/ failure of necessary controls for identified risks), similarly, a small noncompliance will be material, again for the possibility of accumulating nature of the impact of such noncompliance.

6.5 IT Auditors are not always in a position to examine all instances/ transactions/ modules or systems given the resource constrains and the cost benefit of the audit exercise. In such a situation, the IT Auditors may resort to identifying materiality and adopting audit sampling for detailed examination to draw reasonable audit conclusions. Use of IT tools on carrying out different types of sampling may be resorted to. The levels of Inherent Risks and Control Risks would have an impact on the size of the sample. Higher the Inherent Risk or the Control Risk, the bigger should be the size of the sample.

7. Documentation

Requirement:

SAI shall maintain sufficient documentation of the IT Audit process and its results to ensure that any experienced IT Auditor unconnected with the audit could replicate it.

The auditor shall prepare audit documentation that is complete and detailed to provide an overall understanding of an audit.

The review of the documentation should enable any other IT auditor to reach the same audit conclusions.

Explanation:

7.1 The overall documentation requirements in an IT Audit would essentially flow from Level 3 ISSAIs - ISSAIs 100, 200, 300 and 400. These would also apply to an IT Audit. However, the nature of IT Audits may need specific adjustments to the documentation process.

7.2 The role of documentation in an IT audit would be to understand the planning and execution of audit, what work was performed in support of audit findings and conclusions, and arriving at the audit recommendations. Documentation should be sufficiently detailed to enable an experienced IT auditor, with no prior knowledge of the audit, to understand the nature, timing, scope and results of the procedures performed in compliance of relevant ISSAIs, national standards, and the applicable legal and regulatory requirements. The evidence obtained in support of the audit conclusions and recommendations, the reasoning behind all significant matters that required the exercise of professional judgement, and the related conclusions, should also be documented and easily understood by an experienced IT auditor. The documentation should be reliable so that there is no disagreement on the contents of the documentation with the audited entity.

[14] ISSAI 200 – Fundamental Principles of Financial Auditing, ISSAI 300 – Fundamental Principles of Performance Auditing, ISSAI 400 – Fundamental Principles of Compliance Auditing

7.3 Documentation in an IT Audit plays a significant role in ensuring that each step of the audit process and each finding are mapped or referenced to a specific point of compliance or non-compliance with applicable standards or regulations.

7.4 As in any other audit, if any finding in course of an IT Audit is inconsistent with overall audit conclusion on a significant matter or there is a disagreement with the audited entity on audit conclusions, then IT Auditors have to document how they have addressed that inconsistency and/or disagreement.

7.5 Format of IT Audit Documentation

IT Audit Documentation includes paper formats and electronic templates to record information about the audited IT system, details of meetings held with the Management and within the audit team, audit findings, and evidence for audit conclusions. There is no standard format for IT audit documentation in ISSAIs. Further, the formats may differ from SAI to SAI. There may be certain level of standardisation within each SAI in terms of checklists, specimen letters, organisation of working papers, etc.

7.6 Retention of IT Audit Documentation

IT Audit documentation may be retained and protected from any modification and unauthorised deletion. Each SAI may evolve new standards for retention of IT audit documentation or adapt existing standards to meet the requirements of retention of IT Audit related documentation. The period of retention so arrived at would be a function of the mandate of the individual SAI, and the statute(s) governing its activities.

Special attention should be paid to media, the format, the life expectancy, and the storage requirements for this data, to ensure that the same is readable within the time frame defined in each SAI's respective data retention and archiving policy. This may necessitate conversion of data from one format to another to keep up with technological advances and obsolescence.

8. Competence

Requirement:

The SAI shall ensure that the audit team is composed of members that collectively have the competence to perform IT Audit in accordance with the standards.

Explanation:

8.1 The necessary knowledge, skills and competence could be acquired through a combination of training, recruitment and engagement of external resources as per the strategic plan of the SAI.

C. REQUIREMENTS RELATED TO THE IT AUDIT PROCESS

9. Planning IT Audits

Requirement:

The SAI should plan an IT Audit based on risk assessment.

Explanation:

9.1 Planning of IT Audits by an SAI can be undertaken as per legislative mandates, legislative/ executive requests, or as per their initiative.

9.2 Audit planning in the SAIs based on Risk Assessment

SAIs can plan audits on a risk assessment based selection. In this process, the SAI prioritizes and selects what audits will be conducted based on a risk assessment. Planning a risk based IT Audit can be carried out at three levels – Strategic, Annual, and Team Levels, which shall be under the overall Strategic Plan of the SAI. However, an SAI may decide on a mix of any one or more of these levels, as per their resources and requirements of audit, based on risk analysis.

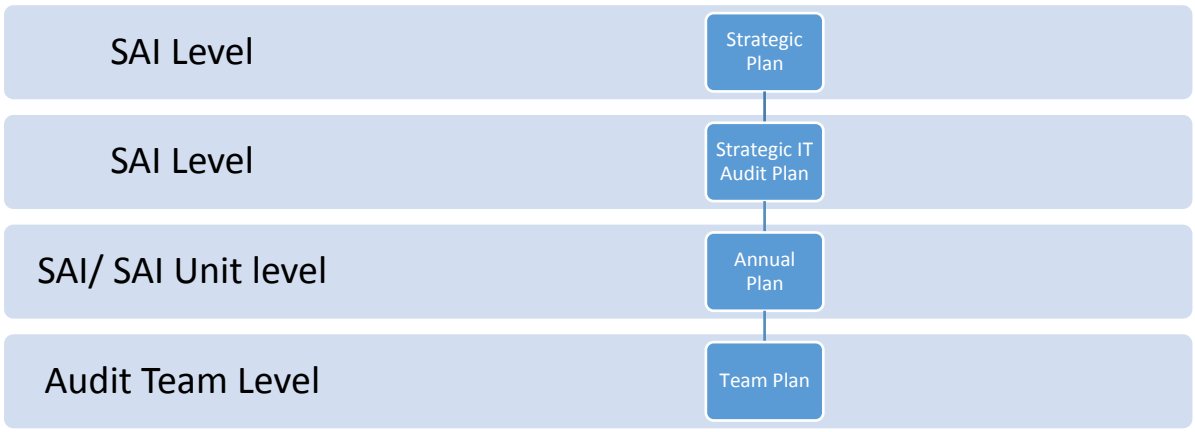

Figure 1: TYPICAL AUDIT PLANNING HIERARCHY FOR SAIs

10. Strategic IT Audit Planning

Requirement:

The Strategic Plan of an SAI shall have a component addressing IT Audit and its associated needs.

The SAI shall develop Strategic IT Audit Plan in accordance with the overall Strategic Audit Plan.

Explanation:

10.1 The Strategic IT Audit Plan contains targets and objectives for audit of IT systems in Government entities under jurisdiction of an SAI. The plan is typically determined for a period of about 3-5 years reflecting developments in the IT environment and adoption by Government entities. The Strategic Plan for the audit of IT Systems should be aligned with the overall Strategic Plan of an SAI.

10.2 The SAIs have their goals of ensuring transparency, accountability and contribution to good governance articulated through their vision, mission, and value statements. As such their Strategic Plan or aims may address Institutional Development, Organisational System Development, and Professional Capacity Development, as required, in response to achieving its strategic goals. For IT Audits, SAIs may 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.

10.3 Identifying the audit universe at this stage will be relevant. The SAIs may identify its priorities of auditing in response to the assessment of its environment and the audit universe, and decide on its Strategic Goals and objectives. To achieve their overall goals, through limited means and resources available, the strategic implementation plan of the SAI would include identifying the needs related to institutional development, which will include the enabling mandate and legal framework for the SAI to conduct IT Audit, organizational system development to establish systems

and procedures in the SAI to conduct IT Audits, and professional capacity development to acquire necessary skills and capacity to be able to conduct IT Audits.

10.4 Risk based Audit Planning

Risk Based Audit Planning would involve addressing the risk elements that will have an impact on the relevance of the audits and correctness of the audit conclusions drawn as a result of audit. The risk assessment at the Strategic IT Audit Planning Level addresses the issue of relevance of the IT Audits with respect to the overall strategic goal of SAIs in ensuring good governance, transparency, and accountability in governance.

10.5 There should be a periodic review and update of the Strategic Plan of the SAI to address its goals of ensuring transparency, accountability and contribution to good governance.

10.6 Reference to ISSAIs, especially, ISSAI 100 – Fundamental Principles of Public Sector Auditing may be made in addressing issues related to the Strategic Planning by an SAI.

11. Annual IT Audit Planning

Requirement:

The Annual IT Audit Plan shall be in accordance with the Strategic IT Audit Plan.

The Annual IT Audit Plan shall cover the matters of significance included in the Strategic IT Audit Plan as per priority determined through risk assessment.

Explanation:

11.1 The SAI needs to devise an Annual Plan for IT Audit that is aligned to the strategic plan for IT Audit. This stage of planning involves selection of the IT System or entity to be audited.

11.2 Within the framework of the Strategic Plan for IT Audits for an SAI, a risk based approach may be used to prioritise and select suitable topics. This will involve creating and using an inventory of auditable organizations/ IT systems along with key criteria for carrying out risk assessment. This inventory can also be the audit universe identified during the Strategic Planning Stage but with specific details on the type and description of the IT Systems/ entities to be utilized in assessing their risk profile. A risk assessment framework developed by the SAIs can subsequently be used for finalizing an audit selection.

11.3 In addition to a risk based approach to select audit topics, many SAIs are required to take on audits by law and by requests by oversight bodies (Congress, Parliament, etc.) or the executive.

12. Team Level IT Audit planning for the selected audit

Requirement:

The Team Level IT Audit Plan shall be in accordance with the Risk Assessment in Annual IT Audit Plan.

The Team level IT Audit Plan shall cover the matters of significant risk areas identified in the Annual IT Audit Plan and comprise a detailed audit program.

Explanation:

12.1 This level would involve development of a detailed audit program beginning with outlining the audit objectives of a selected IT Audit.

12.2 The prerequisite to developing the audit program will be to have a clear understanding of audited entity, its Information Systems and IT related activities.

12.3 The extent of knowledge of the entity and its processes required by IT Auditors will be determined by the nature of the entity and level of detail at which audit work is being performed. The objective or the purpose behind the implementation of an IT system should be identified. Knowledge of entity should include the business, financial and inherent risks facing the entity and its IT Systems. It should also include the extent to which the entity relies on outsourcing to meet its objectives and how completely, the business process has been mapped in an IT environment[15]. 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 IT auditors should be alert.

12.4 As per the risk based audit approach, the Control Risks will be related to these elements of IT General Controls and Application Controls. Higher the Control Risks, greater the need to conduct more substantive tests.

12.5 Generally, IT auditors are called upon to test technology-related controls, whereas non-IT auditors test financial, regulatory and compliance 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 objective. In the case of IT general controls, it is important for the auditor to understand the broad categories and extent of general controls in operation, evaluate the management oversight and staff awareness in the entity for the same, and find out how effective the controls are in order to deliver the intended function. Even in small entities where information systems and business processes relevant to financial reporting are less sophisticated, their role is significant[16]. If general controls are weak, they severely diminish the reliability of controls associated with individual IT applications[17]. It will be important for IT Auditors to understand the function mapped onto the application with the associated work flow. The IT Auditors should be able to identify each input, processes carried out by the application and outputs generated by the application. The understanding of the master data influencing the input, process and outputs and its security will help IT Auditors assess the compliance of the IT system to the requirements of the correctness, completeness, integrity, confidentiality, availability, reliability, relevance and compliance of data throughout the information processing stages of data capture and data processing and delivery/ output of information.

12.6 Based on the understanding developed of the Information System and the audited entity, IT Auditors may decide on their approach for IT Audits. IT Audit would eventually involve audit of IT Governance, IT General Controls and IT Application Controls or a combination of these.

13. Selecting Appropriate Sample for IT Audit

An Audit Sample[18] is the application of audit procedures to less than 100 percent of items within a group or population of audit relevance such that all sampling units have a chance of selection in

[15] Entities changing over from a manual to a computerised environment would normally take up a business process reengineering (BPR) exercise. It may be seen that some of the business processes are being carried out manually still along with an interface with the IT Systems. These special scenarios would present specific interest areas for IT Auditors.

[16] ISSAI 1315 -Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment

[17] WGITA IDI Handbook on IT Audits for Supreme Audit Institutions

[18] ISSAI 1530*, Financial Audit, Audit Sampling*

order to provide the auditor with a reasonable basis on which to draw conclusions about the entire population. This is also applicable to selecting a sample for IT Audit. Furthermore, when designing an audit sample, the IT auditor shall consider the purpose of the audit procedure, the characteristics of the population from which the sample will be drawn and the techniques and tools used to draw the sample and analyse them.

The IT auditor shall determine a sample size sufficient to reduce sampling risk to an acceptably low level. The IT auditor shall select items for the sample in such a way that each sampling unit in the population has a chance of selection. Auditing in an ICT environment may facilitate analysis of 100 percent population, especially at the preliminary assessment stage ***(Section 21 below)***. However, for carrying out any substantive test ***(Section 21 below)*** or detailed examinations, it may be still required to draw a sample. IT Auditors may use the guidelines in ISSAI 1530 or other derived processes in use at their SAI for sample selection.[19]

14. Objectives of IT Audit

Requirement:

The objectives of IT Audit should conform to the Risk areas identified during the Team Level IT Audit Planning depending upon the type of audit approach being contemplated – Financial, Compliance or Performance Audit.

Explanation:

14.1 The objectives of IT Audit shall be to examine whether the IT processes and IT Resources combine together to fulfil the intended objectives of the organization to ensure Effectiveness, Efficiency and Economy in its operations while complying with the extant rules and balancing risks.

14.2 Thus, the IT Audits could be audits of a comprehensive IT System or specific domains like IS Security, Acquisition of the Business Solution, IT General Controls, Application Controls, System Development and Business Continuity, or other areas as mentioned in the WGITA IDI Handbook.

14.3 IT Audits cross cut into the Financial Audit, the Compliance Audit or the Performance Audit domains. The IT Audits can assist the three types of audits or can be conducted under the aegis of either of them or a combination of them, i.e. Financial Audits, Compliance Audits and Performance Audits.[20]

14.4 Objectives with respect to Financial Audits

The definition of Financial Audit [21] outlines the issues of confidence, preparation of financial statements in compliance to a financial reporting framework and presentation of the financial statements fairly conforming to the materiality requirements. This covers the broad objectives of assurance of the financial system to comply with the reporting framework in preparation of the financial statements and reporting of financial results without material errors. An IT system is thus required to map all the requirements for preparation of financial statements, i.e. capture of financial information, application of framework requirements, processing of the information, and presentation in the required format. Broadly, these are issues related to Application Controls of Input, Processing, and Output, apart from Master Data and application security. However, the Application controls are dependent on adequate support from the IT General Controls and IT

[19] ISSAI 1530, Financial Audit Guideline, Audit Sampling, Page15.
[20] ISSAI 100 – "SAIs may also conduct combined audits incorporating financial, performance and/or compliance aspects."
[21] ISSAI 200 – Fundamental Principles of Financial Auditing.

Governance. 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 IT Audit of the system looking at all aspects of IT Governance, IT General Controls, and IT Application Controls.

Once an assurance is derived through a full-fledged IT Audit, it may not be essential to conduct an IT 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 IT Audit.

14.5 Objectives with respect to Compliance Audits

Compliance auditing is the independent assessment of whether a given subject matter is in compliance with applicable authorities identified as criteria. Compliance audits are carried out by assessing whether activities, financial transactions and information comply, in all material respects, with the authorities which govern the audited entity.

The objective of public-sector compliance auditing is to enable the SAI to assess whether the activities of public-sector entities are in accordance with the authorities governing those entities. This involves reporting on the degree to which the audited entity complies with established criteria. IT Audit enables this determination to be made for automated systems. Compliance auditing may be concerned with regularity (adherence to formal criteria such as relevant laws, regulations and agreements) or with propriety (observance of the general principles governing sound financial management and the conduct of public officials). While regularity is the main focus of compliance auditing, propriety may also be pertinent given the public-sector context, in which there are certain expectations concerning financial management and the conduct of public-sector entities and officials. Depending on the mandate of the SAI, the audit scope may therefore include aspects of propriety[22].

The objectives and characteristics of compliance auditing outline the need of compliance to due process, regularity, and propriety. An IT system in a public sector entity is also required to comply with the applicable laws and regulations, as well as standards and guidelines adopted by the entity. IT Auditors should evaluate the IT System's compliance to such regulations as well as the standards, guidelines, and different performance parameters of the entity to derive an audit conclusion. All such evaluation will be carried out against identified criteria derived from the rules, laws, standards, performance criteria or even proprietary requirements. 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.

Audit of compliance by an IT system may, invariably, require use of Computer Assisted Audit Techniques (CAATs) to carry out analysis of information and to identify exceptions.

14.6 Objectives with respect to Performance Auditing

[22] ISSAI 400 – Fundamental Principles of Compliance Auditing

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.

IT Auditors shall examine the IT systems implemented with respect to the criteria of economy, efficiency, and effectiveness and value to the citizen.

Examining for economy in respect to the implementation of IT systems would essentially involve minimising the costs of resources throughout the life cycle of the IT System, i.e. from the system acquisition to system implementation and regular operation. In case of outsourcing of any functions, the cost of such outsourcing needs to be minimised. One of the best ways to minimise such costs is through market discovery. However, inefficient user requirement definition due to inadequate knowledge of the requirements by the entity may hamper such an approach and lead to higher costs. Evaluation of the possibility if the IT services outsourced could have been carried out by available resources will indicate on uneconomic use of resources. During Performance Audit of IT Acquisitions, thus, IT Auditors could highlight the limitations of the entity or the process of acquisition as the case may be.

Examining for efficiency in respect of implementation of IT Systems would involve maximising the utilisation of the resources or, thus, minimising the inefficient utilisation of resources while maintaining the quantity (completeness), quality (correctness and reliability), and timing (availability) of output. Inefficiencies may be pointed out by IT Auditors if there are duplication of any processes, undue idling of any process, unnecessary checks built into the system etc.

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. Non achievement of entity's objectives using the IT System could indicate ineffective utilisation of the IT System.

Performance Auditing also contributes to accountability and transparency. Performance auditing focuses on areas in which it can add value for citizens and which have the greatest potential for improvement. It provides constructive incentives for the responsible parties to take appropriate action. IT implementation in most government and its organisations is most often a new initiative. As such, the performance audit approach in IT Audit to constructively promote governance using IT System should be one of the cornerstones of the IT Auditors approach. The deficiencies noticed should be pointed out in a manner that leads to system improvements, rather than kill the initiative.

14.7 IT Auditors may be called upon to assist in audits in use of CAATs. The terms of engagement in such a case will be helpful in deciding if the engagement would constitute an IT Audit. Use of CAATs to carry out data analysis only is not an IT Audit where evaluation of an IT system is not undertaken.

15. Scope of IT Audit

Requirement:

IT Auditors shall determine the scope of audit during planning stage to ensure achievement of audit objectives.

Explanation:

15.1 Having decided the objectives of IT Audits, IT Auditors should also decide on the scope of audit. The two steps are generally conducted simultaneously. The scoping of IT Audit would involve deciding the extent of audit scrutiny in terms of the coverage of IT systems and their functionalities, IT Processes to be audited, locations of IT systems to be covered, the time period to be covered, and additionally the type of audit (Financial/ Compliance/ Performance Audits). It will be, basically, setting or delineating the boundaries of audit.

15.2 IT Systems support the business functions in an entity and typically involve IT specific process such as inputting data into the system, requesting information, and generating reports. Most IT systems are located in a dedicated location along with associated network equipment. The security of the physical location and the equipment it contains may be covered in the IT Audit.

15.3 The auditor should select the time period for audit analysis (i.e., look at one year's information, 3 years, or more, etc.) so as to enable IT Auditors to draw suitable conclusions on the audits conducted. When auditing the IT system, the typical time period to be covered may be drawn from the requirements of the given audit.

15.4 The scope of audit will also involve focussing on specific domains of the IT system which would be of relevance to the IT Audit Objective. The typical IT domains are IT Governance, Development and Acquisition, IT Operations, Outsourcing, IS Security, Business Continuity Plan & Disaster Recovery Plan, and Application Controls[23]. These domains would generally suffice for any IT System. However, as the field of IT is ever changing, IT Auditors should not preclude possibilities of newer areas to be brought under scope of their audits, if found relevant[24]. A comprehensive IT Audit would involve examination of all the IT Domains.

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

16. Capacities of an SAI to conduct IT Audits

Requirement:

SAI shall have adequate capacity to conduct the IT Audit.

SAI shall develop adequate capacity, if the same is not available, before commencing an IT Audit.

Explanation:

16.1 Core function of all SAIs is to audit and they may already possess audit capacities. However, IT auditing requires specific capacities. Some of the capacities that an IT Audit team should collectively possess, may include:

i. Staff skilled and knowledgeable on IT
ii. Understanding of extant rules and regulations or environment, in which the IT system is operating
iii. Understanding of the IT Audit standards/ guidelines applicable to the SAI
iv. Understanding of IT techniques to collect the audit evidence from automated systems

[23] WGITA-IDI Handbook on IT Audits for Supreme Audit Institutions
[24] Chapter 9, Additional topics of interest, WGITA-IDI Handbook on Information Technology Audits for Supreme Audit Institutions

v. Understandings of adequate IT Audit Tools to collect, analyse, reproduce the results of such analysis or re-perform the audited functions
vi. Adequate IT Infrastructure to capture audit evidence and retain the same
vii. Availability of adequate IT Audit Tools to analyse the collected evidence

17. Allocation of Resources

Requirement:

SAI shall identify and allocate adequate and competent resources to conduct the IT Audit.

Explanation:

17.1 SAIs have many different options to allocate resources to IT Audit.

17.2 The most common approach is to have a central group with IT specialists or experts who assist others in the agency to conduct IT Audits. The SAI is able to leverage the skills of a few to conduct IT Audits if they are first starting down this path.

17.3 Another option is to staff IT specialists in each of the teams within the SAI. However, if each team conducts only a few IT Audits, then this might not be an efficient use of the IT Specialist. As the number of IT Audits increases, SAIs tend to stand up a dedicated IT Audit group or function. This group is then responsible for conducting all of the IT Audits that the SAI undertakes.

17.4 The IT group may interact with other teams at the SAI who have legacy knowledge of the entity, this enables the IT Audit team to quickly get an understanding of the entity's mission and relate business process at the entity to supporting IT System to facilitate the IT Audit.

18. Engaging external resources

Requirement:

SAI may consider engaging external resources to conduct IT Audit, if the capacity is not available in house.

Explanation:

18.1 The SAI may decide on utilizing external resources to conduct IT Audit, or outsourcing the IT Audit to a contractor team, if it is constrained for appropriate resources. Such resources mainly will be that of external consultants or contractors who are skilled in IT Audit techniques and tools, including databases, programming, and other areas relevant to the IT Audit. Resources also include any IT infrastructure needed in the SAI to conduct the audit. These are typically the same as to conduct any other audit, however, and IT Audit might require specific analysis and data conversion and storage tools.

18.2 The work of the external resources, when outsourced by an SAI, should be adequately monitored through a documented contract or a service level agreement by the SAI. The work and final products delivered to the SAI must follow existing processes and standards that the SAI has adopted. This means that the SAI still needs skilled and knowledgeable staff in-house to monitor the work even when the SAI decides to utilise external resources.

19. Engagement with audited entity

Requirement:

SAI shall engage with the audited entity before commencement of audit.

Explanation:

19.1 As in any audit, the audited entity should be familiarized about the scope, objectives and the assessment criteria of the audit should be discussed with them as necessary. The SAI may, if necessary, write the engagement letter to the audited entity where it may also set out the terms of such engagements.

19.2 Specifically for IT Audit, the SAI should ensure 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.

20. Audit Evidence

Requirement:

SAI shall ensure that the audit evidences are sufficient, reliable and accurate to sustain the audit observations.

The audit evidences shall be available for recreating and review the audit process subsequent to closure of the audit.

Explanation:

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

20.2 As such the evidence needs to have the characteristics of sufficiency, reliability, and correctness/ accuracy in accordance with the internal quality assurance standards of the SAI.

20.3 The evidence in an IT audit needs to be appropriately captured and stored in a manner that will be available in the future without the data being altered. IT Auditors need to ensure that the evidence has necessary timestamps[25] for changes whenever there is a risk that the evidence could be altered.

20.4 IT Audits present different and specific manner of identifying, collecting, storing and retaining evidence. The evidence could be collected from the specific tests carried out on the samples under audit observation. IT Auditors could carry out the tests on all the transactions or a sample as required, but the electronic data can always be put to test against a criterion, in full. However, the substantiation of the exceptions can be carried out selectively through a sample, if the exceptions are large in number. The audit sample could be randomly or systematically chosen. Monetary unit sampling could be used or the sample could be selected based on a judgemental based by the IT Auditors.

20.5 The specific techniques and tools to collect audit evidence in IT Audits are discussed subsequently in Section D.

21. Audit Execution – Gathering Audit Evidence

Requirement:

[25] A timestamp is data added to information (electronic, paper, video, etc.) to tag the time the information was generated, collected or edited. Timestamps can be as detailed as needed (day, date, hours, minutes, seconds, milliseconds, etc.) for the information.

The IT Auditor shall gather appropriate and sufficient audit evidence and analyse the same to ensure that the audit objectives are adequately addressed.

Explanation:

21.1 Preliminary Assessment of IT controls

IT Auditors should conduct a preliminary assessment of IT Controls in the system under audit to derive an understanding of assurance that existing IT controls (General IT Controls and Application Controls) are reliable and operate under a suitable IT Governance framework. The assessment of controls at this level would include:

a) Assessment that suitable IT Governance mechanisms are in place and functioning.
b) Assessment that IT objectives are aligned to the Business Objectives.
c) Assessment that suitable mechanisms are in place for:
    i. Effective IT Project Management
    ii. Acquisition and Development of an IT solution (encompassing, IT application, hardware, software, manpower, network, service solutions, etc.)
    iii. Operation of IT systems
    iv. Ensuring Information Security
    v. Ensuring Business Continuity and Disaster Recovery
    vi. Ensure appropriate Change Management
    vii. Ensuring Service Delivery and feedback
    viii. Ensuring Compliance to set rules, regulations, and procedures through Monitoring and Control.

The above, except item at (vii), comprise General IT Controls which are not specific to any individual transaction stream or application but concerned with the entity's overall IT infrastructure, including IT related policies, procedures, and working practice, as well as controls over data centre operations (IT policies and standards), system software acquisition and maintenance, access (physical and logical) security, segregation of duties, business continuity & disaster recovery controls, and application system development & maintenance.

Supplementing the assessment of the IT General controls would be the understanding of the business process, mapping of the business process onto the IT system and the associated IT application controls.

The exceptions identified after preliminary assessment would lead to decisions on substantive testing of the IT system and its controls.

21.2 Substantive Testing

Substantive testing involves detailed testing of the IT Controls, as under preliminary assessment, employing various techniques and tools for enquiry, extraction and data analysis. In substantive testing the tests are designed to substantiate the assertions as per audit objectives. The tests have to be specifically designed using any one or more of the techniques[26] in Section D.

22. Supervision and Review

Requirement:

[26] The techniques can be used both compliance and substantive testing. The IT Auditor can pick one or more of these techniques while conducting any of the two assessments.

The SAI shall ensure that IT audits are supervised and reviewed periodically.

Explanation:

22.1 The work of audit staff should be properly supervised during the audit, and documented work should be reviewed by the Team Leader of the IT Audit Team (Element 5 – 'Performance of Audits and other works' - ISSAI 40). The senior member of the audit staff should have the necessary competence to provide guidance, handholding and mentoring role during conduct of audit.

23. Cases of Fraud, Corruption and other Irregularities

Requirement:

The SAI and IT Auditors should identify and assess the risks and fraud relevant to the audit objectives of IT Audits.

The SAI shall take appropriate necessary actions, as required by the applicable laws to deal with cases of fraud, corruption, and other irregularities.

Explanation:

23.1 As IT Auditors perform their audit, they may come across instances of fraud, corruption, and associated irregularities. Requirements for the reporting of fraud may be the subject of specific provisions in the audit mandate or related laws or regulations, and the Auditor may be required to communicate such issues to parties outside the audited entity, such as regulatory and enforcement authorities. In such a situation, the SAI should take appropriate necessary actions, as defined in their mandates and applicable laws.

23.2 As IT Auditors perform their audit, they should should maintain an attitude of professional scepticism and be alert to the possibility of fraud throughout the audit process.

24. Limitations

Requirement:

SAI should identify, indicate, and communicate limitations at every stage of the audit at appropriate levels.

Explanation:

24.1 Limitations to the IT Audit should be pointed out at every stage of IT Audit at appropriate levels through appropriate documented communication

24.2 Limitations to the IT Audit should be pointed out in the report.

24.3 The typical limitations could be inadequate access to data and information, lack of adequate documentation of the computerisation process, leading IT Auditors to devise their own methods of investigation, and analysis to derive conclusions. Any other limitation faced by IT Auditors should be pointed out in the report appropriately.

25. Follow up

Requirement:

SAI should follow up on the reported matters that IT audit reports as relevant.

Explanation:

25.1 SAIs have a role in monitoring action taken by the responsible party in response to the matters raised in an audit report. Follow up focuses on whether the audited entity has adequately addressed the matters raised, including any wider implications e.g. if the same IT system is used by many governmental organisations, insufficient or unsatisfactory action by the audited entity may call for a further report by the SAI.

D. IT AUDIT TECHNIQUES AND TOOLS

Requirement:

The SAI shall deploy appropriate IT Audit techniques in conformity with the nature of audit engagement and requirements of audit objectives.

Explanation:

26. Identifying techniques specific to IT Audit

26.1 IT auditing techniques relate to deployment of methods and procedures by which the control environment in an IT system can be studied, evidence can be gathered and analysis can be made to obtain assurance on the adequacy of controls.

27. Techniques in planning

27.1 While planning an audit of an IT system, the auditor needs to first understand how a particular application supports a business process of the audited entity. For this purpose, basic information on the way the business functionality flows through the system needs to be obtained. Traditional auditing techniques like document study, interviews with key personnel – both business process owners and persons in the IT organisation, and observation of procedures are useful in gaining a good understanding of how the system supports the business of the entity. Study of IT 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) help understanding of the environment in which the system operates and identifying the business risks from control failures.

27.2 During the annual and team planning stages of IT audits, risk assessments are taken up on IT systems being developed or in use by various audited entities. These can be objectively done by applying techniques described in the Planning section of this Standard document.

28. Techniques in audit execution

28.1 The choice of techniques to use would be critical while conducting compliance and substantive testing. During substantive testing the tests are designed to substantiate the assertions as per audit objectives. The tests have to be specifically designed using any one or more of techniques[27], such as Interview, Questionnaire, Observation, Walk Through, Flow charts, Data capture and analysis, Verification, Re-computation, Reprocessing, Third party confirmation, etc.

28.2 For an assessment of the adequacy of general computer controls – spanning the domains of IT governance, systems development and acquisition, IT operations, Information security and business continuity planning – techniques deployed are similar to those used in other types of audit.

[27] These techniques can be used in both preliminary and substantive testing. Applicability of many of the techniques are available in the WGITA IDI Handbook on IT Audits for Supreme Audit Institutions

28.3 The audit techniques specific to IT audit are primarily deployed for assessment of IT application controls. While testing application controls, the auditor needs to:

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

28.4 For better understanding of the system being audited including its key control points, and developing the testing strategy to be adopted, it is always useful to look at the 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.

28.5 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.

28.6 For assessing Segregation of Duties and input authorization, it would be important to review job descriptions, match them to privileges assigned in the system, review authorization procedures, and confirm existence of action logs of user accounts having administrator privileges. The override activity report need to be tested for evidence of managerial review.

28.7 The audited entities will have their own combination of hardware, operating system, database management systems, application software, network software, etc. IT Auditors should be able to gather information from these sources to carry out the required analysis of the IT application. Understanding of the IT System and database in the organization such as the business processes involved, their criticality to the organisation, the protocols involved, etc., is an essential step for data extraction. Substantive testing of adequacy of application controls involve:

a. Extracting relevant entity business data
b. Transforming and Loading data into a tool
c. Performing data analysis
d. Validating test results
e. Drawing audit conclusions

These procedures can be carried out by IT auditors with the help of techniques described in Annexure A.

29. Deciding appropriate system of preserving information

29.1 Preservation of the audit results and and the audit evidence is to be ensured by IT Auditors so that they conform to the requirements of reliability, completeness, sufficiency, and correctness. It is also important for IT Auditors to ensure that the audit process is also preserved to enable subsequent verification of the audit analysis procedures. This involves suitable documentation techniques which are dealt with subsequently.

29.2 While using data dumps, to the extent possible, a forwarding letter may be taken. If the same is not possible, internal documents should be generated noting down important information like the date on which the data was handed over, from what file the data dump[28] was created, and whether the data was from production environment or from some other environment, etc. The electronic evidence generated and used for audit reporting should be related to such documents.

29.3 The IT Auditors should decide on the appropriateness of the use of one or more of the above techniques and ensure themselves on integrity and usefulness of the technique. The use of any of the above techniques should not impact the integrity of the application system and its data at the audited entity.

30. IT Audit Tools

Requirement:

The SAI shall deploy appropriate IT Audit tools commensurate with the risk assessment in the audit engagement along with the capacity and resources available with the SAI.

Explanation:

30.1 IT Auditing requires sound knowledge about the processes and techniques along with competency in using the IT Audit tools as these audits, by their very nature, deal with information which is stored and processed in electronic form and the audit trail is not outwardly visible.

30.2 **Computer Assisted Audit Techniques (CAATs)** are IT tools, which help an Auditor in carrying out various automated tests to evaluate an IT system or data and are very useful, where a significant volume of audited entity data is available in electronic format. CAATs are useful for test of controls and substantive testing, in Financial Audit, Compliance Audit and Performance Audit. Use of CAATs and the extent of usage are determined by various factors during audit planning and execution stages

30.3 Usefulness of CAATs:

CAATs are very useful to conduct IT Audit activities such as User Log Analysis, Exception Reporting, Totalling, File Comparison, Stratification, Sampling, Duplicate Checks, Gap Detection, Ageing, Virtual Field Calculations, etc. (these are elaborated in the section on IT Audit techniques). Use of CAATs bestow many advantages when compared to manual examination. Some of these are as follows:

a) Substantive testing and analysis of large volumes of data can be done within a short span of time and with less effort
b) Tests can be repeated easily on different files/data
c) Flexible and complex tests can be done with change in parameters
d) Automated Documentation of audit tests and results
e) More efficient deployment of audit resources

30.4 Choice of CAATs when conducting IT Audit: Use of CAATs has associated costs in terms of licensed software, compatible hardware, and deployment of skilled audit personnel. Hence, some important factors which need to be considered while deciding on the use of CAATs in IT Audit are as follows:

[28] Data dump is defined as a large amount of data transferred from one system or location to another

a) Does the use of CAATs provide additional value to audit?
b) 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?
c) Are the transactions processed on-line and/or real-time?
d) Will the use of other audit techniques entail higher costs and extra time?

30.5 Some prominent examples of CAATs are:

- General purpose audit software is developed to meet the specific requirements of auditors, and contain the regular tests that are carried out by auditors as part of IT audit and they include common functions like data extraction, summarizing, aging, stratification, duplicate checks, etc.
- Structured Query Language(SQL) is a non-procedure oriented language and is used for defining and manipulating data in Relational Database Management Systems (RDBMS).
- Spreadsheets are also useful CAATs and can be used for running simple queries like extracting data fulfilling predetermined criteria, sorting, totaling, etc.
- Data mining tools help in discovering patterns in large data sets, and extract information from such datasets and transform them into an understandable structure for further use through data visualization.
- Industry specific audit software is made with an aim to provide functionalities to cater to common audit functions associated with specific industries. i.e. they capture industry specific logic to create audit queries etc. They are found in industries with well documented and established business processes such as banking, manufacturing, oil and gas, shipping, etc.
- Utility Software perform functions designed to help analyze, configure, optimize or maintain the ICT infrastructure. Main examples of IT Audit related utility software interalia are revision control utilities, debuggers, disk space analyzers, file managers, network utilities, and system profilers
- Well-developed systems have embedded audit modules (Specialised Audit Software) which generate standardized as well as customized reports. These come as ready built functionalities of the Enterprise Resource Planning (ERP) applications. In addition, there are off the shelf software which give IT auditors read only access to ERP data through interface based applications

30.6 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 interalia about tables/files relationships, database dictionary/triggers, record layout,control totals, data size/format, and system documentation, before commencing a CAATs enabled audit.

E. REPORTING

Requirement:

The IT Audit reports shall reflect the findings from the IT Audit process depending upon the materiality of such findings vis-a-vis the audit objectives.

The IT Audit report shall be comprehensive, balanced, convincing, timely and easy to read.

Explanation:

31. Requirements of Reporting an IT Audit

31.1 Since an IT Audit can be in nature of a financial audit, a performance audit, a compliance audit, or a combination of these, the reporting requirements in an IT Audit would likewise flow from ISSAIs 100- 400, and depending upon the nature of audit being conducted, from ISSAIs 1700, 1705, and ISSAI 1706 in case of Financial Audit and respective level 4 ISSAIs on Compliance Audit and Performance Audit.

31.2 Some consideration that IT Auditors should be aware of is to limit the use of technical jargon, be aware of the sensitivity of the information presented, for example passwords, usernames, ID, and personal information, in the report.

32. Contents and Format of the IT Audit Report

32.1 The general layout of an IT Audit report includes the following;

a. Audit Objectives
b. Audit Scope
c. Applicable dates of coverage of audit
d. Audit Criteria
e. Audit Methodology
f. Summary
g. Audit findings
h. Audit Conclusions
i. Audit Recommendations
j. Any associated cause(s) and risk(s), restrictions, reservations, limitations, or concerns that the Auditor may hold in relation to the audit conducted by him/her

32.2 Despite the technical nature of an IT Audit, IT Auditors should ensure that the report is fully understandable by senior management, the audited entity, the stakeholders, and the general public.

32.3 IT Auditors may discuss the draft report with the management of the IT system prior to finalisation and release, and include its response to findings, conclusions and recommendations in the final report, where applicable.

32.4 The auditee unit may decide to accept the risk of not correcting a reported condition because of cost, complexity of the corrective action, or other considerations. The IT Audit report should mention such occurrence to responsible authorities in accordance with their internally developed framework.

32.5 In case IT 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 unit's views may be presented in the body of the report or in a cover letter.

32.6 IT Auditors may consider about the potential negative impact of the report once SAIs' audit reports will be published. Thus, if IT auditors finds some security problems in the IT system and have reported them before the IT system is patched, the vulnerability of the IT system is exposed to the

public before being fixed. In such a scenario, SAIs may consider options like reporting after the IT system has been fixed, or not reporting the vulnerability in detail, to avoid the adverse effect of the report.

32.7 Follow-up of any audit is the culmination of the entire IT Audit process. It is conducted to ensure that any deficiencies that have been identified in course of an IT Audit, have been subsequently satisfactorily acted upon. It is generally a result of continuous risk assessment being carried out by a SAI. As part of the follow-up of an IT Audit that has been reported, the IT Auditor revisits an audit after a reasonable lapse of time, to ensure that all recommendations have been implemented.

Annexure A – Data Analysis Techniques

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. IT 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. IT Auditors may also be required to convert data from one form to another to facilitate better reading and analysis.

2. **Transforming and Loading data:**

   Utilize the audit software/ Extract, Transform and Load (ETL) tools for importing data from varied database platforms. Most commonly used data analysis tools (explained in the Section on tools) allow import of data from multiple databases into the tools' native spreadsheet format. These tools commonly use an import wizard to assist in importing (interpretation, conversion, formatting) 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. Generalized audit software or specific utility software could also be used to assess the functioning of various utilities of the IT systems. The usage of any of these or their combination will depend on the audit objectives and scope to be covered in IT Audits.

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 or project;
   - Understand the sample(s) under study;
   - Understand the instruments being used to collect data;
   - Be cognizant of data layouts and formats[29]; and
   - Establish a unique identifier if matching or merging is necessary.
   - IT 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)

[29] This would be one of the most important steps before conducting data analysis. Layout would mean understanding of different databases, tables within, coding pattern utilised and relationships between table and databases. Understanding of different database models will be helpful in this regard.

- Data cleaning procedures (e.g. removing outliers)

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.

4. Understanding Data Types and Representation

Data analysis is usually done on a copy of data received from the audited entity to preserve the original for later confirmations and review, if required.

General Purpose Audit Software or Specialized Audit Software can be used to carry out the information analysis. These tools provide facility to import as well as analyse data. Use of Structured Query Language can also be made in analysing data. For complex systems like ERP systems, the information is available through specified reports. IT Auditors should obtain an understanding of such reports and obtain relevant reports to carry out appropriate analysis. IT Auditors should be careful in ensuring that the data obtained is reliable, competent, reasonable and sufficient. It should be, as far as possible, time stamped and duly vetted by the audited organization.

In particular, the variables in various data fields may require special coding for different data representation

- Numeric
- String
- Date & time
- Monetary

The individual techniques of data analysis for examining integrity of applications are again dependent on the audit objectives. These techniques are:

1. **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.
2. **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 IT 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.
3. **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.

These tests involve certain data analysis techniques that IT Auditors can deploy with the help of common analysis tools or generalized audit software.

1. **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 IT 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 and General Purpose Audit Software provides for easy functions to select a particular data element (field/ column/ tuple) 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.

2. **Summarisation and stratification:** These two techniques help profiling data before any test of controls are undertaken. Summarising data helps totalling of transactions in terms of defined attributes that helps the auditor gain an overall understanding of the transactions. For example, totalling the account receivables by customer types provides a useful insight on the high value payment defaulters. A very useful function available in spreadsheet and General Purpose audit tools 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.

3. **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.

a. Test of input 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.

b. Test of processing controls: For 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.

IT 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.

1. **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.

IT 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.

2. **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 Generalised Audit Software 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.

3. **Working with multiple files:** The source database often contains large number of transaction and master tables to fulfil the need of normalisation 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). GAS allows such 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.

IT Auditors need to apply a combination of these techniques for drawing assurance on application controls.