GUID 5100

Guidance on Audit of Information Systems

INTOSAI

INTOSAI Guidances are issued by the International Organisation of Supreme Audit Institutions, INTOSAI, as part of the INTOSAI Framework of Professional Pronouncements. For more information visit www.issai.org

INTOSAI

1) Endorsed as ISSAI 5100 - Guidelines on IT Audit, in 2016.
2) Revised and renamed GUID 5100 - Guidance on Audit of Information Systems, in 2019.

TABLE OF CONTENTS

1

INTRODUCTION

1.1 GUID 5100 provides the overarching framework for conducting audit of Information Systems within the IFPP. The GUID is 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.

1.2 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).

1.3 Supreme Audit Institutions (SAIs) are mandated to audit governments and their entities per their respective audit mandates.[1] Through their activities, SAIs aim to promote efficiency, accountability, effectiveness and transparency of public administration.[2]

1.4 Governments and other public sector entities have continuously adopted innovations in Information Technology (IT) into their information systems, in order to enhance efficiency and effectiveness in their functioning and delivery of various public services. This is because IT has made it possible to capture, store, process, retrieve and deliver information electronically, which in turn creates significant scope to improve the accuracy, confidentiality and timeliness metrics of information systems. Moreover, the delivery mode of public services is rapidly transitioning from physical to electronic, resulting in governments having to function as digital platforms providing services as well as infrastructure for other IT-driven information systems.

1 INTOSAI-P 1 *The Lima Declaration*
2 United Nations General Assembly Resolution A/66/209

1.5 This transition to computerised information systems and electronic processing by audited entities in the public sector has triggered a significant change in the environment in which SAIs work. The public sector expenditure on IT is growing. There is also a need to ensure that internal IT controls to maintain confidentiality, integrity and availability of data have been adopted by public sector entities. Therefore, it becomes imperative for SAIs to develop appropriate capacity to conduct a thorough examination of controls related to information systems.

2

OBJECTIVE OF THIS GUID

2.1 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.

2.2 The objective of this GUID is to provide guidance to auditors on how 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 Performance audit

2.3 The contents of this GUID may be applied by auditors to the Planning, Conducting, Reporting and Follow Up stages[3] of the audit process.

3 ISSAI 100

3

DEFINITIONS

3.1 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.

3.2 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.

4

SCOPE

4.1 This GUID may be used by auditors to conduct Performance and/or Compliance Audits on the specific subject matter of Information Systems, as well as where audit of information systems is part of a larger audit engagement which may be a Financial, Compliance and/or Performance Audit.

4.2 This guideline provides further guidance on how any audit of Information Systems could be addressed by using financial/performance/compliance auditing and does not contain any further requirements for the conducting the audit.

5

PLANNING IS AUDIT

5.1 SAIs may adopt risk based audit planning for IS Audits, in line with the process described in ISSAI 100, ISSAI 200 (Financial Audit), ISSAI 300 (Performance Audit) and ISSAI 400 (Compliance Audit), depending upon the objectives of the audit engagement.

5.2 The IS audit work will be determined by the objective and the scope of the audit. Examples could include:

1) To evaluate the relevant general controls[4] and application controls[5] 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.
2) To draw assurance on compliance of the processes of the information systems with the laws, policies and standards applicable to the audited entity.
3) 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.

4 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.

5 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.

5.3 Based on risk assessment, the scope of an IS Audit may be drawn from any or all of the following domains[6] of the audited entity:

1) Organizational Policy on IT[7]
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[8]
11) Statutory Compliance Management
12) Business Continuity and Disaster Recovery Management
13) Application Controls Management

5.4 SAIs may select the time period for audit analysis (e.g. one year, three years, etc.) in defining the scope of the IS Audit engagement. An appropriate time period may be selected, that is relevant to the aims defined for the audit engagement.

5.5 Where an IS Audit is a part of an audit engagement the SAI may ensure that the audit team as a whole works in an integrated manner to achieve the overall audit objective. To achieve effective integration, SAIs may consider:

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

6 A majority of the domains described have been adapted from ISO/IEC 27001
7 Including aspects of Strategic Management
8 Including Cyber Security

5.6 SAIs may ensure that the audit team is composed of members that collectively have the competence to conduct IS Audit engagements to achieve the intended audit objectives.

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

5.8 SAIs may ensure that the IS Audit teams collectively have the capacity to

1) 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
2) Understand extant rules, regulations and the environment in which the IT-driven information systems of the audited entity are operating
3) Understand the mapping of business processes into the programming logic for information system of the audited entity
4) 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
5) Evaluate the design and test the operating effectiveness of application controls in relevant information systems
6) Understand the audit methodology, including relevant auditing standards and guidelines applicable to the SAI
7) 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
8) Understand IS techniques to collect the audit evidence from automated systems
9) Understand IS Audit Tools to collect, analyse, and reproduce the results of such analysis or re-perform the audited functions
10) Access and use IS Infrastructure to capture and retain audit evidence
11) Access and use IS Audit Tools to analyse the collected evidence

5.9 SAIs may consider different options to allocate human resources for IS Audit engagements. This could be establishing a central group with IT specialists who assist other audit teams in the SAI to conduct these audits or deploying IT specialists as per requirement. As the number of IS Audit engagements undertaken increases, SAIs may consider establishing a dedicated IS Audit group or function. This group may be entrusted with the responsibility of conducting all IS Audit engagements for the SAI, and interact with other teams at the SAI who have legacy knowledge of the audited entity, in order to quickly get an understanding of the entity's functions and related business processes. As technology becomes more embedded in information systems, SAIs may ensure that all the Auditors acquire appropriate IS Audit skills.

5.10 SAIs may engage external resources such as IT consultants, contractors, specialists and experts to conduct IS Audit, in cases of resource constraints. SAIs may ensure that such external resources are adequately trained and sensitized to the guidelines for professional conduct and for processes and products of IS Audit applicable to the SAI, and that their work is adequately monitored through a documented contract or a service-level agreement and appropriate involvement from staff of the SAI in the Planning, Conducting, Reporting and Follow-Up stages of the audit. SAIs may 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.

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 spelt out below:

1) Inherent Risk would consist 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 audited entity which is required to make available information for all members of the public carries the inherent performance 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. Inherent Risk may be assessed before the influence of Control or Detection Risk is considered by the Auditors.

2) Control Risk for an IS would consist of the probability that IT controls that have been adopted by the audited entity may fail to mitigate the adverse impact that they were designed in response to. For example, an information system of an audited 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.

3) Detection Risk would consist 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.

5.12 For carrying out risk based assessments of IT driven systems, SAIs may select a methodology which is appropriate for their purpose. Such methodologies may range from simple classifications of the risk profile of the IT environment of the audited entity as High, Medium and Low based on the SAI's understanding of the entity and its environment and professional judgement of the IS Audit team of an SAI, to more complex and numeric calculations which quantify the risk rating based on objective data gathered from the audited entity.[9]

5.13 The materiality of an IS Audit issue may be decided under the overall framework for deciding materiality in an SAI. The perspective of materiality may 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 ISSAIs 100, 200, 300 and 400.[10]

9 *WGITA IDI Handbook on IT Audits for Supreme Audit Institutions*

10 ISSAI 200 *Financial Audit Principles*, ISSAI 300 *Performance Audit Principles*, ISSAI 400 *Compliance Audit Principles*

6

CONDUCTING IS AUDIT

6.1 SAIs may conduct IS Audits in line with the process described for Financial Audit (ISSAI 200), Performance Audit (ISSAI 300) and Compliance Audit (ISSAI 400) engagements, as the case may be, based on the nature of the engagement.

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.

6.3 Prior to initiating the assessment of controls in an information system, the auditors may develop an understanding of the system architecture, and the underlying data and its sources in order to identify the required audit tools and techniques.

6.4 In case of receiving data dumps[11] from the audited entity, Auditors may ensure that each data dump is accompanied by a letter from the audited entity. Such a forwarding letter may specify

1) 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[12] and non-repudiation[13]
2) The parameters of extraction used to create the data dump, i.e. queries used/ reports run.
3) If such a forwarding letter from the audited entity is not received,

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

12 Authentication is defined as the act of verifying the identity of a user- ISACA Glossary of Terms

13 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 – ISACA Glossary of Terms

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.

6.5 Auditors may conduct an assessment of IT controls (general and application controls) adopted by the audited entity, in order to examine their reliability and sufficiency. The assessment may be carried out using an appropriate combination of the following techniques: Interview, Questionnaire, Observation, Walk Through, Flow charts, Data Capture and Analysis, Verification, Re-computation, Reprocessing, and Third party confirmation. The scope of the assessment of IT controls may include examination that:

1) IS Policy has been defined, adopted and communicated
2) IS Governance structure is in place and is functional
3) Inventory of IS assets has been periodically carried out and requirements for augmentation, replacement and removal have been identified
4) Processes for sharing of infrastructure and common services for information systems with other public entities are in place and functional
5) Processes for development, acquisition and maintenance of Information Systems have been defined, adopted and communicated (including that of change management)
6) Processes for IT Operations (in-sourcing, out-sourcing, service agreements) have been defined, adopted and communicated
7) Measures to ensure physical security and intended physical working conditions have been adopted.
8) 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
9) Measures to ensure confidentiality, integrity and availability of various communication modes and channels have been adopted
10) Measures for Information Security Management have been adopted

11) Measures for Statutory Compliance Management have been adopted

12) Measures for Business Continuity and Disaster Recovery Management have been adopted

13) Application Controls adopted within each information system are adequate and reliable. Such an assessment may 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.

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

6.7 Depending upon the objective of the audit, Auditors may be concerned with the design, implementation and 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.

6.8 Auditors may 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.

6.9 Based on the assessment of IT controls, Auditors may identify priority areas for taking up Substantive Testing, which involves detailed testing of the IT controls by employing various Computer Aided Audit Techniques (CAATs) for enquiry, extraction and analysis of data. Auditors may design and execute Substantive Testing in order to substantiate the audit objectives. Auditors may select appropriate CAATs, based on their requirements.

6.10 Auditors may use CAATs to execute IS Audit techniques 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 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.

6.11 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, SAIs may, based on materiality considerations, adopt audit sampling for detailed examination to draw reasonable audit conclusions. SAIs may use appropriate CAATs for carrying out different types of sampling, and determine an appropriate sample size, depending on the underlying Inherent and Control Risks. Audit samples[14] 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 within an acceptable level. 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. When doing a sampling within the scope of a financial audit, the IS auditors may apply ISSAI 2530 for sample selection.[15]

6.12 Auditors may 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

14 ISSAI 2530, *Financial Audit, Audit Sampling*, Sections 6 to 9.
15 ISSAI 2530, *Financial Audit, Audit Sampling*, Sections 6 to 9.

Information Systems Reports, etc. and may 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 may 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.

6.13 IS Audit documentation may be retained and protected from any modification and unauthorised deletion. SAIs may evolve new standards for retention of IS Audit documentation or adapt existing standards to meet the requirements of retention of IS 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 may be paid to media, the format, the life expectancy, and the storage requirements for this data, to ensure that the data is readable within the time frame defined in each SAI's data retention and archiving policy. This may necessitate conversion of data from one format to anotherto keep up with technological advances and obsolescence.

6.14 In case of examination of technical Reports prepared by third party auditors on technology specific subject matters, Auditors may adopt appropriate procedures to draw assurance on compliance, financial or performance aspects of such Reports.[16] If, as a result of such procedures, reliance is placed on the contents of such Reports, the fact of reliance may be suitably disclosed.

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.

16 When the scope is within financial audit the auditors may use ISSAI 2402 *Audit Considerations Relating to an Entity Using a Service Organization*

7

REPORTING ON IS AUDIT

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.

7.2 Auditors may 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 may ensure that the report is fully understandable by senior management of the audited entity, the stakeholders, and the general public. Auditors may 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.

7.3 Auditors may 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 may 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.

8

FOLLOW UP

8.1 Since an audit engagement on Information Systems is drawn from one or more of the main types of Audit, Auditors may consider the follow up requirements for such Audit engagements to be on par with those for Financial Audit (ISSAI 200), Performance Audit (ISSAI 300) and Compliance Audit (ISSAI 400).