Revised Draft INTOSAI GUID 5101 – Guidance on Audit of Information security

I. Introduction

1. The transition to computerised information systems and electronic processing of information by auditees in the public sector makes it imperative for SAIs to develop appropriate capacity to audit controls related to information systems. As part of the audit of Information Systems, there is a need to ensure that controls to maintain confidentiality, integrity and availability of Information Systems and data (i.e. Information Security) have been designed and applied by auditees.
2. Information security weaknesses may lead to severe damage (legal, reputational/ credibility, financial, productivity, exposure to further intrusions). Such damage may be caused by security breaches, unauthorised external connections, exposure of information (disclosure of corporate assets and sensitive information to unauthorised parties), insider threats or system vulnerabilities.

II. Objectives of this GUID

3. This GUID supplements GUID 5100 by providing guidance on audit addressing IT-security aspects. The guidance laid out in this GUID is consistent with the Fundamental Principles of Public Sector Auditing (ISSAI 100).
4. While the overall principles and guidance outlined in GUID 5100 are applicable to audit of security of information systems, the objective of this GUID is to provide specific and additional guidance for the compliance audit of information security (including cyber security).
5. Audit of information security can be taken up as a compliance audit or, in certain circumstances, as a performance audit or as part of a financial audit. This GUID covers audit of information security being taken up either as a distinct compliance audit or as part of a larger compliance audit engagement to see whether the IT management meets the necessary standards and requirements for IT security.
6. The contents of this GUID may be applied by auditors in the Planning, Conducting, Reporting and Follow Up stages of the audit process.

III. Definitions

a) **Information Security**: Protection of Information and Information Systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability.

b) **Integrity**: Guarding against improper information modification or destruction and includes ensuring information non-repudiation[1] and authenticity[2]; alternatively, accuracy and completeness of information as well as its validity in accordance with business values and expectations. A loss of integrity is the improper modification or destruction of information.

c) **Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary

[1] Non-repudiation is protection against an individual who falsely denies having performed a certain action and provides the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, or receiving a message.

[2] Authenticity is the property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.

information; alternatively, protection of sensitive information from unauthorized disclosure. A loss of confidentiality is the unauthorized disclosure of information.

d) **Availability**: Timely, reliable access to and use of information or an information system for authorized users; alternatively, information being available when required by the process now and in the future, as also the safeguarding of necessary resources and associated capabilities. A loss of availability is the disruption of access to or use of information or an information system.

e) **Information Security Management System (ISMS)**: According to ISO-27001, the information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

IV. The Subject Matter

7. When audit of information security is taken up as a compliance audit, the compliance in respect of the subject matter (information security or any specific aspect/ component thereof) to the applicable authorities (policy, procedure, standards, practices etc.) is assessed by auditors.
8. The information security audit work will be determined by the objectives and scope of the audit. Elements of such scope of the work could be usefully derived from ISO/IEC 27001 or other legislation/standards/ best practices, as illustrated below:
   a. Information security culture, including leadership and commitment; management direction and policies; information security objectives; organizational roles, responsibilities and authorities (including mobile working, teleworking etc.)
   b. Information security risk management processes, covering
      i. information security risk assessment (including information security risk acceptance criteria, identification, analysis and prioritisation) and information security risk treatment
      ii. Communication (internal and external) and documentation relevant to the information security management system
      iii. Review and continual improvement of information security
   c. Human resources security at different stages from prior to employment, during employment and post-employment
   d. Management and control of information assets, including inventory and classification; rules for acceptable use; transportation, return and disposal
   e. Authentication, authorization and access control – including identify management and authentication, cryptographic controls, and authorization and access controls;
   f. Physical and environmental security;
   g. Network and communication security and cyber security management;
   h. Information security incident management and security testing and monitoring;
   i. Security as part of system acquisition and development;
   j. Operations security, including operating procedures and responsibilities; protection from malware; data backup/ recovery and logging and monitoring;
   k. Information security in supplier relationships;
   l. Compliance with external and internal requirements.

V. Planning audit of Information Security

9. The need for an Audit of Information Security may be triggered, depending on the results of an audit risk assessment, by one or more events, such as (illustratively, refer Annexure A also):

(a) development of a new IT System or replacement/ upgradation of an existing IT System by the audited entity, especially in a critical business area;

(b) non-upgradation/ replacement of a long-standing legacy IT system, where the underlying technological infrastructure is outdated and not currently supported through security patches/ updates;

(c) non-conduct of periodic internal/ external security testing, including and security testing of operational IT systems, especially those which have undergone significant application or infrastructural upgrades;

(d) a *post mortem* of a major security incident or breach which has adversely impacted the concerned IT system, or where a security incident or breach has adversely impacted similarly placed IT systems in other audited entities;

(e) data protection and privacy related concerns have arisen with regard to existing IT systems and the need for upgradation/ updating to comply with the latest applicable statutes relating to protection of personal data;

(f) significant information security threats in the environment or information security risks with regard to the information system of the audited entity have been identified through other audits (internal or SAI/ external audits), evaluations or assessments or control deficiencies identified through past information security audits remain unaddressed or only partly addressed;

(g) significant changes in organisation policies and structures for information systems management and implementation, including information security.

10. The SAI may use the auditee's risk management process (including risk identification, assessment and treatment) as a basis for a risk identification and assessment if performing a risk based audit approach.
11. The materiality of an information security audit issue may be decided under the overall framework for deciding materiality in an SAI, as well as specific guidance for materiality in respect of IS audits.

V.1 Sources of audit criteria

12. As part of the planning of information security audits, SAIs may find it useful to identify and adapt, as appropriate, nationally/ internationally accepted information security frameworks for audit risk assessment (to prioritize information security audits and define the audit objectives and scope) and for detailed audit planning of information security audits. Such frameworks serve as sources for audit criteria.
13. These frameworks and standards could include the ISO 27000 series; the CoBIT framework prepared/ updated by ISACA, the standards and frameworks relating to information and cybersecurity prepared by the National Institute of Standards and Technology (NIST); Center for Information Security (CIS) controls; more narrowly focused/ sector-specific frameworks and standards include the European Union's General Data Protection Regulation (GDPR), PCI DSS (Payment Card Industry Data Security Standard), the US Health Insurance Portability and Accountability Act (HIPAA) for the healthcare sector etc.
14. Which framework the SAI choose to use as appropriate audit criteria may depend on:

- Specific SAI and country context (including legal and regulatory requirements, if any)
- Concerned audited entity/entities
- Scope of the audit.

V.2 Resources

15. The considerations for allocating human resources for IS audit engagements (including information security audits) are discussed in GUID 5100 and are broadly applicable in the case of information security audits.

VI. Conducting Information Security Audits

16. SAIs may conduct information security audits in line with the processes described in ISSAIs as well as GUID 5100. The additional guidance will supplement the guidance in GUID 5101.
17. The audit procedures for an information security audit will be designed with a view to focusing on the objectives of deriving assurance as to (a) confidentiality (b) integrity – including non-repudiability and (c) availability with regard to data and IT systems falling within the scope of the audit engagement.
18. The procedures will typically involve a combination of (a) review of documentation (b) observation, walkthroughs, interviews, questionnaires etc. (c) analysis of electronic data (e.g. relating to audit logs of various types). If Vulnerability Assessment/ Penetration Testing (VA/PT) is to be conducted by the SAI audit team, necessary arrangements with, and agreement of the audited entity for such intrusive testing will have to be made. Vulnerability assessment is meant to identify security issues in IT applications, workstations, or entire organizational network in a systematic and organized way and allows auditors to classify, prioritize, and rank security vulnerabilities according to their risk levels for timely remediation. Penetration Testing is akin to ethical hacking is an authorized simulated hacking or attack on a computer system, performed to evaluate the security of the system.
19. The scope of most information security audits will generally include the information security culture, policies, procedures, organizational roles etc. For these aspects, the audit team should specifically look at not only the availability of relevant policies, procedures etc, but also whether there is adequate awareness and understanding amongst users and also whether these are being reviewed at appropriate intervals of time and updated, as necessary.
20. The risk management process will also generally be covered in the scope of most information security audits. It would be important for audit to examine the frequency of periodic risk reviews, and also the adequacy of follow-up actions to mitigate the identified and assessed risks. The decision on risk acceptance thresholds (and the consequential acceptance of residual risks) is a management decision.
21. Linked to the risk management process (in particular, risk identification and assessment) are the policies for identification, classification and control of information assets, whether the policies are understood by users and whether such policies are implemented effectively.
22. Wherever authentication, authorization and access controls are covered within the scope of the audit engagement, a key aspect that would be looked at is whether multi-factor authentication (typically in addition to password-based authentication) is implemented, if it is mandated or prescribed by policy or the contract.
23. When logs are to be scrutinized to assess whether access control was implemented as planned, the analysis of logs may involve receipt of data dumps or extracts. Where data dumps are received from the audited entity for electronic analysis, the considerations spelt out in para 6.4 of GUID 5100 with regard to ensuring its authenticity, integrity and non-repudiability may be ensured.
24. For audit of information security incident management, in addition to the review of the processes and documentation relating to incident identification and logging,

assessment and resolution, the audit team may consider obtaining feedback on the adequacy of the resolution from a sample of users (where incidents were identified and ticketed by such users).

25. With regard to information security in supplier/ outsourced relationships, the audited entity retains accountability for information security even if the responsibility for certain IS activities has been outsourced to an external supplier. Further, aspects such as segregation of conflicting duties (e.g. between development, testing and production teams) matter equally, whether the development/ implementation/ Operations and Maintenance of the IT system is being done in-house or through an external supplier.
26. For assessing physical and environmental security, in addition to documentation review, interviews etc., the SAI audit team may consider a physical visit (or joint inspection) of the data centre as a supplementary audit procedure.
    (Illustrative high level audit questions mentioned in Annexure B)
27. SAIs may or may not conduct VA/PT of the information systems of the auditee; however, the SAI's information security audit teams should be able to understand the scope of third-party VA/PT and associated information security audits, as well as the findings of such audits and their implications. However, this will depend on the SAI's specific mandate, the environment in which the SAI is working (including consideration of the audited entity), the competencies and resources available for VA/PT audit as well as the SAI's professional judgement in determination of the information security audit scope.
28. An information security audit may include assessment of business continuity and disaster recovery planning and implementation, with a view to assessing the "availability" aspect of information services as well as information security during disaster recovery. Alternatively, such aspects may be covered as part of an audit of IT operations management.

VII. Reporting on audit of information security

29. The guidance on evaluating audit evidence and reporting as per ISSAI 400 as well as the additional guidance under GUID 5100 on reporting (section 7, which also refers to the sensitivity of reporting security risks before necessary mitigating controls have been adopted) may be followed in the case of information security audits.
30. Reporting on information security by auditors may consider the potential business impact of exposing technical shortcomings and security risk in public. In such cases, SAIs may use management letters to share the details and possible impact of the risk with the audited entity.
31. Besides the regular stakeholders of public sector audits, reporting may consider the specific perspectives of stakeholders like outsourced technical providers of support to the auditees.
32. Recommendations may not be limited to presenting the available technical solutions for improving the information security but may also consider the practical implications for the business of the auditee along with a cost benefit analysis.

VIII. Follow up

33. Follow up requirements as per ISSAI 400 for Compliance Audits are to be considered.
34. IT systems are dynamic. They are also increasingly web-based/ cloud hosted. Frequency of follow up audits may consider the significant changes arising out of these factors.

35. Solutions for identified weaknesses from information security audits are likely to be very specific in terms of available technology, costing, system compatibility etc. The follow up plan along with timelines may be reviewed considering these.

Annexure A: Illustrative factors affecting information security

Information security of an organisation is affected by several factors, which tend to be a mix of technical aspects and non-technical aspects like governance, management, organisational culture/ practices, human resources security etc.

- Third Party Service Provider Management - The important consideration for an auditor is the assurance that effective oversight of third-party activities is implemented, and the activities of third-party service providers are governed through comprehensive contractual agreements.
- Governance aspects include the organizational accountability and reporting structures for information security, the organization-wide IT security policy, and the overall policies for incident and problem reporting and management; these will be supplemented by detailed technical and non-technical processes, procedures, guidelines, advisories etc. The adequacy of standards, guidelines and procedures designed to operationalize the policy is also verified in audit.
- Documentation regarding technical architecture, application design and exit management etc. should be periodically updated.
- User Access Controls – The IT application includes the user-roles as per their authority only. Traceability of significant actions performed should be logged in the system. This includes user access through multi-factor authentication, and auto logout features etc.
- Compliance to legal and regulatory frameworks especially in respect of Personally Identifiable information and commercially sensitive information.

In addition, legacy IT applications based on out of support IT components (hardware/ platform/ software) are one of the biggest set risks, since Government organizations often do not focus as much attention on applications which are in production and stabilized.

Annexure B: Suggested High Level Audit Questions

This Annexure contains high level audit questions on the subject matter of Audit of Information Security as guidance and is only indicative, not exhaustive. Relevance of the objects will depend on whether the audited entity is required by law or other obligations to meet the criteria assumed in the objectives. Detailed audit questionnaires would depend on the type of Information system, organisation, framework and audit assignment scope etc.

Sl No	Information Security Domain	Objective	Remarks
1	Information security policy	Whether such policy is defined, adopted and communicated.	Such policy also needs to be reviewed at regular intervals.
2	Information Security organization structure	Whether such a governance structure has been made clearly responsible for Information Security.	Auditors may examine the clarity in definitions, constitution, composition, and mandate.
		Whether the terms of personnel as part of this governance structure, individual roles and reporting mechanism have been defined.	Segregation of duties with distinct roles and responsibilities for each position with reporting hierarchy for escalation of issues should exist within organisation.
		Whether security aspects related to human resources involved with information systems have been addressed.	Human resource related controls are to be exercised at all stages of HR management.
		Whether the organisation promotes a culture of Information security among personnel at every level	Organisational culture plays an important role in determining the level for information security in organisation.
3	Information asset management	Whether inventory of IT assets has been periodically carried out and that security requirements for each asset type have been identified.	Information assets should be appropriately classified, labelled, and managed.
4	Development, acquisition and maintenance of Information Systems	Whether security aspects for each of these processes have been defined, adopted and communicated.	Information security must be a crucial consideration during the entire lifecycle.
		Whether information security is ensured by vendors in all interactions.	Depending on the risks, verify whether the audited entity has had the code and modules of the information system developed/ acquired reviewed by skilled internal or third-

			party resources to ensure that there are no hidden features that may compromise confidentiality, integrity and availability of data.
5	IT Operations	Whether security of IT operations has been defined, adopted and communicated.	Examine contracts/ service level agreements to verify incorporation of non-disclosure, non-compete, non-modification without authorization, non-transmission and other standard provisions related to ensuring confidentiality, integrity and availability of data with parties to whom IT operations are outsourced.
6	Physical and environmental security	Whether security of physical environment of the information system has been ensured.	Verify whether physical barriers (external gates, internal doors, human security guards) which require identification of personnel and restrict access to storage hardware such as servers only to authorized personnel are in place. Facility management is an important aspect of the whole security ecosystem.
7	Network and Communications security	Whether information security is ensured during communication.	Verify whether communication channels ensure encryption of messages, to prevent interception by third parties and loss of confidentiality; also verify use of cryptographic controls for digital communications of a formal nature.
		Whether network security architecture is adequate for ensuring information security.	Wherever applicable, existence of cryptographic and other cyber security controls may be examined by auditors.
9	Statutory Compliance	Whether statutory requirements related to information security aspects have been complied with.	Checks for compliance to statutory and regulatory provisions are to be exercised by auditors in all other domains as applicable. Provision may require specific certification/ assurance related to information to be obtained by entities. Scope and validity of such

			certification may also be examined by auditors.
10	Business Continuity and Disaster Recovery	Whether security aspects related to these processes have been addressed and information security is adequate for DR transition as well as operation.	Auditors may check whether information security facility is adequate during the disaster recovery process.