INTOSAI GUID 5101 – Guidance on Audit of Information Security (Draft Endorsement Version)

I. Introduction

1. GUID 5101 supplements GUID 5100 by providing guidance on audit of information security. The guidance laid out in this GUID is consistent with the Fundamental Principles of Public Sector Auditing (ISSAI 100) as well as with the Compliance Audit Principles (ISSAI 400).
2. 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.
3. Information security breaches may lead to severe legal, reputational/ credibility, financial, productivity damage, and exposure to further intrusions. Security breaches may be caused by weaknesses and vulnerabilities that lead to accidental exposure, or disclosure of information to unauthorised parties, loss of availability or unauthorised changes in systems and data.

II. Objectives of this GUID

4. The guidance applicable to audit of information systems is outlined in GUID 5100. The objective of this GUID is to provide specific and additional guidance for a compliance audit of information security.
5. Audit of information security can be taken up as a compliance audit or, in certain circumstances, as a combined audit incorporating financial, compliance and/or performance aspects. This GUID covers audit of information security being taken up either as a distinct compliance audit or as part of a combined audit engagement to see whether the IT management meets the necessary standards and requirements for information 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. The GUID lists possible subject matters of audit work, risk factors affecting information security, sources of audit criteria and high-level audit questions. These lists are illustrative and not exhaustive.

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) **Cyber Security**: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, and confidentiality.
c) **Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information; alternatively, protection of sensitive information from unauthorized disclosure. A loss of confidentiality is the unauthorized disclosure of information.

d) **Integrity**: Guarding against improper information modification or destruction and includes ensuring information non-repudiation1 and authenticity2; 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.
e) **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.
f) **Vulnerability Assessment/Penetration Testing (VA/PT)**: 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 and is an authorized simulated hacking or attack on a computer system, performed to evaluate the security of the system.

IV. The Subject Matter

7. In audit of information security, the auditor assesses compliance of the subject matter (information security or any specific aspect/ component thereof) with applicable authorities (laws, regulations, policy, procedure, standards, practices etc.).
8. The information security audit work will be determined by the objectives and scope of the audit. The scope of the audit may include different subject matters such as:
    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 thresholds, 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 and risk management
    c. Information security in supplier relationships;
    d. Human resources security at different stages from prior to employment, during employment and post-employment
    e. Management and control of information assets, including inventory and classification; rules for acceptable use; transportation, return and disposal
    f. Authentication, authorization and access control – including identify management and authentication, cryptographic controls, and authorization and access controls;
    g. Physical and environmental security;
    h. Network and communication security and cyber security management;

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.

i. Information security incident management and security testing and monitoring;
j. Security as part of system acquisition and development;
k. Operations security, including operating procedures and responsibilities; protection from malware; data backup/ recovery and logging and monitoring;
l. Compliance with external and internal requirements.
m. New or amended laws.

V. Planning an Audit of Information Security

9. An audit of information security may be initiated as a result of a risk assessment. Some relevant risk factors may be:

(a) development of a new information System or an existing information system has been replaced or upgraded (application and/or infrastructure) by the audited entity, especially in a critical business area;

(b) long-standing legacy information system has not been upgraded or replaced, where the underlying technological infrastructure is outdated and not currently supported through security patches/ updates;

(c) periodic internal/ external security testing have not been conducted, including security testing of operational information 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 information system, or where a security incident or breach has adversely impacted similarly placed information 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;

(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 auditor may assess the auditee's risk management process (including risk identification, assessment and treatment) and consider previous internal or external audits or assessments as part of risk identification and assessment, if performing a risk based audit approach.
11. The auditor may examine availability of relevant policies and procedures, and whether these are being reviewed at appropriate intervals of time and updated as necessary while evaluating the organizational roles. The auditor may also assess whether there is adequate awareness and understanding amongst users, including the information security culture.
12. 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 information systems audits.

V.1 Sources of audit criteria

13. The auditor may use nationally or internationally accepted information security frameworks as sources for audit criteria.
14. The frameworks that serve as sources of audit criteria could include standards such as the ISO/IEC 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.
15. The auditor's choice of 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

16. The considerations for allocating human resources for information systems audit engagements (including information security audits) are discussed in GUID 5100 and are broadly applicable in the case of information security audits. One additional consideration may be that when dealing with sensitive and confidential information, auditors might be required to go through a special screening by relevant authorities.

VI. Conducting an Audit of Information Security

VI.1 Purpose of the audit procedures[3]

17. The audit procedures for an information security audit will be designed with a view to focus on the purposes to assess (a) confidentiality (b) integrity – including non-repudiability and (c) availability of data and IT systems falling within the scope of the audit engagement.

VI.2 Audit procedures for gathering audit evidence

18. The audit procedures may involve a combination of (a) review of documentation (b) observation, walkthroughs, interviews, questionnaires (c) analysis of electronic data, e.g. relating to audit logs of various types (d) Vulnerability Assessment/ Penetration Testing (VA/PT). If VA/PT is to be conducted by the auditor, arrangements and agreement with the audited entity for such intrusive testing may have to be made, including legal safeguards and indemnifications where necessary. If VA/PT has been carried out by a third-party the results of the VA/PT may be included as part of the audit evidence. In this case, the auditor obtains a sufficient understanding of the scope of the VA/PT as well as the findings and their implications.
19. For assessing physical and environmental security, in addition to documentation review, interviews etc., the auditor may consider a physical visit (or joint inspection) of the data centre as a supplementary audit procedure.
20. The auditor may assess the adequacy of standards, guidelines and procedures designed to operationalize information security policy and policies for incident/ problem reporting and management.

[3] Illustrative high-level audit questions are mentioned in Annexure.

21. The audit of the risk management process may include examining the frequency of periodic risk reviews, and 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.
22. Linked to the risk management process (in particular, risk identification and assessment) are the policies for identification, classification and control of information assets. Audit procedures may include examining whether the policies are understood by users and whether such policies are implemented effectively.
23. Audit procedures on authentication, authorization and access controls may include examining whether multi-factor authentication (typically in addition to password-based authentication) is implemented, if it is mandated or prescribed by policy or the contract.
24. 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 auditor may consider requesting a letter as described in para 6.4 of GUID 5100 with regard to ensuring authenticity, including its integrity and non-repudiability.
25. 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 auditor may consider carrying out an inquiry on the adequacy of the resolution from a sample of users (where incidents were identified and ticketed by such users).
26. An information security audit may include an 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 information systems operations management.

VI.3 Considerations related to outsourcing arrangements

27. With regard to information security in supplier/ outsourced relationships, the audited entity retains accountability for information security even if the responsibility for certain information systems activities has been outsourced to an external supplier. Further, aspects such as segregation of conflicting duties (e.g. between development, testing and production teams) are significant, whether the development/ implementation/ operations and maintenance of the information system is being done in-house or through an external supplier.

VII. Reporting on an Audit of Information Security

28. 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.
29. Reporting on information security by auditors may consider the potential business impact of exposing technical shortcomings and security risk in public. In such cases, the auditor may use appropriate mechanisms, including redacting sensitive information or through management letters to share details and possible impact of the risk with the audited entity.
30. Besides the regular stakeholders of public sector audits, reporting may consider the specific perspectives of stakeholders like outsourced technical providers of support to the audited entities.

31. The auditor may provide recommendations for improving information security. When developing the recommendations, the auditor may consider any practical implications for the audited entity, including the cost of implementation.

VIII. Follow-up

32. The auditor considers follow-ups in accordance with the compliance audit principles of ISSAI 400.
33. IT systems are constantly evolving. As an example, IT systems are increasingly web-based/ cloud hosted. The auditor may consider such significant changes when deciding on the timing of follow-up audits.
34. When planning a follow-up, the auditor may consider factors such as available technology, costing, and system compatibility that can impact the audited entity's capability to address the audit findings and implement the recommendations.

Annexure: 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 information systems 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.
8	Business continuity and disaster recovery	Whether security aspects related to these processes have been addressed and information security is adequate for disaster recovery transition as well as operation.	Auditors may check whether information security facility is adequate during the disaster recovery process.

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.