Forum for INTOSAI Professional Pronouncements

Agenda for the February 2024 web-meeting of the

Forum for INTOSAI Professional Pronouncements (FIPP)

The agenda is an overview of all agenda-items planned to be discussed during all sessions. Some items will be discussed in several sessions.		
Meeting day **Tuesday 27 February 2024 - 12:00–16:00 CET**		
Agenda Items	**Purpose**	**Output**
Project Proposal / Exposure Draft / Endorsement version submitted from Goal Chair for discussion / appraisal		
Revised Exposure Draft of GUID 5101 on Information Systems Security Audit	To discuss/appraise/approve according to FIPP Working Procedures and drafting conventions	For FIPP to discuss/approve/vote. See Annex 1 The project group is invited to participate at the meeting to present their work.
Project proposal template		
Project proposal template	An initial discussion on possible updates of the project proposal.	An initial FIPP discussion of possible updates to the Project proposal template. Template-Project-Proposal.docx (live.com)
Information from FIPP chair		
FIPP Chair		- FIPP meetings 2024
Information PSC Secretariat		
PSC Secr		- Available funding for FIPP members for Business trips

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.

Project 2.8 of the SDP 2017-2019

EXPLANATORY MEMORANDUM ON THE 2ND EXPOSURE DRAFT

INTOSAI

REQUEST FOR COMMENTS

This Second Exposure Draft of GUID 5101 *Guidance on Audit of Security of Information Systems* was elaborated by the INTOSAI Working Group on IT Audit (WGITA) of the Knowledge Sharing Committee (KSC) under Project 2.8 of the Strategic Development Plan (SDP) 2017-2019 for the IFPP.

Respondents are asked to submit their comments electronically by [INSERT MONTH AND DATE], 2024 to the e-mail addresses: [INSERT E-MAIL ADDRESSES]. Please submit comments to specific paragraphs using the file circulated at the same time as the exposure draft. General comments may be submitted using PDF or Word documents. All comments will be considered a matter of public record and may be posted on the issai.org website.

Kommentert [MRI1]: The usual comment period is 90 days. The deadline will depend on the date of exposure.

The WGITA will consider all comments received when preparing the final version of the textfor submission to the Forum for INTOSAI Professional Pronouncements (FIPP) for approval.

The FIPP has approved this exposure draft on February 27, 2024 (cf. section 2.1 of the due process for the IFPP). The final pronouncement is expected to take effect from [INSERT MONTH DATE, YEAR].

Kommentert [MRI2]: Check whether the date is correct.

Introduction

The transition to computerised information systems and electronic processing of information by public sector entities make it crucial for SAIs to develop appropriate capacity to identify and assess risks related to information systems and respond to these risks. As part of the audit of information systems, there is a need to ensure that controls to maintain confidentiality, integrity, and availability of information (i.e. Information Security) have been implemented by public sector entities and operate effectively.

In the light of the escalating relevance of information security, GUID 5101 is developed to provide SAIs with non-mandatory specific guidance on the audit of security of information systems. The GUID is closely related to GUID 5100 *Guidance on Audit of Information Systems* and offers additional direction without replicating the content of GUID 5100.

The exposure draft for GUID 5101 focuses on compliance audit. The GUID is intended to support auditors in understanding how to apply the relevant ISSAIs for the subject matter of security of information systems. The GUID covers the planning, conducting, reporting and follow-up stages of the audit process.

Background

The SDP 2017-2019 recognised the need for reviewing the pre-existing ISSAI 5310 *Information System Security Review Methodology* and endorsing a new subject matter specific guidance pronouncement (GUID) on the audit of security of information systems. The development of the new GUID was initiated under Project 2.8, which was approved by FIPP in November 2017. The project team was led by the SAI of India.

Accordingly, the content of ISSAI 5310 was reviewed in the light of the latest developments in the field of security of information systems and was revised and consolidated as GUID 5101. The proposed draft was drawn on GUID 5100 *Guidance on Audit of Information Systems.*

The first exposure draft of GUID 5101 was approved by FIPP in November 2018. However, the comments received from the respondents during the exposure period indicated that the GUID should be further elaborated to add value to auditors. FIPP therefore concluded that the document was not yet ready to be endorsed.

FIPP guided and supported the project team in developing the GUID by providing feedback and advice on how key issues related to the content, scope and structure of the pronouncement should be resolved. Emphasis was placed on focusing the GUID on compliance audit and making its content distinct from GUID 5100.

FIPP approved this second exposure draft of GUID 5101 in February 2024, concluding that the proposed pronouncement is of high quality and adds value to the IFPP.

Questions to consider

The inputs of SAIs, INTOSAI bodies and external stakeholders on this Second Exposure Draft are welcome at this stage. Respondents are especially encouraged to consider the following questions:

1) Does this GUID provide useful guidance for your SAI in carrying out a compliance audit of security of information systems?
2) Does the GUID include the necessary definitions related to the audit of security of information systems?

INTOSAI

IFPP

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

I. Introduction

1. ~~GUID 5101 provides the framework for conducting Audit of Security of Information Systems within the IFPP. The framework laid out in this GUID is consistent with the Fundamental Principles of Public Sector Auditing (ISSAI 100) as well as Guidance on Audit of Information Systems (GUID 5100), which provides the overarching framework for conducting Audit of Information Systems.~~
2. ~~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].~~
3. 1. The transition to computerised information systems and electronic processing of information by auditees e-entities in the public sector makes it imperative for SAIs to develop appropriate capacity to ~~conduct a thorough examination of~~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 ~~adopted~~ designed and applied by ~~public sector entities~~auditees.
4. ~~Information Technology has made it possible to capture, store, process, retrieve and deliver information electronically, and the delivery mode of public services is rapidly transitioning from physical to electronic. Such services and data are increasingly provided and made available over the Internet and public networks, and hence face exposure to a wide variety of threats, resulting in the increased importance of cyber security. Further, the distinction between Information Technology (IT) and Operational Technology (OT)[3] is getting blurred, and cyber security of critical infrastructure[4] systems is increasingly focused on OT systems.~~
5. 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. ~~Therefore, it is imperative for SAIs to develop adequate capacity to conduct an examination of information security (including cyber security) either as part of the audit of Information Systems or separately.~~
6. ~~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):~~

~~[1] INTOSAI-P-1: The Lima Declaration~~

~~[2] United Nations General Assembly Resolution A/66/209~~

~~[3] According to NIST SP 800-37, Operational technology (OT) encompasses a broad range of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems.~~

~~[4] Critical infrastructure are essential services and related assets that underpin society and serve as the backbone of the nation's economy, security, and health. (NISTIR 8183)~~

Kommentert [MRI1]: Berri, Chandra: The six objectives
Kommentert [SC2R1]: As discussed in the meeting, the
formaterte
formaterte
formaterte
formaterte
formaterte
Kommentert [MRI3]: Para 1 could be moved to objectives
Kommentert [SC4R3]: Done
Kommentert [MRI5]: Kristoffer: It is very misleading to
Kommentert [SC6R5]: Done
formaterte
formaterte
formaterte
formaterte
formaterte
formaterte
formaterte
Kommentert [MRI7]: Tiago: there is a need for
Kommentert [SC8R7]: The para has been modified belo
Kommentert [MRI9]: Alex: Delete?
Kommentert [SC10R9]: Done
Kommentert [MRI11]: Kristoffer: Item 2-4 in the
Kommentert [SC12R11]: Para 2 and 4 deleted. Para 3
Kommentert [MRI13]: Alex: Note that we use this phra
Kommentert [SC14R13]: Para deleted
Kommentert [MRI15]: Alex: processing of information
Kommentert [SC16R15]: done
formaterte
formaterte
Kommentert [MRI17]: Alex: Do we examine or audit?
Kommentert [SC18R17]: changed
Kommentert [MRI19]: Chandra: 'designed and applied'
Kommentert [SC20R19]: done
Kommentert [MRI21]: Or use "the auditees"
Kommentert [SC22R21]: Changed to auditees through
formaterte
formaterte
Kommentert [MRI23]: Kristoffer: That message to SAI
Kommentert [SC24R23]: Also, this is a duplication from
Kommentert [MRI25]: Use ISSAI 140
Kommentert [SC26R25]: Redundant sentence, deleted
Kommentert [MRI27]: Kristoffer: perhaps better used a
Kommentert [SC28R27]: Moved

(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 vulnerability assessment 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/ updation 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.

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[4]. This GUID covers audit of information security being taken up either as a distinct compliance audit or may be 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[5] of the audit process.

II. III. Definitions

a) **Audit of Information Systems**[6]: 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.

[5] ISSAI 100
[6] GUID 5100 para 3.2

Kommentert [MRI29]: Jane: change to update / updating

Kommentert [SC30R29]: Moved below

Kommentert [MRI31]: Gerhard: restructuring would be useful in particular for the Objectives section to make it clearer

Kommentert [SC32R31]: Edited the section and reworded the objectives. Brought this section before the section on Definitions.
Coverage of the different types of audit has been amended as per discussion.
Part of the discussion moved to scope of audit section.

formaterte: Skrift: 15 pkt

formaterte: Skrift: 15 pkt

formaterte: Skrift: 15 pkt

Kommentert [MRI33]: Jane: "...or as part of a financial audit

Kommentert [SC34R33]: done

Kommentert [MRI35]: Alex: Delete.. We do not have a clear definition

Kommentert [SC36R35]: done

Kommentert [MRI37]: Kristoffer: The list of definitions seems to contain terms that are not used/essential to the text. In addition item 4 is occupied with defining Operational Technology – but it is not used elsewhere, so why is it important?

Toma: Definitions and Objectives sections should be swapped

Should be chapter 3. Objectives should come first. Several relevant definitions missing.

The definitions should be recognized internationally by IT people. The alternative definition is confusing.

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

Kommentert [MRI38]: Monica: may be removed, duplication

Kommentert [SC39R38]: done

~~b)~~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.

~~c)~~ ~~**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, authentication, confidentiality, and nonrepudiation. Alternatively, the process of protecting information and assets by preventing, detecting and responding to cyber-attacks.~~

~~d)~~b) **Integrity**: Guarding against improper information modification or destruction and includes ensuring information non-repudiation[7] and authenticity[8]; 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)~~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.

~~f)~~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.

~~g)~~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.

~~h) **Audit of Security of Information Systems/ Audit of Information Security**: Depending on the type of audit engagement (Financial Audit, Compliance Audit or Performance Audit) and the audit scope, the examination of controls related to security of information and assets, to derive assurance as to the maintenance of confidentiality, integrity, and availability.~~

~~III. Objectives of this GUID~~

~~GUID 5101 provides the framework for conducting Audit of Security of Information Systems within the IFPP. The framework laid out in this GUID is consistent with the Fundamental Principles of Public Sector Auditing (ISSAI 100) as well as Guidance on Audit of Information Systems (GUID 5100), which provides the overarching framework for conducting Audit of Information Systems.~~

~~i) ISSAI 100, 200, 300 and 400 lay down the basic precepts of auditing as related to Compliance Audit, Performance Audit and Financial Audit. These ISSAIs relate to general principles, procedures, standards, and expectations of an auditor. GUID 5100 lays down subject matter specific guidance regarding audit of Information Systems.~~

[7] 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.

[8] 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.

Kommentert [MRI40]: **Monica:** may be removed as it is
Kommentert [SC41R40]: done
Kommentert [MRI42]: **Monica:** Definition 4, 5, and 6 m
Kommentert [SC43R42]: Can be passed on to the proje
Kommentert [AP44R42]: I agree with Monica… as the
Kommentert [MRI45]: **ISACA definition (ITAF):** The
formaterte
formaterte
formaterte
formaterte
formaterte
Kommentert [MRI46]: **Jane:** is non-repudiaton a techni
Kommentert [SC47R46]: Non-repudiation is a technica
formaterte
formaterte
formaterte
formaterte
formaterte
formaterte
Kommentert [MRI48]: **ISACA definition (ITAF):** Preserv
formaterte
formaterte
formaterte
Kommentert [MRI49]: **ISACA Definition (ITAF):**
formaterte
formaterte
Kommentert [MRI50]: **Monica:** may be removed as it is
Kommentert [SC51R50]: ISO 27001 has been mentione
formaterte
formaterte
Kommentert [MRI52]: **Monica:** may be moved to
Kommentert [SC53R52]: It has been covered in the
Kommentert [MRI54]: **Gerhard:** restructuring would be
Kommentert [SC55R54]: Comment addressed above
Kommentert [MRI56]: Para 1 could be moved to
Kommentert [SC57R56]: Done
Kommentert [MRI58]: **Kristoffer:** It is very misleading t
Kommentert [SC59R58]: Redrafted
Kommentert [MRI60]: **Tiago:** there is a need for
Kommentert [MRI61]: **Chandra:** ISSAI numbering and
formaterte
Formatert

j) Audit of information security can be taken as a compliance audit or, in certain circumstances, as a performance audit or financial audit (or as a combined audit). Accordingly, the audit should be carried out as per the applicable principles (ISSAI 200 for financial audit, ISSAI 300 for performance audit and ISSAI 400 for compliance audit).

k) If 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.

l) If audit of information security is taken up as part of a financial audit, the criteria for performing such audit would be the financial reporting framework and the conclusion of the audit would be reflected in the audit opinion, and not as a separate conclusion.

m) If audit of information security is taken up as a performance audit or as part of a performance audit, the audit objectives would be related to assessing whether the interventions etc. forming part of the subject matter are performing in accordance with the principles of economy, efficiency and effectiveness and whether there is room for improvement, and the resulting audit conclusions would also need to be mapped to the principles of economy, efficiency).

n) This GUID focuses on compliance audit of information security.

o) 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). Audit of information security can be taken either as a distinct compliance audit or may be part of a larger compliance audit engagement.

p) The contents of this GUID may be applied by auditors in the Planning, Conducting, Reporting and Follow Up stages9 of the audit process.

IV. Scope of the auditThe 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.

q)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: 2013 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

[9] ISSAI 100

Kommentert [MRI62]: Jane: "...or as part of a financial audit

Kommentert [SC63R62]: Comment addressed above where section is shifted now

Kommentert [MRI64]: Alex: Delete.. We do not have a clear definition

Kommentert [SC65R64]: Comment addressed above where section is shifted now

Kommentert [MRI66]: Toma: "must"/"should" usage not appropriate at most

Kommentert [SC67R66]: This portion deleted above

Kommentert [MRI68]: Toma: Para. 11-14 can be separated in Scope section

Kommentert [SC69R68]: Comment addressed above where section is shifted now

Kommentert [MRI70]: Kristoffer: may be relevant to address risks of material misstatements

Kommentert [SC71R70]: Comment addressed above where section is shifted now

Kommentert [MRI72]: Kristoffer: may be relevant to ...

Kommentert [SC73R72]: Comment addressed above ...

Kommentert [MRI74]: Chandra, Jane: 'and effectiveness' ...

Kommentert [SC75R74]: Comment addressed above ...

Kommentert [MRI76]: Kristoffer: Add that a compliance ...

Kommentert [SC77R76]: Made the changes

Kommentert [MRI78]: Kristoffer: unclear in whether it ...

Kommentert [SC79R78]: Modified as per next comment

formaterte: Skrift: (Standard) Arial, 11 pkt

Kommentert [MRI80]: Toma: Para. 11-14 can be ...

Kommentert [SC81R80]: Moved. Paras on financial and ...

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte ...

Formatert ...

formaterte: Skrift: (Standard) Arial, 11 pkt

Kommentert [MRI82]: Kristoffer: I miss a message that ...

Kommentert [SC83R82]: done

formaterte ...

formaterte: Skrift: (Standard) Arial, 11 pkt

Kommentert [MRI84]: Josie, Monica, Prachi, Tiago: 202 ...

Kommentert [SC85R84]: done

formaterte ...

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

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.

~~r) In general, SAIs are not expected to directly conduct Vulnerability Assessment/ Penetration Testing (VA/PT) of the information systems of the audited entity; 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.~~

~~s) As part of an information security audit, SAIs are not expected to directly conduct risk identification and assessment for the audited entity's IT systems falling within the audit scope; instead, the SAI may review the audited entity's risk management process (including risk identification, assessment and treatment) for its adequacy and effectiveness. As part of such review, the SAI may highlight certain major risks that have not been appropriately identified and adequately assessed or mitigated.~~

~~t) The scope of 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.~~

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, of operational IT systems, especially those which have undergone significant application or infrastructural upgrades;

Kommentert [MRI86]: Jane: I users understand what cryptographic controls are

Kommentert [SC87R86]: It can be explained here, but maybe better to look up on the internet

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

Formatert: Nummerert + Nivå: 1 + Nummereringsstil: 1, 2, 3, … + Start på: 1 + Justering: Venstre + Justert ved: 0,63 cm + Innrykk ved: 1,27 cm

Kommentert [MRI88]: Kristoffer: Para 18 on VA/PT is overlapping with para 32.

Kristoffer: the GUID make too many judgements on what a SAI is expected to or not expected to do.

Kristoffer: item 18-20 should be moved to chapter 4 (or the Chapter 'Conduction….' Is that chapter 6??)

Kommentert [SC89R88]: Para 18, current para 9 has more details than para 32. It can stay as it is. In para 32 there is just a reference.
Wording changed regarding what SAIs are 'expected' to do Moved to Section VI

Kommentert [MRI90]: Alex: I am not really sure about the intention of this paragraph. What the SAI do or not do would depend on the scope of the audit.

Kommentert [SC91R90]: Wording changed. Although this para is to be seen from the context of what the SAI 'can' do. Usually VAPT is too technical for SAI staff and professional coders are required.

Kommentert [MRI92]: Not consistent with para 47, ISSAI 100

Kommentert [SC93R92]: We can refer this comment to the project team

Kommentert [MRI94]: Toma: Redraft so that using more frequently the Auditor (as in GUID 5100) instead of the …

Kommentert [MRI95]: Monica: Para 19 seems to have a …

Kommentert [SC96R95]: As in the previous comment, …

Kommentert [MRI97]: Josie: Para 20 is not exhaustive. …

Kommentert [SC98R97]: This para mentions that BCP a …

Kommentert [MRI99]: Monica: missing confidentiality …

Kommentert [SC100R99]: Project group can add

Kommentert [MRI101]: Alex: Para 21 and 22 do not …

Kommentert [SC102R101]: These are just passing …

formaterte: Skrift: (Standard) Arial, 11 pkt

Kommentert [MRI103]: Kristoffer: perhaps better used …

Kommentert [SC104R103]: Comment addressed above …

formaterte …

Formatert …

(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.

~~V.~~

~~u)~~ SAIs may ~~adopt risk-based audit planning for audits of information security, in line with the processes described in ISSAI 100~~10 ~~as well as GUID 5100, depending upon the objectives of the audit engagement.~~

~~v)~~10. 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

~~w)~~11. 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.

~~x)~~12. 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..

13. 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.

~~y) The choice of frameworks and their adaption as appropriate may depend on the specific SAI and country context (including legal and regulatory requirements, if any) as well as the concerned auditee entity/ entities or sector. Where statutory requirements in respect of information security do not exist or are limited in scope and~~

[10] ~~ISSAI 100 also states that SAIs may also conduct combined audits incorporating financial, performance and/or compliance aspects.~~

Kommentert [MRI105]: Jane: change to update / updating

Kommentert [SC106R105]: done

formaterte: Skrift: (Standard) Arial, 11 pkt

Formatert: Listeavsnitt, Nummerert + Nivå: 1 + Nummereringsstil: 1, 2, 3, … + Start på: 1 + Justering: Venstre + Justert ved: 0,63 cm + Innrykk ved: 1,27 cm

Kommentert [MRI107]: Toma: "may" usage with ISSAI 100 not appropriate

Kommentert [SC108R107]: That is right. But not sure about using shall/should in a GUID!

Kommentert [AP109R107]: Unfortunately we have the same phrase in GUID 5100. so we might keep it?
ISSAI 100 talks about riskassessment in para 47 so there is indirectly a requirement for a risk based audit.
One suggestion would be to delete the para.

Kommentert [D110R107]: I agree with Alex. We can delete the para

Kommentert [SC111R107]: done

formaterte: Skrift: (Standard) Arial, 11 pkt, Utheving

Kommentert [MRI112]: Chandra: check whether reference is appropriate

Kommentert [AP113R112]: Not corredt reference

Kommentert [MRI114]: Kristoffer: crucial question we …

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte …

formaterte: Skrift: (Standard) Arial, 11 pkt

Formatert …

Kommentert [MRI115]: Kristoffer: Para 23-25 – Some …

Kommentert [SC116R115]: The country context is …

formaterte …

formaterte: Skrift: (Standard) Arial, 11 pkt

Kommentert [MRI117]: Monica: General and specific …

Kommentert [SC118R117]: Added

formaterte: Skrift: (Standard) Arial, 11 pkt, Utheving

formaterte …

formaterte: Utheving

formaterte: Skrift: (Standard) Arial, 11 pkt, Utheving

formaterte: Skrift: (Standard) Arial, 11 pkt, Utheving

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

Formatert …

Kommentert [MRI119]: Alex: Which critera we chose - …

Kommentert [SC120R119]: added

~~coverage, the SAI may consider adopting/ adapting international or domestic frameworks as best practices for the audit assignment.~~

V.2 Resources

~~z)~~ ~~SAIs may ensure that the audit team is composed of members that collectively have the competence to conduct information security audit engagements to achieve the intended audit objectives. 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.~~

~~aa)~~14. 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. ~~With regard to information security audits, it may not generally be practicable to establish a dedicated information security audit group in the SAI.xxxx~~

~~bb)~~ ~~Engagement of external resources may be considered by the SAI, depending on the scope of the specific engagement or series of planned information security audit engagements.~~

~~cc)~~ ~~SAIs may ensure that the information security audit teams collectively, in addition to the collective skill sets required for an information systems auditor as mentioned in Para 5.8 of GUID 5100, have the capacity to perform the illustrative list of tasks below (depending on the scope and objectives of the audit engagement):~~

- ~~a. Understand the overall architecture of the IT system (including "technology stack" – i.e. suite of technologies used to create the overall solution), as well as its security architecture, including the major security related components; this understanding is essential before initiating an assessment of controls,~~
- ~~b. Understand the extant laws, rules and regulations, as well as policies and procedures applicable to information security (including data protection and privacy) in the context of the audited entity,~~
- ~~c. Understand the audit methodology, including relevant auditing standards and guidelines applicable to the SAI, as well as the specific information security criteria against which the audit findings are to be compared,~~
- ~~d. Understand the scope and nature of findings reported through third party information security audits.~~

Conducting Information Security Audits

15. SAIs may conduct information security audits in line with the processes described in ISSAIs as well as GUID 5100.
16. The additional guidance will supplement the guidance in GUID 5101.

~~dd)~~1. ~~The additional guidance is offered in respect of conduct of information security aspects.~~

~~ee)~~2. 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.

3. 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

Kommentert [MRI121]: Toma: "may" not consistent with ISSAI 100, 39

Kommentert [SC122R121]: As above

Kommentert [AP123R121]: Delete the paragraph as it does not bring added value.. As discussed at the meeting.

Kommentert [D124R121]: I agree with Alex. The para may be deleted

Kommentert [SC125R121]: done

Formatert: Nummerert + Nivå: 1 + Nummereringsstil: 1, 2, 3, … + Start på: 1 + Justering: Venstre + Justert ved: 0,63 cm + Innrykk ved: 1,27 cm

Kommentert [MRI126]: The first sentence is sufficient. The second sentence is covered in ISSAI 140 and 150.

Kommentert [MRI127]: Does these kinds of comments

Kommentert [AP128R127]: Agree delete.

Kommentert [D129R127]: Agree. Please delete.

Kommentert [SC130R127]: done

formaterte: Skrift: (Standard) Arial, 11 pkt

Kommentert [MRI131]: Alex: Adding value?

Kommentert [AP132R131]: Delet as discssed at the

Kommentert [D133R131]: The para may be deleted

Kommentert [SC134R131]: done

Kommentert [MRI135]: Monica: Paragraph 29 may be

Kommentert [SC136R135]: deleted

Kommentert [MRI137]: should be rephrased

Kommentert [SC138R137]: deleted

Kommentert [MRI139]: This sentence is general. This is

Kommentert [SC140R139]: deleted

Kommentert [MRI141]: Kristoffer: Numbering of

Kommentert [SC142R141]: This GUID is being develop

Kommentert [SC143R141]: The project team would ha

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

Formatert

Kommentert [MRI144]: Gerhard, Toma: para 30 could

Kommentert [SC145R144]: Modified

formaterte: Standardskrift for avsnitt

formaterte: Skrift: (Standard) Arial, 11 pkt

Kommentert [MRI146]: "authenticity" is missing

formaterte: Standardskrift for avsnitt

formaterte: Skrift: (Standard) Arial, 11 pkt

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.

~~ff) 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 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.~~

~~gg)~~4. 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 Tpolicies, 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.

~~hh)~~5. 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.

~~ii)~~6. 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.

~~jj)~~7. 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.

~~kk)~~8. 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 audite~~d entity e~~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.

~~ll)~~9. 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).

~~mm)~~10. 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 & Maintenance of the IT system is being done in-house or through an external supplier.

~~nn)~~11. 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)

formaterte: Skrift: (Standard) Arial, 11 pkt

Formatert: Nummerert + Nivå: 1 + Nummereringsstil: 1, 2, 3, … + Start på: 1 + Justering: Venstre + Justert ved: 0,63 cm + Innrykk ved: 1,27 cm

Kommentert [MRI147]: Monica: contradicts Paragraph 18. It is highly unlikely for an auditor from SAI to have the competence to directly conduct VAPT.

Kommentert [SC148R147]: To be seen in the context of discussion regarding SAI Norway

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

Kommentert [MRI149]: Chandra: Use of appropriate term whether 'para' (para 37 and other places) or 'section' (para 41 and other places)

Kommentert [SC150R149]: In this case it is para

formaterte: Standardskrift for avsnitt

formaterte: Skrift: (Standard) Arial, 11 pkt

Kommentert [MRI151]: Confidentiality as well?

Kommentert [SC152R151]: Reference to GUID 5100 and its contents

formaterte: Standardskrift for avsnitt

formaterte: Skrift: (Standard) Arial, 11 pkt

Kommentert [MRI153]: Jane: should spell out 'O&M'

Kommentert [SC154R153]: done

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Standardskrift for avsnitt

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt, Ikke Kursiv

formaterte: Skrift: (Standard) Arial, 11 pkt

17. The SAI may use the audited entitys 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 .~~third- party~~

18. 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.

Reporting on audit of information security

12. 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.
13. 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.
14. 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.
15. 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.

~~oo) The guidance on 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.~~

~~pp) Reporting on information security by auditors must 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 of exact risk with the audited entity.~~

Follow up

16. Follow up requirements as per ISSAI 400 for Compliance Audits are to be considered
17. 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.

~~qq) 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. In addition to guidance in section 8 of GUID 5100, if significant risks in information security management have been identified through this information security audit engagement, SAIs may consider a follow-up audit to assess whether these risks have been adequately assessed.~~

~~rr) With IT systems increasingly being cloud hosted/ web-based, the time window for risk mitigation, and therefore for conducting a follow up audit, is considerably reduced. The illustrative aspects mentioned in para 6 of this GUID would also be relevant as triggers for a follow up information security audit.~~

formaterte: Skrift: Ikke Fet, Ikke Kursiv

Kommentert [SC155]: Comment received: This para is a bit odd here. It talks about the planning (that is how I read it, at elast) and the other bulletpoints talks about the conduct and performance. Perhaps it could be moved to the Planning sections.

Kommentert [MRI156]: Josie: Para 20 is not exhaustive. Compared to para 17 more should be assessed other than BCP & DRP.

Kommentert [SC157R156]: This para mentions that BCP and DRP can be included in an IS Audit. It does not precludes the other issues

Kommentert [MRI158]: Monica: missing confidentiality and integrity

Kommentert [SC159R158]: Business continuity and disaster recovery has been mentioned in the specific context of availability

formaterte: Skrift: (Standard) Arial, 11 pkt

Kommentert [MRI160]: The GUID does not provide guidance regarding evaluating audit evidence and forming conclusions (ref. para 58, ISSAI 400)

Tiago: the ED could benefit from a more explicit consideration of the risks associated with conducting an information security audit. This is a significant aspect of the audit process that is currently not addressed in the ED

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

Formatert: Nummerert + Nivå: 1 + Nummereringsstil: 1, 2, 3, … + Start på: 1 + Justering: Venstre + Justert ved: 0,63 cm + Innrykk ved: 1,27 cm

Kommentert [MRI161]: Chandra: Use of appropriate term whether 'para' (para 37 and other places) or 'section' (para 41 and other places)

Kommentert [SC162R161]: Section here

Kommentert [MRI163]: Gerhard, Monica: the para cou…

Kommentert [SC164R163]: Added reference to …

Kommentert [MRI165]: Chandra, Jane, Toma: the term…

Kommentert [SC166R165]: done

Kommentert [MRI167]: Monica: the para should includ…

Formatert …

Kommentert [MRI168]: Toma: Para.43 – not clear for n…

Kommentert [SC169R168]: done

Kommentert [MRI170]: According to para 60 of ISSAI 4…

Kommentert [MRI171]: "addressed"?

Kommentert [MRI172]: Monica: para 44 is not clear

Kommentert [SC173R172]: modified

Annexure A: Illustrative factors affecting information security

~~Annexure: A~~

formaterte: Skrift: (Standard) Arial, 11 pkt

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~~matrix~~

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 objectives 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

Kommentert [MRI174]: Kristoffer: Annexure B – Seems to have lost the focus on compliance audit. Compliance with 'statutory requirements' is stated as one out of a large number of suggested objectives. A suggestion for 'a quick fix' could be to state up front in the annex that 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.

Prachi: Annexure B will need to be synchronized with its reference in the draft since it refers to factors affecting information security, while the draft refers to triggers for an audit of information security

Kommentert [SC175R174]: Done; triggers are in Annexure A

Kommentert [MRI176]: Chandra: the term 'matrix' to be changed to 'questions

Kommentert [SC177R176]: done

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

			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.

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt

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.

formaterte: Skrift: (Standard) Arial, 11 pkt

formaterte: Skrift: (Standard) Arial, 11 pkt