# Agenda for the June 2024 web-meetings 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**<br>**Tuesday 18 June 2024 - 13:00–17:00 CEST**<br>**Tuesday 25 June 2024 - 13:00–17:00 CEST** | | |
| **Agenda Items** | **Purpose** | **Output** |
| **Project Proposal / Exposure Draft / Endorsement version submitted from Goal Chair for discussion / appraisal** | | |
| Endorsement version GUID 5101 *Guidance on Audit of Security of Information Systems* | To discuss/appraise/approve according to FIPP Working Procedures and drafting conventions | For FIPP to discuss/appraise/approve. See Annex 1 |
| **Project proposal template** | | |
| Project proposal template | Continued discussion on possible format for the updated SDP project proposal template.<br><br>Based on the homework from May where FIPP members were invited to give input on possible adjustments to the Project Proposal template | To discuss adjustments in the project proposal template for better guidance to the projects in the SDP 2023-2028 both in direction for the project groups, the responsible Goal Chairs, and the communication to the INTOSAI community (No documents for this agenda item. Summary of the homework will be presented in the meeting) |
| **Preparation for the work on the SDP** | | |
| Future format of the ISSAIs | Follow up on the discussion from the previous FIPP meeting | To prepare for the tasks ahead under SDP 2023-2028 |
| **Information from FIPP chair** | | |
| FIPP Chair | Information | - Invitation is sent by the PSC Secr to the INTOSAI community for participation in the SDP projects<br>- FIPP meetings second half of 2024 |
| **Information PSC Secretariat** | | |
| PSC Secr | Information from the PSC Secr | - More information on the PSC SC agenda 26 June 2024 |

# 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 aspects. 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 are outlined in GUID 5100. The objective of this GUID is to provide specific and additional guidance for the 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, Conduct, Reporting and Follow Up stages of the audit process. The GUID lists elements of scope of audit work, 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, authentication, confidentiality, and nonrepudiation.

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-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.

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 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 shall assess compliance of the subject matter (information security or any specific aspect/ component thereof) to 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. Elements of such scope of the work could be usefully derived from applicable 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 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.

# 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:

(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 have 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 and 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 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 assess the auditee's risk management process (including risk identification, assessment and treatment) as part of 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 information systems audits.

## V.1 Sources of audit criteria

12. Appropriate nationally/ internationally accepted information security frameworks serve as sources for audit criteria. SAIs may find it useful to identify and adapt such frameworks for information security audits and to define the audit objectives and scope of such audits.
13. These frameworks 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. The framework an SAI chooses 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 information systems 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. The audit procedures for an information security audit will be designed with a view to focus on the objectives 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.
17. 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, and agreement with the audited entity for such intrusive testing will have to be made, including legal safeguards and indemnifications where necessary.
18. SAIs may or may not conduct 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.
19. The adequacy of standards, guidelines and procedures designed to operationalize information security policy and policies for incident/ problem reporting and management is verified in audit.
20. The auditor shall examine availability of relevant policies, procedures etc and whether these are being reviewed at appropriate intervals of time and updated, as necessary while evaluating the organizational roles. The auditor shall also assess whether there is adequate awareness and understanding amongst users, including the information security culture.
21. The audit of the risk management process will 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 will 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 will 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 considerations spelt out in para 6.4 of GUID 5100 with regard to ensuring its authenticity, integrity and non-repudiability may be ensured.
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 audit team 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. 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.
27. 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.
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 information systems operations management.
    (Illustrative high level audit questions mentioned in Annexure)

## 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 appropriate mechanisms, including redacting sensitive information or through management letters to share 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 audited entities.
32. Recommendations may be developed after considering the available technical solutions for improving the information security and its practical implications for the business of the audited entity along with a cost benefit analysis, as assessed by the audited entity.

## 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: 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.<br>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.<br>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. |

# ~~Revised Draft~~ INTOSAI GUID 5101 – Guidance on Audit of Information ~~security~~Security
## (Draft Endorsement Version)

## I. Introduction

1. GUID 5101 supplements GUID 5100 by providing guidance on audit of information security aspects. 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).

~~1.~~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~~information systems, there is a need to ensure that controls to maintain confidentiality, integrity and availability of ~~Information Systems~~information systems and data (i.e. ~~Information Security~~information security) have been designed and applied by auditees.

~~2.~~3. Information security ~~weaknesses~~breaches may lead to severe ~~damage (~~legal, reputational/ credibility, financial, productivity~~.~~ damage, and exposure to further intrusions~~). Such damage~~. Security breaches may be caused by ~~security breaches, unauthorised external connections,~~weaknesses and vulnerabilities that lead to accidental exposure ~~of information (~~, or disclosure of ~~corporate assets and sensitive~~ information to unauthorised parties~~), insider threats or system vulnerabilities~~, loss of availability or unauthorised changes in systems and data.

## II. Objectives of this GUID

~~3.1.~~ ~~This GUID supplements GUID 5100 by providing~~The 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) as well as with the Compliance Audit Principles (ISSAI 400).~~

4. ~~While the overall principles and guidance outlined in GUID 5100 are~~ applicable to audit of ~~security of~~ information systems~~, the~~ are outlined in GUID 5100. 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~~combined audit ~~or as part of a~~incorporating financial ~~audit~~, compliance and/or performance aspects. This GUID covers audit of information security being taken up either as a distinct compliance audit or as ~~a~~part of a ~~larger compliance~~combined audit engagement to see whether the IT management meets the necessary standards and requirements for ~~IT~~information security.
6. The contents of this GUID may be applied by auditors in the Planning, ~~Conducting~~Conduct, Reporting and Follow Up stages of the audit process. The GUID lists elements of scope of audit work, factors affecting information security, sources of audit criteria and high level audit questions. These lists are illustrative and not exhaustive.



formaterte: Skrift: 14 pkt
formaterte: Skrift: 14 pkt
formaterte: Standardskrift for avsnitt, Skrift: +Brødtekst (Calibri), 12 pkt

## III. Definitions

a) **Information Security**: Protection of ~~Information~~information and ~~Information Systems~~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, authentication, confidentiality, and nonrepudiation.

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.

~~b)~~d) **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 information; alternatively, protection of sensitive information from unauthorized disclosure. A loss of confidentiality is the unauthorized disclosure of information.~~

~~d)~~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.

~~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.~~

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 is an authorized simulated hacking or attack on a computer system, performed to evaluate the security of the system.

## IV. The Subject Matter

7. ~~When~~In audit of information security ~~is taken up as a~~, the auditor shall assess compliance ~~audit, the compliance in respect~~ of the subject matter (information security or any specific aspect/ component thereof) to ~~the~~ applicable authorities (laws, regulations, policy, procedure, standards, practices etc~~.) is assessed by auditors.~~).

[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.

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~~applicable 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 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;
    ~~c.~~d. Human resources security at different stages from prior to employment, during employment and post-employment
    ~~d.~~e. Management and control of information assets, including inventory and classification; rules for acceptable use; transportation, return and disposal
    ~~e.~~f. Authentication, authorization and access control – including identify management and authentication, cryptographic controls, and authorization and access controls;
    ~~f.~~g. Physical and environmental security;
    ~~g.~~h. Network and communication security and cyber security management;
    ~~h.~~i. Information security incident management and security testing and monitoring;
    ~~i.~~j. Security as part of system acquisition and development;
    ~~j.~~k. 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~~audit of ~~Information Security~~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~~information System or ~~replacement/ upgradation of~~ an existing ~~IT System~~information system has been replaced or upgraded (application and/or infrastructure) by the audited entity, especially in a critical business area;

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

(c) ~~non-conduct of~~ periodic internal/ external security testing have not been conducted, including and security testing of operational ~~IT~~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 ~~IT~~information system, or where a security incident or breach has adversely impacted similarly placed ~~IT~~information systems in other audited entities;

formaterte: Skrift: +Brødtekst (Calibri)

formaterte: Skrift: +Brødtekst (Calibri)

(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~~assess the auditee's risk management process (including risk identification, assessment and treatment) as ~~a basis for~~ apart of 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~~information systems 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,~~Appropriate nationally/ internationally accepted information security frameworks ~~for audit risk assessment (to prioritize~~ serve as sources for audit criteria. SAIs may find it useful to identify and adapt such frameworks for information security audits and to define the audit objectives and scope~~) and for detailed audit planning of information security audits. Such frameworks serve as sources for audit criteria~~ of such audits.
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~~The framework ~~the~~an SAI ~~choose~~chooses 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.

Formatert: Innrykk: Venstre: 1,62 cm

### V.2 Resources

15. The considerations for allocating human resources for ~~IS~~information systems 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 Guidance on Audit of Information Systems. The additional guidance will supplement the guidance in GUID 5100.~~

~~17.~~16. The audit procedures for an information security audit will be designed with a view to ~~focusing~~focus on the objectives ~~of deriving assurance as to~~to assess (a) confidentiality (b) integrity – including non-repudiability and (c) availability ~~with regard to~~of data and IT systems falling within the scope of the audit engagement.

~~18.~~17. 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~~with 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~~, including legal safeguards 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.~~indemnifications where necessary.

18. ~~The scope~~SAIs may or may not conduct VA/PT of ~~most~~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 ~~generally include the information security culture, policies,~~ 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.

19. The adequacy of standards, guidelines and procedures~~, organizational roles etc. For these aspects, the audit team should specifically look at not only the~~ designed to operationalize information security policy and policies for incident/ problem reporting and management is verified in audit.

~~19.~~20. The auditor shall examine availability of relevant policies, procedures etc~~, but also whether there is adequate awareness and understanding amongst users and also~~ and whether these are being reviewed at appropriate intervals of time and updated, as necessary~~.~~ while evaluating the organizational roles. The auditor shall also assess whether there is adequate awareness and understanding amongst users, including the information security culture.

~~20.~~21. The audit of 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~~ include examining 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.~~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 will include examining whether the policies are understood by users and whether such policies are implemented effectively.

~~22.~~23. ~~Wherever~~Audit procedures on authentication, authorization and access controls ~~are covered within the scope of the audit engagement, a key aspect that would be looked at is~~will 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.

23.24. 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 considerations spelt out in para 6.4 of GUID 5100 with regard to ensuring its authenticity, integrity and non-repudiability may be ensured.

24.25. 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 audit team may consider ~~obtaining feedback~~carrying out an inquiry on the adequacy of the resolution from a sample of users (where incidents were identified and ticketed by such users).

25.26. With regard to information security in supplier/ outsourced relationships, the audited entity retains accountability for information security even if the responsibility for certain ~~IS~~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) ~~matter equally~~are significant, whether the development/ implementation/ ~~Operations~~operations and ~~Maintenance~~maintenance of the ~~IT~~information system is being done in-house or through an external supplier.

26.27. 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~~information systems operations management.
(Illustrative high level audit questions mentioned in Annexure)

## 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 appropriate mechanisms, including redacting sensitive information or through 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~~audited entities.

32. Recommendations may ~~not~~ be ~~limited to presenting~~developed after considering the available technical solutions for improving the information security ~~but may also consider the~~and its practical implications for the business of the ~~auditee~~audited entity along with a cost benefit analysis~~.~~, as assessed by the audited entity.

## 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: Suggested High Level Audit Questions

### ~~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~~annexure contains high level audit questions on the subject matter of ~~Audit~~audit of ~~Information Security~~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~~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~~security organization structure | Whether such a governance structure has been made clearly responsible for ~~Information Security~~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~~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~~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~~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.<br>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~~8 | ~~Statutory Compliance~~Business continuity and disaster recovery | Whether ~~statutory requirements~~ security aspects related to these processes have been addressed and | Auditors may check whether information security facility is adequate during the disaster recovery process.~~Checks for compliance to statutory and~~ |

Formatert: Linjeavstand: Flere 1,08 li

| | | | |
|---|---|---|---|
| | | information security ~~aspects have been complied with~~is adequate for disaster recovery transition as well as operation. | ~~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~~9 | ~~Business Continuity and Disaster Recovery~~Statutory compliance | Whether ~~security aspects~~ statutory requirements related to ~~these processes have been addressed and~~ information security ~~is adequate for DR transition as well as operation~~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.~~Auditors may check whether information security facility is adequate during the disaster recovery process.~~ |

Formatert tabell

Algemene Rekenkamer

| | |
|---|---|
| **van** | IT-audit cluster: Sabah Al-Moula, Christiaan Luteijn, Ruud Wissenburg |
| **datum** | 08-05-2024 |
| **aan** | INTOSAI (Professional Standards Committee) |
| **betreft** | Comments Second Exposure Draft of GUID 5101 |

The Netherlands Court of Audit (NCA) received a request for comments from INTOSAI on the Second Exposure Draft of GUID 5101 Guidance on Audit of Security of Information Systems. This memo contains the response from the IT audit cluster of the NCA. We first address the 2 specific questions in the request. We then provide a response for each section of the draft document.

**Kommentert [PT1]:** No action required

**1 Does this GUID provide useful guidance for your SAI in carrying out a compliance audit of security of information systems?**

We think this is a useful document for auditors less familiar with audits in the information security subfield. Overall, we think the document succeeds in getting auditors started without going into too much detail. In some places we would expect a little more or a little less level of detail, see our comments in paragraph 3.

**Kommentert [PT2]:** No action required

We also note that the document can be positioned more clearly as a *supplement* to GUID 5100. Readers may otherwise be under the impression that this is an independently readable guidance, while the document provides additions, specific points of interest and examples that are useful in information security compliance audits. We also make suggestions for this in our commentary in paragraph 3.

**Kommentert [PT3]:** Dealt with in para 3

A third general observation is that the guidance could further emphasize that trends and technologies in information security are evolving extremely rapidly. Think of resilience of encryption against quantum computing or ever-changing modus operandi of cyber criminals. The document can point this out in several places, for example under "IV - The subject matter". In addition, we suggest that the document be reviewed and updated more frequently than other guidances.

**Kommentert [PT4]:** The GUID has been drafted to provide guidance without being technology/IT system specific. Therefore, the document may not require frequent review. However, if there are any major changes in the overall technology ecosystem, it may require review.
No changes are required in the current GUID

NOTITIE

Algemene Rekenkamer

## 2 Are all definitions needed to understand and use this GUID included?

We believe that the definitions included in Section III are sufficient to understand GUID. Explanations of technical terms that the reader may not be familiar with can be easily identified on the internet by anyone.

**Kommentert [PT5]:** No action required

## 3 Comments per section

In the following sub-paragraphs of this memo, we make suggestions for further improvement for each section of the draft.

### 3.1 I – Introduction

1. Align this paragraph with GUID 5100 and use the introduction to position the document. The relationship to other GUIDs is currently covered in paragraph II. It is more clear to the reader if this is done in Section I. The points now included about the relevance of information security can then be mentioned last.
2. Explicitly state that the document has the same structure as the GUID 5100.

**Kommentert [PT6]:** Para 3 from Section II moved to Para 1 in Section I. The structure of the GUID now aligns with GUID 5100

**Kommentert [PT7]:** Since it has been explicitly stated that this GUID is a supplement to GUID 5100, stating that it has the same structure may be redundant. Therefore, no change made to the GUID

### 3.2 II - Objectives of this GUID

3. Make clear in this section that the document provides examples and specific points of interest, but does not claim to be complete.

**Kommentert [PT8]:** A clarification has been added in para 6 of Section II

### 3.3 III – Definitions

No remarks.

### 3.4 IV - The subject matter

4. The first sentence of paragraph 8 (“The information security audit work will be determined by the objectives and scope of the audit.”) seems redundant to us: after all, this applies to any audit.
5. Under item 8b we would add “risk acceptance thresholds” after “acceptance criteria”.
6. Under item 8b we would add after item III as item IV: “Evaluation of the Information security risk management processes”.
7. From item 8 a reference can be made to item 20.

**Kommentert [PT9]:** The sentence provides a context to the elements of scope elaborated subsequently in the paragraph. Therefore, the sentence is not redundant & is proposed to be retained.
Therefore, no change made to the GUID

**Kommentert [PT10]:** Para 8b amended to include risk acceptance thresholds

**Kommentert [PT11]:** Evaluation of risk management has been added to item III that is on review & continual improvement

**Kommentert [PT12]:** Item 20 has been redrafted. So no reference to item 8 required.

Algemene Rekenkamer

### 3.5 V - Planning audit of Information Security

8. Under item 9, we would mention "new or amended laws and regulations."
9. The consequences of disclosure of confidential findings and vulnerabilities is an aspect of information security audits to consider. Paragraph 29 of the draft already addresses this regarding the publication of results. We miss another comment on the requirements for the audit team in this regard: SAI investigators may have to deal with state confidential information in their audits. This requires explicit SAI considerations about screening of auditors by competent authority, such as national security agencies.

### 3.6 VI - Conducting Information Security Audits

10. In this section several things get mixed up, at different levels of abstraction. We think this section could be better structured, possibly with some subheadings.
    a. 17 contains an enumeration of quality aspects,
    b. 18 and 26 deal with sources of evidence
    c. 19 to 24 and 28 are about audit objects: sometimes referred to an audit object, such as culture/organization (19), risk management (20) and asset management (21) and sometimes to a specific control for an audit object, such as 2FA in IAM (22) and authenticity, integrity and non-repudiation of logging (23).
    d. 25 deals with responsibilities in outscourcing.
    e. 27 deals with reliance on third-party audits.
11. We suggest to dedicate item 18 only to vulnerability audits and pen testing (VA/PT): after all, that is a specific method to information security audits while the other data collection methods are generic. Regarding VA/PT, we miss some handles to get readers started. We suggest at least going deeper into the "arrangements and agreements" by pointing out the legal safeguards and indemnifications: VA/PT sometimes require activities that are illegal and VA/PT can also impose risks to the auditee, such as loss of data.
12. The items naming the audit objects, such as 20 and 21, seems more appropriate for Section IV (The subject matter).

### 3.7 VII - Reporting on audit of information security

No remarks.

**Kommentert [PT13]:** When new or amended laws/regulations are brought it, the IT system & organisation policies are appropriately changed. (If the entity has not made changes to the system/policies in aligning with the legal/regulatory amendments, such issue will not be under the scope of an Information Security audit). Therefore, this need is covered in item 9(a) – "development of new IT system or replacement/upgradation of an existing IT system" and item 9(g) significant changes in organisation policies & structures for IS management & implementation. Therefore, no changes made to the GUID

**Kommentert [PT14]:** Confidentiality is a fundamental value of the Auditor. It is applicable for every engagement & there need not be any requirement for screening the Auditor. Further, Audit of information security may not involve dealing with state confidential information (beyond the scope of a regular audit of information systems). Sensitivity to reporting any security weakness has already been covered in Para 29. Therefore, no change made to the GUID

**Kommentert [PT15]:** Paragraphs in the section have been redrafted & re-sequenced for clarity. All paras deal with conducting IS audit

**Kommentert [PT16]:** The concerned paras relating to VA/PT have been redrafted

NOTITIE

Algemene Rekenkamer

### 3.8 VIII - Follow up

13. In our view, item 34 should (also) be mentioned under item 9: “The need for an Audit of Information Security...”.

**Kommentert [PT17]:** Item 9 and Annex A includes illustrative lists of triggers that may necessitate an Information Security audit. Dynamic nature of IT sytems pointed out in Item 34 is already part of the lists, like point 9 (a), (b) & (g).
Therefore, no changes made to GUID

### 3.9 Annexure A

14. The enumeration may inspire SAIs but also seems somewhat arbitrary. One can think of many other factors that affect information security such as organizational culture, vulnerability management, change management, behavioural aspects, awareness training, SOC/SIEM et cetera. As far as we are concerned, the annexure is not really necessary.

**Kommentert [PT18]:** Annexure A has been deleted. The elements have been incorporated in the GUID

### 3.10 Annexure B

15. We wondered if this annexure is based on a model, standard or other guidance. If so, this can be referenced.

**Kommentert [PT19]:** It is not based on models, but includes all domains relating to information security. Therefore, no change made to GUID

16. It would be nice if this table could be mapped to the domains described in item 8 in Section IV (“The Subject Matter”).

**Kommentert [PT20]:** Para 8 items have been covered in the Annexure. A few changes have been made in the sequence to map the two

17. 'Whether the organization promotes a culture...' does not really fit under 'Information Security organization structure'. We would make a separate section 'Organization culture' for this (in line with the domains in item 8).

**Kommentert [PT21]:** Security culture has been dealt along with organisation structure in item 8 as well. Therefore, no change made to GUID

18. Number 8 seems to be missing from the table.

**Kommentert [PT22]:** Necessary correction has been carried out in the GUID

**0 – 0 – 0**

NOTITIE

# 1 Answer to the questions

## 1.1 Does this GUID provide useful guidance for your SAI in carrying out a compliance audit of security and information systems?

The GUID is not precise enough in terms of understanding the subject matter and complying with the ISSAI framework. The GUID is very focused on "checklist" auditing and does not cover how to audit security and information systems based on risk and materiality.

The wording in some of the paragraphs is a bit ambiguous and difficult to understand. Simplifying the language is advisable for the GUID to provide useful guidance for everyone to understand.

## 1.2 Are all definitions needed to understand and use this GUID included?

The GUID uses IT security and information security interchangeably. Cyber security is also mentioned but not defined. Information security is the only one of these three terms that is defined. If they are all to be used in the GUID, they should all be included in the definitions paragraph with an explanation of what the differences between them are.

# 2 Overall comments

Our understanding is that the GUID will give additional guidance on how to conduct a compliance audit when the subject matter is on information security. ISSAI 400 contains the principles in compliance auditing. ISSAI 4000 is the compliance audit standard containing all the requirements you must follow to be ISSAI compliant, and the standard gives you all the steps in a compliance audit.

After assessing GUID 5101, we do not find that this GUID give us additional guidance to conduct a compliance audit when the subject matter is information security. In addition, we recommend you to look at ISSAI 4000 and GUID 4900 and align the GUID after compliance audit terminology.

The first step in an audit, is that the auditor identifies **areas** that are **significant for the intended user (ISSAI 4000/64).** What is specific when it comes to information security? Are there areas with potential risk of non-compliance that are significant for the intended user?

When identifying the **intended user and responsible party** (ISSAI 400/35 and ISSAI 4000/101) is there anything particular to take into consideration when it comes to information Security?

**Subject matter** – The subject matter shall be measured or evaluated against criteria (ISSAI 400/31 and ISSAI 4000/107). Please identify audit criteria in a different paragraph than the paragraph about the subject matter. These are two different elements in an audit. Despite this we will not recommend using ISO/IEC 27001. Not all SAIs use this as source for audit criteria because it is not mandatory for public sector entities to comply with this standard in many countries.

**Audit criteria** –Applicable authorities are laws and regulations, not only policy, procedures, standard and practises. Look at ISSAI 400, ISSAI 4000 and GUID 4900 for more information about audit criteria.
**Type of engagement** – is this guidance for direct reporting engagement (ISSAI 100/29, ISSAI 400/15 and ISSAI 4000/37-42)?
**Type of assurance** – is this guidance for audit with reasonable assurance or limited assurance (ISSAI 400/41 and ISSAI 4000/33 - 36)?
There are **general principles (ISSAI 400)** and **requirements (ISSAI 4000)** of compliance audit such as objectivity and ethics, audit risks, risk of fraud, professional judgment and scepticism, quality control, documentation, and communication. We recommend you to discuss these principles and requirements and consider if there is anything special to highlight for the IT-security area.

**Kommentert [PT1]:** Cyber security has also been included in the definitions. Any reference to IT security in the GUID has been removed, as it only a component of information security

**Kommentert [PT2]:** Changes have been made in the GUID to align terminology

**Kommentert [PT3]:** These have been covered in Section V.
Therefore, no change made to GUID

**Kommentert [PT4]:** GUID 5101 provides additional guidance. There is no additional information on intended user(s) & responsible party required for Information Security audit.
Therefore, no change made to GUID

**Kommentert [PT5]:** The section is on compliance of subject matter to applicable authorities. Identifying criteria in the section ensures clarity on the issue. It is also in sync with ISSAI 4000/107
Therefore, no change made to GUID

**Kommentert [PT6]:** The references also clarifies that these are to be used only where applicable.
Therefore, no change made to GUID

**Kommentert [PT7]:** Paras 7 & 8 modified

**Kommentert [PT8]:** GUID 5101 intends to provide additional guidance. Where there are no differences from the principles & standards, no mention has been made in the GUID. References have been made to areas like audit risks, documentation, communication etc where additional guidance was required.
Therefore, no change made to GUID

In the chapter about the audit process, we recommended you highlight the methods and techniques that are used in this type of audit, because it differs from other compliance audits. The methods and techniques depend on the audit objectives and the audit questions.

**Kommentert [PT9]:** Methods & techniques have been mentioned in para 18 and in other paras in Section VI. Therefore, no change made to GUID

# 3 Comments to specific paragraphs

| | |
|---|---|
| I - Introduction | |
| 1 | This paragraph is copied from GUID 5100 – it should be rewritten to be more relevant for Information Security Audits. Sentence no 2 is unclear – is the GUID saying that if you conduct an IS audit you also need to include information security in that audit? |
| 2 | Suggested phrasing: 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 by insiders, loss of availability or unauthorised changes in systems and data due to cyber-attacks. |
| II – Objective of the GUID | |
| 3 | The reference to ISSAI 4000 is missing. If a SAI uses ISSAI 4000 as their authoritative standard, there are requirements and not only principles the SAI must follow to be ISSAI compliant.IT-security aspects – it is better to use information security to avoid inconsistencies. See also comment under question 2. |
| 4 | Repetition of paragraph 3 – delete or merge |
| 5 | This paragraph is confusing. Just refer to ISSAI 400, paragraph 20 which states the three different perspectives of compliance audit. |
| 6 | Ok, however a bit redundant. |
| III - Definitions | |
| a) | Ok, but should probably also include definitions for cyber security and IT security if these terms are to be used throughout the GUID. |
| b) | Ok |
| c) | Ok |
| d) | Ok |
| d) | Ok |
| e) | Ok |
| IV - The Subject Matter | This section should be under Planning an audit of Information Security – after sources of criteria and risk assessment. |

**Kommentert [PT10]:** The paragraph is specific to information security.
Therefore, no change made to GUID

**Kommentert [PT11]:** The sentence states that there is a need to ensure controls. Where there is a risk of lack of such controls, audit of information security may be needed.
Therefore, no change made to GUID

**Kommentert [PT12]:** The paragraph has been redrafted

**Kommentert [PT13]:** SAIs may have their own standards. ISSAI 400 covers the requirements

**Kommentert [PT14]:** Retained because para 3 has been moved to introduction.
Therefore, no change made to GUID

**Kommentert [PT15]:** The paragraph has been redrafted in sync with ISSAI 400/9

**Kommentert [PT16]:** Cyber security has been defined.

**Kommentert [PT17]:** The GUID follows the structure of ISSAI 4000, with subject matter & scope (ISSAI 4000/43-44) followed by the planning process (Chapter 6 of ISSAI 4000)
Therefore, no change made to GUID

| | |
|---|---|
| 7 | Difficult sentence to understand. Suggest rephrasing. Please look at subject matter and audit criteria in the email. |
| 8 | Again, difficult to understand. Suggest rephrasing to make the point clear. The subject matter should always be determined by risk and materiality. The audit objective and audit questions are key to the scope. Further, audit questions contain audit criteria and are a concretisation of the audit objective. The list of elements may be counterproductive and seen as exhaustive. If examples of subject matters are needed, we suggest that they are moved to the annexure. We are also unsure about the use of ISO/IEC 27001. Not all countries use this as a source of audit criteria. |
| V – Planning audit of Information Security | |
| 9 | Is this the overall risk assessment to determine risk and materiality of the audit, or is this risk assessment when determining criteria and scope? The list of examples: revise language and consider moving to annexure. |
| 10 | Should this have been 9 h)? Would we normally recommend that auditors use the risk assessment done by the auditee instead of performing both an overall risk assessment and a more detailed risk assessment when criteria are deduced? Normally, the entity's own risk assessment is part of knowing the entity. |
| 11 | This paragraph is a bit vague and could be explained in more detail. Why is information security important? What is the importance of the information values that the auditee has? |
| 12 | Long and complicated sentence. As it is now, it does not make sense. Should not the GUID give guidance on how to deduce objective and scope from criteria? And not standards for audit risk assessment and planning of audits. We already have standards for this – the ISSAI framework. |
| 13 | There is some confusion here on what is audit standard and what is criteria. Audit standards govern the auditors' work, i.e. the ISSAI framework – in this context ISSAI 400 and 4000. Audit criteria are laws, regulations, standards etc. that the auditees are obliged to adhere to and to which the auditor benchmark the audit findings. This is not clear in these paragraphs. Consider revising. |
| 14 | This paragraph should be the first under planning and should focus on laws and regulations as authorities to draw criteria from. |
| 15 | |
| VI – Conducting IT Security Audits | |
| 16 | Repetitive. This is covered in the introduction. |
| 17 | Content ok but very verbose – simplify the language to make the point clear. |
| 18 | Move definitions of Pen testing and vuln assessment to definitions section. Remove the example (e.g. relating to audit logs of various types) as it is not necessary. |
| | It is important to remember that the methods and techniques which are used depend on the audit objectives and the audit questions. |
| 19 | The scope of the audit should be covered under planning. |
| 20 | These are all pertaining to the scope of the audit, which is determined in the planning of the audit. The scope of the audit and specific audit procedures are usually risk-based; hence the auditor should determine what to focus on during the audit based on risk. This is too detailed and suggestive. It presents as an audit program. Examples should be moved to annexure to emphasise that they are only examples and not mandatory audit procedures |
| 21 | |
| 22 | |
| 23 | |
| 24 | |
| 25 | |

**Kommentert [PT18]:** Sentence has been rephrased

**Kommentert [PT19]:** It is clarified that the list is illustrative. ISO has been referred only where it is applicable. The sentence has been redrafted to provide clarity.

**Kommentert [PT20]:** It is clarified in the GUID that it is illustrative. Moving it to annexure may reduce readability

**Kommentert [PT21]:** The para has been redrafted for clarity

**Kommentert [PT22]:** The para is structured on GUID 5100. It further adds that materiality considerations specific to information system as provided in GUID 5100 would apply.
Therefore, no change made to the GUID

**Kommentert [PT23]:** The paragraph has been redrafted

**Kommentert [PT24]:** The word 'standards' in the para refers to information security standards & not audit standards. The word has been removed to avoid confusion.

**Kommentert [PT25]:** Section V.1 is on source of criteria. The structure of the sections is that it identifies international information security frameworks/standards in the initial part. It then provides guidance to SAIs on choosing the appropriate framework.
Therefore, no change made to the GUID

**Kommentert [PT26]:** The para has been deleted

**Kommentert [PT27]:** The para has been redrafted

**Kommentert [PT28]:** PA/VT has been moved to definition. The example quoted improves clarity. So it has been retained.

**Kommentert [PT29]:** The para has been redrafted

**Kommentert [PT30]:** The para has been redrafted. Providing examples in the GUID improves readability. ISSAI 4000 also includes several examples which provides clarity to the reader

| | |
|---|---|
| 26 | |
| 27 | |
| 28 | |
| VII – Reporting on audit of IT security | |
| 29 | Include ISSAI 4000 |
| 30 | There are other alternatives to management letters. For example, some SAIs has the mandate to redact sensitive information. Consider rephrasing to include other alternatives. |
| 31 | Again, language is a bit difficult. Please use clear language to make the GUID more user friendly. |
| 32 | What is meant by technical solutions here? This sentence is difficult to understand. Should the auditor assess technical solutions and conduct a cost-benefit analysis, or should the entity do this? |
| VIII Follow up | |
| 33 | The need to comply with ISSAI 400 is already covered. Remember also that there are “principles” in ISSAI 400. In ISSAI 4000 there are “requirements”. |
| 34 | What does this paragraph mean? Usually, the SAI will have one follow-up of a compliance audit. The extent and scope of the follow-up is determined based on the risk that the auditee has not complied with the recommendations and has not mitigated risks and vulnerabilities. If the audit is carried out on a regular basis, the follow-up is done in the next cycle. |
| 35 | |
| Annexure A | |
| | We don’t understand the point of this annexure. |
| Annexure B | |
| | We don’t understand the point of this annexure. It is already stated earlier that ISO 270001/2 is the basis of this GUID – audit procedures could be drawn from this or other standards based on risk assessment. The annexure does not provide any guidance on how to audit. |

**Kommentert [PT31]:** SAIs may have their own standards. ISSAI 400 covers the requirements

**Kommentert [PT32]:** Para has been rephrased

**Kommentert [PT33]:** Para has been redrafted

**Kommentert [PT34]:** The para has been redrafted for clarity

**Kommentert [PT35]:** SAIs may have their own standards. ISSAI 400 covers the requirements

**Kommentert [PT36]:** The para clarifies dynamic nature of information technology, which needs to be factored in while planning follow-up
Therefore, no change made to GUID

**Kommentert [PT37]:** Annexure A has been deleted. The elements have been incorporated in the GUID

**Kommentert [PT38]:** The annexure provides high level audit questions, which would be useful in information security audits
Therefore, no change made to GUID

**GAO's Response to the International Organization of Supreme Audit Institutions' ExposureDraft: GUID 5101 *Guidance on Audit of Information Systems***

This letter provides the U.S. Government Accountability Office's (GAO) responses to questions in theexplanatory memorandum for the International Organization of Supreme Audit Institutions' (INTOSAI)exposure draft, GUID 5101, *Guidance on Audit of Information Systems*, as well as GAO's additional comments on the exposure draft.

**Responses to Questions**

1. **Does this GUID provide useful guidance for your SAI in carrying out a compliance audit ofsecurity of information systems?**

   Yes, this GUID provides useful guidance for supreme audit institutions (SAI) for carrying out suchcompliance audits.

2. **Are all definitions needed to understand and use this GUID included?**

   Yes, the GUID includes all definitions needed to understand and use it.

**Additional Comments**

We suggest clarifying the bolded terms used on page 7 of the PDF (see text block below). Rephrasing these sentences to explain the terms more clearly, thus showing how the examples used in each bullet relate to the remainder of the sentence, might be helpful to readers.

> Paragraph 9: The need for an Audit of Information Security may be triggered, depending onthe 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 ITSystem 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 throughsecurity patches/ updates;
>
> (c) **non-conduct** of periodic internal/ external security testing, including and security testing of operational IT systems, especially those which have undergone significantapplication or infrastructural upgrades.

**Kommentert [PT1]:** The paragraphs have been redrafted to bring in more clarity

**FIPP's formal appraisal against criteria for approval**

**Endorsement version GUID 5101 Guidance *Guidance on Audit of Security of Information Systems***

FIPP has received the endorsement version from KSC and has in accordance with the INTOSAI Due Process appraised the endorsement version against the criteria for approval. The results of FIPP's appraisal are recorded in the table below.

| **Criteria for appraisal as stated in INTOSAI Due Process** | **FIPP's assessment of the endorsement version against criteria** |
|---|---|
| 1. That the comments provided in the exposure process are appropriately reflected in the endorsement version of the document | |
| 2. That the document can be forwarded to the INTOSAI Governing Board | |