Agenda for the September 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 Tuesday 3 September 2024 - 13:00–17:00 CEST Tuesday 5 September 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 ensure that the draft endorsement version reflects the comments given during the Exposure process and that the document is ready for Endorsement.	FIPPs approval of the Endorsement version for the Governing Board. See Annex 1
Preparation for the work on the SDP		
Discussion paper on "Not changing the way we do audits"	Discussion on the draft paper on the premise that the SDG projects will not change the way SAIs perform audits	A finalized discussion paper for the PSC SC meeting in September 2024. Annex 2
LO Information		
Revised Exposure Draft on GUID 5340 *Guidance on audits of Public Private Partnerships*	Information from the LO about the status and the process for the draft	Preparation of FIPP for the upcoming process of the GUID 5340
Information from FIPP chair		
FIPP Chair	Information	- FIPP report Annex 3 - FIPP call for candidates: Enhancing the membership of the FIPP Annex 4 - Agenda for the November FIPP meeting
Information PSC Secretariat		
PSC Secr	Information from the PSC Secr	- Info about the PSC Steering Committee meeting - FIPP recruitment for 2024 - Implementation of the SDP.

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

I. Introduction

1. GUID 5101 supplements GUID 5100 by providing guidance on audit of information security. The guidance laid out in this GUID is consistent with the Fundamental Principles of Public Sector Auditing (ISSAI 100) as well as with the Compliance Audit Principles (ISSAI 400).
2. The transition to computerised information systems and electronic processing of information by auditees in the public sector makes it imperative for SAIs to develop appropriate capacity to audit controls related to information systems. As part of the audit of information systems, there is a need to ensure that controls to maintain confidentiality, integrity and availability of information systems and data (i.e. information security) have been designed and applied by auditees.
3. Information security breaches may lead to severe legal, reputational/ credibility, financial, productivity damage, and exposure to further intrusions. Security breaches may be caused by weaknesses and vulnerabilities that lead to accidental exposure, or disclosure of information to unauthorised parties, loss of availability or unauthorised changes in systems and data.

II. Objectives of this GUID

4. The guidance applicable to audit of information systems is outlined in GUID 5100. The objective of this GUID is to provide specific and additional guidance for a compliance audit of information security.
5. Audit of information security can be taken up as a compliance audit or, in certain circumstances, as a combined audit incorporating financial, compliance and/or performance aspects. This GUID covers audit of information security being taken up either as a distinct compliance audit or as part of a combined audit engagement to see whether the IT management meets the necessary standards and requirements for information security.
6. The contents of this GUID may be applied by auditors in the Planning, Conducting, Reporting and Follow Up stages of the audit process. The GUID lists 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 and is an authorized simulated hacking or attack on a computer system, performed to evaluate the security of the system.

IV. The Subject Matter

7. In audit of information security, the auditor assesses compliance of the subject matter (information security or any specific aspect/ component thereof) with applicable authorities (laws, regulations, policy, procedure, standards, practices etc.).
8. The information security audit work will be determined by the objectives and scope of the audit. 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;

[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.

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

V. Planning an Audit of Information Security

9. 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 has not been upgraded or replaced, where the underlying technological infrastructure is outdated and not currently supported through security patches/ updates;

(c) periodic internal/ external security testing have not been conducted, including security testing of operational information systems, especially those which have undergone significant application or infrastructural upgrades;

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

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

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

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

10. The auditor may assess the auditee's risk management process (including risk identification, assessment and treatment) as part of risk identification and assessment, if performing a risk based audit approach.
11. The auditor may examine availability of relevant policies and procedures, and whether these are being reviewed at appropriate intervals of time and updated as necessary while evaluating the organizational roles. The auditor may also assess whether there is adequate awareness and understanding amongst users, including the information security culture.
12. The materiality of an information security audit issue may be decided under the overall framework for deciding materiality in an SAI, as well as specific guidance for materiality in respect of information systems audits.

V.1 Sources of audit criteria

13. The auditor may use nationally or internationally accepted information security frameworks as sources for audit criteria.
14. The frameworks that serve as sources of audit criteria could include standards such as the ISO/IEC 27000 series; the CoBIT framework prepared/ updated by ISACA, the standards and frameworks relating to information and cybersecurity prepared by the National Institute of Standards and Technology (NIST); Center for Information Security (CIS) controls; more narrowly focused/ sector-specific frameworks and standards include the European Union's General Data Protection Regulation (GDPR), PCI DSS (Payment Card Industry Data Security Standard), the US Health Insurance Portability and Accountability Act (HIPAA) for the healthcare sector etc.
15. The auditor's choice of audit criteria may depend on:
    - Specific SAI and country context (including legal and regulatory requirements, if any)
    - Concerned audited entity/entities
    - Scope of the audit.

V.2 Resources

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

VI. Conducting an Audit of Information Security

VI.1 Purpose of the audit procedures[3]

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

VI.2 Audit procedures for gathering audit evidence

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

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

21. The audit of the risk management process may include examining the frequency of periodic risk reviews, and the adequacy of follow-up actions to mitigate the identified and assessed risks. The decision on risk acceptance thresholds (and the consequential acceptance of residual risks) is a management decision.
22. Linked to the risk management process (in particular, risk identification and assessment) are the policies for identification, classification and control of information assets. Audit procedures may include examining whether the policies are understood by users and whether such policies are implemented effectively.
23. Audit procedures on authentication, authorization and access controls may include examining whether multi-factor authentication (typically in addition to password-based authentication) is implemented, if it is mandated or prescribed by policy or the contract.
24. When logs are to be scrutinized to assess whether access control was implemented as planned, the analysis of logs may involve receipt of data dumps or extracts. Where data dumps are received from the audited entity for electronic analysis, the auditor may consider requesting a letter as described in para 6.4 of GUID 5100 with regard to ensuring authenticity, including its integrity and non-repudiability.
25. For audit of information security incident management, in addition to the review of the processes and documentation relating to incident identification and logging, assessment and resolution, the auditor may consider carrying out an inquiry on the adequacy of the resolution from a sample of users (where incidents were identified and ticketed by such users).
26. An information security audit may include an assessment of business continuity and disaster recovery planning and implementation, with a view to assessing the "availability" aspect of information services as well as information security during disaster recovery. Alternatively, such aspects may be covered as part of an audit of information systems operations management.

VI.3 Considerations related to outsourcing arrangements

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

VII. Reporting on an Audit of Information Security

28. The guidance on evaluating audit evidence and reporting as per ISSAI 400, as well as the additional guidance under GUID 5100 on reporting (section 7, which also refers to the sensitivity of reporting security risks before necessary mitigating controls have been adopted) may be followed in the case of information security audits.
29. Reporting on information security by auditors may consider the potential business impact of exposing technical shortcomings and security risk in public. In such cases, the auditor may use appropriate mechanisms, including redacting sensitive information or through management letters to share details and possible impact of the risk with the audited entity.
30. Besides the regular stakeholders of public sector audits, reporting may consider the specific perspectives of stakeholders like outsourced technical providers of support to the audited entities.

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

VIII. Follow-up

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

Annexure: Suggested High Level Audit Questions

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

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

			developed/ acquired reviewed by skilled internal or third-party resources to ensure that there are no hidden features that may compromise confidentiality, integrity and availability of data.
5	IT operations	Whether security of IT operations has been defined, adopted and communicated.	Examine contracts/ service level agreements to verify incorporation of non-disclosure, non-compete, non-modification without authorization, non-transmission and other standard provisions related to ensuring confidentiality, integrity and availability of data with parties to whom IT operations are outsourced.
6	Physical and environmental security	Whether security of physical environment of the information system has been ensured.	Verify whether physical barriers (external gates, internal doors, human security guards) which require identification of personnel and restrict access to storage hardware such as servers only to authorized personnel are in place. Facility management is an important aspect of the whole security ecosystem.
7	Network and Communications security	Whether information security is ensured during communication.	Verify whether communication channels ensure encryption of messages, to prevent interception by third parties and loss of confidentiality; also verify use of cryptographic controls for digital communications of a formal nature.
		Whether network security architecture is adequate for ensuring information security.	Wherever applicable, existence of cryptographic and other cyber security controls may be examined by auditors.
8	Business continuity and disaster recovery	Whether security aspects related to these processes have been addressed and information security is adequate for disaster recovery transition as well as operation.	Auditors may check whether information security facility is adequate during the disaster recovery process.

9	Statutory compliance	Whether statutory requirements related to information security aspects have been complied with.	Checks for compliance to statutory and regulatory provisions are to be exercised by auditors in all other domains as applicable. Provision may require specific certification/ assurance related to information to be obtained by entities. Scope and validity of such certification may also be examined by auditors.

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~~is outlined in GUID 5100. The objective of this GUID is to provide specific and additional guidance for ~~the~~a compliance audit of information security.
5. Audit of information security can be taken up as a compliance audit or, in certain circumstances, as a combined audit incorporating financial, compliance and/or performance aspects. This GUID covers audit of information security being taken up either as a distinct compliance audit or as part of a combined audit engagement to see whether the IT management meets the necessary standards and requirements for information security.
6. The contents of this GUID may be applied by auditors in the Planning, ~~Conduct~~Conducting, 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

Stildefinisjon ... (×30)
Formatert ... (×2)
formaterte ... (×1)
Formatert ... (×1)
formaterte ... (×2)
Formatert ... (×1)
formaterte ... (×3)
Formatert ... (×1)
formaterte ... (×3)
Formatert ... (×1)
formaterte ... (×2)
Formatert ... (×1)
formaterte ... (×1)
Formatert ... (×1)

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

IV. The Subject Matter

7. In audit of information security, the auditor ~~shall assess~~assesses compliance of the subject matter (information security or any specific aspect/ component thereof) ~~to~~with applicable authorities (laws, regulations, policy, procedure, standards, practices etc.).
8. The information security audit work will be determined by the objectives and scope of the audit. 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

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.

formaterte: Standardskrift for avsnitt, Skrift: Calibri, 12 pkt, Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Standardskrift for avsnitt, Skrift: Calibri, 12 pkt, Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

Formatert: Flere nivåer + Nivå: 1 + Nummereringsstil: I, II, III, … + Start på: 1 + Justering: Høyre + Justert ved: 0 cm + Innrykk ved: 0,76 cm

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

Formatert: Normal, Flere nivåer + Nivå: 1 + Nummereringsstil: 1, 2, 3, … + Start på: 1 + Justering: Venstre + Justert ved: 0,63 cm + Innrykk ved: 1,27 cm, Kantlinje: Topp: (Ingen kantlinje), Bunn: (Ingen kantlinje), Venstre: (Ingen kantlinje), Høyre: (Ingen kantlinje), Mellom : (Ingen kantlinje)

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Standardskrift for avsnitt

formaterte: Skrift: 10 pkt, Skriftfarge: Svart

formaterte: Skrift: 10 pkt, Skriftfarge: Svart, Engelsk (India)

formaterte: Skrift: 10 pkt, Skriftfarge: Svart

Formatert: Normal, Kantlinje: Topp: (Ingen kantlinje), Bunn: (Ingen kantlinje), Venstre: (Ingen kantlinje), Høyre: (Ingen kantlinje), Mellom : (Ingen kantlinje)

formaterte: Skriftfarge: Svart, Engelsk (India)

formaterte: Standardskrift for avsnitt

formaterte: Skrift: 10 pkt, Skriftfarge: Svart

formaterte: Skrift: 10 pkt, Skriftfarge: Svart, Engelsk (India)

formaterte: Skrift: 10 pkt, Skriftfarge: Svart

formaterte: Skriftfarge: Svart, Engelsk (India)

formaterte: Skriftfarge: Svart, Engelsk (India)

formaterte: Skriftfarge: Svart, Engelsk (India)

Formatert: Normal, Kantlinje: Topp: (Ingen kantlinje), Bunn: (Ingen kantlinje), Venstre: (Ingen kantlinje), Høyre: (Ingen kantlinje), Mellom : (Ingen kantlinje), Tabulatorstopp: 7,96 cm, Midtstilt + 15,92 cm, Høyre

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

V. Planning ~~audit~~an 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~~has not been upgraded or replaced, where the underlying technological infrastructure is outdated and not currently supported through security patches/ updates;

(c) periodic internal/ external security testing have not been conducted, including ~~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~~auditor 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 auditor may examine availability of relevant policies and procedures, and whether these are being reviewed at appropriate intervals of time and updated as necessary while evaluating the organizational roles. The auditor may also assess whether there is adequate awareness and understanding amongst users, including the information security culture.

Formatert: Flere nivåer + Nivå: 1 + Nummereringsstil: I, II, III, … + Start på: 1 + Justering: Høyre + Justert ved: 0 cm + Innrykk ved: 0,76 cm

formaterte: Skriftfarge: Svart

Formatert: Normal, Flere nivåer + Nivå: 1 + Nummereringsstil: 1, 2, 3, … + Start på: 1 + Justering: Venstre + Justert ved: 0,63 cm + Innrykk ved: 1,27 cm, Kantlinje: Topp: (Ingen kantlinje), Bunn: (Ingen kantlinje), Venstre: (Ingen kantlinje), Høyre: (Ingen kantlinje), Mellom : (Ingen kantlinje)

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

Formatert: Normal, Flere nivåer + Nivå: 1 + Nummereringsstil: 1, 2, 3, … + Start på: 1 + Justering: Venstre + Justert ved: 0,63 cm + Innrykk ved: 1,27 cm, Kantlinje: Topp: (Ingen kantlinje), Bunn: (Ingen kantlinje), Venstre: (Ingen kantlinje), Høyre: (Ingen kantlinje), Mellom : (Ingen kantlinje)

formaterte: Skriftfarge: Svart, Engelsk (India)

formaterte: Skriftfarge: Svart, Engelsk (India)

Formatert: Normal, Kantlinje: Topp: (Ingen kantlinje), Bunn: (Ingen kantlinje), Venstre: (Ingen kantlinje), Høyre: (Ingen kantlinje), Mellom : (Ingen kantlinje), Tabulatorstopp: 7,96 cm, Midtstilt + 15,92 cm, Høyre

~~11.~~12. The materiality of an information security audit issue may be decided under the overall framework for deciding materiality in an SAI, as well as specific guidance for materiality in respect of information systems audits.

V.1 Sources of audit criteria

13. ~~Appropriate~~The auditor may use nationally~~/~~ or internationally accepted information security frameworks ~~serve~~ as sources for audit criteria. ~~SAIs may find it useful to identify and adapt such~~

~~12.~~ The frameworks ~~for information security audits and to define the~~ that serve as sources of audit ~~objectives and scope of such audits.~~

~~13.~~14. ~~These frameworks~~criteria could include standards such as the ISO/IEC 27000 series; the CoBIT framework prepared/ updated by ISACA, the standards and frameworks relating to information and cybersecurity prepared by the National Institute of Standards and Technology (NIST); Center for Information Security (CIS) controls; more narrowly focused/ sector-specific frameworks and standards include the European Union's General Data Protection Regulation (GDPR), PCI DSS (Payment Card Industry Data Security Standard), the US Health Insurance Portability and Accountability Act (HIPAA) for the healthcare sector etc.

~~14.~~15. ~~The framework an SAI chooses to use as appropriate~~The auditor's choice of audit criteria may depend on:

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

V.2 Resources

~~15.~~16. The considerations for allocating human resources for information systems audit engagements (including information security audits) are discussed in GUID 5100 and are broadly applicable in the case of information security audits. One additional consideration may be that when dealing with sensitive and confidential information, auditors might be required to go through a special screening by relevant authorities.

VI. Conducting an Audit of Information Security ~~Audits~~

VI.1 Purpose of the audit procedures[3]

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

VI.2 ~~The~~Audit procedures ~~will typically~~for gathering audit evidence

~~17.~~18. The audit procedures may 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~~ (d) Vulnerability Assessment/ Penetration Testing (VA/PT~~)~~). If VA/PT is to be conducted by the ~~SAI audit team, necessary~~auditor, arrangements, and agreement with the audited entity for such intrusive testing ~~will~~may have to be made, including legal safeguards and indemnifications where necessary. If VA/PT has been carried out by a third-party the results of the VA/PT may be included as part of the audit evidence. In this case, the

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

formaterte: Skriftfarge: Svart
Formatert
Formatert
formaterte: Skriftfarge: Svart
formaterte: Skriftfarge: Svart
formaterte: Skriftfarge: Svart
formaterte: Skriftfarge: Svart
formaterte: Skriftfarge: Svart
formaterte: Skriftfarge: Svart
formaterte: Skriftfarge: Svart
formaterte: Skriftfarge: Svart
Formatert
formaterte: Skriftfarge: Svart
formaterte: Skrift: Calibri, Skriftfarge: Svart
formaterte: Skriftfarge: Svart
formaterte: Skrift: Calibri, Skriftfarge: Svart
formaterte: Skriftfarge: Svart
formaterte: Skrift: Calibri, Skriftfarge: Svart
Formatert
formaterte: Skriftfarge: Svart
Formatert
formaterte: Skriftfarge: Svart
Formatert
formaterte: Skriftfarge: Svart
Formatert
formaterte: Skriftfarge: Svart
formaterte: Skrift: Calibri, 13 pkt
formaterte: Skriftfarge: Svart
Formatert
formaterte: Skriftfarge: Svart
formaterte: Skriftfarge: Svart
formaterte: Skriftfarge: Svart
formaterte: Skriftfarge: Svart
formaterte: Skriftfarge: Svart
formaterte: Skriftfarge: Svart
formaterte: Skriftfarge: Svart, Engelsk (India)
Formatert
formaterte: Skriftfarge: Svart, Engelsk (India)

auditor obtains a sufficient understanding of the scope of the VA/PT as well as the findings and their implications.

~~18.~~ For assessing physical and environmental security, in addition to documentation review, interviews etc., ~~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 auditor may consider a physical visit (or joint inspection) of the data centre as a supplementary audit procedure.

~~19.~~20. The auditor may assess the adequacy of standards, guidelines and procedures designed to operationalize information security policy and policies for incident/ problem reporting and management ~~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~~may include examining the frequency of periodic risk reviews, and the adequacy of follow-up actions to mitigate the identified and assessed risks. The decision on risk acceptance thresholds (and the consequential acceptance of residual risks) is a management decision.
22. Linked to the risk management process (in particular, risk identification and assessment) are the policies for identification, classification and control of information assets. Audit procedures ~~will~~may include examining whether the policies are understood by users and whether such policies are implemented effectively.
23. Audit procedures on authentication, authorization and access controls ~~will~~may include examining whether multi-factor authentication (typically in addition to password-based authentication) is implemented, if it is mandated or prescribed by policy or the contract.
24. When logs are to be scrutinized to assess whether access control was implemented as planned, the analysis of logs may involve receipt of data dumps or extracts. Where data dumps are received from the audited entity for electronic analysis, the ~~considerations spelt out~~auditor may consider requesting a letter as described in para 6.4 of GUID 5100 with regard to ensuring ~~its~~ authenticity, including its 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~~auditor may consider carrying out an inquiry on the adequacy of the resolution from a sample of users (where incidents were identified and ticketed by such users).
26. An information security audit may include an assessment of business continuity and disaster recovery planning and implementation, with a view to assessing the "availability" aspect of information services as well as information security during disaster recovery. Alternatively, such aspects may be covered as part of an audit of information systems operations management.

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

Formatert: Normal, Flere nivåer + Nivå: 1 + Nummereringsstil: 1, 2, 3, … + Start på: 1 + Justering: Venstre + Justert ved: 0,63 cm + Innrykk ved: 1,27 cm, Kantlinje: Topp: (Ingen kantlinje), Bunn: (Ingen kantlinje), Venstre: (Ingen kantlinje), Høyre: (Ingen kantlinje), Mellom : (Ingen kantlinje)

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

Formatert: Normal, Flere nivåer + Nivå: 1 + Nummereringsstil: 1, 2, 3, … + Start på: 1 + Justering: Venstre + Justert ved: 0,63 cm + Innrykk ved: 1,27 cm, Kantlinje: Topp: (Ingen kantlinje), Bunn: (Ingen kantlinje), Venstre: (Ingen kantlinje), Høyre: (Ingen kantlinje), Mellom : (Ingen kantlinje)

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart, Engelsk (India)

formaterte: Skriftfarge: Svart, Engelsk (India)

Formatert: Normal, Kantlinje: Topp: (Ingen kantlinje), Bunn: (Ingen kantlinje), Venstre: (Ingen kantlinje), Høyre: (Ingen kantlinje), Mellom : (Ingen kantlinje), Tabulatorstopp: 7,96 cm, Midtstilt + 15,92 cm, Høyre

VI.3 Considerations related to outsourcing arrangements

~~26.~~27. With regard to information security in supplier/ outsourced relationships, the audited entity retains accountability for information security even if the responsibility for certain information systems activities has been outsourced to an external supplier. Further, aspects such as segregation of conflicting duties (e.g. between development, testing and production teams) are significant, whether the development/ implementation/ operations and maintenance of the information system is being done in-house or through an external supplier.

~~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.~~1. ~~An information security audit may include assessment of business continuity and dicastor recovery planning and implomentation, with a view to assessing the "availability" aspect of information services as well as information security during dicastor recovery. Alternativoly, 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~~an Audit of ~~information security~~Information Security

~~29.~~28. The guidance on evaluating audit evidence and reporting as per ISSAI 400, as well as the additional guidance under GUID 5100 on reporting (section 7, which also refers to the sensitivity of reporting security risks before necessary mitigating controls have been adopted) may be followed in the case of information security audits.

~~30.~~29. Reporting on information security by auditors may consider the potential business impact of exposing technical shortcomings and security risk in public. In such cases, ~~SAIs~~the auditor may use appropriate mechanisms, including redacting sensitive information or through management letters to share details and possible impact of the risk with the audited entity.

~~31.~~30. Besides the regular stakeholders of public sector audits, reporting may consider the specific perspectives of stakeholders like outsourced technical providers of support to the audited entities.

~~32.~~31. ~~Recommendations~~The auditor may ~~be developed after considering the available technical solutions~~provide recommendations for improving ~~the~~ information security ~~and its~~. When developing the recommendations, the auditor may consider any practical implications for the ~~business of the~~ audited entity ~~along with a~~, including the cost ~~benefit analysis, as assessed by the audited entity.~~ of implementation.

VIII. Follow--up

32. ~~Follow up requirements as per~~The auditor considers follow-ups in accordance with the compliance audit principles of ISSAI 400 ~~for Compliance Audits~~.

~~33.~~ IT systems are ~~to be considered.~~

33. constantly evolving. As an example, IT systems are ~~dynamic. They are also~~ increasingly web-based/ cloud hosted. ~~Frequency of follow up audits~~The auditor may consider ~~the~~such significant changes ~~arising out of these~~when deciding on the timing of follow-up audits.

~~34.~~ When planning a follow-up, the auditor may consider factors~~.~~

formaterte: Skriftfarge: Svart

Formatert: Normal, Flere nivåer + Nivå: 1 + Nummereringsstil: 1, 2, 3, … + Start på: 1 + Justering: Venstre + Justert ved: 0,63 cm + Innrykk ved: 1,27 cm, Kantlinje: Topp: (Ingen kantlinje), Bunn: (Ingen kantlinje), Venstre: (Ingen kantlinje), Høyre: (Ingen kantlinje), Mellom : (Ingen kantlinje)

formaterte: Skriftfarge: Svart

Formatert: Normal, Flere nivåer + Nivå: 1 + Nummereringsstil: 1, 2, 3, … + Start på: 1 + Justering: Venstre + Justert ved: 0,63 cm + Innrykk ved: 1,27 cm, Kantlinje: Topp: (Ingen kantlinje), Bunn: (Ingen kantlinje), Venstre: (Ingen kantlinje), Høyre: (Ingen kantlinje), Mellom : (Ingen kantlinje)

Formatert: Flere nivåer + Nivå: 1 + Nummereringsstil: I, II, III, … + Start på: 1 + Justering: Høyre + Justert ved: 0 cm + Innrykk ved: 0,76 cm

formaterte: Skriftfarge: Svart

Formatert: Normal, Flere nivåer + Nivå: 1 + Nummereringsstil: 1, 2, 3, … + Start på: 1 + Justering: Venstre + Justert ved: 0,63 cm + Innrykk ved: 1,27 cm, Kantlinje: Topp: (Ingen kantlinje), Bunn: (Ingen kantlinje), Venstre: (Ingen kantlinje), Høyre: (Ingen kantlinje), Mellom : (Ingen kantlinje)

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

Formatert: Flere nivåer + Nivå: 1 + Nummereringsstil: I, II, III, … + Start på: 1 + Justering: Høyre + Justert ved: 0 cm + Innrykk ved: 0,76 cm

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart, Engelsk (India)

formaterte: Skriftfarge: Svart, Engelsk (India)

Formatert …

35.34. ~~Solutions for identified weaknesses from information security audits are likely to be very specific in terms of~~ such as available technology, costing, and system compatibility ~~etc. The follow up plan along with timelines may be reviewed considering these~~that can impact the audited entity's capability to address the audit findings and implement the recommendations.

Formatert: Normal, Flere nivåer + Nivå: 1 + Nummereringsstil: 1, 2, 3, … + Start på: 1 + Justering: Venstre + Justert ved: 0,63 cm + Innrykk ved: 1,27 cm, Kantlinje: Topp: (Ingen kantlinje), Bunn: (Ingen kantlinje), Venstre: (Ingen kantlinje), Høyre: (Ingen kantlinje), Mellom : (Ingen kantlinje)

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skriftfarge: Svart

formaterte: Skrift: Calibri, 12 pkt

formaterte: Skriftfarge: Svart, Engelsk (India)

formaterte: Skriftfarge: Svart, Engelsk (India)

Formatert: Normal, Kantlinje: Topp: (Ingen kantlinje), Bunn: (Ingen kantlinje), Venstre: (Ingen kantlinje), Høyre: (Ingen kantlinje), Mellom : (Ingen kantlinje), Tabulatorstopp: 7,96 cm, Midtstilt + 15,92 cm, Høyre

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

formaterte: Skriftfarge: Svart

Formatert tabell

formaterte: Skriftfarge: Svart, Engelsk (India)

formaterte: Skriftfarge: Svart, Engelsk (India)

Formatert: Normal, Kantlinje: Topp: (Ingen kantlinje), Bunn: (Ingen kantlinje), Venstre: (Ingen kantlinje), Høyre: (Ingen kantlinje), Mellom : (Ingen kantlinje), Tabulatorstopp: 7,96 cm, Midtstilt + 15,92 cm, Høyre

			developed/ acquired reviewed by skilled internal or third-party resources to ensure that there are no hidden features that may compromise confidentiality, integrity and availability of data.
5	IT operations	Whether security of IT operations has been defined, adopted and communicated.	Examine contracts/ service level agreements to verify incorporation of non-disclosure, non-compete, non-modification without authorization, non-transmission and other standard provisions related to ensuring confidentiality, integrity and availability of data with parties to whom IT operations are outsourced.
6	Physical and environmental security	Whether security of physical environment of the information system has been ensured.	Verify whether physical barriers (external gates, internal doors, human security guards) which require identification of personnel and restrict access to storage hardware such as servers only to authorized personnel are in place. Facility management is an important aspect of the whole security ecosystem.
7	Network and Communications security	Whether information security is ensured during communication.	Verify whether communication channels ensure encryption of messages, to prevent interception by third parties and loss of confidentiality; also verify use of cryptographic controls for digital communications of a formal nature.
		Whether network security architecture is adequate for ensuring information security.	Wherever applicable, existence of cryptographic and other cyber security controls may be examined by auditors.
8	Business continuity and disaster recovery	Whether security aspects related to these processes have been addressed and information security is adequate for disaster recovery transition as well as operation.	Auditors may check whether information security facility is adequate during the disaster recovery process.

formaterte: Skriftfarge: Svart, Engelsk (India)

formaterte: Skriftfarge: Svart, Engelsk (India)

Formatert: Normal, Kantlinje: Topp: (Ingen kantlinje), Bunn: (Ingen kantlinje), Venstre: (Ingen kantlinje), Høyre: (Ingen kantlinje), Mellom : (Ingen kantlinje), Tabulatorstopp: 7,96 cm, Midtstilt + 15,92 cm, Høyre

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: Skriftfarge: Svart

Formatert: Normal, Innrykk: Venstre: 1,27 cm, Kantlinje: Topp: (Ingen kantlinje), Bunn: (Ingen kantlinje), Venstre: (Ingen kantlinje), Høyre: (Ingen kantlinje), Mellom : (Ingen kantlinje)

formaterte: Skriftfarge: Svart, Engelsk (India)

formaterte: Skriftfarge: Svart, Engelsk (India)

Formatert: Normal, Kantlinje: Topp: (Ingen kantlinje), Bunn: (Ingen kantlinje), Venstre: (Ingen kantlinje), Høyre: (Ingen kantlinje), Mellom : (Ingen kantlinje), Tabulatorstopp: 7,96 cm, Midtstilt + 15,92 cm, Høyre

Compliance to Comments on the Exposure Draft

SAI	Para reference (Pre revised GUID)/ General Comments	Comment	Action taken/Remarks
Russia	Para 9	V. Planning an Audit of Information Security item 'e' The clause limits the decision-making on the need to conduct an information security audit when recording problems related to the protection of personal data only. It is proposed to exclude the words "protection of personal data" from the clause, which will allow conduct an information security audit to comply with any change in national legislation in the sphere of confidential information protection	Reference to protection of personal data has been deleted to cover protection of all data
Myanmar	Para 6	To correct as “Conducting”	Language change has been carried out
	Definitions	To include a citation to (CNSS, 2010) at the end of the paragraph, as this definition is directly sourced from the Committee on National Security Systems' National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, dated April 26, 2010.	Since other definitions have not been reference, this may not be needed. No changes made to draft
	Para 26	To insert “Maintenance plan,”	Para 26 is specific to ‘Availability’, hence only business continuity is mentioned. No changes made to draft
Lithuania	Para 8	Business continuity could be added	Business continuity has been covered in para 26
	Para 9	An event could be added where an organisation introduces new innovations and technological solutions that have just appeared on the market, e.g. AI-based solutions	This is covered in point 9(a). No changes made to draft

	Para 15	Since the following is about the possibility of an SAI team to perform VA/PT tests, it would be useful to mention the competences that such a team would need to have if it were decided to perform such tests. It would also be good to discuss in general terms the competency requirements for auditors when conducting security audits, as this is a specific area that requires appropriate competencies.	Specific skills are not mentioned in the draft to keep the document at higher level. No changes made to draft
	Para 18	Could be complemented by external experts from the AAI team or contracted by the SAI	This is already covered in the para. The para has been redrafted for more clarity
	Para 18	Maybe these explanations can be added to the definitions	This part has been moved to the definitions
	Para 26 & Annexure	INTOSAI WGITA has currently drafted and is coordinating with the SAIs a "Suggested Audit Design Matrix for WGITA-IDI Handbook on IT Audit for SAIs 2022". This document provides a very detailed set of issues, including security aspects, with sources of information and suggested methods and test examples. It is suggested that the questions in Annex B of GUID 5101 be aligned with this document or that the questions related to security issues be moved from it here.	GUID 5101 being a higher level FIPP document cannot be reference to a lower level non FIPP document. Accordingly, annexures have been kept generic.
	Para 27	This is proposed to be moved up under point 18, where it already refers to VA/PT tests	The paras have been redrafted
Fiji	Generic	If it's possible to have some Practice Notes with examples so that users can have a workflow process to follow as per the rationale of this exposure draft	Practice notes are not part of GUID. No change made to draft
Estonia	Para 8	IV The Subject Matter – the list in p 8 is quite thorough, but maybe it would be beneficial to mention information security management related specifically to cloud platform usage, e.g. as an example under "Information security in supplier relationships"	Various elements have been pointed out in the para without limiting it to specific platforms. No change made to draft
	Para 9	V Planning an Audit of Information Security (p. 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, (a list of 7 potential triggers). We would add that an audit may sometimes be triggered based on a risk-analysis of a random sample of wider stakeholders	The trigger mentioned in only indicative and SAIs may use additional triggers. No changes made to draft

	Generic	The GUID could additionally include potential audit intervention points – whether there could/should be some audit procedures (e.g. contractor risk assessment) before developing an information system	Information security in outsourced relationships has been covered in para 27. No change made to draft
Denmark	Generic	"Data" and "information" are used interchangeably when describing availability. We recommend that the GUID either provide a word definition or use one word consistently	The draft has been reviewed to avoid any interchangeable usage
	Generic	"Authentication" and "non-repudiation" are defined as elements of integrity but are also listed next to integrity as separate concerns. We recommend that "authentication" and "non-repudiation" are removed from lists that already include "integrity".	The draft has been reviewed & changes carried out
	Para 9	"Post Mortem" is used but not defined in the GUID. We recommend that the phrase is either defined or removed	It is a commonly used term and therefore has not been defined
	Generic	The comprehensibility of the GUID will benefit from a proofreading ensuring consistent formatting, spelling, use of serial comma, use of uppercase and lowercase letters, removal of redundant words, and avoidance of long sentences	Proof reading has been done as suggested
Bahrain	Para 14	ISO/IEC 27000	Changes carried out in the draft
		This para should be added to Follow up section: It is important to recognize that some findings and recommendations identified during the audit may not be applicable for follow-up procedures due to changes in technology, organizational structure, or external factors. As technology evolves rapidly, previously identified vulnerabilities or control weaknesses may become obsolete or irrelevant. Therefore, auditors should assess the current relevance of past findings and adjust follow-up procedures accordingly. This ensures that the audit remains focused on current and emerging risks, providing value to the organization in maintaining robust information security practices.	No changes done in Follow up section, as paras 33/ 34 address concerns relating to changing technology
Argentina	Generic	GUID 5101 is compatible with the current regulations and is consistent with the Fundamental Principles of Public Sector Auditing (ISSAI 100) as well as the Compliance Audit Principles (ISSAI 400). The GUID project is very useful for supporting the audit work	No changes made to the draft

Algeria	Generic	Clarity and scope: the introduction effectively sets the stage for understanding the importance of auditing information security within the broader context of guid 5100. it clearly defines the relevance of this guidance for ensuring the confidentiality, integrity, and availability of information systems	No changes made to the draft
	Introduction (Paras 1-3)	Document positioning: it would be beneficial to explicitly state that guid 5101 is intended as a supplement to guid 5100. this clarification will help prevent any confusion about whether this guidance stands alone or complements existing standards	This has already been stated in the introduction. No changes made to the draft
	Introduction (Paras 1-3)	Detail level: the introduction provides a solid overview but could benefit from highlighting the rapidly evolving nature of information security threats and technologies. emphasizing the need for continuous updates and adaptations in auditing practices would align the document with current trends	The evolving nature of the subject has already been covered in the follow-up section. No changes made to the draft
	Generic	Applicability: the guidance's applicability to both distinct compliance audits and combined audit engagements is clearly presented. it would be useful to provide more specific examples of how these scenarios might be applied in practice	Applicability has been covered in the Objectives section of the GUID. Including specific examples may necessitate frequent modifications of the GUID. No changes made to the draft
	Generic	Alignment with standards : the guide provides a solid foundation for auditing information security. however, it would be beneficial to further clarify how it aligns with recognized standards such as iso 27001, cobit, and nist. this would enhance the guide's credibility and ensure greater compliance with best practices in information security.	These have been mentioned in the Sources of audit criteria section (paras 12 -14). No changes made to the draft
	Generic	Evolving standards : it is also relevant to highlight that information security standards are evolving rapidly. for instance, updates to iso 27001 or new nist guidelines could impact auditing practices. the guide should reflect this dynamic to remain relevant and up-to-date	The evolving nature of the subject has already been covered in the follow-up section. No changes made to the draft
	IV The Subject Matter	Clarity of objectives and audit scope : the text clearly defines that the audit of information security should assess compliance with applicable policies, procedures, standards, and practices. however, it would be helpful to	The GUID has been drafted to provide overall guidance & specific

		elaborate on how auditors can prioritize elements within their audits based on specific objectives. providing concrete examples of prioritization criteria could enhance practical understanding.	examples have been avoided. No changes made to the draft
	IV The Subject Matter	Implementation of components : the audit elements such as information asset management, access control, and physical security are well covered. to improve this section, additional guidelines on how to effectively audit each component would be beneficial. for instance, including evaluation criteria or specific audit techniques for each area could offer further guidance	Such additional guidelines could limit the applicability of the GUID. No changes made to the draft
	IV The Subject Matter	Integration with current practices: the section could benefit from mentioning how to incorporate recent trends and innovative practices in information security auditing. for example, addressing new threats such as sophisticated cyberattacks or compliance requirements for cloud environments would make the guidance more relevant and up-to-date	Such additional details could limit the applicability of the GUID. No changes made to the draft
	Generic	The guide on auditing information security provides a comprehensive framework for evaluating compliance with relevant policies, standards, and best practices. However, it is essential to address the growing influence of Artificial Intelligence (AI) in both enhancing and challenging information security measures.	The GUID covers all aspects of audit of information security. Impact of AI & other emerging technologies on these aspects need not be part of this document. No changes made to the draft
	Generic	AI in Risk assessment and management : AI technologies offer significant improvements in risk assessment by analyzing large datasets to identify vulnerabilities and predict potential threats. Incorporating AI tools in the audit process can enhance the depth of risk assessments and improve accuracy. The guide should include guidance on how to integrate AI-driven insights into traditional risk management frameworks	The GUID covers all aspects of audit of information security. Impact of AI & other emerging technologies on these aspects need not be part of this document. No changes made to the draft
	Generic	AI in security monitoring and incident management : AI enhances security monitoring through advanced threat detection mechanisms and automated incident responses. The chapter should address how auditors can evaluate the effectiveness and reliability of AI-powered security solutions. This includes assessing the impact of these technologies on overall security management and ensuring they align with established security standards	The GUID covers all aspects of audit of information security. Impact of AI & other emerging technologies on these aspects need not be part of this document. No changes made to the draft

	Generic	Challenges and considerations: While AI introduces advanced capabilities, it also brings new challenges, such as ensuring transparency and accountability in AI-driven decisions. The guide should explore how to audit AI systems for compliance with information security standards, focusing on the evaluation of algorithms and data handling practices to ensure that AI solutions meet the required security and ethical standards	The GUID covers all aspects of audit of information security. Impact of AI & other emerging technologies on these aspects need not be part of this document. No changes made to the draft
	V. Planning Audit of Information Security	The chapter provides a solid framework for planning information security audits, covering key triggers and risk management processes. To enhance it, add guidance on prioritizing audit triggers, detail how auditors should engage with risk management processes, and include concrete examples to illustrate these concepts	Such additional details could limit the applicability of the GUID. No changes made to the draft
	V. Planning Audit of Information Security	Objectives of the audit (14): The section effectively outlines the core objectives of the information security audit, including confidentiality, integrity, and availability. To enhance this section, it would be helpful to define each objective separately and provide guidance on prioritizing them based on specific audit scenarios	Such additional details could limit the applicability of the GUID. No changes made to the draft
	V. Planning Audit of Information Security	Evidence collection procedures (15 and 18):Section 18 details various evidence collection procedures, such as documentation review, observation, and analysis of electronic data. For further clarity, it would be beneficial to distinguish between the different types of evidence and explain how each contributes to the audit outcomes. Additionally, the mention of physical visits or joint inspections in Section 26 could be expanded to include guidelines on how these should be conducted and integrated with other evidence sources	Such additional details could limit the applicability of the GUID. No changes made to the draft
	V. Planning Audit of Information Security	Audit objects and controls (16, 19-24, and 28):Sections 19 to 24 cover various audit objects and related controls, including information security culture, risk management processes, and specific controls like multi-factor authentication. For improved clarity, consider breaking this section into sub-sections for each audit object and control type. Furthermore, Section 28, which discusses business continuity and disaster recovery planning, could be better integrated with other audit objects to show how these elements fit into the overall security posture assessment	Such additional details could limit the applicability of the GUID. No changes made to the draft

Egypt	Definitions	□ Definitions that need to be added to the guideline: 1- Management and Control of Information Assets: Information assets management and control refers to the methodological processes and procedures aiming to protect an organization's information assets to ensure their confidentiality, saindness, and availability. This includes identifying and classifying information assets, assessing the associated risks, setting necessary controls and procedures for their protection, regularly monitoring compliance with these procedures and continuously updating security measures to address emerging threats and challenges. Information assets, include data and electronic information, software, devices , networks and any other components used to process, store or transmit information. 2- Information Security Incidents` Management: Refers to a set of organized processes and procedures implemented to handle security incidents that affect information as well as information systems. These processes include detecting incidents, assessing them, containing them, eliminating threats, restoring affected systems and services and investigating the incident in order to understand its causes and prevent future occurrences. It also involves documenting the incidents and actions taken as well as communicating with relevant stakeholders within and outside the organization to ensure an effective and coordinated response.	No change is done in Definition section, as those terms are defined which have reference to the document and are relevant specifically to Information Security
	Definitions	□ Definition of Cyber Security and information security We propose to enhance clarifying the distinguish between Information Security and cyber Security. Adding an example to Definition of Information Security Example: This includes protecting paper files containing sensitive information by storing them in locked cabinets and controlling access to them as well as using encryption to protect data stored on electronic devices. Suggestion: Adding a Comparison Table between Information Security and Cyber security	Difference between Information security and Cyber security is already there as these are mentioned in Definitions. No changes made to the draft

highlighting the differences between both across various domains.

We suggest the following table for clarity

Domain	Information Security	Cyber security
Scope	All types of information regardless of the medium or location.	The cyberspace and internet-connected systems.
Tools	Encryption, assets management systems, firewalls, intrusion detection systems.	Antivirus programs, malware detection systems, network security technologies.
Technologies	Identity management, information security management, backups.	Strong encryption, digital forensics, cyber defense technologies.
Threats	Unauthorized access, unauthorized modification or deletion, data leakage, theft.	Viruses, malware, ransomware attacks, denial-of-service attacks, breaches.

<table>
<tr>
<td></td>
<td></td>
<td>
<table>
<tr><td>Risks</td><td>Leakage of sensitive information, loss of important data, damage to the organization's reputation.</td><td>Disruption of electronic services, theft of digital data, breaches, significant financial damages.</td></tr>
<tr><td>Procedures</td><td>Setting security management policies, employee training, regular audits.</td><td>Response plans for cyber Incidents, network and system monitoring, regular software updates.</td></tr>
<tr><td>Measures</td><td>Access controls, encryption, backup management, physical controls.</td><td>Firewalls, antivirus systems, intrusion detection technologies, network security protocols.</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Generic</td>
<td>General Suggestions

▪ References and Resources: Consider adding a section that includes links to additional resources, such as detailed frameworks, recent publications or tools that could assist auditors in performing information security audits.</td>
<td>Specific examples & case studies have been avoided in the GUID. No changes made to the draft</td>
</tr>
</table>

		▪ Case Studies: Including brief case studies or examples of past audits could help illustrate how the guidance could applied in real-world situations. ▪ Sources of Audit Criteria Suggestion for point 15: The auditor's choice of audit criteria may depend on: Emerging risks and Technological advancements. In case of agreeing to add this point, we suggest adding the Definition of Emerging Technologies: Emerging technologies are modern technologies that are rapidly developing and have a significant impact on various operations and activities. These technologies include, among others, artificial intelligence, the Internet of Things (IoT), blockchain technology, virtual and augmented reality. While these technologies could offer substantial benefits, they also carry potential security risks that require careful accurate assessment and effective management	
Latvia		We suggest considering whether an explanation of the connection between information security audits and information systems audits, and the overlap of these two audits in certain areas, should be included in sections three or four of the guidance. The scope of both the information security audit and the information systems audit involves the evaluation of the same controls concerning, for example, confidentiality, integrity, and availability. The scope of information systems audits as indicated in GUID5100 includes checks of the same controls (e.g., ensuring confidentiality, integrity, and availability), which are also the focus of this guidance regarding information security assessments. Auditors who are less familiar with IT fields may fail to distinguish this connection and may mistakenly plan to carry out two separate audit tasks – an information systems audit and an information security audit	The relationship between GUID 5101 & GUID 5100 has already been clarified in the Introduction section. No changes made to the draft

		In the third section of the guidance, the definition of “cyber security” is explained. Based on our experience in communication with various auditees, we have identified different understandings in practice whether physical security should be included in or excluded from the scope of cyber security (for example, whether cyber security also includes specific physical security measures and protection mechanisms related to data transmission equipment and network-related devices, or whether the issue of cyber security covers only the digital protection of these networks and communication channels, encryption, monitoring of information flow, etc.). Therefore, we suggest considering whether the explanation of the cyber security definition or the section "7: Network and Communication Security" in the annexure should be supplemented accordingly	Network and communication security is technology specific and hence not addressed. No changes made to the draft
		We suggest adding to section five "Planning an Audit of Information Security" in paragraphs 10 and 11 the requirement for the auditor to identify whether an internal or external audit/assessment has been conducted regarding the audit subject, and if such an audit has been carried out, to review the report of this internal or external audit/assessment and the recommendations provided. We consider this task as a significant component of the planning phase to obtain information about risks and risk mitigation measures, if recommendations have been made and implemented. Additionally, it is important for resource efficiency, as it allows reliance on the work done by another auditor	This would be in the scope of a guidance on reliance on the work of internal auditors. Follow-up section looks into external audit. No changes made to the draft

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	

Forum for INTOSAI Professional Pronouncements

Achieving the ambitions of the SDP without 'changing the way SAIs do their audits'

The 'T' and 'I' initiatives of the Strategic Development Plan for IFPP 2024-2028 (SDP) aim to improve the clarity of the ISSAIs. The 'T' initiative on terminology provides input to the 'I' Initiative on revision of the ISSAIs as well as other initiatives. The SDP sets the following ambitions for the two initiatives:

The ambitions as stated in the SDP (extract)

The 'T' initiative - Developing clear and consistent terminology for the IFPP

To define the terminology that will be used in all future professional pronouncements and when updating the current ones. Future revisions and updates of the terminology will be carried out when relevant. The terminology developed will be based on the concepts defined in ISSAI 100 Fundamental principles of public sector auditing, and the additional concepts defined in other key pronouncements. The resulting terminology will include the professional language for different types of audit and steps in the audit process as well as the concepts used to define the authority of the ISSAIs and what it means to comply with them

The 'I' initiative - Ensuring the clarity of the ISSAIs

To achieve a clear and understandable set of ISSAIs that can support SAIs in delivering high-quality audits regardless of the approach the SAI is using when applying the ISSAIs

According to the supplementary scoping paper, the ambition of the SDP is to not change the way that the audits are carried out in accordance with the present ISSAIs. This to limit the consequences of the changes that can result from the 'I' initiative. This reflects that it has been part of the PSC Steering Committee's promises in connection with 'the Component 1' analysis and the subsequent development and approval of the SDP that the revision of the ISSAIs in 2024-2028 ***will not change the way SAIs do their audits.***

FIPP is committed to work as a safeguard that this pledge will be respected when the projects are carried through and project proposals and exposure drafts are assessed and approved by FIPP. With this paper FIPP wishes to explain to the PSC Steering Committee how FIPP will handle the issues arising from the pledge 'not to change the way SAIs do their audits' in an operational way.

The aim for the I initiative is to ensure quality in audit work, focusing on clarity. This will affect *the text* of the standards. Any changes in the text of an auditing standard may potentially at some level of details affect the obligations of auditors following the standards. There will therefore be a balance to strike so INTOSAI can achieve the ambitions of the SDP without 'changing the way SAIs do their audits'.

FIPP's analysis

The IFPP include INTOSAI Ps, ISSAIs and GUIDs. ISSAI 100 and the principles for Financial Auditing (ISSAI 200), Performance Auditing (ISSAI 300) and Compliance Auditing (ISSAI 400) that flow from ISSAI 100 can be used to establish authoritative standards in three ways:

- as a basis on which SAIs can develop standards;
- as a basis for the adoption of consistent national standards;
- as a basis for adoption of the ISSAIs

Component 1 identified many inconsistencies in the IFPP between the principles in the ISSAIs (ISSAI 100-400) and the requirements (ISSAI 2000-4000), both horizontally and vertically. Horizontal inconsistencies occur when principles in ISSAI 100 is missing in the related ISSAI 200-400 or the other way around or when there are inconsistencies between ISSAI 200-400 without any obvious reason. Vertical inconsistencies occur when principles is not reflected in the requirements or the other way around. Both vertical and horizontal inconsistencies will need to be considered and solved through the revision of the ISSAIs.

Below we have listed different types of changes that may be relevant to achieve the ambitions of the SDP and how they may impact on the obligations of SAIs and auditors using the ISSAIs. FIPP will use the analysis in its dialogue with the two project teams when FIPP considers changes in the current text.

Type of change in the ISSAIs	Possibility for impact on SAIs
Moving a principle from ISSAI 100 to ISSAI 200-400	Unlikely to impact the audit work. Might however affect those who uses the ISSAI 100-400 to develop their own standards if they have not been aware that ISSAI 100 applies to all engagements.
Developing a requirement in 2000-4999 based on a principle	Might affect those who only uses the ISSAIs in 2000-4999 and do not consider the principles in ISSAI 100-400.
Moving a principle that exists for all three audit types in ISSAI 200, ISSAI 300 and ISSAI 400 to ISSAI 100	Unlikely/little impact on the audit work
Developing a principle in ISSAI 100/200/300/400 based on existing requirements in ISSAs 2000s, ISSAI 3000 and/or ISSAI 4000	May affect SAIs that use national standards that are based on/consistent with the principles of the ISSAIs
Copying a principle or requirement from one audit type to one or two of the others	May affect the SAIs – especially SAIs using the ISSAIs to carry out audits of a single type rather than combining two or all audit types into one audit process.
Replacing one technical term with another term to achieve a better professional language	Unlikely/little impact on the audit work. But may have effect if the meaning of principles/requirements change.
Changing language into better English	Unlikely to impact on the audit work

How FIPP will handle the issues

As a general approach FIPP will in its guidance to the project groups and approvals of drafts seek to ensure:

1. That the ambitions of the T-initiatives and I-initiatives as stated in the SDP are successfully met
2. That the results of the 'T'- and 'I'-initiatives are closely based on the existing ISSAI-texts and are achieved through the type of changes illustrated in the table above with due consideration to the possible impact on SAIs
3. That all resulting edits in the texts of the ISSAIs are limited to those that serve the purpose of reaching the ambitions of the SDP. Any potential revisions based on other motivations (improve audit quality in other ways, provide more flexibility, respond to new developments etc.) will have to be postponed to a future project under a new SDP.
4. When the resulting texts are exposed to the INTOSAI community for 90-days as provided by INTOSAI's due process all SAIs will be asked whether the proposed changes to the ISSAIs will affect the way they currently carry out their audits in any unacceptable way. This will ensure that FIPP is made aware of any issues that may not have been probably addressed.

Forum for INTOSAI Professional Pronouncements

September 2024

To: The Steering Committee of the Professional Standards Committee (PSC-SC)
From: FIPP

Report by the Forum for INTOSAI Professional Pronouncements (FIPP)

Motion

The PSC SC is requested to take note of the report including the overview of FIPP activities 2023/2024 and the status of the projects in the IFPP Strategic Development Plans for 2017-2019 and 2020-2022.

Reflections from the FIPP chair

INTOSAI's work focuses on the development, dissemination, and maintenance of professional pronouncements (principles, standards and guidance) for the public sector audit profession as well as fostering SAIs' capacity development and knowledge sharing. Timely release of professional pronouncements of high quality that covers the needs of the SAIs is essential to continue to strengthen INTOSAIs reputation as a professional standard-setting organisation.

FIPP was established in 2016 to act as a gatekeeper for the ISSAI framework (now the IFPP). This includes follow and facilitate the development of all pronouncements, ensure their technical quality and approve their inclusion in the INTOSAI Framework of Professional Pronouncements (IFPP). Since then, FIPP has developed into an important part of the standard setting "production cycle". This involves ensuring quality of the IFPP by approving new pronouncements and setting the level of requirements for the INTOSAI community in collaboration with the various project groups developing draft pronouncements.

FIPP has now been in place for 8 years. Due process, classification principles, FIPP terms of reference and drafting conventions are important documents in our day-to-day work. Developing standards should be done in a way that ensures global recognition for the standards and for INTOSAI as a standard-setting organization. FIPP has previously conducted an internal self-evaluation of strengths, weaknesses, opportunities and threats (SWOT). However, it is now time to have an external evaluation of the entire standard-setting organization. I look forward to this important work in order to strengthen and further develop the standard setting part of our organization. We can also draw inspiration from other standard setters around the world. I believe there is potential to improve both the efficiency in developing the pronouncements and the quality of the IFPP. This requires a professional and streamlined organization, a strong governance function and SAIs being willing to appoint competent people to participate in this important work.

Collectively, the membership in FIPP should reflect the necessary skills, the different types of public-sector auditing and the diversity of the INTOSAI membership. FIPP members are appointed for a three-year period which can be prolonged, for one or two periods, up to nine years in total. INTOSAI as an organisation is complex and it takes time to get a good understanding and overview of its many committees and roles, procedures and processes. In order for FIPP to fulfill this role it is essential to have available members with solid INTOSAI standard setting knowledge and experience as well as dedicated time assigned to the multifaceted work in the forum.

In 2024 three of the longest standing members of FIPP will retire and in 2025 there will no longer be any original members of FIPP left. This poses a challenge to knowledge retention. In spite of mitigating measures such as a short introduction to the FIPP role for new members, preparative topics on subjects such as the content of the IFPP and the SDP at the FIPP meetings as well as the FIPP web page with extensive information of the SDP projects, due process, working procedures and other important INTOSAI information the balance between rotation and continuity will always be a challenge.

Developing new standards and guidelines requires people who can drive projects, research the issues, facilitate deliberation and balancing views, and find solutions. In addition, there is a need for a secretarial function responsible for documentation, communication and information.

FIPP operates in close cooperation with the Goal chairs. The development of the new SDP (2024-2028) is the result of an inclusive process with periodical meetings between all the Goal chairs, the General Secretariat and FIPP. This has proven to be an effective way of working that in my opinion should be used also for future processes. I believe this has improved the quality of the current strategic development plan, compared to previous SDPs.

In the years leading up to this plan, information from several sources including the Component 1 report and the IDI global stocktaking report highlights the implementation challenges when adopting the ISSAIs. The SDP endorsed by Governing Board last year therefore focuses on the quality of the framework in general and on the ISSAIs especially. It is my hope that the next SDP will help the INTOSAI community gain a better understanding of the ISSAIs and that the initiatives will lead to a smoother implementation in the individual SAIs.

In the process of developing the current SDP, professionalized support was highlighted as a prerequisite for the SDP. The discussions reported to the PSC SC June 2023 focused on two different needs for support:

a. The need for support in the individual project.
b. The need for more secretarial support to ensure standard setting of high quality.

The conclusions from the discussions were that for a) FIPP could improve the relevant templates to clarify what is expected from the project/working group. One example is to update the template for approval of project proposals to ensure the project group would understand what is to be expected from them in developing a new pronouncement including the documentation that needs to be developed. The different initiatives and the related projects will require different kinds of support and qualifications to ensure timely deliveries and progress.

For b) this would be part of a long-term ambition where INTOSAI work as a professional standard setter and is considered so by both internal as well as external stakeholders. This requires a robust, separate secretariat that is not dependent on the SAI hosting the PSC or FIPP but has a robust set-up with a technical support, continuous digital systems, routines and documentation in place and that is easily available when the position as Chair of any of the relevant stakeholders is transferred to another SAI.

The FIPP are now working extensively regarding the update and procedures of improvement of templates and how to give each project individual support through ample guidance.

Moving forward with the initiatives in the SDP, FIPP needs to work closely with the project groups to reach the ambitious goals that have been set for this SDP and to ensure efficiency in our processes.

I look forward to exploring how we together in the INTOSAI community can be more effective and even better in see new solutions where we together can find better and more agile working procedures. FIPP are prepared for this important work, and I look forward to an interesting new year in FIPP.

Forum for INTOSAI Professional Pronouncements

September 2024

Report by the Forum for INTOSAI Professional Pronouncements (FIPP)

The purpose of this report is to inform the PSC SC[1] about: main results of FIPP's activities; status and challenges in projects; and progress of the elaboration of SDP 2023-2025. As the report is presented to the PSC SC prior to the yearly Governing Board meeting, the report covers the period October 2023 - September 2024.

Overview of content

**

1. Status of projects from the IFPP Strategic Development Plan (SDP) 2023-2028

The SDP 2023-2028 was finally endorsed by the Governing Board in November 2023. The SDP includes five initiatives. Together with the Goal Chairs and the General Secretariat, FIPP have developed scoping papers to give a deeper understanding of what the initiatives aim to achieve. FIPP have had initial discussions internally to prepare for these initiatives. The project groups related to the initiatives are now in the making. FIPP will invite project leads to discuss the project plans in due time.

2. Status of projects from the IFPP Strategic Development Plan 2017-2019 and 2020-2022

2023.

a) Pronouncements endorsed by the INTOSAI Governing Board in 2023

- ISSAI 140 is now available in all the official INTOSAI languages and will take effect from January 2025.

b) Pronouncements to be endorsed by the INTOSAI Governing Board in 2024

- GUID 5101 has been out on exposure and FIPP plan to approve the endorsement version in 2024. Estimated to be finally endorsed by the Governing Board in October 2024.

c) On-going pronouncement projects from SDP 2017-2019

- SDP 2.3 Using ISSAIs in accordance with the SAI's mandate and carrying out combined audits. Pending within the PSC

[1] The PSC SC is the governance body for FIPP. The responsibilities of PSC SC regarding FIPP are defined in paragraph 2 of the PSC SC Terms of Refence.

- SDP 2.5 Consolidated and improved guidance on understanding internal control in an audit. Pending within the PSC
- SDP 2.6 Consolidated and improved guidance on reliance on the work of internal auditors. A guidance outside the IFPP have been developed
- SDP 2.7 Guidelines for audits of Public-Private partnerships – and updated Exposure Draft will be presented to FIPP for discussion/approval in late 2024-early 2025.
- SDP 2.8 Consolidating and aligning guidance on IT-audit with ISSAI 100 - the Endorsement version will be appraised by FIPP in 2024 and at the earliest presented for the Governing Board to be finally approved in October 2024

d) Status of projects from the IFPP Strategic Development Plan 2020-2022

The ISSAI 140 Quality Management for SAIs was finally endorsed at the Governing Board 2023 with effective date from January 2025.

3. FIPP meetings

FIPP has carried out 5 sessions of web-meetings in the first half of 2024 and is planning web-meetings in September and October 2024, and one in-person meeting in November/December 2024.

FIPP has in addition invited observers from all three goal chairs (CBC, KSC and PSC) to each meeting in 2023/2024. All FIPP meetings are documented at the FIPP webpage: https://www.intosaifipp.org/fipp-meetings/

FIPP aims to coordinate the future in-person meetings in the best possible way, adjoining other INTOSAI meetings where potential participants attend, in order to be eco conscious as well as prudent with government funding for SAIs participating.

Second half of 2023
FIPP web-meetings – 3 Sessions September 2023
Last meeting in 2023 - FIPP in-person meeting Vienna, Austria 22-23 November 2023 - a combined FIPP meeting and an SDP Joint Seminar for FIPP/GCC/ INTOSAI General Secretariat.

2024
FIPP web-meeting – January 2024
FIPP web-meeting – February 2024
FIPP web-meeting – May 2024
FIPP web-meetings –June 2024
FIPP web-meeting September 2024

Planned meetings
FIPP web-meeting – October 2024
FIPP in-person meeting in Sofia, Bulgaria, 25-29 November 2024

September 2024

On behalf of FIPP

Åse Kristin Hemsen
FIPP chair

Annex 1 On-going pronouncement projects from SDP 2017-2019

No.	Title	Status	Endorsement
#2.3	GUID 5000 Using ISSAIs in accordance with the SAI's mandate and carrying out combined audits	**Project Proposal** conditionally approved at the 12th FIPP meeting December 2019 – An outline of the GUID and the project proposal will be further discussed by FIPP depending on decisions by the PSC. The project is awaiting clarification by the PSC. The project group is on hold.	Not planned
#2.5	GUID 5150 Consolidated and improved guidance on understanding internal control in an audit	A **Project proposal** is being developed by the project group and has been initially appraised by FIPP February 2020. The project is awaiting clarification by the PSC and the subcommittees CAS, FAAS and PAS.	Not planned
#2.6	GUID 5160 Consolidated and improved guidance on reliance on the work of internal auditors	An **updated project proposal** was approved by FIPP in the FIPP web-meetings in September 2020. A guidance on the subject-matter has been published outside the IFPP. The project has been in dialogue with FIPP regarding the placement of the paper where the conclusion was that in the present form the guidance gives good support on the subject outside the framework. The guidance will be reviewed in accordance with all other GUIDs and guidance with the criteria decided after the result of the G-initiative.	
#2.7	GUID 5340 Guidelines on audit of Public-Private Partnerships (PPP)	An **updated Exposure Draft with Explanatory Memorandum** was discussed at the FIPP April 2022 meeting. The conclusion was that the project should be reviewed by the KSC. A new project lead/group composition has been formed in 2023. The project has developed an updated Exposure Draft, which currently is on an alignment round with the relevant Sub-committees PAS and CAS, before FIPP will make an appraisal in late 2024/early 2025.	Governing Board November 2025
#2.8	GUID 5101 Consolidating and aligning guidance on IT-audit with ISSAI 100	**Endorsement version** has been prepared by the project group but based on the exposure comments, FIPP concluded that the GUID was not ready for approval at the 11th FIPP meeting, June 2019. At the 12th FIPP meeting, December 2019, FIPP reviewed the amended endorsement version with a gap analysis and FIPP carried out a new appraisal against the criteria. FIPP concluded that GUID 5101 should not be forwarded to the INTOSAI Governing Board due to the feedback received in the exposure phase. The updated Endorsement version is planned to be appraised by FIPP prior to the Governing Board 2024 for final endorsement.	Governing Board 2024

Annex 2 Status of projects from the IFPP Strategic Development Plan 2020-2022

Component 1 Reviewing and refining the conceptual framework	The conclusion made by the PSC Secr on the Component 1 analysis have been presented as a report to the PSC SC 2022, and the report have been distributed for information to the INCOSAI 2022.	Completed - the analysis of the report is one of three components for the next SDP to build upon
Component 2	The Governing Board approved two projects to be included in the SDP 2020-2022 under Component 2 at the 2020 November meeting after recommendations from FIPP according to due process. • Guidance for implementing INTOSAI P-50 Principles of SAIs of jurisdictional activities (KSC) The project group have been simultaneously working on a project proposal and an exposure draft. The two drafts have been discussed at a number of FIPP meetings in 2021/2022. At the FIPP December 2022 meeting the project group, the KSC and FIPP agreed and concluded that the document Guidance for implementing INTOSAI P-50 Principles of SAIs of jurisdictional activities is already approved by the Forum for Jurisdictional activities and is considered very useful guidance. Due to the proposed content of one of the initiatives in the next Strategic Development Plan 2023-2025 on guidance/GUIDs - the 'G' initiative, and also considering that the Forum already has approved the document, at this stage the document will be a Guidance outside the IFPP rather than a GUID. When the new SDP is adopted, the project group will consider if there is a need for further discussions regarding an addition to the jurisdictional activities in the IFPP. • ISSAI 140 Quality management for SAIs (PSC) The project proposal was approved by FIPP in June 2022. The Exposure Draft, along with the explanatory memorandum, was approved by FIPP February/March 2023 and placed on INTOSAI exposure according to due process. The Endorsement version will be approved by FIPP in September 2023, and will be distributed for a final approval by the Governing Board November 2023	Finalized – endorsed by Governing Board 2023

Component 3	Framework for Competency management	Finalized - Endorsed by Governing Board 2022

Enhancing the membership of the FIPP

A discussion paper

September 2024

INTOSAI PSC | Professional Standards Committee

Contents

Introduction

FIPP candidates and members are currently drawn from three groups of stakeholders:

i. Individual SAI members of INTOSAI;
ii. the IDI, and
iii. staff from INTOSAI SAIs being members of INTOSAI's Committees, Working Groups established under the Committees or the INTOSAI Regions (the latter with the prior authorisation of the employing SAI member of INTOSAI)[1] .

There is no suggestion that FIPP does not function effectively and is not well managed . The purpose of this paper is rather to take a critical look at some aspects of the forum and consider how the PSC could help enhance its capabilities according to the tasks attributed to it in due process, make it better future-proof and, in so doing, add value to its activities.

Any change to the composition of FIPP membership or working arrangements would entail modifications to due process, terms of reference, require discussions with FIPP, the consensus and involvement of the Goal chairs and will need approval by the PSC Steering Committee and ultimately the Governing Board.

We make no concrete recommendations in this document on how to address the issues, but instead suggest reflection points. At this early stage we simply seek the views and comments of the Steering Committee members on which of these points they would wish to pursue further and how. These may be longer-term ambitions which the Goal Chairs and FIPP may choose to enact themselves or could be used for further reflections or initiatives. In the case of the former, the PSC secretariat, in consultation with FIPP and the Goal Chairs, will report to a future Steering Committee meeting with a detailed proposal and a road map for its implementation.

1. Requirements of the INTOSAI strategic plan for the PSC

The PSC is charged with providing, maintaining, and advocating for internationally recognised professional principles, standards and guidance for public sector audits.

Particularly, the PSC is required to assure the consistency, professionalism, quality and relevance of the IFPP, and regularly update the IFPP technical content in response to developments in the audit profession and user feedback (for example, through the Strategic Development Plan)[2].

The PSC is fortunate to have at its disposal three specialised subcommittees, representing the three audit types as set out in the ISSAIs 200, 300 and 400. The professional membership of those bodies is complemented by a range of consultative and advisory bodies to bring in the views of a wider range of stakeholders. We also have a fourth subcommittee specialised in internal control matters.

[1] *FIPP Terms of Reference, paragraph 2.6*
[2] *INTOSAI Strategic Plan 2023 to 2028. Strategic Objective 1.2*

While the PSC has overall responsibility for ensuring the effective operation of INTOSAI's standard-setting activities, the FIPP is responsible for the content and technical quality of the IFPP, either through individual standards or through its input to the SDPs. Collectively, FIPP's membership should reflect the necessary skills, the different types of public sector auditing and the diversity of the INTOSAI membership[3]. FIPP's current membership from SAIs and the IDI fulfils this requirement. However, it is questionable if the views, considerations and needs of the IFPP users, and the users of reports produced in adherence to the IFPP pronouncements, for example governments, parliaments or civil society (some of our wider stakeholders), or from the wider audit profession are sufficiently represented in the FIPP.

Investing in quality stakeholder management

Access to regular wider stakeholder perspectives could broaden the PSC and FIPP's decision-making processes. Establishing dialogues with multiple IFPP stakeholder groups could enrich both the PSC and FIPP's capacity for analysis and bring to the forum multiple points of view and information sources to which the PSC and FIPP would otherwise not have access.

Creating trust and legitimacy through strategic stakeholder engagement is critical, especially if our activities directly or indirectly affect them. Whilst our standards and guidance are targeted in the first instance to audit practitioners, the effects of our pronouncements also impact the users of audit reports or the recipients of the recommendations arising from them. Engagement with groups that are directly or indirectly affected by INTOSAI's standard-setting process may enhance our credibility as a public sector standard-setter.

Policy and practice with other standard setters

Whilst there are no direct comparisons between INTOSAI's standard setting process in other international standard-setting bodies, the composition of some of their comparable committees gives an insight into the diversity and ethos of their membership.

IFAC

The International Auditing and Assurance Standards Board (IAASB) and International Ethics Standards Board for Accountants (IESBA) (the "Boards") have established the Stakeholder Advisory Council (SAC) to provide a forum for them to obtain input from, and engage with, a diverse range of stakeholders on matters relevant to their remits. The objective of the Stakeholder Advisory Council is to provide the Boards at a strategic level with an identification of matters of public interest, and the use of their standards globally and to provide advice on proposals to start new standard-setting projects, including objective, scope and direction of the projects.

The members of Stakeholder Advisory Council represent users that, make decisions on the basis of financial and non-financial information (such as investors, financial analysts, lenders or creditors), preparers and professional accountants in the public

[3] *FIPP ibid*

and not-for-profit sectors, those charged with corporate governance, international and national regulatory and inspection communities, national or international standard-setting organisations, the accountancy profession internationally, governmental and other international organisations, and academics[4].

IIA

The mission of the International Internal Audit Standards Board is to develop, issue, maintain, and promote the International Standards for the Professional Practice of Internal Auditing on a worldwide basis. Its members are drawn from a wide basis with the condition that they all have Certified Internal Auditor certifications.

As such, the IIA does not have an adjacent body reporting on stakeholder views.

Convergence with the discussion paper, "The Engagement of Stakeholders in Professional Standards Setting Process".

At the PSC Steering Committee meeting in September 2023, Messrs Mahmood and Buti presented a discussion paper which colleagues from ARABOSAI and AFROSAI-E had written analysing the *Engagement of Stakeholders in the Professional Standards Setting Process*.

Their paper argued that the engagement of stakeholders in the standards-setting process is crucial because it:

- ensures that the standards reflect the needs and perspectives of all relevant parties,
- promotes the credibility of SAIs and enhances public trust in their work; and
- promotes the adoption and implementation of standards once they are adopted and published.

Based on their research of publicly available documents and following discussions with the World Bank and the Institute of Internal Auditors, the authors posited that stakeholders could be better involved in the standards-setting process by serving on task forces to provide input on specific standards or projects.

Arguably FIPP, consisting of experts who promote public-sector auditing of a high quality to the benefit of users of SAI audit reports and the general public[5], could fall into this category of task force.

Reflection points

i. Should we expand the pool from which FIPP members may apply so to allow the following (up to a pre-determined number) to apply for vacant positions: practitioners from the private sector accounting or audit professions or standard-setting bodies, local civil society groups, local authorities, or other relevant stakeholders?

ii. Should the total number of FIPP members remain at 16?

---

[4] *SSB SAC Terms of Reference, May-2023*

[5] *Due process for INTOSAI Framework of Professional Pronouncements, paragraph 1.1. "Basic definitions and general roles and responsibilities".*

iii. Should we create a pool of potential FIPP members to avoid having to go through an administratively long selection process each year?

2. Knowledge retention

The FIPP terms of reference stipulate that the duration of a FIPP member's mandate is temporary, it was not intended that FIPP members ever become permanent. The consequence is that long-standing members, who have made significant contributions to the work of the forum and who hold much of the "institutional memory" of the forum, are leaving. On the other hand, it allows new colleagues to join with perhaps fresh ideas and innovative energy, from making a contribution to INTOSAI.

A consequence of this is that knowledge retention for FIPP as a body becomes an issue. FIPP needs to have the ability to retain and preserve the knowledge and expertise of its members. Doing so will involve putting strategies and practices in place now to ensure that valuable knowledge, skills, and information are not lost when members depart.

The whole idea of knowledge management is to give structure to the intellectual capital of an organisation, to add to it on a continuous basis and to make it easily accessible for all members of staff. Knowledge management works by, among other things, harnessing the value of the knowledge of individuals in order to generate collective skills. The aim is to make it permanently available, actively supported, encouraged and strengthened by all FIPP colleagues.

At the 24th meeting of the PSC Steering Committee, the PSC, with the help of the other Goal Chairs, committed to helping FIPP to:

1. manage staff turn-over,
2. document processes, principles and final agreements and keep these widely accessible on the website, for example, and
3. continuously work to integrate new(er) FIPP members in the institutional memory of FIPP, in how work is carried out and why.

Reflection points

FIPP is unique as an organisation:

i. what knowledge retention techniques would suit it best?

ii. Is there an added value in setting up a platform where knowledge is consolidated and shared within the Forum. It might contain key documents such as decisions on pronouncements and the key reference documents for each area under the responsibility of the Forum. In addition, it could provide a collaborative space for colleagues, and a repository for different information products: internal presentations, briefs, blog posts, etc.

3. Succession planning for FIPP leadership and other functions

The Goal Chairs are responsible for appointing the chair of FIPP, who will primarily be selected among FIPP`s members[6]. FIPP has been fortunate that during its existence, it has had two excellent Chairs for this sensitive function, both in office for many years. Consideration might be given to whether job rotation (limiting the term of office) for this post might be beneficial for the whole Forum and how potential candidates could be prepared. This could also improve adaptability and teamwork within the FIPP team and would allow other suitable FIPP members to gain a holistic perspective, making them more versatile and valuable assets to the Forum. This would also help to enhance knowledge retention practices.

It would also contribute to making FIPP more future proof by decreasing the risk of individuals leaving the Forum and taking their knowledge and experience with them.

Reflection points

i. Is there any need to rotate the top job(s) within FIPP?
ii. If yes, with which frequency, and what benefits would it bring?
iii. What are the disadvantages?
iv. What is the purpose of selecting the FIPP chair from *primarily* among FIPP members? Where else might we seek a chair?
v. Would it be necessary to offer training/development programmes for new FIPP members?

In a wider sense too, the exercise of succession planning might also be used for other key functions within FIPP, for example secretarial and administrative support as until present these have been supported by the SAI employing the chair.

Reflection points

i. What are the critical / vulnerable / key positions in FIPP?
ii. Are there advantages in identifying potential successors (e.g., targeted calls for expression of interest)?
iii. What competency and skills gaps and training needs are required?

6 FIPP ibid 3.3