Forum for INTOSAI Professional Pronouncements

Agenda for the January 2024 web-meeting of the

Forum for INTOSAI Professional Pronouncements (FIPP)

The agenda is an overview of all agenda-items planned to be discussed during all sessions. Some items will be discussed in several sessions.		
Meeting day **Tuesday 30 January 2024 - 12:00–16:00 CET**		
Agenda Items	**Purpose**	**Output**
Project Proposal / Exposure Draft / Endorsement version submitted from Goal Chair for discussion / appraisal		
Revised Exposure Draft of GUID 5101 on Information Systems Security Audit	To discuss/appraise/approve according to FIPP Working Procedures and drafting conventions	For FIPP to discuss/approve/vote. See Annex 1
Information		
AoB	FIPP Chair	• An introduction to the two new FIPP members: Jared Nyasani and Tiago Costa • Short info about FIPP and FIPP work in 2024 • AoB
Information PSC Secr		
Process with the SDP 2023-2028	PSC Secr	Short status on the work with the core group, the SDP planned work ahead in 2024, possible in-person/web meetings etc
Concluding the meeting		
Summary of activities	FIPP Chair	
Summary of key decisions in the minutes	FIPP Chair	

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

1 Introduction

1. GUID 5101 provides the framework for conducting Audit of Security of Information Systems within the IFPP. The framework laid out in this GUID is consistent with the Fundamental Principles of Public Sector Auditing (ISSAI 100) as well as Guidance on Audit of Information Systems (GUID 5100), which provides the overarching framework for conducting Audit of Information Systems.
2. Supreme Audit Institutions (SAIs) are mandated to audit governments and their entities per their respective audit mandates[1]. Through their activities, SAIs aim to promote efficiency, accountability, effectiveness and transparency of public administration[2].
3. The transition to computerised information systems and electronic processing by auditee entities in the public sector makes it imperative for SAIs to develop appropriate capacity to conduct a thorough examination of controls related to information systems. As part of the audit of Information Systems, there is a need to ensure that controls to maintain confidentiality, integrity and availability of Information Systems and data (i.e. Information Security) have been adopted by public sector entities.
4. Information Technology has made it possible to capture, store, process, retrieve and deliver information electronically, and the delivery mode of public services is rapidly transitioning from physical to electronic. Such services and data are increasingly provided and made available over the Internet and public networks, and hence face exposure to a wide variety of threats, resulting in the increased importance of cyber security. Further, the distinction between Information Technology (IT) and Operational Technology (OT)[3] is getting blurred, and cyber security of critical infrastructure[4] systems is increasingly focused on OT systems.
5. Information security weaknesses may lead to severe damage (legal, reputational/ credibility, financial, productivity, exposure to further intrusions). Such damage may be caused by security breaches, unauthorised external connections, exposure of information (disclosure of corporate assets and sensitive information to unauthorised parties), insider threats or system vulnerabilities. Therefore, it is imperative for SAIs

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

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

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

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

to develop adequate capacity to conduct an examination of information security (including cyber security) either as part of the audit of Information Systems or separately.

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

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

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

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

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

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

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

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

2 Definitions

1. **Audit of Information Systems**[5]: The examination of controls related to IT-driven information systems, in order to identify instances of deviation from criteria, which have in turn been identified based on the type of audit engagement – i.e. Financial Audit, Compliance Audit or Performance Audit.
2. **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.
3. **Cyber Security**: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire

[5] GUID 5100 para 3.2

communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Alternatively, the process of protecting information and assets by preventing, detecting and responding to cyber-attacks.

4. **Integrity**: Guarding against improper information modification or destruction and includes ensuring information non-repudiation[6] and authenticity[7]; 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.
5. **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.
6. **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.
7. **Information Security Management System (ISMS)**: According to ISO-27001, the information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.
8. **Audit of Security of Information Systems/ Audit of Information Security:** Depending on the type of audit engagement (Financial Audit, Compliance Audit or Performance Audit) and the audit scope, the examination of controls related to security of information and assets, to derive assurance as to the maintenance of confidentiality, integrity, and availability.

3 Objectives of this GUID

9. ISSAI 100, 200, 300 and 400 lay down the basic precepts of auditing as related to Compliance Audit, Performance Audit and Financial Audit. These ISSAIs relate to general principles, procedures, standards, and expectations of an auditor. GUID 5100 lays down subject matter specific guidance regarding audit of Information Systems.
10. Audit of information security can be taken as a compliance audit or, in certain circumstances, as a performance audit or financial audit (or as a combined audit). Accordingly, the audit should be carried out as per the applicable principles (ISSAI 200 for financial audit, ISSAI 300 for performance audit and ISSAI 400 for compliance audit).

[6] 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.

[7] 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.

11. If audit of information security is taken up as a compliance audit, the compliance in respect of the subject matter (information security or any specific aspect/ component thereof) to the applicable authorities (policy, procedure, standards, practices etc.) is assessed by auditors.
12. If audit of information security is taken up as part of a financial audit, the criteria for performing such audit would be the financial reporting framework and the conclusion of the audit would be reflected in the audit opinion, and not as a separate conclusion.
13. If audit of information security is taken up as a performance audit or as part of a performance audit, the audit objectives would be related to assessing whether the interventions etc. forming part of the subject matter are performing in accordance with the principles of economy, efficiency and effectiveness and whether there is room for improvement, and the resulting audit conclusions would also need to be mapped to the principles of economy, efficiency.
14. This GUID focuses on compliance audit of information security.
15. While the overall principles and guidance outlined in GUID 5100 are applicable to audit of security of information systems, the objective of this GUID is to provide specific and additional guidance for the compliance audit of information security (including cyber security). Audit of information security can be taken either as a distinct compliance audit or may be part of a larger compliance audit engagement.
16. The contents of this GUID may be applied by auditors in the Planning, Conducting, Reporting and Follow Up stages[8] of the audit process.

4 Scope of the audit

17. The information security audit work will be determined by the objectives and scope of the audit. Elements of such scope of the work could be usefully derived from ISO/IEC 27001: 2013 or other standards/ best practices, as illustrated below:
    a. Information security culture, including leadership and commitment; management direction and policies; information security objectives; organizational roles, responsibilities and authorities (including mobile working, teleworking etc.)
    b. Information security risk management processes, covering
        i. information security risk assessment (including information security risk acceptance criteria, identification, analysis and prioritisation) and information security risk treatment
        ii. Communication (internal and external) and documentation relevant to the information security management system
        iii. Review and continual improvement of information security
    c. Human resources security at different stages from prior to employment, during employment and post-employment
    d. Management and control of information assets, including inventory and classification; rules for acceptable use; transportation, return and disposal
    e. Authentication, authorization and access control – including identify management and authentication, cryptographic controls, and authorization and access controls;

[8] ISSAI 100

f. Physical and environmental security;
g. Network and communication security and cyber security management;
h. Information security incident management and security testing and monitoring;
i. Security as part of system acquisition and development;
j. Operations security, including operating procedures and responsibilities; protection from malware; data backup/ recovery and logging and monitoring;
k. Information security in supplier relationships;
l. Compliance with external and internal requirements.

18. In general, SAIs are not expected to directly conduct Vulnerability Assessment/ Penetration Testing (VA/PT) of the information systems of the audited entity; however, the SAI's information security audit teams should be able to understand the scope of third party VA/PT and associated information security audits, as well as the findings of such audits and their implications. However, this will depend on the SAI's specific mandate, the environment in which the SAI is working (including consideration of the audited entity), the competencies and resources available for VA/PT audit as well as the SAI's professional judgement in determination of the information security audit scope.
19. As part of an information security audit, SAIs are not expected to directly conduct risk identification and assessment for the audited entity's IT systems falling within the audit scope; instead, the SAI may review the audited entity's risk management process (including risk identification, assessment and treatment) for its adequacy and effectiveness. As part of such review, the SAI may highlight certain major risks that have not been appropriately identified and adequately assessed or mitigated.
20. The scope of an information security audit may include assessment of business continuity and disaster recovery planning and implementation, with a view to assessing the "availability" aspect of information services as well as information security during disaster recovery. Alternatively, such aspects may be covered as part of an audit of IT operations management.

5 Planning audit of Information Security

21. SAIs may adopt risk-based audit planning for audits of information security, in line with the processes described in ISSAI 100[9] as well as GUID 5100, depending upon the objectives of the audit engagement.
22. The materiality of an information security audit issue may be decided under the overall framework for deciding materiality in an SAI, as well as specific guidance for materiality in respect of IS audits.

5.1 Sources of audit criteria

23. As part of the planning of information security audits, SAIs may find it useful to identify and adapt, as appropriate, nationally/ internationally accepted information security frameworks for audit risk assessment (to prioritize information security audits and

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

define the audit objectives and scope) and for detailed audit planning of information security audits. Such frameworks serve as sources for audit criteria.

24. These frameworks and standards could include the ISO 27000 series; the CoBIT framework prepared/ updated by ISACA, the standards and frameworks relating to information and cybersecurity prepared by the National Institute of Standards and Technology (NIST); 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..
25. The choice of frameworks and their adaption as appropriate may depend on the specific SAI and country context (including legal and regulatory requirements, if any) as well as the concerned auditee entity/ entities or sector. Where statutory requirements in respect of information security do not exist or are limited in scope and coverage, the SAI may consider adopting/ adapting international or domestic frameworks as best practices for the audit assignment.

5.2 Resources

26. SAIs may ensure that the audit team is composed of members that collectively have the competence to conduct information security audit engagements to achieve the intended audit objectives. The necessary knowledge, skills and competence may be acquired through a combination of training, recruitment and engagement of external resources, per the strategic plan of the SAI.
27. The considerations for allocating human resources for IS audit engagements (including information security audits) are discussed in GUID 5100 and are broadly applicable in the case of information security audits. With regard to information security audits, it may not generally be practicable to establish a dedicated information security audit group in the SAI.
28. Engagement of external resources may be considered by the SAI, depending on the scope of the specific engagement or series of planned information security audit engagements.
29. SAIs may ensure that the information security audit teams collectively, in addition to the collective skill sets required for an information systems auditor as mentioned in Para 5.8 of GUID 5100, have the capacity to perform the illustrative list of tasks below (depending on the scope and objectives of the audit engagement):
    a. Understand the overall architecture of the IT system (including "technology stack" – i.e. suite of technologies used to create the overall solution), as well as its security architecture, including the major security related components; this understanding is essential before initiating an assessment of controls,
    b. Understand the extant laws, rules and regulations, as well as policies and procedures applicable to information security (including data protection and privacy) in the context of the audited entity,
    c. Understand the audit methodology, including relevant auditing standards and guidelines applicable to the SAI, as well as the specific information security criteria against which the audit findings are to be compared,

d. Understand the scope and nature of findings reported through third party information security audits.

Conducting Information Security Audits

30. SAIs may conduct information security audits in line with the processes described in ISSAIs as well as GUID 5100. The additional guidance is offered in respect of conduct of information security aspects.
31. The audit procedures for an information security audit will be designed with a view to focusing on the objectives of deriving assurance as to (a) confidentiality (b) integrity – including non-repudiability and (c) availability with regard to data and IT systems falling within the scope of the audit engagement.
32. The procedures will typically involve a combination of (a) review of documentation (b) observation, walkthroughs, interviews, questionnaires etc. (c) analysis of electronic data (e.g. relating to audit logs of various types). If VA/ PT is to be conducted by the SAI audit team, necessary arrangements with, and agreement of the audited entity for such intrusive testing will have to be made.
33. The scope of most information security audits will generally include the information security culture, policies, procedures, organizational roles etc. For these aspects, the audit team should specifically look at not only the availability of relevant policies, procedures etc, but also whether there is adequate awareness and understanding amongst users and also whether these are being reviewed at appropriate intervals of time and updated, as necessary.
34. The risk management process will also generally be covered in the scope of most information security audits. It would be important for audit to examine the frequency of periodic risk reviews, and also the adequacy of follow-up actions to mitigate the identified and assessed risks. The decision on risk acceptance thresholds (and the consequential acceptance of residual risks) is a management decision.
35. Linked to the risk management process (in particular, risk identification and assessment) are the policies for identification, classification and control of information assets, whether the policies are understood by users and whether such policies are implemented effectively.
36. Wherever authentication, authorization and access controls are covered within the scope of the audit engagement, a key aspect that would be looked at is whether multi-factor authentication (typically in addition to password-based authentication) is implemented, if it is mandated or prescribed by policy or the contract.
37. When logs are to be scrutinized to assess whether access control was implemented as planned, the analysis of logs may involve receipt of data dumps or extracts. Where data dumps are received from the audited entity for electronic analysis, the considerations spelt out in para 6.4 of GUID 5100 with regard to ensuring its authenticity, integrity and non-repudiability may be ensured.
38. For audit of information security incident management, in addition to the review of the processes and documentation relating to incident identification and logging, assessment and resolution, the audit team may consider obtaining feedback on the

adequacy of the resolution from a sample of users (where incidents were identified and ticketed by such users).

39. With regard to information security in supplier/ outsourced relationships, the audited entity retains accountability for information security even if the responsibility for certain IS activities has been outsourced to an external supplier. Further, aspects such as segregation of conflicting duties (e.g. between development, testing and production teams) matter equally, whether the development/ implementation/ O&M of the IT system is being done in-house or through an external supplier.
40. For assessing physical and environmental security, in addition to documentation review, interviews etc., the SAI audit team may consider a physical visit (or joint inspection) of the data centre as a supplementary audit procedure.
(*Illustrative high level audit questions mentioned in Annexure B*)

Reporting on audit of information security

41. The guidance on reporting as per ISSAI 400 as well as the additional guidance under GUID 5100 on reporting (section 7, which also refers to the sensitivity of reporting security risks before necessary mitigating controls have been adopted) may be followed in the case of information security audits.
42. Reporting on information security by auditors must consider the potential business impact of exposing technical shortcomings and security risk in public. In such cases, SAIs may use management letters to share the details of exact risk with the audited entity.

Follow up

43. In addition to guidance in section 8 of GUID 5100, if significant risks in information security management have been identified through this information security audit engagement, SAIs may consider a follow-up audit to assess whether these risks have been adequately assessed.
44. With IT systems increasingly being cloud hosted/ web-based, the time window for risk mitigation, and therefore for conducting a follow up audit, is considerably reduced. The illustrative aspects mentioned in para 6 of this GUID would also be relevant as triggers for a follow up information security audit.

Annexure: A

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

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

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

Annexure B: Suggested High level audit matrix

This Annexure contains high level audit questions on the subject matter of Audit of Information Security as guidance and is only indicative, not exhaustive. Detailed audit questionnaires would depend on the type of Information system, organisation, framework and audit assignment scope etc.

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

		defined, adopted and communicated.	
		Whether information security is ensured by vendors in all interactions.	Depending on the risks, verify whether the audited entity has had the code and modules of the information system developed/ acquired reviewed by skilled internal or third-party resources to ensure that there are no hidden features that may compromise confidentiality, integrity and availability of data.
5	IT Operations	Whether security of IT operations has been defined, adopted and communicated.	Examine contracts/ service level agreements to verify incorporation of non-disclosure, non-compete, non-modification without authorization, non-transmission and other standard provisions related to ensuring confidentiality, integrity and availability of data with parties to whom IT operations are outsourced.
6	Physical and environmental security	Whether security of physical environment of the information system has been ensured.	Verify whether physical barriers (external gates, internal doors, human security guards) which require identification of personnel and restrict access to storage hardware such as servers only to authorized personnel are in place. Facility management is an important aspect of the whole security ecosystem.
7	Network and Communications security	Whether information security is ensured during communication.	Verify whether communication channels ensure encryption of messages, to prevent interception by third parties and loss of confidentiality; also verify use of cryptographic controls for

			digital communications of a formal nature.
		Whether network security architecture is adequate for ensuring information security.	Wherever applicable, existence of cryptographic and other cyber security controls may be examined by auditors.
9	Statutory Compliance	Whether statutory requirements related to information security aspects have been complied with.	Checks for compliance to statutory and regulatory provisions are to be exercised by auditors in all other domains as applicable. Provision may require specific certification/ assurance related to information to be obtained by entities. Scope and validity of such certification may also be examined by auditors.
10	Business Continuity and Disaster Recovery	Whether security aspects related to these processes have been addressed and information security is adequate for DR transition as well as operation.	Auditors may check whether information security facility is adequate during the disaster recovery process.

Sr No	Comment	Update by team
1.	The GUID covers an important subject but is not relevant in its current form.	The draft has been strengthened and made relevant and also covers all recommended areas.
2	The project group needs to decide which audit type to support with this GUID. The scope will need to be changed accordingly.	This GUID primarily focuses guidance on compliance audit of information security (including cyber security). Audit of information security can be taken either as a distinct compliance audit or may be part of a larger compliance audit engagement. This is specifically addressed in the Guidance document. It also adds further specific guidance on what to be done if IS Security Audit is taken up as a part of a Performance/ Financial Audit. Suitable reference in Para 11-15
3 a	If financial audit is to be covered, please be aware of information already covered in the ISSAI 2315 to avoid duplications. The criteria for performing audit of information security as part of a financial audit will be the financial reporting framework. The conclusion of the IS audit will be through an audit opinion and not as a separate conclusion. This should be clearly stated in the GUID.	The current document focusses on Compliance Audit. However, the document also clearly mentions that if IS Security is taken up as a part of financial audit, the criteria for performing such audit would be the financial reporting framework and the conclusion of the audit would be reflected in the audit opinion. Refer Para 12.
3 b	Compliance audit is the most relevant audit type to use when auditing information security. The criteria for such an audit will be ISO standards or other acceptable standards and the conclusion will be drawn on the basis of those criteria	The current document focusses on Compliance Audit. Para 17, section 4 addresses the criteria for the IS Security audit to be ISO/IEC 27001: 2013 or other notified/ applicable standards/ best practices or in the absence of notified standards, best practices or other criteria to be identified by the SAI. A further explanation to clarify the requirements for the audit criteria is also added.
3 c	Performance audit might be less relevant but if PA is part of the GUID, this needs to be linked to audit objective of the three Es.	This GUID focuses on compliance audit of information security (Section 3, Para 14). It also adds further specific guidance on what to be done if IS Security Audit is taken up as a part of a Performance Audit. It specifies that in case of IS Security Audit being done as a part of Performance Audit, the resulting audit conclusions would also need to be mapped to the principles of economy, efficiency. Para 12, Section 3.

4	The GUID can cover audits that aim to provide a conclusion that IT Security Management is in compliance with one or more relevant technical standards on the subject.	The GUID sufficiently provides for audits that are carried out against the technical Standards. Scope of audit (Section 4) and the Sources of audit criteria (Section 5.1) provides guidance on conduct of audit using required technical criteria and for assessment of compliance with one or more relevant technical standards on the subject.
5	The GUID may then be suitable for those SAIs which provide an assurance for IT Security Management.	As above.
6	IT Security Management may be an issue for consideration while conducting financial audits and elements of compliance and performance audits may be considered in course of financial audits. However, this GUID needs to focus on the specific subject area as mentioned above i.e. compliance audit of IT Security Management to be of relevance. Coverage of financial or performance audits might make the GUID complicated and render it inadequate for any of the audits.	This GUID primarily focuses guidance on compliance audit of information security (including cyber security). Audit of information security can be taken either as a distinct compliance audit or may be part of a larger compliance audit engagement. This is specifically addressed in the Guidance document. It also adds further specific guidance on what to be done if IS Security Audit is taken up as a part of a Performance/ Financial Audit.
7	GUIDs on FA and PA may be considered at a later stage under the overall umbrella of GUID 5100.	Agreed. This GUID primarily focuses guidance on compliance audit of information security (including cyber security). Audit of information security can be taken either as a distinct compliance audit or may be part of a larger compliance audit engagement. This is specifically addressed in the Guidance document. It also adds further specific guidance on what to be done if IS Security Audit is taken up as a part of a Performance/ Financial Audit.
8	While reorganising the GUID, the content and substance on the subject need to be suitably strengthened to provide sufficient material to enable all stages of an audit in the subject area. The GUID can also have annexes with more specific guidance (e.g. "security audit tools and techniques", "threat, vulnerability and risk	We agreed with the FIPP's suggestion. The following sections have been added in the updated GUID to address concerns of : • Planning audit of Information Security • Conducting Information Security Audits • Reporting on audit of information security and • Follow up.

	assessments", "audit tasks", "assessing gaps between existing controls and the required controls" or others) in order to add value to the audit.	Further, high level guidance for factors affecting Information Security and suggested High level Audit Matrix have been included to further aid designing IS Security Audits. Regarding addition of further checklists, it would be difficult to determine which checklists to include and which to exclude The current form of the Guidance is also expected to keep the IS Security Audits flexible.
9	Stages of audit like Reporting and Follow-up need to be suitably covered.	Audit reporting and follow-up have been added suitably in Para 41-44
10	GUID 5100 provides overarching Guidance on Audit of Information Systems. This GUID needs to be suitably referenced and distinguished from the contents of GUID 5100.	Suitable references to GUID 5100 have been given in the different paragraphs of the Exposure Draft.