**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 elaborate on how auditors can prioritize elements within their audits based on specific objectives. providing concrete examples of prioritization criteria could enhance practical understanding. | The GUID has been drafted to provide overall guidance & specific 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  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. | | **Risks** | Leakage of sensitive information, loss of important data, damage to the organization's reputation. | Disruption of electronic services, theft of digital data, breaches, significant financial damages. | | **Procedures** | Setting security management policies, employee training, regular audits. | Response plans for cyber Incidents, network and system monitoring, regular software updates. | | **Measures** | Access controls, encryption, backup management, physical controls. | Firewalls, antivirus systems, intrusion detection technologies, network security protocols. |   **Top of Form**  **Bottom of Form** | Difference between Information security and Cyber security is already there as these are mentioned in Definitions. No changes made to the draft |
|  | Generic | 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. * 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 | Specific examples & case studies have been avoided in the GUID. No changes made to the draft |
| 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 |