Overview of Comments on the Exposure drafts of GUID 5101 on "Guidance on Audit of Security of Information Systems"

A. Overview of Comments on the Exposure draft of GUID 5101 on "Guidance on Audit of Security of Information Systems"

SAI	Para No /Topic	Comment	WGITA Remarks
France	Para 1.3	5101, the proposed amendments concerned the development of cyber-attacks and the strengthening of defence measures	Project Team: The suggested comment is agreed to and the following modification is suggested in Para 1.3 *"Such entities also increasingly provide public services in electronic mode over the Internet and public networks, and hence, may face exposure to the risk of attacks from cyber threats which are numerous, sophisticated and persistent."*
	Para 5.3	Strengthening of the control of strategic and tactical security posture	Project Team: The suggested comment is agreed to and the following modification is suggested in Para 5.3 where a footnote has been added *"Including aspects of Strategic Management".*
Lithuania	3.1 Information Security of an information system may be defined as a	Information technology related objects such as network hardware, routers, firewalls,	Project Team: Information Technology refers to both

	set of controls related to policies, structures and processes that aim to prevent unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information stored in an information system. Hence, for an IT driven system, Information Security Management consists of those IT controls that aim to ensure confidentiality, integrity and availability of data in the information system.	backup hardware have a significant impact on information systems security and the data they process, therefore it might be more appropriate to use the broader term "information systems and technologies" or "ICT – information and communication technologies".	hardware and software technologies used for information systems. To ensure consistency in terminologies, proposed to retain the current definitions and terms.
	5.3 Within the above broad objective, the scope of objectives and sub-objectives of an Audit engagement on Security of Information Systems may be drawn from any or all of the following domains[1] of the audited entity. The Annexure to this guidance contains an illustrative list of audit and sub-audit objectives related to these domains- • Organizational Policy on Information Security • Organizational Governance Structure on the subject of Information Security • Security of Information Assets	In line with state level legislation, including national cyber security laws, strategies, technical and organizational requirements.	Project Team: Organization Policy may be drawn from the sources suggested, that would then be Audit Criteria. The list of domains at Section 5.3 is drawn from the source ISO 27001 document and hence, it is proposed to retain the terms.

[1] Adapted from ISO/IEC 27001

	5.5 SAIs may note that Information Security is a horizontal function, which impacts all the other above domains of an entity in which IT plays a crucial role. SAIs may have to consider various technological drivers[2] such as • Platforms and tools used • Network connectivity (internal, third-party, public) • Level of IT complexity • Operational support for security • User community and capabilities • New or emerging security tools that may impact Information Security of the audited entity.	Also emerging new trends, for example, internet of things security.	Project Team: Agreed. It is proposed to modify text to include new and emerging tools and trends, but without specifying any technology by name. Text modified to *"New or emerging security tools and trends".*
	6.2 SAIs may conduct an assessment of IT controls adopted by the audited entity for Security of Information Systems, in order to examine their reliability and sufficiency, using the techniques described in GUID 5100. The scope of the assessment of IT controls for security may include examination that- • Organizational Information Security Policy has been defined, adopted and communicated	And is in line with national requirements and globally accepted standards, frameworks and best practices	Project Team: Organization Policy may be drawn from the sources suggested which could then be the Audit Criteria. The list of controls at Section 6.2 has been mapped to the domains listed under Risk Assessment, which in turn is drawn from the source ISO 27001 document. Therefore, it is proposed to retain the terms.

[2]Cyber Security Fundamentals Study Guide 2015 - ISACA

	•		
	6.2. Contd… • Organizational Information Security Governance structure is in place and functional • Inventory of IT assets has been periodically carried out and that security requirements for each asset type have been identified • Security processes for development, acquisition and maintenance of Information Systems have been defined, adopted and communicated	Including the inventory of the data stored. Levels of confidentiality for each data type are determined and appropriate controls are foreseen.	Project Team: Information Technology assets includes hardware, software and electronic data related to information systems. No changes proposed.
	6.2 Contd… • Application Controls related to security within each information system are adequate and reliable. Such an assessment may include identification of significant application components, identification of the criticality of the application to the entity, review of available documentation, interview of personnel, understanding of application control security risks and their impact on entity, and development of tests to examine	Also, risk analysis (for information security and cyber threats) have to be performed routinely and actions plans prepared.	Project Team: The list of controls at Section 6.2 has been mapped to the domains listed under Risk Assessment, which in turn is drawn from the source ISO 27001 document and hence, proposed to retain the terms. "Risk analysis (for information security and cyber threats) have to be performed routinely and actions plans prepared" would need to be covered as a sub-objective under the head "Measures to ensure confidentiality, integrity and availability of various

	adequacy and reliability of such application controls.		communication modes and channels", which is listed at Section 6.2, for individual IS Security Audit assignments.
	Annexure A Sl. No.7., (Last column) Verify whether Management Roles and their Responsibilities, such as Chief Information Officer, Data Custodian, System Owner, Security Administrator, Security Analyst, etc. have been clearly defined.	Reviews / audits of assigned roles and access privileges are routinely performed by the IT department staff.	Project Team: Agreed to. It is proposed to incorporate text *"Verify whether review of assigned roles and access privileges have been conducted at periodic intervals by the IT Department of the organization."*
Kenya	Annexure	Even though the GUID states that Annexure A is generic, it is not comprehensive despite the column heading intimating that it is comprehensive. a) Either make the Annexure comprehensive or b) Change Column 4 heading to e.g. 'Examples of Sub-Objectives, column 5 to e.g. 'Examples of Assessment to be carried out' c) The objective under column 3 should be precise.	Project Team: Column heading does not indicate that the list is comprehensive. The section above the table clearly specifies that the list is indicative, not exhaustive. No changes are therefore proposed.
SAI Columbia	Header in the first page For more information visit www.issai.org	Specific for cybersecurity the ISO27032 is a good reference https://www.iso27001security.com/html/27032.html	Project Team: We do not agree. The header cannot be modified from the standardized format. References to ISO in the

			document have been reviewed and found to be sufficient.
	1.3 Many audited entities in the public sector process and deal with confidential data related to the State, as well as sensitive data on citizens- demographic, biometric, banking, stock markets, medical history, educational attainment, employment history, taxation, court records, criminal records etc., which are required to be transmitted and stored in a secure manner in the public interest.	This point is important in the Data Governance projects of the Comptroller's Office and in the implementation and compliance with the principle of Demonstrated Responsibility or Accountability.	Project Team: This is a General Comment. Agreed to. No change is required.
	1.3 The custodians of such information systems need to ensure that the information is available when required and used only by authorized personnel for intended purposes. Therefore, it becomes imperative for an SAI to develop an appropriate capacity to conduct a thorough examination of controls related to Security of Information Systems in the public sector.	In the ISO2700 there are 3 items: confidentiality, integrity and availability. Integrity is important concept and is missing https://www.iso.org/isoiec-27001-information-security.html	Project Team: GUID contains references to Confidentiality, Integrity and Availability. No changes are proposed.
	3. Definitions	It is suggested to include more basic definitions, such as "Information", "Controls", "information systems", "confidential, classified or reserved	Project Team: The GUID is intended for SAI practitioners who intend to take up IS Security Audits. The current

		information" in accordance with local regulations, among others.	level of granularity of definitions has been reviewed and no changes are proposed.
	3.2 External attacks on such information systems-which may either hosted on or connected to the Internet-may be initiated by malicious individuals, state sponsored entities, or groups who have an interest in the data or want to disrupt business operations.	For cybersecurity assessments there a good element in https://ics-cert.us-cert.gov/Assessments also an interesting tool (CSET) https://ics-cert.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_CSET_S508C.pdf	Project Team: Agreed to. *It is proposed to include this as a reference in the footnote for assessments "Assessment using Cyber Security Evaluation Tool (CERT-US)".*
	3.2 Since many public sector information systems collect and store sensitive information on citizens, it is imperative that such information systems adopt appropriate Cyber Security measures. Such Cyber Security measures may include key functions (Footnote 4) concerned with incident management,	Also some elements of the NIST https://www.nist.gov/ like cybersecurity https://www.nist.gov/topics/cybersecurity and forensic https://www.nist.gov/topics/digital-evidence	Project Team: The level of granularity of references has been reviewed and no changes are proposed.
	3.2 • Response initiation after learning of security events • Recovery on time from compromised capabilities and services	These components are directly related to the attention of Security Incidents, the manual and other documents that comprise it.	Project Team: This is a General Comment. No change is required.
	3.3 Audit of Security, including Cyber Security, of Information Systems may therefore be defined as a subject matter	ISO 2700 (information security) has a standard to certify auditors, then could be a good element to have certified people to perform this kind of exercises in order to	Project Team: The suggestion is noted. But this is a SAI specific initiative, and may not be required to be included in the GUID.

	specific audit engagement involving the examination of IT controls which are part of Information Security Management, in order to identify instances of deviation from criteria, which have in turn been identified based on the type of audit engagement.	handle the best practices from different edges	
	3.3. For example, the auditor intends to draw assurance	It is suggested that the auditor is equally trained in issues of classification of information assets and protection of personal data, or that the audit team has a trained member in these issues to determine security levels and identify vulnerabilities.	Project Team: Section 1.3 specifies that SAIs may need to build capacity to conduct IS Security Audit engagements. However, content of training requirements of personnel for these engagements is beyond the scope of the document.
	5.3 Within the above broad objective, the scope of objectives and sub-objectives of an Audit engagement on Security of Information Systems may be drawn from any or all of the following domains of the audited entity. The Annexure to this guidance contains an illustrative list of audit and sub-audit objectives related to these domains- • Organizational Policy on Information Security	It is suggested to include the Personal Information Treatment Policy	Project Team: The domains are drawn from the source ISO 27001 document and hence, proposed it is proposed to retain the list as per the source. It is felt that Policy on security of personal information would be covered as a component of overall Organizational Policy on Information Security.
	5.3.	There are other domains missing: BYOD, mobile, Telework, cryptography, incident management, access controls, relation with providers, acquisition and development of	Project Team: The GUID is intended to be technology-agnostic, so that it does not require frequent updates.

	• Security aspects in Application Controls in individual information systems	information systems, (in short all of the ISO 27000) not optional. Could be used the phrase " when applicable"	Project Team: Cryptography would be covered under Communications Management domain. Development, Acquisition and Maintenance of Information Systems is listed as a separate domain. Relationship with service providers would be covered under IT Operations domain. No changes are therefore proposed.
	6.2 SAIs may conduct an assessment of IT controls adopted by the audited entity for Security of Information Systems, in order to examine their reliability and sufficiency, using the techniques described in GUID 5100.	Similar to the comment for 5.3 item	Project Team: The controls listed under Section 6.2 have been mapped to the domains listed under Risk Assessment. No changes are therefore proposed.
	6.2. The scope of the assessment of IT controls for security may include examination that-	A reference to metrics in security is the book "Security Metrics. Replacing Fear, Uncertainty, and Doubt" author Andrew Jaquith, Addison-Wesley	Project Team: Level of detail proposed is not consistent with the overall tone and the source documents of the GUID.
	6.2. • Organizational Information Security Policy has been defined, adopted and communicated	Likewise, it is suggested to include the Personal Information Treatment Policy in these standards.	Project Team: It is felt that Policy on security of personal information would be covered as a component of overall Organizational Policy on Information Security.

	6.2 • Security measures for screening of candidates before recruitment, training and sensitization of human resources on information security aspects, definition of various roles and segregation of roles, and security measures to be enforced on termination of employment, have been adopted • Measures to ensure confidentiality, integrity and availability of various communication modes and channels have been adopted	Items related to the documents provided in the implementation of the Data Protection Regime, that is, contractual clauses and confidentiality agreement.	Project Team: Input is not clear. No draft modification has been suggested either. No changes are therefore proposed.
	8.1. The guidance for follow up would broadly be similar to the requirements described in GUID 5100.	This document has a good guide with another links and Tools https://www.iso27001security.com/ISO27k_Guideline_on_ISMS_audit_v2.docx	Project Team: We have sufficient references at Footnotes 7 and 8, from the same source, i.e. ISO 27000.
	Annexure Sl.No.1	It is suggested that the Personal Information Treatment Policy be included in the analysis, taking into account that a large part of the Entity's information assets are related to personal data.	Project Team: It is felt that Policy on security of personal information would be covered as a component of overall Organizational Policy on Information Security.
	Sl No 4 Item 3 Col 3 & 4 Whether maintenance vendors are provided access only to those modules	This corresponds to the immediate fulfillment of the data protection law, its legal basis is found in literals d) and e) in accordance with the principles contained in article 4 of law 1581 of 2012.	Project Team: The proposal is not clear. No changes are therefore proposed.

	of the information system and only that data which is required to carry out the maintenance function.		
	Sl No 4 Item 4 Col 3 & 4 Whether security requirements of the organization are incorporated into contracts/ service level agreements with vendors for these processes.	This corresponds to the immediate fulfillment of the data protection law, its legal basis is mainly found in literals b), d), e), f), g) and h) of article 4 of law 1581 of 2012.	Project Team: The proposal is not clear. No changes are therefore proposed. The same may be SAI specific. No changes are therefore proposed.
	Sl No 9 Verify documentation on internal communication on this subject, to all stakeholders.	Including those related to the principle of demonstrated responsibility or accountability	Project Team: No changes are proposed.
IIA	General – Definitions Para 1.2	In general, The IIA suggests in reference to Guidance on Audit of Security of Information Systems that the revision maintains clear definitions of, and references consistently, Information Systems Security and Cyber Security. Given the inconsistencies in the exposure draft definitions, for example of information systems, The IIA also suggests item 1.2 be removed to avoid any future misalignment between guidance and the WGITA-IDI Handbook on IT Audit.	Project Team: The GUID is higher in hierarchy compared to the Handbook. The Handbook has to ensure alignment with the GUID and the higher level ISSAIs as and when updated. GUID is specifically intended to bridge ISSAIs with the Handbook. So Para 1.2 is proposed to be retained.
	General	Equipping the team with generalized knowledge for technical exposure, SAIs may also want to consider how this knowledge will be sustained and react to changes in technology and information systems. This may be pertinent to increasing	Project Team: Input to the draft GUID at this stage of the drafting process is not clear. No suggested draft paragraph has been forwarded for consideration. Issues related to

		awareness of cloud-based information systems provided as software as a service (SaaS). The IIA is aware that information systems providing end-to-end finance and ERP applications for small to medium enterprises are migrating at an increasing pace to cloud-based SaaS solutions. With many information systems no longer being hosted locally and provided in the cloud as SaaS, the auditee may wish to take an alternative view of risk for items that they lose control of as a SaaS user, such as management of users and passwords and where data is stored and backed up. There may also be international regulatory considerations regarding data protection and information governance within constituent countries. For EU member states, this is prescribed by the General Data Protection Regulation (GDPR). This may provide SAIs with an opportunity to address the strategic importance to attach to information system security relative to cyber security, noting that the former may prove more of an imperative from the auditees' risk profile.	information systems deployed as Software as a Service can be covered under the domain Asset Management, which is listed as Section on Risk Assessment. However, a tentative listing of the issue has been indicated in the Annexure under the Asset Management Domain. Project Team: Input is not specific to the draft under consideration.
Mexico	Para 3.1 Definition	This definition is almost the same as cybersecurity (see NIST definition and 3.2 there is not a big difference). In this case, maybe the GUID could be renamed as Guidance of Cybersecurity.	Project Team: We do not agree with the point of view expressed.

		NIST definition of Cybersecurity "the prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems" If the GUID remains the same, what are the difference between Information Security and Cybersecurity in the perspective of INTOSAI? The main difference between information security and cybersecurity is that information security also takes in consideration other sources of information such as paper, knowledge and not only digital information. In all the document's content, the difference between Cybersecurity and Information security it is not clear, so it is recommended to define the scope of the GUID.	Project Team: We do not agree. The main difference is that Information Security covers information systems which may or may not be connected to the Internet, while Cyber Security covers information systems which are either connected to the Internet, or hosted on the Internet itself, as a cloud-based solution. Project Team: It is proposed to slightly modify Section 3.2 as follows- *"Cyber Security*

			Management may be defined as a set of controls related to policies, structures and processes that aim to protect digital assets[3]- hardware and information which are either hosted on or connected to the Internet- of information systems from damage, unauthorized access or modification, or exploitation[4] from external attacks initiated by malicious individuals, state sponsored entities, or groups who have an interest in the data or want to disrupt business operations."
	Para 5.3 Domains	It is important to consider other security domains such as: Third party and outsourcing Supply chain Incidence response Security on Cloud Security on IOT	Project Team: These aspects would be covered under the existing domains listed- Third party outsourcing- IT Operations Supply Chain- Development, Acquisition and Maintenance of Information Systems Security on Cloud- Asset Management Security on IOT- Application Controls and Communications Management.

[3]Cyber Security Fundamentals Study Guide 2015 - ISACA
[4] Glossary of terms, US-CERT

	Para 5.3	To add Security aspects in the Business Continuity and Disaster Recovery Management processes **and resilience**	Terms are drawn from source document ISO 27001. It is proposed to retain the same.
	Annexure A	Although the Annex is indicative and not exhaustive, it is preferred to provide a list of recommend IT controls from frameworks such as: ISO 27001, ISO 27032, COBIT, NIST Cybersecurity Framework, CIS.	Project Team: Agreed to. It is proposed to include references as a footnote to the Annexure.