Guidance pronouncements (GUIDs) are issued by INTOSAI, the International Organisation of Supreme Audit Institutions. For more information visit *www.issai.org*

INTOSAI

Exposure Draft

Guidance on Audit of Security of Information Systems

November 2018

I N T O S A I

INTOSAI General Secretariat – RECHNUNGSHOF
(Austrian Court of Audit)
DAMPFSCHIFFSTRASSE 2
A-1033 VIENNA
AUSTRIA
Tel.: ++43 (1) 711 71 • Fax: ++43 (1) 718 09 69

E-MAIL: intosai@rechnungshof.gv.at;
WORLD WIDE WEB: http://www.intosai.org

Table of Contents

1. Introduction

1.1 GUID5101 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), Performance Audit Principles (ISSAI 300),Compliance Audit Principles (ISSAI 400) and Guidance on Audit of Information Systems (GUID 5100).

1.2 GUID 5101 introduces concepts and guidance on Audit of Security of Information Systems, including Cyber Security, which are further elaborated in detail for the benefit of practitioners in SAIs in the WGITA-IDI Handbook on IT Audit.

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. 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.

2. Objectives of this GUID

2.1 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. While GUID 5100 lays down subject matter specific guidance on Audit of Information Systems, including the domain of Security of Information Systems, the objective of this GUID is to provide further procedural guidance to auditors on conduct of audit areas specific to Security of Information Systems.

2.2 The contents of this GUID may be applied by auditors in the Planning, Conducting, Reporting and Follow Up stages[1] of the audit process.

3. Definitions

3.1 Information Security of an information system may be defined as a 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.

3.2 Cyber Security Management may be defined as a set of controls related to policies, structures and processes that aim to protect digital assets[2]- hardware and information-from damage, unauthorized access or modification, or exploitation[3]. 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. Since many public sector information systems collect and store sensitive information on citizens, it is imperative that such information systems adopt

[1]ISSAI 100

[2]Cyber Security Fundamentals Study Guide 2015 - ISACA

[3] Glossary of terms, US-CERT

appropriate Cyber Security measures. Such Cyber Security measures may include key functions[4] concerned with incident management, such as

- Identification of risk levels applicable to systems, assets, data and capabilities
- Protection of critical infrastructure and services from the impact of potential threats
- Detection of occurrence of a security events
- Response initiation after learning of security events
- Recovery on time from compromised capabilities and services

3.3 Audit of Security, including Cyber Security, of Information Systems may therefore be defined as a subject matter 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. For example, the auditor intends to draw assurance

- As part of a Financial Audit, that the IT driven system is secure enough to ensure adherence to the accepted financial reporting and regulatory framework.
- As part of a Performance Audit, that the IT driven system is secure enough to enable the interventions, programmes and institutions perform in accordance with the principles of economy, efficiency and effectiveness.
- As part of a Compliance Audit, that the IT driven system is secure enough to ensure compliance with the laws/ regulations which are applicable.

4. Scope

4.1 This GUID may be used by auditors to conduct Financial/ Performance/ Compliance Audits on the specific subject matter of Security of Information Systems.

4.2 This guideline provides further guidance on how Audit of Security of Information Systems could be addressed by using financial/ performance/ compliance auditing and does not contain any further requirements for the conducting of the audit.

[4]Adapted from Cyber Security frameworks by the National Institute of Standards and Technology (NIST) and the European Union Agency for Network and Information Security (ENISA)

5. Planning Audit of Security of Information Systems

5.1 SAIs may adopt risk based audit planning for examining the security of Information Systems, in line with the process described for Financial Audit (ISSAI 200), Performance Audit (ISSAI 300), Compliance Audit (ISSAI 400) and Audit of Information Systems (GUID 5100).

5.2 The aim of an Audit engagement on Security of Information Systems is to examine the IT controls adopted by the audited entity in its information systems in order to ensure confidentiality, integrity and availability of information.

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[5] 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
- Security in the processes of Development, Acquisition and Maintenance of Information Systems
- Security of IT Operations
- Security of Physical Environment
- Security aspects related to Human Resources involved with Information Systems
- Security of Communications Management
- Security aspects related to Statutory Compliance requirements
- Security aspects in the Business Continuity and Disaster Recovery Management processes
- Security aspects in Application Controls in individual information systems[6]

5.4 Auditors may consider adapting from existing Information Security frameworks[7], for analysis of potential audit objectives. An indicative, but not exhaustive list of objectives and sub-objectives for each of the above domains is at Annexure A.

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[8] 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.

[5] Adapted from ISO/IEC 27001

[6] Application Controls are automated or manual procedures incorporated into an IT driven system which relate to validation of input data, accurate processing of data, delivery of output data and controls related to integrity of master data.

[7] Annexure on Reference control objectives and controls in ISO/IEC 27001; Part VI of "Information Security Management Audit Program" by ISACA

[8] Cyber Security Fundamentals Study Guide 2015 - ISACA

6. Conducting Audit of Security of Information Systems

6.1 Auditors may adopt the processes described for Financial Audit (ISSAI 200), Performance Audit (ISSAI 300), Compliance Audit (ISSAI 400) and Audit of Information Systems (GUID 5100), while conducting audit of Security of Information Systems.

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
- 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
- Processes for security of IT Operations (in-sourcing, out-sourcing, service agreements) have been defined, adopted and communicated
- Measures to ensure physical security and secure the intended physical working conditions have been adopted.
- 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
- Measures for security of Statutory Compliance requirements have been adopted
- Measures for security of Business Continuity and Disaster Recovery Management processes have been adopted
- 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 adequacy and reliability of such application controls.

6.3 The assessment of IT controls related to Information Security may cover the audited entity's policies, processes, people and systems, in line with the Audit objectives. This comprehensive assessment may be adapted by SAIs from existing Information Security frameworks[9] or by developing appropriate new frameworks. An indicative, but not exhaustive list of assessments mapped to sub-objectives for each of the above domains is at Annexure A.

7. Reporting on Audit of Security of Information Systems

7.1 Since an audit engagement on Security of Information Systems is drawn from one or more of the main types of Audit, Auditors may consider the reporting requirements for such Audit engagements to be on par with those for Financial Audit (ISSAI 200), Performance Audit

[9] Annexure on Reference control objectives and controls in ISO/IEC 27001:2013; Part VI of "Information Security Management Audit Program" by ISACA

(ISSAI 300) and Compliance Audit (ISSAI 400). The guidance for reporting would broadly be similar to the requirements described in GUID 5100.

8. Follow Up

8.1 Since an audit engagement on Security of Information Systems is drawn from one or more of the main types of Audit, Auditors may consider the follow up requirements for such Audit engagements to be on par with those for Financial Audit (ISSAI 200), Performance Audit (ISSAI 300) and Compliance Audit (ISSAI 400). The guidance for follow up would broadly be similar to the requirements described in GUID 5100.

Annexure A- Indicative Audit Matrix

This Annexure contains generic objectives on the subject matter of Audit of Information Security as guidance and is only indicative, not exhaustive. For more detailed Audit checklists and Audit matrices for each of the IT domains and related security aspects, SAIs may refer to the WGITA- IDI Handbook on IT Audit.

Sl No	Information Security Domain	Objective	Sub-Objective	Assessment to be carried out
1	Organizational Information Security Policy	Whether such policy is defined, adopted and communicated.	NA	Verify documentation for clarity in definitions and objectives, verify adoption by Competent Authority and verify communication/ publication/ notification to all stakeholders.
2	Organizational Information Security Governance structure	Whether such structure is in place and functional.	Whether such a governance structure has been made clearly responsible for all issues related to Information Security.	Verify documentation for 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.	Verify documentation for clarity in terms of individual personnel, roles and responsibilities for each personnel and reporting hierarchy for escalation of issues.
			Whether the governance structure is reviewing issues related to Information Security at periodic intervals and recommended action is being taken on issues identified.	Verify documentation to examine frequency and agenda for meetings taken by the governance structure, list of issues identified as requiring action to be taken and actual action taken on the same.
3	Asset Management	Whether inventory of IT assets has	Whether inventory of all IT assets of the	Verify system module on materials management, inspection reports and other

		been periodically carried out and that security requirements for each asset type have been identified.	organization has been carried out at periodic intervals.	documentation related to inventory of IT assets. Examine on sample basis to verify completeness of list of assets is correct and whether the same is maintained up to date.
			Whether IT assets have been classified on the basis of criticality to organizational requirements.	Verify system module/ documentation to examine whether IT assets are classified on the basis of replacement cost, cost to organization in case of failure or any other metric.
			Whether security requirements for each asset type have been identified.	Verify system module/ documentation to examine whether requirement of augmentation of capacity of assets for each asset type, list of assets for each asset type which are required to be replaced due to technological obsolescence, list of assets for each asset type which are to be decommissioned as they are no longer secure from new external threats have been identified at periodic intervals.
4	Development, acquisition and maintenance of Information Systems	Whether security aspects for each of these processes have been defined, adopted and communicated.	Whether criteria for development versus acquisition decision for information systems includes criteria related to ensuring information security.	Verify whether cost benefit analysis carried out to enable decision making on development versus acquisition has taken into account the indirect cost of ensuring security of information shared with development vendor or supplier vendor in case of acquisition, as the vendors in either case would need access to at least historical data for conducting user acceptance tests and other tests.
			Whether information systems developed using vendors/ acquired from supplier vendors have been	Verify whether 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

			reviewed to prevent attacks through hidden features.	compromise confidentiality, integrity and availability of data.
			Whether maintenance vendors are provided access only to those modules of the information system and only that data which is required to carry out the maintenance function.	Verify whether access controls have been implemented in the information system to prevent maintenance vendor from causing unauthorized changes to the information system that may compromise confidentiality, integrity and availability of data.
			Whether security requirements of the organization are incorporated into contracts/ service level agreements with vendors for these processes.	Examine the 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.
5	IT Operations	Whether security of IT operations has been defined, adopted and communicated.	NA	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 Environment	Whether security of physical environment of the information system has been ensured.	Whether physical access to the storage hardware for the information system is restricted to authorized personnel only.	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.
			Whether physical access to the client locations from which logical	Verify whether physical barriers (external gates, internal doors, human security guards) which require identification of

			access to stored data is possible is restricted to authorized personnel only.	personnel and restrict access to storage hardware such as servers only to authorized personnel are in place.
			Whether physical environment for storage of hardware for information systems can maintain intended physical conditions such as temperature, humidity, clean air, moisture and pest free environment.	Verify whether construction design, materials and layout are adequate to ensure moisture and pest free environment. Verify whether Heating, Ventilation and Air Conditioning (HVAC) equipment is in place, functioning correctly and have been serviced at regular intervals to ensure maintenance of desired temperature, humidity and clean environment.
			Whether provision for continuous supply of electric power and emergency back- up supply have been made.	Verify whether regular and emergency electric power supply are in place and are adequate to reduce risk of power outage to within acceptable level.
7	Human Resources	Whether security aspects related to human resources involved with information systems have been addressed.	Whether adequate training has been imparted to human resources on the importance of maintaining confidentiality, integrity and availability of data.	Verify whether regular training has been imparted on aspects such as creating a culture of security awareness, importance of non-disclosure and non-transmission of information to unauthorized personnel to maintain confidentiality, importance of modifying data only after obtaining due authorizations to maintain integrity of data and non-sharing of passwords and other login credentials to prevent denial of service attacks by malicious users.
			Whether roles and access privileges for each user are clearly defined.	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.
			Whether segregation of roles has been implemented to ensure checks and balances.	Verify whether there is a clear segregation of roles to prevent conflicts of interest, especially those which in conjunction may create scope to violate confidentiality, integrity and availability of data.
8	Communications Management	Whether security aspects related to communication modes and channels have been addressed.	Whether communication messages are encrypted.	Verify whether communication channels ensure encryption of all messages, to prevent interception by third parties and loss of confidentiality.
			Whether communication messages can be disowned by sender at a later point of time.	Verify whether communication channels have incorporated feature of non-repudiation.
			Whether peak concurrent user limit has been defined.	Verify whether peak concurrent user limit has been defined and is operational, to prevent additional users from concurrently accessing the information system but ensuring that availability of data is not compromised for the users up to the defined limit at any point of time.
9	Statutory Compliance	Whether statutory requirements related to information security aspects have been complied with.	Whether statutory compliance requirements have been communicated internally by the audited entity.	Verify documentation on internal communication on this subject, to all stakeholders.
			Whether internal responsibility centres for ensuring statutory compliance have been notified.	Verify documentation on internal communication on this subject, to all stakeholders.
			Whether statutory	Verify whether each statutory requirement has been

			compliance requirements related to information security have been mapped to programming logic/ internal controls of information systems.	adequately mapped to programming logic/ internal controls within the information systems used by the audited entity.
			Whether status of compliance with statutory requirements are reported as per prescribed intervals to appropriate authorities.	Verify whether reports on status of compliance/ exceptions are filed with prescribed appropriate authorities, by the audited entity.
10	Business Continuity and Disaster Recovery Management.	Whether security aspects related to these processes have been addressed.	Whether off-site back up location also has similar physical security arrangements as main site.	Verify whether adequate arrangements have been replicated for off-site location.
			Whether periodicity of back up has been defined in line with security risk.	Verify whether periodicity of back up is commensurate with function and criticality of the information system to the organization. For information systems which rely on real time data collection, storage and processing, having a live mirror site may be more appropriate than once a day back up, even if such back up costs are high.
			Whether back up site is reasonably secure from natural disasters such as earthquakes and tsunamis.	Verify whether back up site is located in relatively low risk seismic zone and where risk of such natural disasters is acceptably low.
			Whether mock drills to use the data stored in back up location have been conducted.	Verify whether data from back up off-site has been periodically tested for use at least in test environment, so that all users and personnel are familiar with the

				processes to be followed for business continuity.
11	Application Controls	Whether adequate application controls have been adopted in the information system.	Whether authorizations and access privileges have been clearly defined.	Verify the master data of personnel who have been authorized to access various types of data, and examine for deviation from the definitions.
			Whether authentication of personnel has been carried out correctly before providing viewing access to data.	Verify whether personnel are able to access data as per authorizations, only on presenting correct credentials such as passwords or biometrics, and examine for deviation from the same, from the transactions data.
			Whether modification of data has been carried out only by authorized personnel.	Verify, from the user logs, whether modification to data has been carried out only by those personnel who had authorizations to make such modifications.
			Whether personnel are authorized to access or modify data from any client location or at any time.	Verify, from user logs and time stamps, whether any personnel, including authorized personnel, have accessed/ made modifications to the data from locations apart from their work/ home sites and outside of defined working hours.
			Whether personnel are authorized to transmit/ stake personal back up of data.	Verify, from user logs and time stamps, whether any personnel, including authorized personnel, have accessed/ made modifications to the data and subsequently transmitted the same through any communication mode outside of work/ taken personal back up of the data.