SAI ITMA

SUPREME AUDIT INSTITUTION
INFORMATION TECHNOLOGY MATURITY ASSESSMENT

SAI ITMA

Version 2.0

June 2024

PILLARS, LEVELS & REQUIREMENTS

Developed by:

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by:
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

INTOSAI IDI
DEVELOPMENT INITIATIVE

In collaboration with:

OLACEFS | CCC
Fuerza Tarea sobre Geotecnologías

AFROSAI-E

As a federally owned enterprise, GIZ supports the German Government in achieving its objectives in the field of international cooperation for sustainable development.

Published by:
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn, Germany

Sector Programme Good Financial Governance
Friedrich-Ebert-Allee 36
53113 Bonn Germany

E sai-itma@giz.de
I www.giz.de

Editor: GIZ Sector Programme "Good Financial Governance"

Contributors: Davit Shavgulidze (main author), INTOSAI Development Initiative, OLACEFS Capacity Building Committe, AFROSAI-E Secretariat, Sector Programme Good Financial Governance

The publication is supported by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, Sector Programme Good Financial Governance, on behalf of the German Federal Ministry for Economic Cooperation and Development (BMZ).

Bonn, June 2024

Abbreviations, Acronyms and Glossary

Application	Type of software or computer program designed to perform a group of functions, tasks, or activities to support user tasks.
Big Data	Big data refers to extremely large datasets that may be analysed computationally to reveal patterns, trends, and associations, especially relating to human behaviour and interactions
CAATs	Computer Aided Audit Techniques
CCC	OLACEFS Capacity Building Committee (*Comité de Creación de Capacidades*)
CISA	Certified Information Systems Auditor (CISA) issued by the ISACA
Cloud Computing	A network of remote servers hosted on the Internet to store, manage and process data, instead of a local server or a personal computer.
Data Analytics	The science of analyzing raw data to draw conclusions about that information.
Data model (including geographic ones)	Logical and physical definition of how the data will be stored and how it will be accessed.
Databases	Set of data belonging to the same context and systematically stored for later use.
DP / CD	Development Partners (*Cooperantes de Desarrollo*)
EGDI	E-Government Development Index issued by the United Nations
EUROSAI	European Organization of Supreme Audit Institutions
Facilitators	Person or persons who have the task of guiding the entire SAI ITMA implementation process.
FPO World	Finance Performance Oversight (consulting company that developed the first version of SAI ITMA)
Geographic Databases	Set of geographic data organized in such a way as to allow analysis and management of geographically referenced information within Geographic Information System (GIS) applications.
Geographic Information Systems	Any information system capable of integrating, storing, editing, analyzing, sharing and displaying geographically referenced information.
Geotechnologies (Geographic Information Science & Technology)	Remote sensors, location systems, matrix data and vector data, GIS. They are included within the concept of Information Technology according to GUID 5100.
GIT	Geographic Information Technology
GIS	Geographic Information Systems (software applications)
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH
GUID	INTOSAI Guidelines (GUIDs) are issued by the International Organization of Supreme Audit Institutions (INTOSAI) as part of the INTOSAI Framework of Professional Pronouncements.
Help desk	Center of attention to users, the service desk is the single point of contact between the IT service provider and users for day-to-day activities.
ICT	Information and Communications Technology
IFPP	INTOSAI Framework of Professional Pronouncements
INCOSAI	International Congress of Supreme Audit Institutions

Information Systems	Information Systems can be defined as a combination of the strategic, managerial and operational activities carried out in the collection, processing, storage, distribution and use of information and its related technologies. (GUID 5100)
Information Systems Audit	The Information Systems audit can be defined as the examination of the controls related to Information Systems based on Information Technology, in order to determine cases of deviation from the criteria, which in turn have been identified on the basis of the adopted audit type, that is, the financial audit, the compliance audit or the performance audit. (GUID 5100)
Information Technology	Information Technology includes hardware, computer programs (software - GIS), communications and other *facilities* used to enter, store, process, transmit and issue data in any form. (GUID 5100)
INTOSAI	International Association of Supreme Auditing Institutions
INTOSAI-P	INTOSAI Principles (INTOSAI-P) are part of the INTOSAI Framework of Professional Pronouncements (IFPP) and they consist of Founding Principles and Main Principles. The founding principles have a historical significance and specify the role and functions to which Supreme Audit Institutions (SAIs) should aspire.
ISA	International Standards on Auditing
ISO	International Organization for Standardization
ISSAI	International Standards of Supreme Audit Institutions
ITASA	IT Audit Self-Assessment
ITSA	Information Technology Self-Assessment
ITWG	EUROSAI IT Working Group
Map	Geographical representation of the Earth, or part of it, on a flat surface, according to a scale.
Metadata	It literally means "beyond the data," which can be interpreted as data describing the data.
OLACEFS	Organization of Latin American and Caribbean Supreme Audit Institutions (*Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores*)
QM	Quality management
QMS	Quality Management System (processes focused on achieving quality policies and objectives)
Personnel clearance procedures	Procedures for personalized attention for software inquiries.
SaaS	Software as a Service, a cloud-based software distribution model centralized on a server.
SAI	Supreme Audit Institution
SAI ITMA	Supreme Audit Institution Information Technology Maturity Assessment developed by GIZ
SAI PMF	Supreme Audit Institutions Performance Measurement Framework developed by IDI
SDG	Sustainable Development Goals defined by the United Nations
Spatial Analysis	A process in which problems are geographically modeled, results are obtained through computer processing, and then those results are explored and examined.
Spatial information	All data that has a geographic reference associated with it, in such a way that we can find exactly where it is located within a map.
TCU	Federal Court of Accounts (SAI of Brazil)
WebGIS	Distributed information system application, comprising at least one server and one client, where the server is a GIS server and the client is a web browser. It can be a desktop or mobile application.

1 Pillar — Institutional Requirements

Mandate and Independence

1 Level

Level 1 requirements deal with the fundamental principles of SAI independence and mandate. The prerequisite of the SAI technological development is to have sound legal mandate related for adopting technology for its internal work processes and for the external work processes – auditing information technologies. This includes legal mandate for auditing e-government systems and financial independence to adopt appropriate ICT solutions.

Level 1 requirements address INTOSAI-P - 1 - The Lima Declaration regarding the SAI's audit mandate of government electronic systems. In the era of rapid digital transformation, it is crucial that the SAIs have sound mandate to audit rapidly advancing government electronic systems.

The SAIs are ongoing digital transformation efforts which affect their internal processes, like implementing audit management systems, advanced data analysis and security assessment tools. Those ICT solutions require infrastructure, human resources, sufficient trainings and investments, which all translates to the sufficient financial resources. It is crucial that there is no interfering with the budget approval process from the executive branch, which could potentially be a violation of SAI independence and that the SAI is provided with the proper financial resources to achieve its objectives.

.1	The SAI is mandated to conduct an audit of Information Systems.	ISSAIs 100, 200, 300 and 400 establish the basic precepts of the audit in relation to Financial Audit, Performance Audit and Compliance Audit. These ISSAIs relate to the general principles, procedures, standards and expectations of an auditor. They are equally applicable to audits of information systems. The SAI's mandate authorizes it to conduct I) integrated audits in which the Information Systems audit is part, and ii) separate Information Systems audits. ***Suggested Evidence:*** Review the Law on the SAI and related regulatory documents.

1.2	The SAI has access to proper financial resources to implement ICT solutions to achieve its mandate.	SAIs should have available, necessary and reasonable resources, and should manage their own budgets without interference or control from the Executive. In terms of ICT, the financial independence is critical since it requires long-term planning and continuous investments in capacity, infrastructure, and performance. ***Suggested Evidence:*** Review the SAI budget with the focus on the ICT.
1.3	During the last 3 years there have been no cases of undue interference from the Executive branch regarding SAI's budget proposal or access to financial resources.	SAIs must have the necessary and reasonable available resources and must manage their own budgets without interference or control from the Executive branch. In terms of ICT, there should not be documented case, when the Executive branch denied or restricted SAI to get access to financial resources required for ICT projects. ***Suggested Evidence:*** Review the budget approval process, interview the SAI staff and collect any evidence of interference from the Executive branch.

1 Pillar — Institutional Requirements

Understanding Independence and transparency of ICT

2 Level

Level 2 requirements refer to the SAI's capability to understand and disclose ICT requirements.

At this entry level, the SAI should be capable of conducting regular self-assessments and periodic reviews of the ICT. This creates the foundation for the ICT Governance and sets the tone at the top. In the era of digital transformations, ICT development should be one of the top priorities of the SAI management.

In parallel to the SAI technological developments, the auditees are also evolving and processing audit data with modern technologies. Traditionally, SAIs accessed and extracted traditional information carriers (like paper-based documents), however, the SAI should not be limited to access new formats of information, such are: structured data, unstructured data, geotechnical data, raw data and back-ups, and etc.

2.1	SAI personnel have the right of access to the facilities of the audited bodies to conduct field work that the SAI deems necessary.	SAI personnel should be able to access any type of information provider (information carrier) at the audited entity's facilities, regardless of its form (documentary or electronic), allowing the SAI to efficiently and effectively plan and implement its audit procedures (tests, analytics, etc.). Reference to INTOSAI-P 10 - MEXICO DECLARATION, Principle 4, Unrestricted Access to Information. ***Suggested Evidence:*** Interview the SAI staff regarding the access to information and identify any potential limitations to SAI data collection practice.

2.2	The SAI has reviewed the adequacy of its Information Systems infrastructure in the last 3 years, and proposals for improvement have been addressed. Building Capacity in Supreme Audit Institutions p. 48-50, SAI PMF Task Force (For example, using the EUROSAI IT self-assessment methodology (ITSA)).	The SAI needs to demonstrate effective planning and use of its Information Systems infrastructure and equipment. This can be observed by the SAI's IT needs assessment (as an example, the EUROSAI IT Self-Assessment Methodology (ITSA)). ***Suggested Evidence:*** Review the SAI practice on Needs Identification and use of ICT in its work.
2.3	The SAI reports on any deficiencies related to its Information Systems assets and infrastructure in its annual report or similar reports when relevant matters arise.	The SAI should be able to emphasize the importance of ICT in fulfilling its mandate to those who make budget decisions. This criterion is linked to requirement #1.2, which emphasizes that SAIs understand their Information Systems needs and communicate them to interested parties. ***Suggested Evidence:*** Collect evidence on the formal reports (for example, SAI annual report) stating the deficiencies related to the ICT capabilities.

1 Pillar — Institutional Requirements

Establishing ICT Governance

3 Level

Level 3 relates to the establishment of SAI ICT Governance function and identifying IT/IS auditing needs.

At this level, SAI management should be able to establish ICT Governance processes. This includes selection of the ICT governance framework and allocating sufficient financial resources to support ICT initiatives.

At this level, SAI management should be able to identify external auditing requirements towards information technologies by conducting self-assessments or periodic reviews of the IT auditing needs.

3.1	The SAI has defined Governance Framework and Maintains it.	**<u>The SAI Governance Framework Setting and Maintenance should:</u>** Analyze and articulate the requirements for the governance of SAI IT. Put in place and maintain governance components with clarity of authority and responsibilities to achieve the SAI's mission, goals and objectives. **<u>The Process should cover:</u>** EDM01.01 Evaluate the governance system. EDM01.02 Direct the governance system. EDM01.03 Monitor the governance system. ***Suggested Evidence:*** Review the processes and respective documentation related to SAI IT Governance framework. For example, SAI charter, ICT Strategy, ICT action Plan, organizational structure, steering committees, etc. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*

3.2	The SAI ensures Benefits Delivery.	**<u>The SAI Benefits Delivery practice should:</u>** Optimize the value to the business from investments in business processes, IT services and IT assets. **<u>The Process should cover:</u>** EDM02.01 Establish the target investment mix. EDM02.02 Evaluate value optimization. EDM02.03 Direct value optimization. EDM02.04 Monitor value optimization. ***Suggested Evidence:*** Review the processes and respective documentation on how SAI identified ICT needs and makes decision between proposed ICT projects to be implemented in the next financial year. For example, SAI ICT project portfolio, proposed annual budget, approval annual budget etc. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
3.3	During the last five years, the SAI has applied ITASA or any other type of assessment of its information systems' audit needs.	In addition to the IT Audit self-assessment (ITASA), the SAI understands its Information Systems auditing needs, allowing it to plan to close the gaps. This can be clearly reflected in the SAI's overall corporate strategy or in separate Information Systems audit development plans. ***Suggested Evidence:*** Review the evidence of ITASA Assessments, SAI Strategy, SAI ICT auditing strategy or any other formal document reflecting the SAI needs in terms of ICT auditing.

1 Pillar — Institutional Requirements

4 Level — Country context – technological landscape

At this level, SAI should be able to assess the country's technological landscape. This includes gathering information and assess risks regarding the technological development in auditees, ongoing large-scale e-government (GovTech) projects and national critical information infrastructure.

At this level, SAI should be able to establish IT Risk Optimization process and ensure Resource optimization is in place.

At this level, SAI should ensure that its mandate allows auditors to get direct and continuous access to auditee data. In modern interconnected GovTech systems, auditees exchange information between each other (from one system to another) to create flexible solutions for citizens (G2C), for businesses (G2B) and to other government (G2G) organizations. Hence, SAI should not be limited to get direct access due to security or other concerns.

4.1	The SAI assesses its environment through surveys, interaction with auditees, assessment of direction and development of technological solutions and their adoption by auditees, and any other legal or mandatory requirements.	The SAI continuously interacts with its environment to assess the dynamics and adequacy of its audit strategies and approaches. ***Suggested Evidence:*** Review the evidence of surveys, questionnaires or other assessments done by SAI to collect information from its audit universe (auditees) on the adoption of ICT.
4.2	The SAI top management ensures Risk Optimization.	**The SAI Risk Optimization practice should:** Ensure that the SAI's risk appetite and tolerance are understood, articulated and communicated, and that risk to SAI value related to the use of IT is identified and managed. **The Process should cover:** EDM03.01 Evaluate risk management. EDM03.02 Direct risk management. EDM03.03 Monitor risk management.

		Suggested Evidence: Review the SAI practice and related documentation on how ICT risks are managed. For example, SAI risk portfolio, risk treatment plans, risk acceptance decisions etc. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
4.3	The SAI top management ensures Resource Optimization.	**The SAI Resource Optimization practice should:** Ensure that adequate and sufficient business and IT-related resources (people, process and technology) are available to support SAI objectives effectively and, at optimal cost. **The Process should cover:** EDM04.01 Evaluate resource management. EDM04.02 Direct resource management. EDM04.03 Monitor resource management. ***Suggested Evidence:*** Review the SAI practice and related documentation on how IT-related resources are available to support SAI objectives. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
4.4	During the last 3 years, the SAI identified risks associated with electronic-government projects (e-government).	The SAI should monitor the risks of ongoing electronic-government projects (e-government projects), both at an operational and strategic level. ***Suggested Evidence:*** Review the SAI work related to the eGovernment (GovTech) projects.
4.5	During the last 3 years, the SAI identified risks associated with the National Critical Information Infrastructure Protection.	The SAI should monitor the risks related to the National Critical Information Infrastructure protection. ***Suggested Evidence:*** Review the SAI work related to the National Critical Information Infrastructure auditing. For example, audit reports, annual reports, public / parliamentary hearings etc.
4.6	The SAI has the legal power/authority to obtain direct and continuous access to the information of the audited entity.	The SAI has reliable and continuous access to the information of the audited body through a direct and continuous connection. ***Suggested Evidence:*** Review the practical cases of the direct access to auditee information. Discuss any limitations in the mandate with the SAI staff.
4.7	The SAI is mandated to adopt any Critical and emerging technology (CET) based on the SAI objectives.	SAIs assesses and identify specific CETs that could significantly benefit their operation/mandate. ***Suggested Evidence:*** Review pilot studies, reports, technology adoption plans, technology governance frameworks, etc.

1 Pillar — Institutional Requirements

External communications

5 Level

At level 5, the SAI communicates with external stakeholders about the IT aspects of its mandate. On the one hand, the SAI should demonstrate to stakeholders that it has developed its mission, vision and role with respect to technological changes in public administration and what changes they imply for the SAI's performance.

It should also promote awareness among its stakeholders of the importance of IT performance and monitoring for effective public administration and e-government.

The SAI should be able to use ICTs for community participation initiatives (crowdsourcing), as interactive modules for any purpose of its external communication.

5.1	The SAI developed and communicated plans due to technological changes in the public service.	The SAI should demonstrate to stakeholders that it has aligned its mission, vision and role with respect to technological changes in public administration. ***Suggested Evidence***: "SWAT analysis" or any other types of tools used to align strategic objectives with the technological changes in public sectors.

5.2	The SAI ensures stakeholder engagement.	**<u>The SAI stakeholder engagement practice should:</u>** Ensure that stakeholders are identified and engaged in the IT governance system and that SAI IT performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and necessary remedial actions. **<u>The Process should cover:</u>** EDM05.01 Evaluate stakeholder engagement and reporting requirements. EDM05.02 Direct stakeholder engagement communication and reporting. EDM05.03 Monitor stakeholder engagement. ***Suggested Evidence***: Review how SAI collects ICT requirements from its stakeholders. For example, ICT requirements from Parliament, citizens, CSOs etc. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
5.3	The SAI communicates with external stakeholders, such as Parliament/Congress, Civil Society Organizations, and others, about the importance of Information Systems performance and monitoring for effective public administration.	The SAI makes its stakeholders aware of the importance of Information Systems performance and monitoring for effective public administration and e-governance. ***Suggested Evidence:*** Conferences, public and working meetings, public reports and awareness raising campaigns.
5.4	The SAI uses Information Systems in interactive community engagement initiatives (e.g., enabling stakeholders to engage in selecting topics/areas for audit (planning), online forms on fraud and corruption cases, crowdsourcing projects, collaborative maps, user-friendly and easy communication on complex issues of public finance management, summaries of follow-up recommendations, etc.).	The SAI can use the Information Systems for community engagement initiatives, such as interactive modules for any purpose of its external communication. ***Suggested Evidence:*** SAI official web-platform, SAI social media channels etc.

2 Pillar — INPUTS

Strategic management

1 Level

Level 1 requirements address the vision and direction of SAI leadership.

The top management of the SAI should define its strategic vision related to **Information Systems auditing**. The main objective is to establish medium-term strategic objectives, which are derived from the mandate of the SAI, the external context and the internal needs identified (Pillar 1).

The same should be done for the use of IT. The SAI should adopt **Information Technology strategy**, considering broader objectives of SAI to the needs of stakeholders. Therefore, the process of formulating an IT strategy should be based on the corporate objectives of the SAI and then these objectives linked with IT needs and related objectives.

1.1	The SAI has defined the IT Management Framework	**<u>The SAI IT Management Framework should:</u>** Design the management system for enterprise IT based on enterprise goals and other design factors. Based on this design, implement all required components of the management system. **<u>The Process should cover:</u>** APO01.01 Design the management system for enterprise IT. APO01.02 Communicate management objectives, direction and decisions made. APO01.03 Implement management processes (to support the achievement of governance and management objectives). APO01.04 Define and implement the organizational structures. APO01.05 Establish roles and responsibilities. APO01.06 Optimize the placement of the IT function. APO01.07 Define information (data) and system ownership. APO01.08 Define target skills and competencies. APO01.09 Define and communicate policies and procedures.

		Suggested Evidence: Review the SAI internal policies and documentation on IT management framework. Evaluate whether the IT management framework is defined, approved and communicated. Interview the SAI staff about their roles and responsibilities. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
1.2	The SAI has defined a strategy for Information Systems.	The SAI should define a strategic plan for ICTs that satisfies the SAI's requirements for Information Systems. The strategy should allow the SAI to be transparent about benefits, costs and risks. **The Strategy should:** Provide a holistic view of the current SAI processes and IT environment, the future direction, and the initiatives required to migrate to the desired future environment. Ensure that the desired level of digitization is integral to the future direction and the IT strategy. Assess the SAI's current digital maturity and develop a road map to close the gaps. With the SAI processes, rethink internal operations as well as stakeholder-facing activities. Ensure focus on the transformation journey across the organization. Leverage enterprise architecture building blocks, governance components and the SAI's ecosystem, including externally provided services and related capabilities, to enable reliable but agile and efficient response to strategic objectives. **The process should cover:** *AP002.01 Understand enterprise context and direction* *AP002.03 Define target digital capabilities* *AP002.04 Conduct a gap analysis* *AP002.05 Define the strategic plan and road map* *AP002.06 Communicate the ICT strategy and direction* ***Suggested Evidence:*** *Review the SAI ICT strategy and evaluate whether its in-line with SAI strategy, approved and communicated with the stakeholders. Interview the SAI staff to learn more about the process of ICT strategy elaboration.* *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
1.3	A strategic information systems audit plan is defined and coordinated with the SAI's overall audit strategy.	The SAI has a clearly defined Information Systems audit strategy. This is in line with and coordinated with the SAI's overall audit strategy.

		The Information Systems audit strategy is: - approved. - in line with the overall SAI strategy. ***Suggested Evidence:*** Review the SAI strategy on auditing information systems and evaluate whether its in line with SAI strategy. Interview the SAI staff to learn more about the process of strategy elaboration.

2 Pillar — INPUTS

2 Level — Operational Management

Level 2 requirements refer to the identification of the appropriate technology architecture for SAI information systems. This should be in line with the SAI enterprise architecture and should serve as an enabler for the SAI's information technology strategy.

At this initial level of maturity, the SAI may not be able to perform Information Systems audits, although the SAI should be able to identify and recognize the role of information systems auditing to achieve its overall audit objectives. For some SAIs operating in the highly developed digital ecosystems, the role will be critical, however, for the other SAIs in the underdeveloped digital ecosystems, the role of information systems auditing will be lower.

2.1	The SAI has defined its Enterprise Architecture.	**<u>The SAI Enterprise Architecture should:</u>** Establish a common architecture consisting of business process, information, data, application and technology architecture layers. Create key models and practices that describe the baseline and target architectures, in line with the enterprise and IT strategy. Define requirements for taxonomy, standards, guidelines, procedures, templates and tools, and provide a linkage for these components. Improve alignment, increase agility, improve quality of information and generate potential cost savings through initiatives such as re-use of building block components. **<u>The Process should cover:</u>** APO03.01 Develop the enterprise architecture vision. APO03.02 Define reference architecture. APO03.03 Select opportunities and solutions. APO03.04 Define architecture implementation. APO03.05 Provide enterprise architecture services. ***Suggested Evidence:*** *Review the SAI enterprise architecture. Evaluate whether the enterprise architecture is approved and communicated. Review the process of architecture definition.* *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*

2.2	The Information Systems audit is recognized as an important function for the fulfillment of the SAI's mission.	The Information Systems audit is recognized as an important function for the fulfillment of the SAI's mission. The top and middle management of the SAI are: - Aware of the need to audit Information Systems; - Aware of the importance of the Information Systems audit; - Aware of the benefits of the Information Systems audit. ***Suggested Evidence:*** Interviews with the SAI staff, review the SAI internal policies and manuals to collect sound evidence.

2 Pillar — INPUTS

Investment management and Information Systems Management

3 Level

Level 3 refers to the basic capacity of the SAI in Information Systems auditing and the basic IT processes.

At this level of maturity, **in terms of IT management,** the SAI should be able to manage

- IT cost accounting. This includes definition of IT budget, identification of the IT costs and prioritizing the cost allocation;
- IT vendors. This includes managing the risks related to the third-party services;
- Information security. This includes establishment of the Information Security Management System (ISMS).

In terms of **Information systems auditing**, the SAI should be able to:

- Define the approach to information systems auditing by elaborating specific audit manuals;
- Include IT control testing in the FA, CA and PA and involve IT auditors in regular audits;
- Financial, compliance and performance auditors understand the specialized audit tools, like CAATs and respective benefits.

3.1	The SAI has defined budget and costs for IT.	**<u>The SAI IT Budget and Cost management should:</u>** Manage the IT-related financial activities in both the business and IT functions, covering budget, cost and benefit management and prioritization of spending through the use of formal budgeting practices and a fair and equitable system of allocating costs to the enterprise. Consult stakeholders to identify and control the total costs and benefits within the context of the IT strategic and tactical plans. Initiate corrective action where needed. **<u>The Process should cover:</u>** AP006.01 Manage finance and accounting.

		AP006.02 Prioritize resource allocation. AP006.03 Create and maintain budgets. AP006.04 Model and allocate costs. AP006.05 Manage costs. ***Suggested Evidence:*** *Review the SAI budgeting process focusing on the identification of ICT budget and resource allocation. Interviews with the ICT staff, SAI finance and budgeting departments.* *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
3.2	The SAI has a clearly defined and described Information Systems audit approach, for example, in an audit manual.	The SAI has a clearly defined IT audit approach described, for example, in an Information Systems audit manual. [former ISSAI 1315-A79, A80, ISSAI 5310] ***Suggested Evidence:*** Review the SAI practice to determine whether the SAI has: - An established practice of Information Systems auditing; - A specific manual for Information Systems auditing; - The Information Systems Audit Manual is approved
3.3	Information Systems auditors cover specific needs in financial, compliance and performance audits.	Information Systems auditors cover the specific Information Systems needs of financial, compliance and performance audits. ***Suggested Evidence:*** To test controls and cover IT issues, Information Systems auditors should participate in: - Financial auditing; - Compliance auditing; - Performance auditing.
3.4	Auditors in the financial, performance and/or compliance domains are aware of the potential use of Computer Aided Audit Techniques (CAATs) for auditing purposes.	Auditors in financial, performance and / or compliance auditing are aware of the potential use of CAATs for auditing purposes. [former ISSAI 1520, ISSAI 1530] ***Suggested Evidence:*** Regular financial, compliance and performance audit auditors have an adequate understanding of: - The benefits of the CAATs; - The CAAT's use cases; - The need for CAATs.

3.5	The SAI manages vendors.	**<u>The SAI Vendor Management should:</u>** Manage IT-related products and services provided by all types of vendors to meet enterprise requirements. This includes the search for and selection of vendors, management of relationships, management of contracts, and reviewing and monitoring of vendor performance and vendor ecosystem (including upstream supply chain) for effectiveness and compliance. **<u>The Process should cover:</u>** APO10.01 Identify and evaluate vendor relationships and contracts. APO10.02 Select vendors. APO10.03 Manage vendor relationships and contracts. APO10.04 Manage vendor risk. APO10.05 Monitor vendor performance and compliance. ***Suggested Evidence**: Review the SAI practice related to vendor management. Review the internal documents, policies and decisions. Interview the ICT, information security and procurement staff to assess vendor management processes.* *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
3.6	The SAI manages security.	**<u>The SAI security Management should:</u>** Define, operate and monitor an information security management system. **<u>The Process should cover:</u>** APO13.01 Establish and maintain an information security management system (ISMS). APO13.02 Define and manage an information security and privacy risk treatment plan. APO13.03 Monitor and review the information security management system (ISMS). ***Suggested Evidence:** Review the SAI information security practices, including approved security policies, procedures and compliance requirements. If possible, rely on third-party certificates (like ISO/IEC 27001 and etc.) SAI may have.* *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*

2 Pillar — INPUTS

4 Level — Establishment of the Information Systems audit capacity

At level 4, a SAI should be able to establish a decent Information Systems audit capacity. This should encompass qualified IT audit personnel (certifications like CISA can be a good indicator), who have the right audit tools to carry out most audit procedures.

Additionally, SAI should have established processes to regularly train its Information Systems auditors and regular auditors (financial and compliance) in auditing IT controls, using CAATs and other appropriate techniques. As a result, IT audit tools should be used widely throughout the SAI for the purposes of all types of auditing.

In terms of IT capacity, the SAI should be able to

- Establish the process to Manage innovation. This should enable the SAI to identify the context it operates in and assure that innovative initiatives are captured and developed.
- Review the potential use of Critical and Emerging technologies to achieve SAI mission. This should enable the SAI to search for the emerging technologies (like AI, Blockchain, cloud computing etc.), in line with the national efforts (some of the countries are adopting and establishing national strategies for CEtTs).

4.1	The SAI manages Innovation	**<u>The SAI Innovation management should:</u>** Maintain an awareness of IT and related service trends and monitor emerging technology trends. Proactively identify innovation opportunities and plan how to benefit from innovation in relation to business needs and the defined IT strategy. Analyze what opportunities for business innovation or improvement can be created by emerging technologies, services or IT-enabled business innovation; through existing established technologies; and by business and IT process innovation. Influence strategic planning and enterprise architecture decisions. **<u>The Process should cover:</u>** APO04.01 Create an environment conducive to innovation. APO04.02 Maintain an understanding of the enterprise environment. APO04.03 Monitor and scan the technology environment. APO04.04 Assess the potential of emerging technologies and innovative ideas.

		AP004.05 Recommend appropriate further initiatives. AP004.06 Monitor the implementation and use of innovation. ***Suggested Evidence:*** *Review the SAI practice related to innovation management. Review internal policies, procedures and processes. Interview the SAI staff. Review innovation projects and success cases the SAI may have.* *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
4.2	The SAI has defined procedures to identify appropriate Critical and Emerging Technology (like GIS, AI, Blockchain etc.).	The SAI should be able to adopt emerging technologies. The SAI should have specific mechanisms to identify appropriate Critical and Emerging Technologies, which would serve the SAI mission. ***Suggested Evidence:*** Interview the SAI staff, review the SAI practices and procedures in place. For example: pilot projects, technology adoption and etc.
4.3	The SAI has adequate auditing software: CAATs (ACL, IDEA, Access ...) to ensure adequate IT audit support for financial, compliance and performance audits.	The SAI has adequate auditing software – CAATs (ACL, IDEA, Access ...) to ensure adequate Information Systems audit support for: - financial audits; - compliance audits; and - performance audits. [former ISSAI 1330 A16-A27, GUID 5101 (former ISSAI 5310)] ***Suggested Evidence:*** Software inventory of CAATs, ratio of CAAT licenses and audit staff.
4.4	Information Systems audit staff are adequately skilled.	Human resources for Information Systems audit are adequately skilled. To perform the Information Systems audit tasks, they: - are certified as CISA (Certified Information Systems Auditor); or - have equivalent experience. [former ISSAI 1220 – A11] - Participate in tracks of learning or other educational methods based on skills and competencies. ***Suggested Evidence:*** list of CISA certified (or other relevant certifications like Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP) and etc.) auditors, list of trainings received, Professional Education Plans and etc.

4.5	There is sufficient training for the Information Systems control audit across SAI audit functions.	To increase the level of awareness about Information Systems audit matters, there is: - Sufficient training for auditors in Information Systems auditing; - Sufficient training for non-IT auditors on issues related to the Information Systems audit. [former ISSAI 1220 - A11] ***Suggested Evidence:*** list of trainings for SAI auditors, number of trained staff, training domains (for example audit of general IT controls, audit of specific technologies, etc.) and etc.
4.6	Information Systems audit tools are used within the SAI.	Information Systems audit tools are used by: - The Information Systems audit unit/department; - regular audit teams/departments. ***Suggested Evidence:*** audit work papers, record of use CAATs in regular audits, and etc.

2 Pillar — INPUTS

5 Level — Information Systems Audit Capacity Optimization

Level 5 requirements are oriented on the continuous improvement cycles / processes.

At this level, the SAI should start optimizing the results achieved at levels 1-4. The SAI should endeavor to meet its needs related to personnel for Information Systems auditing to satisfy its requirements on external audits. The SAI should be able to assure that:

- auditors are equipped with the sufficient software tools to conduct complex audits;
- not only IT/IS auditors are skilled to perform assessment of basic IT control tests;
- number of IT/IS auditors are sufficient to support the needs of FA, CA and PA teams;
- if needed, there are mechanisms and resources to acquire short term experts for the advanced tech audit purposes.

To this end, it is recommended that the SAI implement effective human resource policies to reduce the knowledge gap between Information Systems auditors and regular auditors by providing appropriate training programs and distributing the skill set among SAI departments.

In terms of IT capacity, at this level, SAI should be able to:

- Pilot selected / identified Critical and Emerging Technologies.
- Establish direct access to auditee data, if that is required by the audit objectives.

5.1	There is an adequate distribution of Information Systems auditing skills.	There is an adequate distribution of Information Systems auditing skills between: - The Information Systems Auditors and FA, CA, PA auditors working in other units/departments. ***Suggested Evidence:*** tech skillset of information systems auditors, tech skillset of FA, CA, PA auditors.

5.2	The SAI has adequate Information Systems auditing software to perform its technical audit tests.	The SAI has a suitable Information Systems audit software to perform technical audit tests on: - hacking programs; - vulnerability analysis tools; - digital forensic tools; - special analysis tools. [former ISSAI 1330-A29] ***Suggested Evidence***: software inventory list, license agreements, and etc.
5.3	The SAI has defined procedures to pilot appropriate Critical and Emerging Technology (like GIS, AI, Blockchain etc.).	The SAI should be able to adopt emerging technologies. The SAI should have specific mechanisms to pilot appropriate Critical and Emerging Technologies, which would serve the SAI mission. ***Suggested Evidence:*** *SAI procedures on adopting new technologies,* list of pilot projects, technology initiatives and etc.
5.4	There are sufficient Information Systems auditors for the level of auditing required by the SAI.	The SAI has sufficient Information Systems audit personnel to satisfy: - IT audit requirements; - IT audit requests from other departments. [GUID 5090, GUID 5091, Best practices] ***Suggested Evidence:*** SAI audit and human resource planning documents, internal memos and decisions on involving information systems auditors in FA, CA, PA.
5.5	If there is not enough knowledge or there is a lack of resources within the institution, there are procedures to subcontract technical tasks of Information Systems auditing.	The SAI should have defined procedures for hiring qualified short-term personnel to perform specific tasks related to the Information Systems audit. ***Suggested Evidence:*** past contracts with the external consultants, approved procedures for procurement of consultancy services, quality control and assurance procedures for the use of expert's work and etc.
5.6	The SAI has external access from its facilities to the Information Systems and databases of the audited entities.	The SAI has direct technical access and is able to collect: - data; - information on the selected audited entity.

		Suggested Evidence: inventory of external sources (data), list of auditors who excess those data, roles and privileges, and etc.

3 Pillar — PROCESSES

1 Level — IT solutions implementation

Level 1 requirements refer to SAI's IT management processes.

At this level, SAI should be able to manage:

- IT requirements definition. This process should enable the SAI to structure its requirements towards IT solutions before acquiring or building them.
- IT solutions identification and build. This process focuses on identifying appropriate solutions based on the identified requirements.
- Availability and capacity. This process enables SAI to maintain uninterrupted services for its internal and external stakeholders.
- IT assets. This process assures that IT assets (like hardware, software, IT services, facilities, etc.) are recorded, prioritized based on criticality and maintained through their lifecycle.

1.1	The SAI manages Requirements Definition.	**<u>The SAI Requirements Definition Management should:</u>** Identify solutions and analyze requirements before acquisition or creation to ensure that they align with SAI strategic requirements covering business processes, applications, information/data, infrastructure, and services. Coordinate the review of feasible options with affected stakeholders, including relative costs and benefits, risk analysis, and approval of requirements and proposed solutions **<u>The Process should cover:</u>** BAI02.01 Define and maintain business functional and technical requirements. BAI02.02 Perform a feasibility study and formulate alternative solutions. BAI02.03 Manage requirements risk. BAI02.04 Obtain approval of requirements and solutions ***Suggested Evidence:*** *Review the SAI requirements definition process. Review the process for technical requirements definition, including feasibility study and risk management process. Interview the SAI staff to learn more about the process.* *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*

1.2	The SAI manages Solutions Identification and Build.	**<u>The SAI Solutions Identification and Build should:</u>** Establish and maintain identified products and services (technology, business processes and workflows) in line with enterprise requirements covering design, development, procurement/sourcing and partnering with vendors. Manage configuration, test preparation, testing, requirements management and maintenance of business processes, applications, information/data, infrastructure and services. **<u>The Process should cover:</u>** BAI03.01 Design high-level solutions. BAI03.02 Design detailed solution components. BAI03.03 Develop solution components. BAI03.04 Procure solution components. BAI03.05 Build solutions. BAI03.06 Perform quality assurance (QA). ***Suggested Evidence:*** *Review the SAI process related to identification and building of ICT solutions. Review the internal practices related to development and procurement. Interview the SAI staff on the quality assurance practice and review any QA documents (like inspection memos).* *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
1.3	The SAI manages Availability and Capacity.	**<u>The SAI Availability and Capacity Management should:</u>** Balance current and future needs for availability, performance, and capacity with cost-effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements. **<u>The Process should cover:</u>** BAI04.01 Assess current availability, performance and capacity and create a baseline. BAI04.02 Assess business impact. BAI04.03 Plan for new or changed service requirements. BAI04.04 Monitor and review availability and capacity. BAI04.05 Investigate and address availability, performance and capacity issues. ***Suggested Evidence:*** Review the SAI practices related to availability and capacity management. Interview the SAI staff to identify how business impact assessment is done, how is the availability

		monitored and measured and how are capacity requirements defined. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
1.4	The SAI manages assets	**<u>The SAI asset management should:</u>** Manage IT assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose), and they are accounted for and physically protected. Ensure that those assets that are critical to support service capability are reliable and available. Manage software licenses to ensure that the optimal number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with license agreements. **<u>The Process should cover:</u>** BAI09.01 Identify and record current assets. BAI09.02 Manage critical assets. BAI09.03 Manage the asset life cycle. BAI09.04 Optimize asset value. BAI09.05 Manage licenses. ***Suggested Evidence:*** Review the SAI asset management practice. Review the asset inventory and asset management lifecycle. Review whether asset inventory includes and classifies all the IT assets (software, hardware, licenses and etc.). Interview the SAI staff on the inventory review process. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*

3 Pillar — PROCESSES

2 Level — Information Systems audit resource sharing

Level 2 focusses on the utilization of the Information Systems audit function/capacity for the audit work, which at this stage is often a scarce resource. Therefore, the SAI should have effective risk assessment procedures, which will allow the identification of high-risk areas in all types of audits. Next, a SAI should be able to direct Information Systems auditors to the audits with the greatest impact.

In terms of information systems auditing, at this level, SAI should:

- Promote experience sharing between IT/IS auditors and regular auditors;
- Establish procedures for audit departments to request IT/IS auditors support;
- Establish risk assessment procedures for IT audit selection;

In terms of IT capacity, at this level, SAI should be able to manage:

- IT changes, which include evaluation, prioritization, and authorization of changes. The process should also cover how the emergency changes are implemented and documented.
- IT operations, which refer to the establishment of IT operational procedures, including monitoring and managing outsourced services.

1.1	The SAI manages IT changes	**<u>The SAI IT change management should:</u>** Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritization and authorization, emergency changes, tracking, reporting, closure, and documentation. **<u>The process should cover:</u>** BAI06.01 Evaluate, prioritize and authorize change requests.

		BAI06.02 Manage emergency changes. BAI06.03 Track and report change status. BAI06.04 Close and document the changes. ***Suggested Evidence:*** Review the SAI IT change management practice. Interview the responsible staff (like change advisory board (CAB)). Review the process of change requests, change approvals and reporting. Review the sample documentation related to full lifecycle of change management. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
2.2	The SAI manages operations	**The SAI operations management should:** Coordinate and execute the activities and operational procedures required to deliver internal and outsourced IT services. Include the execution of predefined standard operating procedures and the required monitoring activities. **The Process should cover:** DSS01.01 Perform operational procedures. DSS01.02 Manage outsourced IT services. DSS01.03 Monitor IT infrastructure. DSS01.04 Manage the environment. DSS01.05 Manage facilities. ***Suggested Evidence:*** Review the SAI operations management practice. Interview the SAI staff. Review the operational procedures and policies. Review the technical tools to monitor outsourced IT services, infrastructure and facilities (Data centers). *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
2.3	There is an exchange of experiences with information systems auditing among all auditors within the SAI.	The SAI has established a process for exchanging experiences related to Information Systems auditing among Information Sy stems auditors and other auditors (performance, compliance and/or financial). ***Suggested Evidence:*** list of experience sharing workshops, trainings and internal policies.
2.4	The SAI has established procedures to obtain Information Systems audit support for financial, compliance and/or performance audits.	The SAI has effective and established procedures for audit departments to request technical support from Information Systems auditors. ***Suggested Evidence:*** human resource planning reports / documents, service requests from different departments and etc.
2.5	The SAI selects Information Systems audits after a prior risk analysis.	The SAI selects Information Systems audits based on risk analysis. [former ISSAI 1000, ISSAI 1200-A40, A50, ISSAI 1210 - A18, ISSAI 1220-A9, ISSAI 1240-P11-P14, ISSAI 1315-P5-P18, and former ISSAI 5310 to become GUID 1501] ***Suggested Evidence:*** audit work papers, audit planning memos and etc.

2.6	When planning audits, the SAI performs a prior analysis of the information systems involved to plan potential Information Systems audit support. Information Systems auditors (or other name adopted by the country) are also consulted.	When planning financial, compliance and performance audits, the SAI has predefined procedures to: - Carry out prior analysis of the information systems; - Endorse and suggest data and models (including geographic ones) from various sources;- There is a geographic data coordination function and/or committee to streamline the development, access and maintenance of this data and its infrastructure - Identify the need for participation or involvement of the Information Systems auditors (audit support); - Make consultations with auditors(s) of Information Systems. [former ISSAI 1300] ***Suggested Evidence:*** Audit manuals, audit management process, interviews with the SAI staff and etc.

3 Pillar — PROCESSES

3 Level — IT control testing and reporting the results

After the SAI identifies its audit engagements, in which it plans to involve Information Systems auditors, the SAI should have predefined procedures for audit work. This would ideally include assessing the IT control environment to evaluate the reliability of the audited data.

In terms of information systems auditing, at this level, SAI should:

- Develop IT control assessment procedures for financial, compliance and performance audits;
- Reflect IT control assessment results in the regular audit reports.

In terms of IT capacity, at this level, SAI should be able to manage:

- Configuration. This includes establishing configuration model and maintaining configuration repository.
- Problems. This includes, identification and classification of problems, diagnosis and resolution efforts.

3.1	The SAI manages the configuration.	**<u>The SAI Configuration Management should:</u>** Define and maintain descriptions and relationships among key resources and capabilities required to deliver IT-enabled services. Include collecting configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository. **<u>The Process should cover:</u>** BAI10.01 Establish and maintain a configuration model. BAI10.02 Establish and maintain a configuration repository and baseline. BAI10.03 Maintain and control configuration items. BAI10.04 Produce status and configuration reports. BAI10.05 Verify and review integrity of the configuration repository. ***Suggested Evidence:*** Review the SAI configuration management practices. Review the internal policies and documentation. Review the sample of configuration records / reports. Interviews with the SAI staff.

		For additional guidance, refer to COBIT 2019 Governance and Management Framework.
3.2	The SAI manages problems.	**<u>The SAI Problem Management should:</u>** Identify and classify problems and their root causes. Provide timely resolution to prevent recurring incidents. Provide recommendations for improvements. **<u>The Process should cover:</u>** DSS03.01 Identify and classify problems. DSS03.02 Investigate and diagnose problems. DSS03.03 Raise known errors. DSS03.04 Resolve and close problems. DSS03.05 Perform proactive problem management. ***Suggested Evidence:*** Review the SAI problem management practices. Review the inventory of known problems, classification schemas and problem diagnostic procedures. Interviews with the SAI staff. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
3.3	The SAI performs a comprehensive/global assessment on general and application controls to evaluate the reliability of the data.	Before starting the audit work for financial, compliance and performance audits, the SAI evaluates the reliability of data by performing a comprehensive assessment on: - General controls of Information Systems; - Application controls [former ISSAI 1315-A95-A97] **Suggested Evidence:** Audit manuals, audit procedures, interviews with the SAI staff and etc.
3.4	The results of the Information Systems audits are considered in the financial, performance and compliance audits.	The Information Systems auditor's participation in financial, compliance and performance audits should be documented and reflected in the audit results. **Suggested Evidence:** a sample of audit reports.

3 Pillar — PROCESSES

4 Level — Audit documentation

At level 4, the SAI must have adequate procedures in place to document the results of the audit procedures. The requirements focus on the IT control testing/Information Systems audit part of the audit engagements.

In terms of information systems auditing, at this level, SAI should:

- Document IT related evidence in financial, compliance and performance audits;
- Document references to appropriate IT criteria used in audit process.

In terms of IT capacity, at this level, SAI should be able to manage:

- Service requests and incidents. This includes classification schemes of service requests and incidents, record keeping, diagnosis and resolution statuses, closure and status tracking.

4.1	The permanent files (audit documentation) include general information about the Information Systems environment of the audited entities.	The support and participation/involvement of the Information Systems audit should be adequately documented. For that purpose, the permanent files of the audit work (whether financial, compliance or performance) should include general information about the auditee's information systems control environment. [former ISSAI 1230 Audit documentation] ***Suggested Evidence***: a sample of audit files.
4.2	The SAI manages Service Requests and Incidents.	**The SAI Service Request and Incident Management should:** Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents. **The Process should cover:** DSS02.01 Define classification schemes for incidents and service requests. DSS02.02 Record, classify and prioritize requests and incidents.

		DSS02.03 Verify, approve and fulfil service requests. DSS02.04 Investigate, diagnose and allocate incidents. DSS02.05 Resolve and recover from incidents. DSS02.06 Close service requests and incidents. DSS02.07 Track status and produce reports. ***Suggested Evidence:*** Review the SAI service requests and incident management practice. Review the inventory for service requests (for example, tools by Atlassian, ManageEngine and etc.). Review the process of classification, review and escalation. Interview the SAI staff - users and IT staff including. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
4.3	When performing Information Systems audit tasks, the audit documentation refers to IS auditing standards or guidelines.	When performing Information Systems auditing tasks, auditors should refer to the Information Systems auditing standards and guidelines. [former ISSAI 1230] ***Suggested Evidence:*** a sample of audit reports, reference guidelines and standards and etc.

3 Pillar — PROCESSES

Evidence and Documentation

5 Level

At this level, the SAI should be able to manage most of the Information Systems processes described in this pillar. After implementing relevant and appropriate IT solutions, the SAI must be able to maintain them, which also provides day-to-day activities such as incident management, configuration management, and problem management. To this end, the SAI should establish effective controls to collect incidents, analyze them, and address identified problems whenever possible.

In the case of IT audit capacity, at Level 5, a SAI should be able to have effective oversight over government electronic systems and initiatives. Ideally, the SAI would identify and follow up on ongoing projects in government (to establish some kind of project registry), while maintaining independence in the audit process. More precisely, in most cases, government IT projects require several years to implement and therefore the SAI should strive to preserve its independence in the process of auditing ongoing projects.

5.1	The findings and conclusions regarding Information Systems audit are issued in accordance with objective criteria similar to those of the financial, compliance and performance audit (materiality, relevance, etc.).	Findings and conclusions regarding the Information Systems audit should be issued in accordance with objective criteria similar to those for financial, compliance and performance audit (materiality, relevance, etc.). [former ISSAI 1230, ISSAI 1500] ***Suggested Evidence:*** a sample of audit reports to analyze similarities.
5.2	Information Systems audit work is properly documented (including records of any type of data manipulation during Information Systems audit tests).	Like all audit procedures, Information Systems audit work should be documented in accordance with the documentation standard defined by the SAI, including available and up-to-date metadata for geographic data. This should also include records of any data manipulation during Information Systems audit tests. [former ISSAI 1330-A63, ISSAI 1230, ISSAI 1500] **Suggested Evidence:** a sample of audit documentation, record of data manipulation, log data and etc.
5.3	The portfolio of all government Information Systems projects and all government Information Systems applications is available to the SAI.	The SAI has a portfolio of all government Information Systems projects and all government Information Systems applications available for audit purposes. ***Suggested Evidence:*** register / inventory of government projects.

4 Pillar — OUTPUTS

1 Level — Reports

Level 1 requirements are related to the SAI's practice of publishing Information Systems audit reports. The SAI should have procedures for the approval and publication of Information Systems audit reports, as it does in the case of financial, compliance and performance audits.

1.1	Information Systems audit reports follow approval procedures similar to those of financial, compliance and performance audit reports.	The SAI should have established approval procedures for all types of audits. This should also include the Information Systems audit work. [former ISSAI 1700, Good Practices] ***Suggested Evidence:*** audit manuals, internal procedures for report approval and etc.
1.2	Information Systems audit reports are published in the same way as financial, compliance and performance audit reports.	The SAI should have established publication procedures for all types of audits. This should also include the Information Systems audit work. [former ISSAI 1700, Good Practices] ***Suggested Evidence:*** a list of published audit reports, the SAI website and etc.

4 Pillar — OUTPUTS

2 Level — Reporting Structure

The level 2 requirements refer to the SAI's reporting format practice. Whenever Information Systems audit support is used in financial, compliance and performance audits, the SAI should have established procedures/practices to include IT-related results in a separate chapter of the audit report.

This way, whenever the SAI publishes Information Systems audit reports, the structure and format of the report must be defined and consistent. Also, findings should be linked to documentation, and referenced.

2.1	Information Systems audit work is conducted to support financial, compliance and performance audits; in these reports there is a separate section dedicated to the Information Systems audit work performed.	Financial, compliance and performance audit reports should have a separate section dedicated to Information Systems audit work performed in the scope of the audit. [former ISSAI 1000, ISSAI 1230] ***Suggested Evidence:*** a sample of FA, CA, PA reports, internal procedures and etc.
2.2	Information Systems audit reports have a predefined structure to be respected, including cartographic patterns and visual communication.	The Information Systems audit should have a predefined structure to follow. The SAI should approve this structure. ***Suggested Evidence:*** approved audit manual, audit procedures, audit templates or audit report template.
2.3	The content of the Information Systems audit report is referenced and identified with the audit documentation. The findings and conclusions mentioned can be easily found in the audit documentation.	The content of the Information Systems audit report should be referenced and identified with the audit documentation. The findings and conclusions mentioned in the report should be easily found in the audit documentation. [former ISSAI 1000, ISSAI 1230, ISSAI 1700; ISSAI 3000] ***Suggested Evidence:*** a sample of audit reports and respective audit documentation.
2.4	The performance and efficacy of investments in Information Systems are audited.	Within the Information Systems audit work, the SAI should audit the performance and efficacy of Information Systems investments in the governmental sector. ***Suggested Evidence:*** a sample of audit reports.

2.5	Information Systems audit findings are incorporated into financial, performance and compliance audit reports where appropriate.	The findings related to the Information Systems audit should be incorporated into the financial, performance and compliance audit reports. [former ISSAI 1700, Good Practices] ***Suggested Evidence:*** a sample of audit reports.

4 Pillar — OUTPUTS

3 Level — Security Operations

Level 3 is related to the SAI's ability to ensure internal IT systems are resilient and accessible to SAI staff without major interruptions. SAI takes advantage of the use of Information Systems to achieve better results in the audit work (including all types of audits), which means that the SAI must be able to manage and guarantee the continuity and security of its services, and monitor and manage the performance and capacity of its systems.

In terms of IT capacity, at this level, SAI should be able to manage:

- Continuity, which covers the business requirements for reliable information systems and services.
- Information security services, which refer to establishment of security operations, including anti-malware protection, endpoint and network security, physical security, identity management etc.

In terms of audit capacity, the SAI should be able:

- To implement audit management system, which allows systemic approach to audit process, including definition of audit procedures, stages, documentation requirements etc.

3.1	The SAI documents audit process in the Audit Management System.	The SAI has deployed automated solution to document the audit process, audit projects, audit findings and audit reports in the Audit Management System. ***Suggested Evidence:*** the SAI solutions to document audit process.
3.2	The SAI Manages Continuity.	**The SAI Continuity Management should:** Establish and maintain a plan to enable the business and IT organizations to respond to incidents and quickly adapt to disruptions. This will enable continued operations of critical business processes and required IT services and maintain availability of resources, assets and information at a level acceptable to the enterprise. **The Process should cover:** DSS04.01 Define the business continuity policy, objectives and scope. DSS04.02 Maintain business resilience.

		DSS04.03 Develop and implement a business continuity response. DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP). DSS04.05 Review, maintain and improve the continuity plans. DSS04.06 Conduct continuity plan training. ***Suggested Evidence:*** Review the SAI continuity management practices. Review the SAI policies and procedures. Interview the staff to evaluate whether they have been trained in line with the policies and plans. Review the documentation related to testing contingency plans. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
3.3	The SAI manages Security Services.	**The SAI Security Service Management should:** Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access privileges. Perform security monitoring. **The Process should cover:** DSS05.01 Protect against malicious software. DSS05.02 Manage network and connectivity security. DSS05.03 Manage endpoint security. DSS05.04 Manage user identity and logical access. DSS05.05 Manage physical access to IT assets. DSS05.06 Manage sensitive documents and output devices. DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events. ***Suggested Evidence:*** Review the SAI information security practices. Review the inventory of security solutions. Review the policies, procedures and documentation related to security controls. If possible, rely on third party certifications (like ISO/IEC 27001 and etc.). If possible, rely on third party audits, assessments, penetration testing results. It is mandatory to review the scope of certification and external assessments when using them as an evidence for the ITMA assessment. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*

4 Pillar — OUTPUTS

4 Level — Information Systems Audit Areas

At level 4, the SAI should be able to use the Information Systems audit function in a mature manner to produce outputs (audits) related to the different fields of Information Technology. This would anticipate and include the audit of investments in Information Systems, procurements, projects, and security.

In terms of information systems auditing, at this level, SAI should be able to audit:

- Information security of auditee electronic systems;
- IT project management practices of auditee;
- IT procurement practices;

These fields require specific knowledge and experience, as well as specialized tools in some cases, which must be accessible to the SAI at this level.

In terms of IT capacity, the SAI should be able:

- Record and track findings and respective recommendations in the specialized / dedicated tracking system.

4.1	Compliance audits that are conducted with regard to the accuracy of accounts according to accounting principles (for example, ISA 315 and 330) include elements of Information Systems auditing.	Compliance audits that are carried out with regard to the accuracy of accounts according to accounting principles (for example, ISA 315 and 330) include elements of Information Systems audit. [former ISSAI 1315-P17-P18, ISSAI 1330 – A10, A33, A57] ***Suggested Evidence:*** a sample of audit reports.
4.2	The SAI Manages Business Process Controls.	**The SAI Business Process Control Management should:** Define and maintain appropriate business process controls to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements. Identify the relevant information control requirements. Manage and operate adequate input, throughput and output controls (application controls) to ensure that information and information processing satisfy these requirements. **The Process should cover:** DSS06.01 Align control activities embedded in business processes with enterprise objectives.

		DSS06.02 Control the processing of information. DSS06.03 Manage roles, responsibilities, access privileges and levels of authority. DSS06.04 Manage errors and exceptions. DSS06.05 Ensure traceability and accountability for information events. DSS06.06 Secure information assets. ***Suggested Evidence:*** Review the SAI policies, procedures and practices related to business process controls. Review the inventory of SAI systems, scope of policies on business process controls. Interview the SAI staff to identify their approach to business process controls. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
4.3	The SAI tracks recommendations via Specialized recommendation tracking system.	The SAI tracks recommendation statuses via electronic system. The system records all the recommendations issues by the SAI and provides internal users with the updated statuses. ***Suggested Evidence:*** recommendation tracking system.
4.4	The SAI audits the security of Information Systems (loss of confidentiality, integrity, or availability).	Information Systems security is audited (loss of confidentiality, integrity or availability). [former ISSAI 1315-A56, A81, GUID 1501] ***Suggested Evidence:*** a sample of audit reports.
4.5	The SAI conducts audits of Information Systems projects.	The SAI conducts Information Systems audits of government IT projects. ***Suggested Evidence:*** a sample of audit reports.
4.6	The SAI conducts compliance audits of Information Systems procurements.	The SAI conducts Information Systems compliance audits of government procurements, including those procured in a subscription model (SaaS - Software as a Service). [former ISSAI 1315-A63, P14] ***Suggested Evidence:*** a sample of audit reports.

4 Pillar — OUTPUTS

5 Level — Data management and recommendations tracking

At this level, the SAI should be able to manage most of the IT functions.

In terms of IT capacity, the SAI should be able to manage:

- Data, irrespective of its type. The process should include definition or roles and responsibilities over data assets, identification of data criticality and managing full lifecycle of the data.

Data is the most valuable asset for the purposes of audit work. Therefore, data storage, deletion, and backups must be properly managed by the SAI.

In terms of IT and overall audit capacity, at this level, SAI should be able to audit:

- Manage recommendation tracking system, available for its external stakeholders.

5.1	The SAI manages the data.	**<u>The SAI Data Management should:</u>** Achieve and sustain effective management of the enterprise data assets across the data life cycle, from creation through delivery, maintenance and archiving. **<u>The Process should cover:</u>** APO14.01 Define and communicate the organization's data management strategy and roles and responsibilities. APO14.05 Establish data profiling methodologies, processes and tools. APO14.08 Manage the life cycle of data assets. ***Suggested Evidence:*** Review the SAI strategy on data management. Review the roles and responsibilities of the respective staff. Review the full life cycle of the data management. Review the inventory of data. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
5.2	The SAI recommendation tracking system is accessible for external stakeholders.	The SAI recommendation tracking system is accessible from outside of the SAI by the external stakeholders of the SAI. The SAI may integrate recommendation tracking system on the website or may

		have dedicated online portal. ***Suggested Evidence:*** recommendation tracking system is operational and accessible.

5 Pillar — QUALITY AND OPTIMIZATION

1 Level — Human Resources

Level 1 requirements address the SAI's focus on IT human resources. Information systems generate value for the organization if users are able to use them. Therefore, the SAI should strive to regularly train its IT personnel, educate them, identify key personnel, and retain their knowledge.

1.1	The SAI manages IT Human Resources.	**<u>The SAI Human Resource Management should:</u>** Provide a structured approach to ensure optimal recruitment/acquisition, planning, evaluation and development of human resources (both internal and external). **<u>The Process should cover (suggested evidence):</u>** AP007.01 Acquire and maintain adequate and appropriate staffing. AP007.02 Identify key IT personnel. AP007.03 Maintain the skills and competencies of personnel. AP007.04 Assess and recognize/reward employee job performance. AP007.05 Plan and track the usage of IT and business human resources. AP007.06 Manage contract staff. ***Suggested Evidence:*** Review the SAI practices related to IT human resource management. Review the inventory of key IT personnel. Review the skills and competences required for IT personnel. Review the past trainings and certification programs arranged for IT personnel. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*

Pillar QUALITY AND OPTIMIZATION

2 Level Information Systems Quality Management

Level 2 requirements refer to the SAI's Quality Management System (QMS) for information technology.

In terms of IT capacity, the SAI should be able to manage:

- IT risks, which includes full life-cycle of the IT risk management. More precisely, starting from risk related data collection to analysis and risk treatment decisions.
- IT projects, in line with predefined IT project management practice. This process envisages full life-cycle of IT project management, including quality management process.

2.1	The SAI manages risks.	**The SAI Risk Management should:** Continually identify, assess and reduce IT-related risk within tolerance levels set by enterprise executive management. **The Process should cover (suggested evidence):** APO12.01 Collect data. APO12.02 Analyze risk. APO12.03 Maintain a risk profile. APO12.04 Articulate risk. APO12.05 Define a risk management action portfolio. APO12.06 Respond to risk. ***Suggested Evidence:*** Review the SAI risk management practices. Review the organizational structure for risk management. Review the risk management policy, including process of data collection, risk analysis and risk treatment. Review the up to date inventory of IT risks and sample of risk response activities. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
2.2	The SAI manages projects.	**The SAI Project Management should:** Manage all projects that are initiated within the enterprise in alignment with enterprise strategy and in a

		coordinated way based on the standard project management approach. Initiate, plan, control and execute projects, and close with a post-implementation review. **<u>The Process should cover:</u>** BAI11.01 Maintain a standard approach for project management. BAI11.02 Start up and initiate a project. BAI11.03 Manage stakeholder engagement. BAI11.04 Develop and maintain the project plan. BAI11.05 Manage project quality. ***Suggested Evidence:*** Review the SAI project management practices. Review the policies and procedures. Review the inventory of recent IT projects. Review the sample project plans and quality management mechanisms. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*

5 Pillar — QUALITY AND OPTIMIZATION

3 Level — Monitoring and Evaluation

Level 3 builds on Level 2 – Information Systems Quality Management. After the SAI establishes quality management controls, it must be able to measure actual services. This would include monitoring IT performance, evaluating the effectiveness of IT control, and meeting regulatory requirements. The monitoring results should be compared and evaluated against the predefined/established KPIs for the SAI.

In terms of IT capacity, the SAI should be able to manage:

- IT performance and conformance monitoring. This should envisage the establishment of monitoring approach, including specific KPIs, targets states and monitoring processes.
- IT internal control system. This should envisage monitoring of IT control effectiveness. In addition to continuous monitoring efforts, SAI may undergo control self-assessment exercises or periodic reviews.
- Compliance with external IT requirements. This should take into consideration all the potential legal or contractual requirements toward SAI IT systems.

In terms of IT/IS audit capacity, at this level, SAI should be able to:

- Establish quality assurance procedures for IT/IS audit procedures.

3.1	The SAI manages Performance and Conformance Monitoring.	**The SAI Performance and Conformance Monitoring should:** Collect, validate and evaluate enterprise and alignment goals and metrics. Monitor that processes and practices are performing against agreed performance and conformance goals and metrics. Provide reporting that is systematic and timely. **The Process should cover:** MEA01.01 Establish a monitoring approach. MEA01.02 Set performance and conformance targets. MEA01.03 Collect and process performance and conformance data. MEA01.04 Analyze and report performance. MEA01.05 Ensure the implementation of corrective actions. ***Suggested Evidence:*** Review the SAI IT performance and conformance monitoring practice. Review the monitoring approach. Review the tools and mechanisms to collect and analyze data. Review the sample

		of SAI reports on performance and conformance. Review the sample of recent corrective actions. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
3.2	The SAI manages internal control system.	**The SAI System of Internal Controls should:** Continuously monitor and evaluate the control environment, including self-assessments and self-awareness. Enable management to identify control deficiencies and inefficiencies and to initiate improvement actions. Plan, organize and maintain standards for internal control assessment and process control effectiveness. **The Process should cover:** MEA02.01 Monitor internal controls. MEA02.02 Review effectiveness of business process controls. MEA02.03 Perform control self-assessments. MEA02.04 Identify and report control deficiencies. ***Suggested Evidence:*** Review the SAI IT internal control system. Review the inventory of IT controls in place. Review the SAI practice to assess effectiveness of IT controls. Review the sample of recent self-assessment reports. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
3.3	The SAI manages compliance with the external requirements.	**The SAI External Requirements Compliance should:** Evaluate that IT processes and IT-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with; integrate IT compliance with overall enterprise compliance. **The Process should cover:** MEA03.01 Identify external compliance requirements. MEA03.02 Optimize response to external requirements. MEA03.03 Confirm external compliance. MEA03.04 Obtain assurance of external compliance. ***Suggested Evidence:*** Review the SAI practices related to compliance with the external requirements. Review the list of national regulations affecting the SAI (like information security laws, privacy laws, ICT supply chain security requirements, data breach notification obligations and etc.). Review the recent compliance assessment results (for example, external audits, compliance reports and etc.).

		For additional guidance, refer to COBIT 2019 Governance and Management Framework.
3.4	The SAI has a quality assurance function that verifies that Information Systems audits comply with the requirements.	The SAI should ensure quality of information systems audit in a similar structure to the FA, CA, PA. SAI quality control and assurance procedures should include information systems auditing as well. Reference to ISSAI 140, Element 5. ***Suggested Evidence:*** quality assurance manual and practice.

5 Pillar — QUALITY AND OPTIMIZATION

4 Level — Data Analysis (including Big Data)

At level 4, the SAI should have a well-established IT audit function, covering audit planning, audit work, reporting, quality control and quality assurance. At this level, the SAI's quality assurance function should be able to issue specific quality control reports related to IT audit.

At this level, the SAI should be mature enough to implement data analytics, including Big Data, Data Analytics and Spatial Analysis, to generate even more business value from the use of ICT. The prerequisite for this function should be the well-established/mature IT and IT audit function in the organization. SAI financial, compliance and performance audits should also be considered as beneficiaries of Big Data analysis (BDA) as it relates to all sectors of audits.

In the initial stage of BDA development, the SAI can start with data from various sources, which can be collected and managed from different auditors. In the next stage, the SAI may also try to implement multi-perspective data, which will open up new perspectives to analysis by auditors.

In terms of IT capacity, the SAI should be able to manage:

- Assurance. This envisages acquiring assurance that SAI IT systems meet expectations (legal, contractual, strategic, operational and etc.);

In terms of IT/IS audit and overall audit capacity, at this level, SAI should be able to:

- Assure quality of conducted IT/IS audits. The quality assurance department should be capable of covering IT/IS audit procedures and issuing the respective report on quality of work.
- Enable big data auditing, which envisages acquisition of appropriate infrastructure, software, skills and competences.

4.1	The quality assurance function issues report on the Information Systems audit function.	The SAI's quality assurance function should issue separate reports on the Information Systems audit function. [former ISSAI 1000 – Quality Assurance Processes 64-66] ***Suggested Evidence**:* a sample of quality assurance reports.
4.3	The SAI manages Assurance.	**The SAI Assurance Management should:** Plan, scope and execute assurance initiatives to comply with internal requirements, laws, regulations and strategic objectives. Enable management

		to deliver adequate and sustainable assurance in the enterprise by performing independent assurance reviews and activities. **<u>The Process should Cover:</u>** MEA04.01 Ensure that assurance providers are independent and qualified. MEA04.02 Develop risk-based planning of assurance initiatives. MEA04.03 Determine the objectives of the assurance initiative. MEA04.04 Define the scope of the assurance initiative. MEA04.05 Define the work program for the assurance initiative. MEA04.06 Execute the assurance initiative, focusing on design effectiveness. MEA04.07 Execute the assurance initiative, focusing on operating effectiveness. MEA04.08 Report and follow up on the assurance initiative. MEA04.09 Follow up on recommendations and actions. ***Suggested Evidence****:* Review the SAI IT assurance management practices. Review the recent assurance providers and criteria for their selection. Review the list of assurance initiatives / engagements. Review the follow up activities and recommended actions. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
4.4	The SAI has appropriate tools and infrastructure to enable Big Data Auditing.	The SAI should deploy necessary tools, infrastructure, skills and procedures to enable advanced data analytics (big data auditing). **Reference**: Guidance on Conducting Audit Activities with Data Analytics, INTOSAI Working Group on Big Data ***Suggested Evidence:*** the SAI hardware and software inventory, internal memos, external evaluation and etc.

5 Pillar — QUALITY AND OPTIMIZATION

5 Level — Model Organization

At this level, the SAI should be able to maximize the benefits of ICT for its audit work. To take advantage of level 4 results, the SAI must be able to implement Multi-technical and multi-mode approaches to Data Analysis.

This means that the SAI should be able to collect multi-source, multi-perspective and multi-relationship data from government entities (but not limited, since the SAI can also use open data) to take advantage of all the benefits of multiple techniques and multimode approaches. These approaches would also allow for continuous audits/monitoring of specific entities and fields, so that online and stored data can also be combined. The realization of benefits is fully dependent on the SAI's ability to set clear analytical objectives and technical maturity to analyze the data.

Advanced data analytics from SAI, such as Big Data, can be part of the Information Systems audit function. Therefore, a SAI should strive to enhance its IT audit function by ensuring quality audit work. This should be achieved by implementing effective internal controls and regularly conducting external assessments and audits for independent opinion.

In addition to Data Analysis (including Big Data), the SAI must also be able to ensure that it complies with best practices for IT governance. IT as a prerequisite for the BDA should be optimized to maximize the results of the analysis.

5.1	The SAI conducts Big Data Auditing.	The SAI should comprehensively integrate multi-industry electronic data around audit objectives and scope, investigation items, research, etc. for analysis and utilization. **Reference: Guidance on Conducting Audit Activities with Data Analytics, INTOSAI Working Group on Big Data** ***Suggested Evidence:*** a sample of audit reports.
5.2	The SAI uses Geographical Information Systems (GIS) for the audit purposes.	The SAI integrates GIS technology in the audit process to meet audit objectives. ***Suggested Evidence:*** a sample of audit reports.

5.4	The SAI manages the quality of IT.	**<u>The SAI Quality Management should:</u>** Define and communicate quality requirements in all processes, procedures and related enterprise outcomes. Enable controls, ongoing monitoring, and the use of proven practices and standards in continuous improvement and efficiency efforts. **<u>The Process should cover:</u>** APO11.01 Establish a quality management system (QMS). APO11.02 Focus quality management on users. APO11.03 Manage quality standards, practices and procedures and integrate quality management into key processes and solutions. APO11.04 Perform quality monitoring, control and reviews. APO11.05 Maintain continuous improvement. ***Suggested Evidence:*** Review the SAI IT quality management practices. Review the results of the quality monitoring, control and reviews. *For additional guidance, refer to COBIT 2019 Governance and Management Framework.*
5.5	The Information Systems audit function has been evaluated by an external/internal body.	The SAI should ensure that the Information Systems audit function is evaluated by an external/internal body. Reference to ISSAI P-20, Principle 9. ***Suggested Evidence:*** a sample of external evaluation report.