Addressing the Challenges of IT Audits by Supreme Audit Institutions

Supreme Audit Institutions (SAIs) refer to the national agencies entrusted with ensuring accountability in the functioning of national governments through external audit. The mandates, responsibilities and organization of SAIs for conducting external public-sector audit vary across the international community based on national governance systems and government policies. Independence of the SAIs from the state and its executive is of prime importance. The audit powers span across the audits of public authorities, tax audits, public contracts and public works, commercial enterprises with public participation, subsidized institutions, and international and supranational organizations.

The International Organization of Supreme Audit Institutions (INTOSAI) operates as an umbrella organization for the external government audit community. It provides an institutionalized framework for SAIs to promote development and transfer of knowledge; improve government auditing worldwide; and enhance the professional capacities, standing and influence of member SAIs in their respective countries. INTOSAI is structured into seven regional organizations as well as several committees and working groups that deliberate on subjects of technical importance for member SAIs. These include the INTOSAI Working Group on IT Audit (WGITA) that deals with IT audits.

Challenges in IT Audits by SAIs

As shown in **figure 1**, challenges in conducting IT audits by SAIs can be classified under four categories.

These challenges, described as follows, are not mutually exclusive:

1. **Institutional challenges**—These pertain to the absence of adequate mandate and/or legislations to enable the SAI to conduct IT audits.
2. **Organizational challenges**—These pertain to the systems and structures in the SAI that enable IT audits. Some of the ways in which this can be manifested include:

Figure 1—Challenges in IT Audits by SAIs

- Creating an IT unit within the SAI; establishing a proper management and supervisory system
- Integrating IT issues in other audits
- Establishing effective policy
- Properly monitoring indicators
- Making available proper tools and techniques for conducting IT audits

3. **Professional staff challenges**—These pertain to the availability of adequately trained and skilled staff for conducting IT audits.
4. **Establishing relevance for the public sector**—This is imperative for SAIs given the increasing computerization of administration and service delivery by the public sector.

Shourjo Chatterjee, CIA
Is currently working as accountant general (Accounts and Entitlements), Jammu and Kashmir, India. A member of the Indian Audit and Accounts Service since 2001, he has previously served as director of audit for the Income Tax Department and Indian Air Force, and also as the strategy and knowledge manager at the International Organization of Supreme Audit Institutions (INTOSAI) Development Initiative, Oslo, Norway. He has been the editor of in-house journals and newsletters such as *Audit Eye* (Office of the Principal Director of Audit [Central], Kolkata, India), *Rupee Trail* (Journal of Revenue Audit, Office of the Comptroller and Auditor General of India) and *IDI Focus* (IDI Newsletter).

Addressing the Challenges

Over the years, the SAI community and individual SAIs have made great efforts to establish robust IT audit functions in different SAIs. This has been done by addressing the challenges, as shown in **figure 2**. Some of these are covered in this article.

Mandates of SAIs to Conduct IT Audits

As mentioned in the Lima Declaration of Guidelines on Auditing Precepts, 1977, the traditional task of SAIs is to audit the legality and regularity of financial management and accounting.[1] In addition, SAIs conduct performance audits oriented toward examining the performance, economy, efficiency and effectiveness of public administration. Elaborating further on the audit powers of SAIs, the Declaration mentions that the SAIs draw their audit powers from the constitutions of their respective countries, which are further enacted through relevant legislations.

Section 22 of the Lima Declaration discusses audit of electronic data processing facilities:

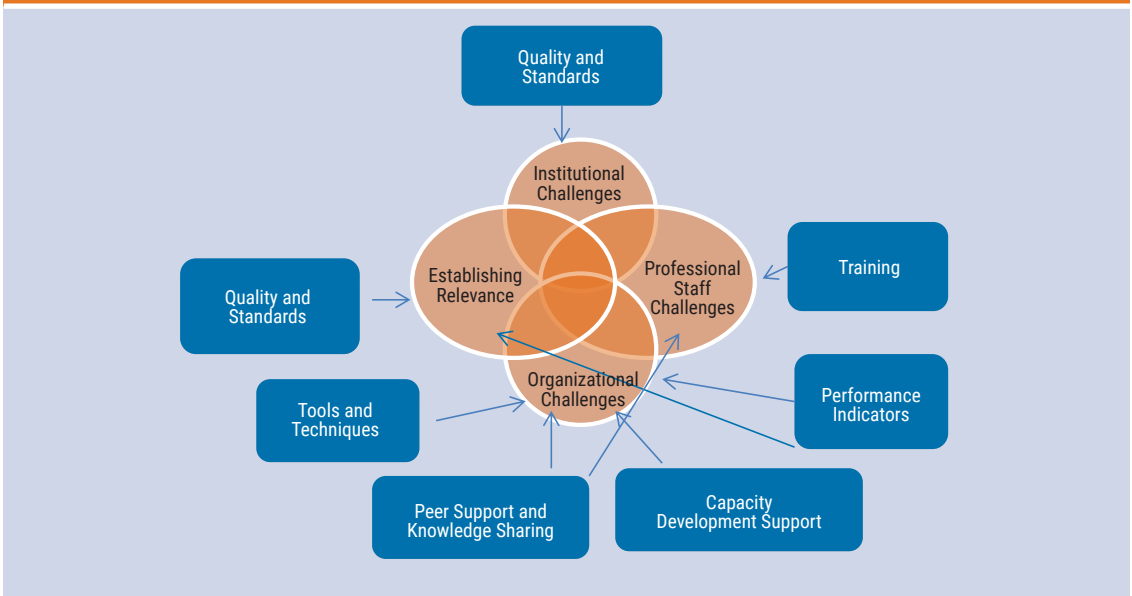
> *The considerable funds spent on electronic data processing facilities also calls for appropriate auditing. Such audits shall be systems-based and cover aspects such as planning for requirements; economical use of data processing equipment; use of staff with appropriate expertise, preferably from within the administration of the audited organisation; prevention of misuse; and the usefulness of the information produced.*[2]

Following up on the Lima Declaration, the SAI community initiated IT audits as part of its mandates by getting relevant legislations enacted in different countries.

Peer Support and Knowledge Sharing Among SAIs

Through the efforts of INTOSAI, INTOSAI WGITA, INTOSAI regions, individual SAIs and the INTOSAI Development Initiative (IDI), the capacity development arm of INTOSAI, the discipline of IT audits by SAIs has evolved substantially over the past two decades. INTOSAI WGITA, being the professional volunteer grouping on IT audit within INTOSAI, was set up in Berlin in 1989 to address SAIs' interests in the area of IT audit. The grouping currently has 44 member countries and is involved in setting the IT audit agenda for SAIs.

Figure 2—Addressing Challenges in IT Audits by SAIs



Enjoying this article?

- Learn more about, discuss and collaborate on it audit tools and techniques in the Knowledge Center. *www.isaca.org/it-audit-tools-and-techniques*

Through the years, WGITA has supported the SAIs' efforts to build their IT audit mandates and portfolio. In addition to regular seminars and knowledge-sharing workshops, it has published several guides on the subject.[3] WGITA also cooperates with ISACA®, which supports the development of IT audit in the public sector.

Quality and Standards in IT Audits

IT audits as a workstream for SAIs have evolved in a period when the SAI community has been actively working toward development and implementation of standards for public-sector auditing. Development and implementation of standards are two of the most important instruments for ensuring quality in audit engagements. INTOSAI has also developed the officially authorized and endorsed International Standards for Supreme Audit Institutions (ISSAIs), aimed at setting international standards for public-sector auditing. One such standard has also been developed specifically for information systems security review methodology, ISSAI 5310. The ISSAI framework is organized in four levels:

1. Founding principles
2. Prerequisites for the functioning of SAIs
3. Fundamental auditing principles for carrying out auditing of public entities
4. Auditing guidelines that translate the fundamental auditing principles into specific, detailed operational guidelines such as ISSAI 5310

> "DEVELOPMENT AND IMPLEMENTATION OF STANDARDS ARE TWO OF THE MOST IMPORTANT INSTRUMENTS FOR ENSURING QUALITY IN AUDIT ENGAGEMENTS."

The integrated framework of standards and guidance supports good quality and standardized IT audits as part of audits integrated with other issues. INTOSAI and member SAIs have also drawn on the different principles of COBIT® as a valuable reference standard for planning and conducting audits. The major reference source for SAIs in this regard is the WGITA-IDI *IT Audit Handbook for Supreme Audit Institutions* that is being used by several SAIs.

Capacity Development Support for SAIs

During 2013-2016, there was an IDI-WGITA cooperation program for IT audit[4] aimed at supporting SAIs in enhancing their capacity and performance in IT auditing. This program was undertaken because SAIs are facing increasing challenges of auditing in a computerized system environment, thus creating a need for SAIs to build capacity in the area of IT audit to be able to give acceptable recommendations on the client's systems and financial reports in accordance with the INTOSAI standards and best practices. This program involved the development and dissemination of the WGITA-IDI *IT Audit Handbook for Supreme Audit Institutions*, a blended learning program on IT audit for SAI teams, and support in conducting IT audits based on the ISSAIs. Besides being supported with professional guidance material and support from mentors, the SAIs also benefited from peer support and experience sharing from the other participants as part of this cooperative audit. SAIs from different regions participated in the program, including:

- **Asia**—19
- **Africa**—5
- **Caribbean**—5
- **Europe**—7
- **Pacific**—4

Training and Professionalization

SAIs have organized training for their staff conducting IT audits. These training sessions have covered the different facets of IT audits and

have involved resource persons from professional agencies and peer SAIs. In addition, SAIs have encouraged their staff to obtain professionally benchmarked certifications such as the Certified Information Systems Auditor® (CISA®) and the Certified Information Security Manager® (CISM®). SAIs have been providing coaching for such certifications as well as reimbursing the costs involved. This has helped the SAIs to develop a pool of trained and certified IT audit professionals.

Established Tools and Techniques and Development of New Tools

Different SAIs have used audit software such as Audit Command Language (ACL), Interactive Data Extraction and Analysis (IDEA) and TeamMate Analytics. The EUROSAI IT Working Group[5] has developed a specialized audit tool for SAIs—Control Space for e-Government Audit Project (CUBE)—which is a tool meant to facilitate audits of e-government.

Performance Indicators and Benchmarking

The SAI Performance Measurement Framework (SAI PMF)[6] is an international framework for self-peer or external assessment of an SAI's performance against the ISSAIs and other established international good practices, thereby providing a holistic and evidence-based evaluation of the SAI's performance, including its audit function. Another self-assessment tool specific to the IT audit function is the Information Technology Audit Self-Assessment (ITASA), which is an audit-quality instrument that takes the form of a workshop with participants from audit and IT audit at various levels. The approach allows for a focused and pragmatic solution definition. ITASA is led by a moderator who comes from another SAI.

Establishing Relevance

IT audits are not limited to strict IT audits that examine issues exclusively related to IT systems. Rather, SAIs also use IT audit tools as part of integrated audits. In addition, SAIs also use IT audit tools for planning and supplementing other audits. SAIs can establish their relevance only by conducting stand-alone IT audits as well as integrated audits that have been selected on the basis of proper risk assessment, conducted professionally with practical recommendations and properly followed up.

Since the SAIs' mandates span the sphere of governance, the IT audits conducted across the countries cover a wide variety of issues. Some of the IT audits conducted by SAIs from different developing and developed countries are mentioned in **figure 3**. This is just an indicative list of subjects where the SAIs have utilized the tools and techniques of IT audits. To be of contemporary relevance, these indicative audits have been drawn from those undertaken by the SAIs during 2014-2018. Some of these audits are discussed in greater detail in the next section.

"SINCE THE SAIS' MANDATES SPAN THE SPHERE OF GOVERNANCE, THE IT AUDITS CONDUCTED ACROSS THE COUNTRIES COVER A WIDE VARIETY OF ISSUES."

Subject to confidentiality constraints and different mandates of the SAIs in regard to publishing the reports, these may or may not be available on their respective websites. SAIs have different mandates in terms of publishing their reports. While some treat the submission of reports to the legislatures as publishing, others may upload the reports on their websites for access by the general public.

The IT audits listed in **figure 3** have examined and reported on the entire spectrum of issues related to the procurement, operation, security, etc., of one or more IT systems under study in each of the audits. Indicative results from the previously mentioned audits are summarized under the areas as noted.

IT Governance

The Office of the Auditor General of Canada conducted a performance audit on information technology investments pertaining to the Canada Border Service Agency (Agency) in 2015. The audit focused on assessing whether the agency has the

Figure 3—Illustrative List of IT Audits Conducted by Select SAIs During 2014-2018	
Name of SAI (Country)	**IT Audits Conducted**
Australian National Audit Office	• Administration of Medicare Electronic Claiming Arrangements, 2018[7] • myGov Digital Services, 2017[8] • Cyber Resilience Across Entities, 2016[9]
Office of the Auditor General of Canada	• Information Technology Shared Services, 2015[10] • Information Technology Investments—Canada Border Services Agency, 2015[11]
Rigsrevisionen, Denmark	• Protection of IT systems and health data in three Danish regions, 2017[12] • Management of IT security in systems outsourced to external suppliers, 2016[13] • Usability of public digital services directed at businesses, 2015[14]
Riigikontroll, Estonia	• Usability of public e-services, 2016[15] • Effectiveness of development of broadband network or high-speed Internet, 2015[16]
National Audit Office, Finland	• Planning and monitoring costs and benefits of information system procurement, 2017[17] • Steering of the operational reliability of electronic services, 2017[18] • Cyberprotection arrangements, 2017[19]
Office of the Comptroller and Auditor General of India	• IT Audit of Billing (Electricity) Systems in Telangana, 2017[20] • IT Audit of Value-Added Tax Implementation System in Andhra Pradesh, 2016[21] • IT Audit of Haryana Registration (Property) Information System, 2015[22]
Office of Auditor General, Nepal	• IT Audit of Accounting Software—Rural Water Supply and Sanitation Fund Development Board, 2016[23] • IT Audit of VRS Software in Transport Management Office, 2015[24]
Riksrevisjonen, Norway	• Investigation of Digitisation of Municipal Services, 2016[25]
Government Accountability Office, USA	• Veteran Affairs Health IT Modernization, 2018[26] • Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices, 2017[27] • Federal Human Resources Data: OPM (Office of Personnel Management) Should Improve the Availability and Reliability of Payroll Data to Support Accountability and Workforce Analytics, 2016[28]

corporate and management practices in place to enable the delivery of IT investments that align with and support its strategic corporate objectives. The agency had developed the necessary corporate and management practices to deliver on IT investments through its project portfolio management framework. However, the agency had not put into practice all the elements of the framework that would enable it to ensure that the delivery of IT investments align with and support its strategic corporate objective.

Development and Acquisition

In 2016, the Comptroller and Auditor General of India published an IT audit report on the implementation of VATIS, an IT application for use in the Commercial Tax (Value-Added Tax [VAT]) Department in the Government of Andhra Pradesh. In addition to other issues, this report examined issues pertaining to development and acquisition. Processes relating to dealer registration, VAT returns, VAT audit and assessment, and the Goods Information System (GIS) that monitors interstate transactions, etc., were computerized under this. The audit revealed deficiencies in the system relating to planning and use of IT applications, mapping of business rules, access controls, data capture and validations, data integrity and system security issues, etc.

IT Operations

In 2016, the National Audit Office of Estonia analyzed eight e-services of four information systems (Public Procurement Register, the information system for submission of data for national statistics, public e-File and information system for spatial planning procedures) and found that some of the reviewed public e-services are not easy or convenient to use. For example, not all of the services in the sample could be used without guidance or instruction materials. Also, using some of the services was inconvenient for certain user groups; no simplified or adaptive websites had been created for using the e-services on smart devices.

Outsourcing

The Office of the Auditor General of Denmark conducted an audit on the management of IT security in systems outsourced to external suppliers in 2016. The audit concluded that when IT processes are outsourced to external suppliers, the authorities no longer have direct control of the IT security, but remain responsible for managing the security of the IT systems. Controls in relation to access control and logging were not in place. Responsibilities for monitoring the supervision of the security of the outsourced service were also not defined properly. The majority of the examined authorities needed to improve their risk assessments, which would provide them the basis for managing IT security at their suppliers. IT systems consist of various technical layers/components, which, together, make up the infrastructure of the systems. In principle, each of these layers could represent a potential risk. It is, therefore, essential that the risk assessments conducted by the authorities take into consideration the risk associated with each of the layers of the IT infrastructure. Through this approach, the authorities can determine whether they need to impose requirements on and monitor the IT security in all technical layers.

> “IT IS…ESSENTIAL THAT THE RISK ASSESSMENTS CONDUCTED BY THE AUTHORITIES TAKE INTO CONSIDERATION THE RISK ASSOCIATED WITH EACH OF THE LAYERS OF THE IT INFRASTRUCTURE.”

Information Security

The Australian National Audit Office (ANAO) presented an audit report, “Cyber Resilience Across Entities,” in 2016. This was a follow-up to another specific audit on the issue of vulnerability to cyberattacks on information systems in seven public agencies of the Government of Australia. In the previous audit, ANAO examined implementation of the mandatory strategies in the Australian Government *Information Security Manual* (ISM). ANAO detected that security controls in place in these seven agencies provide a reasonable level of protection from breaches and disclosures from internal sources but not against cyberattacks from external sources.

Application Controls

In a 2016 report, “Federal Human Resources Data: OPM Should Improve the Availability and Reliability of Payroll Data to Support Accountability and Workforce Analytics,” the US Government Accountability Office (GAO) found, among other issues, that although some elements of the data are sufficiently reliable for general use, weaknesses in OPM’s internal controls for Enterprise Human Resources Integration (EHRI) payroll data needed to be addressed to enhance the reliability of other data elements. These weaknesses pertain to design and implementation of control activities over the IT infrastructure, performing continuous monitoring of the design and operating effectiveness of the internal control system as part of the normal course of operations, and evaluation and documentation of such monitoring.

Other Issues

In their audits, SAIs have also examined other issues such as the business continuity plan, disaster recovery plan, management of legacy systems and data migration.

Conclusion

The SAI community is actively engaged in conducting IT audits across different IT systems in operation in public agencies in their respective countries. The INTOSAI and its agencies are facilitating such audits through knowledge sharing and peer support initiatives. For citizens to harness the benefits of IT systems in operation in public entities while being reassured of the safety of operations and information, it is imperative that the SAIs continue to strengthen this important area of their mandates and reassure the respective governments about the robust functioning of their IT systems. This will, in turn, increase the effectiveness of citizen-centric service delivery through the use of IT systems.

Author's Note

The respective SAIs have the sole copyright of all the audit reports/findings/recommendations mentioned in this article. Audit topics and references to reports have been sourced only from information/reports available to the public on the websites of the respective SAIs. The opinions expressed in the article are the author's own and do not represent the views of the Office of Accountant General (Accounts and Entitlements), Jammu and Kashmir, or the office of the Comptroller and Auditor General of India.

Endnotes

1 International Standards of Supreme Audit Institutions, "Lima Declaration of Guidelines on Auditing Precepts," 1977, *www.issai.org/en_us/site-issai/issai-framework/*

2 *Ibid*.

3 These include the *WGITA-IDI Handbook on IT Audit for SAIs* in Arabic, English, French and Spanish; the *Guide to Developing IT Strategies in SAIs*; and *Auditing IT Service Management—Risk Assessment*

4 International Organization of Supreme Audit Institutions (INTOSAI) Development Initiative, Appendix to Performance and Accountability Report 2015, *www.idi.no/en/about-idi/reports*

5 EUROSAI IT Working Group, "Information Technology Self-Assessment," *www.eurosai-it.org/*

6 INTOSAI Development Initiative, "SAI Performance Measurement Framework," March 2017, *www.idi.no/en/idi-cpd/sai-pmf*

7 Australia National Audit Office, "Administration of Medicare Electronic Claiming Arrangements," 2018, *https://www.anao.gov.au/work/performance-audit/administration-medicare-electronic-claiming-arrangements*

8 Australia National Audit Office, "myGov Digital Services," 2017, *https://www.anao.gov.au/work/performance-audit/mygov-digital-services*

9 Australia National Audit Office, "Cyber Resilience Across Entities," 2016, *https://www.anao.gov.au/work/performance-audit/cyber-resilience*

10 Office of Auditor General of Canada, "Report 4—Information Technology Shared Services," 2015, *www.oag-bvg.gc.ca/internet/English/parl_oag_201602_04_e_41061.html*

11 Office of Auditor General of Canada, "Information Technology Investments—Canada Border Services Agency," 2015, *www.oag-bvg.gc.ca/internet/English/parl_oag_201504_05_e_40351.html*

12 Rigsrevisionen Denmark (RRD), "Report on the Protection of IT Systems and Health Data in Three Danish Regions," 28 November 2017, *http://rigsrevisionen.dk/publications/2017/42017/*

13 Rigsrevisionen Denmark, "Report on Management of IT Security in Systems Outsourced to External Suppliers," 15 December 2016, *http://rigsrevisionen.dk/publications/2016/52016/*

14 Rigsrevisionen Denmark, "Report on Usability of Public Digital Services Directed at Businesses," 21 December 2015, *http://uk.rigsrevisionen.dk/publications/2015/42015/*

15 National Audit Office of Estonia, "Usability of Public e-Services," 2016, *https://www.riigikontroll.ee/tabid/206/Audit/2411/language/en-US/Default.aspx*

16 National Audit Office of Estonia, "Effectiveness of Development of Broadband Network or High-Speed Internet," 2015, *https://www.riigikontroll.ee/tabid/206/Audit/2346/language/en-US/Default.aspx*

17 National Audit Office of Finland, "Planning and Monitoring Costs and Benefits of Information System Procurement," 2017, *https://www.vtv.fi/en/publication/planning_and_monitoring_costs_and_benefits_of_information_system_procurement.5380.xhtml*

18 National Audit Office of Finland, "Steering of the Operational Reliability of Electronic Services," 2017, *https://www.vtv.fi/en/publications/steering-of-the-operational-reliability-of-electronic-services/*

19 National Audit Office of Finland, *Cyber Protection Arrangements*, 2017, *https://www.vtv.fi/en/publications/cyber-protection-arrangements/*

20 Comptroller and Auditor General of India, "Overview Telangana Report No. 2 of 2017 on Public Sector Undertakings," 2017, *www.cag.gov.in/content/report-no-2-2017-public-sector-undertakings-telangana*

21 Comptroller and Auditor General of India, "Report of the Comptroller and Auditor General of India (Revenue Sector) for the Year Ended March 2015," *www.cag.gov.in/sites/default/files/audit_report_files/Andhra_Pradesh_Revenue_Sector_Report_2_2016.pdf*

22 Comptroller and Auditor General of India, "Compliance on Revenue Sector of Government of Haryana," *www.cag.gov.in/content/report-no-3-2015-compliance-revenue-sector-government-haryana*

23 Office of the Auditor General Nepal, "IT Audit of Accounting Software-Rural Water Supply and Sanitation Fund Development Board," 2016, *www.oagnep.gov.np/downloadfile/IT%20Audit%20Report%202072%20final_1461490103.pdf*

24 Office of the Auditor General Nepal, "IT Audit of VRS Software in Transport Management Office, 2015," *www.oagnep.gov.np/downloadfile/IT%20Audit%20Report%202071_1434870225.pdf*

25 Office of Auditor General of Norway, "The Office of the Auditor General's Investigation of Digitisation of Municipal Services," 2016, *https://www.riksrevisjonen.no/en/Reports/Pages/Digitalisationmunicipalservices.aspx*

26 Government Accountability Office, "Historical Perspective on Prior Contracts and Update on Plans for New Initiative," USA, 18 January 2018, *https://www.gao.gov/products/GAO-18-208*

27 Government Accountability Office, "Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices," USA, 2017, *https://www.gao.gov/products/GAO-17-549*

28 Government Accountability Office, "Federal Human Resources Data: OPM Should Improve the Availability and Reliability of Payroll Data to Support Accountability and Workforce Analytics," USA, 2016, *https://www.gao.gov/products/GAO-17-127*