

Word Count – 3,890
(excluding Reference and Appendix)

Implementation of Forensic Audits in Supreme Audit Institutions

Ms. Sutthida Paiboon
Auditor, Professional Level
State Audit Office of the Kingdom of Thailand

1. Introduction

Fraud and corruption have increased significantly, urging Supreme Audit Institutions (SAIs) to strengthen their role in fraud detection and prevention. Discussion on this matter first emerged in the 12th UN-INTOSAI Seminar in 1996 (UN/INTOSAI, 1996) and expanded at the 16th INCOSAI (1998), emphasizing two key aspects: (1) the role of SAIs in preventing and detecting fraud and corruption and (2) new auditing methods and techniques to support this role (Borge, 1999).

To further enhance the role of SAIs in combating fraud and corruption, the Congress of 17th INCOSAI (2001) established the "Task Force on Fighting Fraud and Corruption", later upgraded to the "Working Group on Fighting Against Corruption and Money Laundering (WGFACML)" at the 19th INCOSAI (2007) to reinforce the proactive role of SAIs in countering corruption and money laundering (WFAGML, 2024).

The term "**Forensic Audit**" was first introduced in the 16th INCOSAI (1998), promoting specialized forensic audit units within SAIs to detect fraud and gather evidence for legal proceedings. Despite its benefits, some SAIs face limitations in investigative powers (Borge, 1999; Dye, 2007). Over the past two decades, forensic auditing has been continuously promoted through training courses, guidelines, and academic publications (INTOSAI, 2000; Chatterji, 2001; Vasudevan, 2004; COA, 2012; AFROSAI-E, 2015; ASEANSAI, 2018; SAO, 2024).

To update the current situation regarding the implementation of forensic audits within SAIs, this paper explores:

- (a) the definition of forensic audit in the context of public sector auditing
- (b) the objectives of implementing forensic audits in SAIs.

This study is based on a literature review and survey data from SAIs with forensic audit experience.

2. Definition of Forensic Audit in the Context of Public Sector Auditing

A review of literature from the SAI community over the past two decades, the definition of forensic audit has evolved from an accounting and legal perspective to incorporating information technology in data analysis.

Early studies, such as Chatterji (2001), broadly defined forensic auditing as the application of audit skills in legally significant cases. Vasudevan (2004) further described it as an integration of financial, compliance, performance, and investigative auditing techniques to uncover and expose financial misconduct. The SAI Canada Forensic Audit Manual (OAG, 2005) defined forensic auditing as a combination of investigation, auditing, and forensic accounting for civil or criminal cases. Similarly, AFROSAI-E Forensic Audit Manual (AFROSAI-E, 2015) emphasized forensic auditing as combining accounting knowledge, investigative methods, and evidence collection for legal proceedings.

Furthermore, the AFROSAI-E manual highlights five key differences between forensic and regular audits (Financial Audit, Performance Audit, and Compliance Audit) conducted by SAIs: objective, scope, methodology, timing, and evidence (see Table 1).

Table 1: The Difference between Regular Audits and Forensic Audits

Aspect	Regular Audits	Forensic Audits
Objective	FA – Expressing opinions on financial statements; CA – Identifying compliance issues; PA – Identifying operational effectiveness and efficiency issues	Determining whether fraud has occurred and identifying the responsible party based on legally mandated authority
Scope	FA – Examining financial information; CA – Evaluating legal compliance; PA – Assessing operational effectiveness and efficiency	Investigating specific fraud indicators or allegations
Methodology	Collecting and examining related documents/transactions and interviewing relevant individuals	Uses similar techniques as regular audits but with a deeper analytical approach
Timing	Conducted on a regular and ongoing basis, with audits limited to specific financial periods	Conducted only when fraud indicators are present, with no time limitations
Evidence	Evidence is collected to support audit conclusions	Evidence must be legally admissible in court

Source: AFROSAI-E (2015, p.9-10)

In later research, the definition of forensic auditing has increasingly focused on accounting knowledge to expose financial crimes. Gichure & Nabwana (2017) emphasize that forensic auditors must go beyond financial figures to uncover the motives behind misconduct, as their findings may be used in legal proceedings. Šnjegota & Šnjegota (2017) highlight the importance of financial statement analysis in detecting criminal activities.

Recent definitions stress the role of technology in forensic auditing. The Guyana SAI Forensic Audit Manual (AOG, 2024) outlines three key components: Forensic Audit Thinking (professional skepticism), Forensic Audit Procedures (fraud risk identification), and Forensic Data Analysis (IT tools and data analytics).

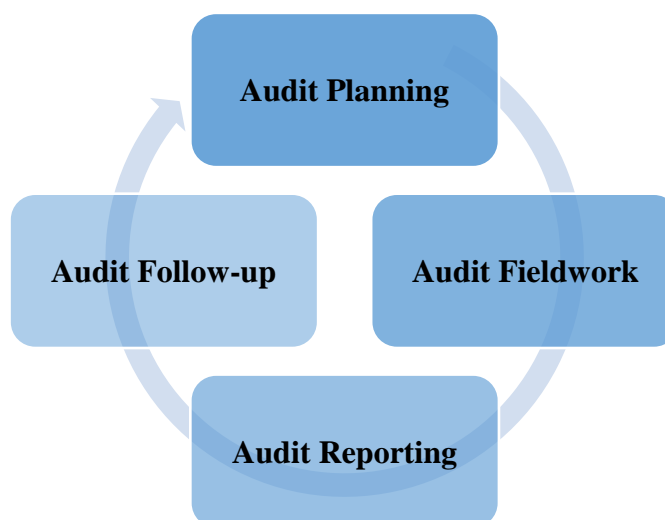
In summary, forensic auditing in public sector auditing refers to an audit approach that aimed to detect fraud and financial misconduct by integrating knowledge from multiple disciplines (e.g., accounting, law, and information technology) with audit and investigative techniques, along with data analysis, to assess and gather evidence for legal proceedings.

3. Objectives of Implementing Forensic Audits in Supreme Audit Institutions

This section explores the objectives of forensic audits implementation in SAIs through the following methods:

- (a) Literature review of forensic auditing publications within the SAI community.
- (b) Surveys conducted with SAIs that have forensic audit experience (Appendix 1 and 2).
The selection process involved randomly choosing SAIs with experience in forensic auditing that also publish forensic audit-related information in English on their official websites. The sample was drawn from 89 countries whose SAIs have investigative authority, as documented in the Global SAI Stocktaking Report 2023 by the INTOSAI Development Initiative (IDI). Priority was given to regions with the highest percentage of SAIs possessing investigative authority, in the following order: OLACEFS: 87%, AFROSAI-E: 74%, CREFIAF: 73%, PASAI: 67%, CAROSAI: 61%, No Region: 50%, ARABOSAI: 43%, ASOSAI: 29%, EUROSAI: 26% (IDI, 2023). As a result of this selection process, eight countries were chosen for the study: **Mexico, Kenya, Tanzania, Zambia, Indonesia, Philippines, Guyana, and United States.**
- (c) Content analysis of all collected data, carried out using the Principles Related to the Audit Process outlined in ISSAI 100: Fundamental Principles of Public Sector Auditing, to assess the application of forensic auditing (Figure 1).

Figure 1: The Principles Related to the Audit Process accounting to ISSAI 100: Fundamental Principles of Public Sector Auditing



Source: INTOSAI (2019a)

The study found that SAIs currently use “Forensic Audit” for two main objectives:

- (1) enhancing the capacity to identify and assess fraud risk in audit planning.
- (2) collecting evidence to verify fraud indicators in audit follow-up.

However, the application of forensic auditing varies depending on the legal authority of SAIs in each country.

3.1 Enhancing the Capacity to Identify and Assess Fraud Risk in Audit Planning

All SAIs can achieve this objective by integrating forensic auditing knowledge to strengthen existing regular audit practices. According to ISSAI standards, public sector auditing, classified as an Assurance Engagement, follows a risk-based approach. During the audit planning stage, auditors must not only identify and assess risks related to audit objectives but also consider fraud risks. To enhance their ability to detect and evaluate fraud risks, auditors can incorporate forensic auditing techniques into their audit processes, improving overall audit effectiveness.

(1) Public Sector Auditing as an Assurance Engagement

Public sector auditing consists of Financial, Performance, and Compliance Audits, each with distinct objectives but all classified as Assurance Engagements under ISSAI standards (INTOSAI, 2019a). These engagements require auditors to collect sufficient and appropriate evidence to enhance confidence in the audited subject matter.

Assurance engagements are categorized into Attestation Engagements, where the audited entity prepares the subject matter, and Direct Reporting Engagements, where auditors produce and report findings. They can provide either Reasonable Assurance, requiring extensive audit evidence, or Limited Assurance, with lower evidence requirements.

To clarify how assurance engagements relate to public sector auditing, Table 2 shows the connection between audit types, assurance engagement types, and assurance levels.

Table 2: Relationship Between Audit Type, Engagement Type, and Assurance Level

Assurance Level	Attestation Engagement (AE)	Direct Reporting Engagement (DR)
Reasonable Assurance (RA)	RA-AE: Financial Audit, Compliance Audit	RA-DR: Performance Audit, Compliance Audit
Limited Assurance (LA)	LA-AE: Financial Review, Compliance Audit	LA-DR: Performance Audit, Compliance Audit

Source: Adapted from INTOSAI (2019a), INTOSAI (2019b), INTOSAI (2020a), INTOSAI (2020b), IDI (2020a), IDI (2020b), IDI (2020c), PASAI (2020a), PASAI (2020b)

- Financial Audits follow an attestation engagement and always provide reasonable assurance, though limited assurance may be allowed under International Standards on Auditing (ISAs) or Generally Accepted Government Auditing Standards (GAGAS) (INTOSAI, 2020a; PASAI, 2020a).
- Performance Audits use a direct reporting engagement, with some SAIs offering only reasonable assurance, while others allow both reasonable and limited assurance (PASAI, 2020b).
- Compliance Audits may follow either attestation or direct reporting engagement, depending on whether compliance reports are prepared by the audited entity, and can offer reasonable or limited assurance (IDI, 2020a).

(2) Assurance Engagements Conducted by SAIs Using a Risk-Based Approach

In performing assurance engagements, ISSAI standards require auditors to consider "Audit Risk", which refers to the risk that the auditor may issue an inappropriate conclusion (INTOSAI, 2019a; INTOSAI, 2019b; INTOSAI, 2020a; INTOSAI, 2020b). While auditors must reduce this risk to an acceptably low level in reasonable assurance engagements, it cannot be fully eliminated due to inherent limitations. In limited assurance engagements, the acceptable risk level remains higher but must still be managed effectively.

To mitigate audit risk, auditors focus on:

- **Audit Planning & Audit Fieldwork** – Identifying and assessing risks, designing appropriate responses, and evaluating audit evidence.
- **Audit Reporting & Audit Follow-Up** – Ensuring reports are based on sufficient evidence and implementing follow-up mechanisms to monitor findings.

(3) Fraud Risk Assessment in Audit Planning

According to ISSAI standards, auditors are not primarily responsible for preventing or detecting fraud but must identify and assess fraud risks during audit planning (INTOSAI, 2019a; INTOSAI, 2019b; INTOSAI, 2020a; INTOSAI, 2020b). Maintaining professional skepticism ensures that fraud does not materially misstate audit findings.

To assess fraud risk, ISSAI standards require auditors to apply the Fraud Triangle Theory, which includes three key factors: Pressure (Incentive), Opportunity, and Rationalization. Auditors may identify red flags indicating fraud risks, as shown in Table 3.

Table 3: Examples of Red Flags Indicating Fraud Risk by Audit Type

Audit Type	Audit Type
Financial Audit	<ul style="list-style-type: none"> • Inaccurate financial reporting or budgeting. • Suspicious or large fund transfers occurring before, at, or after the fiscal year-end. • Expenditures significantly exceeding or falling below estimates. • Incomplete, improperly recorded, or inconsistent transactions. • Missing documents, lack of original records, or signs of document alterations.
Performance Audit	<ul style="list-style-type: none"> • Low output, poor quality, lack of outcomes, or ineffective operational systems. • Failure to deliver projects or services. • Redundancy or overlap in projects or services.
Compliance Audit	<ul style="list-style-type: none"> • Violation or failure to comply with laws, regulations, procedures, and government best practices. • Unauthorized transactions or misuse of assets. • Unapproved budget adjustments. • Unauthorized access to systems and data records.

Source: IMF (2022)

Once fraud indicators are confirmed, SAIs may use different follow-up mechanisms based on their investigative authority (G20, 2023).

- **Non-Investigative SAIs** refer fraud cases to law enforcement agencies (e.g., India, China) (P.K.Tiwari, 2015; Raiss Shaghaghi, 2023).
- **Investigative SAIs** conduct evidence collection before forwarding cases to law enforcement agencies (e.g., Mexico, Kenya, Tanzania, Zambia, Indonesia, Philippines, Guyana, US) (Refer to Section 3.2 for details).

(4) Applying Forensic Auditing Knowledge to Enhance Fraud Risk Assessment

SAIs can apply forensic auditing knowledge to improve fraud risk assessment during audit planning (SAO, 2024; NAOT, 2024). Key forensic auditing applications are as follows:

- Understanding the definitions, types, and schemes of fraud.
- Identifying fraud indicators and warning signs.
- Using the Fraud Triangle/Fraud Diamond theory¹.
- Data analytics for fraud detection.

SAIs apply forensic auditing through:

- Training programs (e.g., Mauritius, Australia, South Korea, China, Oman, Canada, France, India, Italy, Japan, South Africa, Turkey, UK, US) (G20, 2023).
- Creating fraud and corruption databases (See Box 1).

Box 1: Example of Fraud and Corruption Databases by SAI India

India

SAI India has collected corruption-related data and published research reports for auditor capacity-building programs, including:

- Research on Fraud Indicators and Anti-Corruption Measures related to:
 - Public Works projects.
 - Accounts Payable Process in government agencies.
 - Pension Payments.
 - Provident Fund Payments.
- Research on Corruption in the Government Sector, including:
 - Case studies of fraud detection in public agencies.
 - Statistical analysis of fraud patterns in different sectors.

Source: <https://cag.gov.in/rti/nagpur/en/page-rti-nagpur-res-papers-rti-ngp>

- Updating indicators and data analysis methods related to fraud and corruption for the Data Analysis Center (DAC) within SAIs. (See Box 2).

¹ Fraud Diamond Theory (SAO, 2024) is an extension of the Fraud Triangle Theory, consists of four key factors: Pressure/Incentive – the motivation or pressure to commit fraud, Opportunity – the circumstances that allow fraud to occur, Rationalization – the justification used to legitimize fraudulent actions, and Capability – the ability to carry out fraudulent activities effectively.

Box 2: Examples of Data Analysis Centers within SAIs

United Kingdom

SAI UK has established the "Data Service" to provide big data analysis support for auditors. The Data Service is responsible for:

- Managing large datasets.
- Storing data in centralized databases.
- Integrating datasets for auditors to use in investigations.
- Offering guidance and analytics support via SharePoint.
- Hosting a Methods, Economics, and Statistics Hub (MESH) to develop advanced data models.

Italy

SAI Italy has established the "Data Analysis Competency Centre", comprising a cross-functional team of experts from various disciplines. This unit supports audit teams in areas such as artificial intelligence, data analysis, predictive analytics, and other data analysis techniques. However, the center is currently in its early stages of development.

Turkey

In 2017, SAI Turkey launched the "Data Analysis Group" with the aim to:

- Develop Computer-Assisted Audit Techniques (CAATs).
- Enhance risk assessment in municipal audits.
- Reduce auditors' manual workload.
- Analyze large-scale financial data.
- Identify data processing errors.
- Continuously monitor audit results.

The group developed "VERA", an automated risk assessment system used to analyze more than 1,400 municipalities and assist in audit planning and fraud detection.

Source: OECD (2022)

3.2 Collecting Evidence to Verify Fraud Indicators in Audit Follow-Up

SAIs can achieve this objective through the following seven key components: (1) Investigative Power (2) Special Audit Unit (3) Special Audit Team Qualification (4) Tools for Audit (5) Standard/Manual for Audit (6) Receiving Cases from Internal/External Sources and (7) Reporting Cases to Authorities.

In practice, forensic audit is used in integration with investigative auditing, particularly in forensic analytics, to collect evidence that confirms fraud indicators during the audit follow-up process.

(1) Seven Components Supporting Forensic Auditing in SAIs

An analysis of forensic auditing practices in eight countries (*Mexico, Kenya, Tanzania, Zambia, Indonesia, the Philippines, Guyana, and the United States*) identified the following seven essential components for supporting forensic auditing in SAIs (details in Appendix 1):

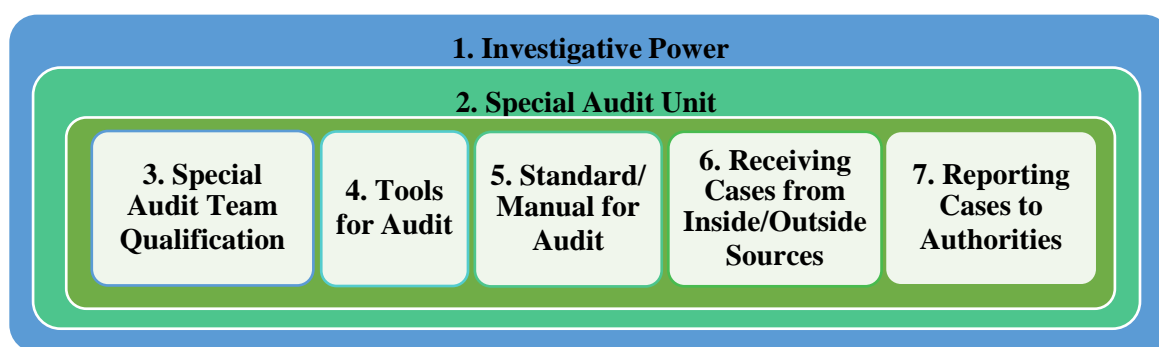


Figure 2: Seven Essential Components for Supporting Forensic Audit in SAIs

Source: Author

1. Investigative Power

Every SAI has "Investigative Power" defined in their national constitution or audit laws. These laws grant SAIs the authority to:

- Conduct investigative audits and/or forensic audits.
- Access all types of financial documents and related data from the audited entity.

With this investigative power, SAIs can independently conduct forensic audits and collect evidence before forwarding fraud cases to law enforcement agencies.

2. Special Audit Unit

Every SAI conducting forensic audits has a dedicated "Special Audit Unit" responsible for investigating fraud cases, collecting evidence, and conducting forensic analytics.

Operational models of Special Audit Units are two roles:

- (1) Proactive Role: The unit identifies fraud indicators independently before launching investigations.
- (2) Reactive Role: The unit receives fraud reports and investigates based on incoming fraud indicators.

In organizational structure perspective, some SAIs have established specialized forensic audit units dedicated exclusively to investigative auditing and forensic accounting. Examples include: Tanzania - Forensic Audit Unit, Guyana - Forensic Audit Unit, Indonesia - Investigative Audit Unit, US - Forensic Audits and Investigative Service (FAIS), Kenya - Forensic Audit, Zambia - Forensic and Investigation Audit, and Philippines - Fraud Audit Office.

Meanwhile, other SAIs incorporate forensic and investigative auditing functions within broader audit divisions, which oversee multiple areas under special audit departments. For example: Mexico – The General Directorate of Forensic Audit (DGAF) operates under the Special Audit of Financial Compliance (AECF).

3. Special Audit Team Qualification

Each forensic audit team consists of "Multidisciplinary Experts", including:

- Accounting: Certified Public Accountants (CPA), Forensic Experts.
- Law & Investigation: Certified Fraud Examiners (CFE), Lawyers.
- IT & Data Analysis: IT Experts, Data Analysts.
- Other Fields: Engineers, Public Administration Experts.

4. Tools for Audit

Forensic auditing relies heavily on “Data Analytics Tools” to detect fraud (See Box 3).

Box 3: Examples of Forensic Audit Tools Used by SAIs

Mexico - Forensic Laboratory

SAI Mexico established a Forensic Laboratory within the General Directorate of Forensic Audits (DGAF) under the Special Audit of Financial Compliance (AECF). Its aim is to gather and safeguard digital evidence; analyze physical and digital storage devices; and conduct forensic analysis to support fraud investigations.

Activities Conducted in the Forensic Laboratory:

- Digital Forensic Imaging – Capturing forensic images to preserve data integrity.
- Data Recovery & Digital Analysis – Retrieving deleted files and tracking fraudulent transactions.
- Data Matching & Pattern Detection – Identifying financial anomalies through data comparison.
- Network Analysis & Data Visualization – Investigating suspicious financial connections.
- Document Forgery Detection – Identifying fake or altered financial records.
- Secure Data Management – Ensuring safe handling and transfer of forensic data.
- Secure Data Erasure – Permanently deleting irrelevant or legally required data.

Tanzania - Digital Forensic Laboratory

SAI Tanzania established a Digital Forensic Laboratory to assist forensic auditors in: financial fraud detection, government loss estimation, and providing expert witness testimony.

High-Tech Forensic Software Used:

- Forensic Toolkit (FTK) – Forensic data analysis and investigation.
- Forensic Explorer – Digital forensic auditing and fraud detection.
- EnCase – Data recovery and fraud analytics.
- CaseWare IDEA – Financial data analysis and fraud pattern detection.
- ABBYY FineReader – Optical Character Recognition (OCR) for document digitization.

Forensic Hardware Used:

- FRED SR – High-powered forensic analysis computer.
- FRED Laptops – Portable forensic computing devices for field investigations.
- Tableau Forensic Imager TX1 – Specialized device for forensic data collection and duplication.

Zambia - Forensic Data Analysis Software

SAI Zambia employs specialized forensic tools to enhance financial fraud detection, including: EnCase – Forensic investigation of financial data; Forensic Toolkit (FTK) – Digital forensic auditing; ACL (Audit Command Language) – Advanced audit data analytics.

Indonesia - Digital Forensic Laboratory (LED)

SAI Indonesia established the Digital Forensic Laboratory (LED) to assist in: investigative audits, fraud detection and analysis, and legal calculations of government financial losses.

Key Forensic Tools Used:

- Data Analytics Tools – Identify financial anomalies, fraud risks, and suspicious patterns in financial data.
- Optical Character Recognition (OCR) Software – Convert scanned financial documents into searchable, analyzable text.
- Audit Trail System – Utilize cloud storage (OneDrive) to automatically record audit activities.
- Digital Forensic Investigation Software (e.g., EnCase, FTK, Cellebrite, Oxygen) – Recover digital evidence and investigate cyber fraud.
- Data Visualization Software (e.g., Power BI) – Convert complex financial data into visual graphs to detect fraud trends.

United States

SAI US employs advanced forensic data analytics to detect fraud. The Fraud Detection Software Used is IDEA – Forensic data analysis, used for:

- Data matching (cross-checking transactions).
- Data mining (detecting fraud patterns).
- Internal control evaluations.
- Statistical sampling for fraud risk analysis.

5. Standard/Manual for Audit

To ensure the efficiency of forensic accounting audits conducted by specialized audit units, each SAI adopts different “Standard/Manual” based on their specific needs and regulatory frameworks.

Examples of Audit Standard/Manual defined by SAIs:

- US – Generally Accepted Government Auditing Standards (GAGAS)
- Philippines, Guyana, Tanzania, Zambia – Forensic Auditing Manual
- Indonesia – SAI Indonesia Regulation No. 1 & 2, 2020 and Standard Operating Procedures for Digital Forensic, used for investigative audits, calculating state financial losses, and serving as expert witnesses in court proceedings.

Examples of Audit Standard/Manual of other agencies adopted by SAIs:

- Tanzania – Adapting knowledge from the Fraud Examiners Manual by the Association of Certified Fraud Examiners (ACFE)
- US – Using Quality Standards for Investigation Build of Council of the Inspectors General on Integrity and Efficiency (CIGIE) for conducting investigative audits.

6. Receiving Cases from Internal/External Sources

Each SAI receives fraud reports through two main channels:

- Internal Reports: From regular audit departments or direct orders from the Auditor General or Parliament.
- External Complaints: Reports from the public through websites, hotlines, and complaint platforms. For example, Mexico – Ethical Line for Complaints (LED);

Tanzania – SAI Tanzania Website; Zambia – Hotline by the Zambia Information Technology Authority (ZICTA), Indonesia – Citizen Helpdesk, Philippines – Citizens' Desk Reporting System (CDRS), US – FraudNet.

7. Reporting Cases to Authorities

Every SAI must refer fraud cases to law enforcement agencies in accordance with its legal mandate. These agencies include National Police Departments, Anti-Corruption Agencies, and Prosecution Offices, ensuring that fraud cases are thoroughly investigated and prosecuted.

(2) Forensic Audit Practices: Case Study of SAI US

The example of a case study of forensic audit practices by SAI is provided in Box 4.

Box 4: Forensic Audit Practices: Case Study of SAI US

SAI US has established “Forensic Audits and Investigative Service (FAIS)”, a specialized audit office focused on (1) Forensic Audits (2) Security and Vulnerability Assessments and (3) Special Investigations. FAIS follows an Integrated Audit Approach, combining forensic auditing with investigative techniques (See Figure 5).

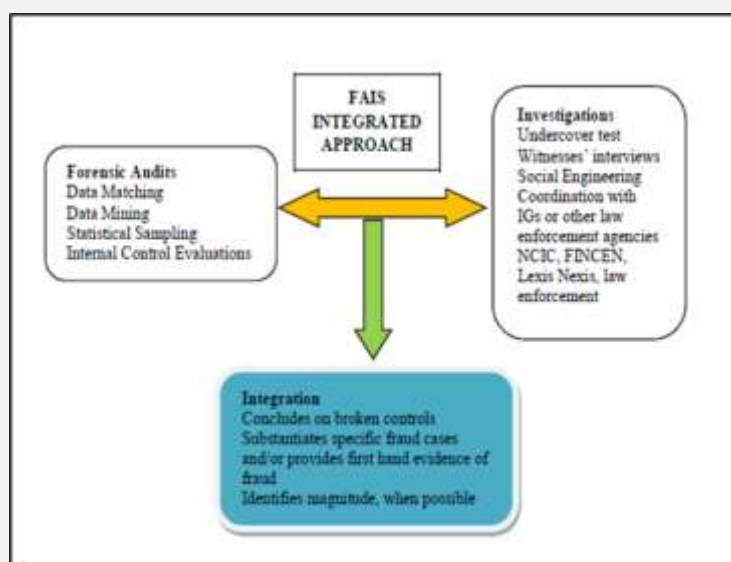


Figure 5: Integrated Audit Approach Conducted by FAIS

Source: ALSAI (2018, p.44)

Forensic auditing Methods – Forensic Analytics

- **Data Matching** – Scans and compares internal and external databases to detect inconsistencies.
- **Data Mining** – Identifies fraudulent patterns and tests internal controls for weaknesses and non-compliance. The steps of data mining are as follows:
 - Defining the target population of transactions for analysis.
 - Establishing data criteria and designing queries for data extraction.
 - Summarizing transaction patterns for further investigation and forensic analysis.

Forensic Data Analysis Tools used by FAIS is IDEA Software – Used for data extraction, comparison, and summarization.

- **Internal Control Evaluation** – FAIS evaluates internal control systems in accordance with Generally Accepted Government Auditing Standards (GAGAS), particularly in the area of performance audits, by: (a) Testing pre-designed internal controls to assess their effectiveness and (b) Identifying gaps in fraud prevention mechanisms to strengthen accountability and risk management. Additionally, FAIS follows two key frameworks for evaluating internal controls: (a) Standards for Internal Control in the Federal Government ("Green Book") and (b) A Framework for Managing Fraud Risks in Federal Programs.
- **Statistical Sampling** – Ensures accuracy and reliability in forensic audits.

Investigative Techniques

- **Covert Testing** – Secretly examines an organization's publicly available information to identify control weaknesses and vulnerabilities. Criminal investigators conduct covert testing through surveillance, false identification, fictitious companies and addresses, social engineering, concealed photography/video recording, and consensual monitoring.
- **Witness Interviews** – Collects statements to verify forensic findings.
- **Collaboration with Law Enforcement Agencies** – Works closely with the Office of Inspector General (IG) and other law enforcement agencies.
- **Accessing Law Enforcement Databases** – Utilizes specialized law enforcement tools, including: National Criminal Information Center (NCIC) – Crime database, Financial Crimes Enforcement Network (FINCEN) – Financial fraud network, Lexis-Nexis Law Enforcement – Legal database, and Forensic Audit Outcomes.

FAIS Audit Reports

FAIS audit reports summarize: (a) Internal control failures (b) Fraud-related evidence and (c) Financial impact and severity of fraud cases.

Source: ALSAI (2018), (GAO, 2003)

4. Conclusion

For over two decades, the promotion of "Forensic Audits" has been an ongoing effort within SAI community, beginning with discussions at the 16th INCOSAI Conference in 1998. As financial fraud becomes increasingly complex, forensic auditing has emerged as an essential methodology for detecting fraud and strengthening public sector auditing.

Forensic audit is a specialized methodology for detecting financial fraud by integrating accounting, law, IT, investigation, and data analytics. Its primary goal is to gather admissible evidence to support legal proceedings and ensure fraud is thoroughly investigated and addressed.

In practical application, SAIs apply forensic audits to achieve two key objectives. First, forensic audit techniques play a crucial role in enhancing fraud risk assessment during audit planning, allowing SAIs to identify potential fraud risks more effectively within regular audits. Second, forensic audits are used to gather evidence to confirm fraud indicators during audit follow-ups, a process often carried out by specialized audit units conducting in-depth forensic investigations.

Forensic auditing enables SAIs to strengthen fraud detection, enhance investigations, and support legal proceedings, reinforcing transparency, accountability, and public trust. To

maximize its impact, SAIs must commit to capacity-building, collaboration, and adherence to international standards.

Reference

- AFROSAI-E. (2015). GUIDELINE: FORENSIC AUDIT MANUAL. African Organisation of English-speaking Supreme Audit Institutions.
- ALSAI. (2018). Strategic Papers of ALSAI Auditors for the GAO's Fellowship. Retrieved from <https://panel.klsh.org.al/storage/php1bREBE.pdf>
- AOG. (2004). Rules, Policies and Procedures Manual 2004. The Audit Office of Guyana. Retrieved from <https://audit.org.gy/site/images/AOG/RPPM.pdf>
- AOG. (2019). SAI Performance Report - Audit Office of Guyana. Retrieved from <https://www.audit.org.gy/site/pubs/SAI-PMF-2019.pdf>
- AOG. (2024). Forensic Auditing Manual for the Audit Office of Guyana. Retrieved from <https://www.audit.org.gy/site/images/standards/Forensic%20Audit%20Manual%20-%20IDB.pdf>
- ASEANSAI. (2018). ASEANSAI-GUIDELINE AUDIT REVENUE. Retrieved from <https://www.aseansai.org/wp-content/uploads/2018/09/Guideline-on-Audit-of-Revenue1.pdf>
- ASF. (2019). Forensic Audits in Mexico. Retrieved from https://wgfacml.asa.gov.eg/EN/meeting2019/Forensic_Audits_Mexico.pdf
- Borge, M. (1999). The role of Supreme Audit Institutions (SAIs) in Combating Corruption. *9th International Anti-Corruption Conference, 10-15 October 1999, Durban, South Africa*.
- BPK. (2020). Strategic Plan 2020-2024. The Audit Board of the Republic of Indonesia. Retrieved from https://www.bpk.go.id/assets/files/upload/Buku-Renstra-BPK-2020_english-B.pdf
- BPK. (2023). OBTAINING KAN ACCREDITATION, BPK GUARANTEES THE QUALITY AND RELIABILITY OF THE LFD TESTRESULTS. Retrieved from <https://www.bpk.go.id/news/obtaining-kan-accreditation-bpk-guarantees-the-quality-and-reliability-of-the-lfd-test-results>
- Chatterji, A. (2001). Forensic Auditing. *ASOSAI Journal* 2001.
- COA. (2012). Commission on Audit Hosts ASOSAI Sponsored Workshop on Dealing with Fraud and Corruption. Retrieved from https://www.coa.gov.ph/wpfd_file/commission-on-audit-hosts-asosai-sponsored-workshop-on-dealing-with-fraud-and-corruption/
- COA. (2023). BEST PRACTICES AND EXPERIENCES OF THE COMMISSION ON AUDIT, THE SUPREME AUDIT INSTITUTION OF THE PHILIPPINES, IN THE FIELD OF FIGHTING CORRUPTION AND MONEY LAUNDERING. Retrieved from https://wgfacml.asa.gov.eg/EN/Meeting2023/13-Philippines,Best_Practices.pdf
- Dye, K. M. (2007). Corruption and Fraud Detection by Public Sector Auditors. (A. SHAH, Ed.) *PERFORMANCE ACCOUNTABILITY AND COMBATING CORRUPTION*, pp. 303-321.
- G20. (2023). COMPENDIUM OF GOOD PRACTICES IN ENHANCING THE ROLE OF AUDITING IN TACKLING CORRUPTION (pp. 1–51). ANTI-CORRUPTION WORKING GROUP. Retrieved from https://www.unodc.org/documents/corruption/G20-Anti-Corruption-Resources/Other-Deliverables/2023_G20_compendium_of_good_practices_on_enhancing_role_of_auditing_in_tackling_corruption.pdf

- GAO. (2003). AUDIT GUIDE-Auditing and Investigating the Internal Control of Government Purchase Card Programs. U.S. Government Accountability Office. Retrieved from <https://www.gao.gov/assets/gao-04-87g.pdf>
- GAO. (2019). GAO's Agency Protocols, 19-21. U.S. Government Accountability Office. Retrieved from <https://www.gao.gov/products/gao-19-55g>
- Gichure, F., & Nabwana, J. (2017). Forensic Audit: Looking beyond the figures. *Supreme Auditor*(6), 2-3. The Office of Auditor-General, Kenya. Retrieved from <https://www.oagkenya.go.ke/wp-content/uploads/2021/09/Supreme-Auditor-6th-edition.pdf>
- IDI. (2020a). IDI Compliance Audit ISSAI Implementation Handbook-Version 1. INTOSAI Development Initiative. Retrieved from <https://idi.no/elibrary/professional-sais/issai-implementation-handbooks/handbooks-english/1452-compliance-audit-handbook-v1-english-211213>.
- IDI. (2020b). IDI Financial Audit ISSAI Implementation Handbook-Version 1. INTOSAI Development Initiative. Retrieved from <https://idi.no/elibrary/professional-sais/issai-implementation-handbooks/handbooks-english/1118-financial-audit-issai-implementation-handbook-version-1-english-light-touch-review-2020/file>.
- IDI. (2020c). IDI Performance Audit ISSAI Implementation Handbook-Version 1. INTOSAI Development Initiative. Retrieved from <https://www.idi.no/elibrary/professional-sais/issai-implementation-handbooks/handbooks-english/1330-idi-performance-audit-issai-implementation-handbook-v1-en>.
- IDI. (2023). GLOBAL SAI STOCKTAKING REPORT 2023. Retrieved from <https://gsr.idi.no/>
- IFAC. (2018). INTERNATIONAL STANDARD ON AUDITING 240 THE AUDITOR'S RESPONSIBILITIES RELATING TO FRAUD IN AN AUDIT OF FINANCIAL STATEMENTS . International Federation of Accountants.
- IMF. (2022). Good Governance in Sub-Saharan Africa: Opportunities and Lessons. *Ch.12- The Role of Supreme Audit Institutions in Addressing Corruption, Including in Emergency Settings*, 209-231.
- INTOSAI. (2000). 17th Commonwealth Auditors-General Conference. *International Journal of Government Auditing*, 27, 7-10.
- INTOSAI. (2019a). ISSAI 100: Fundamental Principles of Public-Sector Auditing. International-Organization of Supreme Audit Institutions.
- INTOSAI. (2019b). ISSAI 300: Performance Audit Principles. International-Organization of Supreme Audit Institutions. Retrieved from https://www.intosai.org/fileadmin/downloads/documents/open_access/ISSAI_100_to_400/issai_300/ISSAI_300_en_2019.pdf
- INTOSAI. (2020a). ISSAI 200: Financial Audit Principles. International-Organization of Supreme Audit Institutions. Retrieved from https://www.intosai.org/fileadmin/downloads/documents/open_access/ISSAI_100_to_400/issai_200/ISSAI_200_en_2020.pdf
- INTOSAI. (2020b). ISSAI 400: Compliance Audit Principles. International-Organization of Supreme Audit Institutions.
- NAOT. (2024). Towards an integrated vision: non - governmental community efforts in combating corruption. National Audit Office of Tanzania. Retrieved from <https://wgfacml.asa.gov.eg/EN/Meeting2024/Exploring-Forensic-and-special-Audits-Within-SAIs-SAI-Tanzania.pdf>

- Nasution, L. R., Kaharuddin, & Cahyowati, R. (2022). Investigative Audit Authority of the Supreme Audit Agency in Auditing the Management and Responsibility of State Finances. *International Journal of Multicultural and Multireligious Understanding*, 9(3), 319-328. doi: <http://dx.doi.org/10.18415/ijmmu.v9i3.3432>
- OAG. (2005). Wrongdoing and Fraud Audit Guidance. Office of the Auditor General of Canada. Retrieved from <https://www.audit.org.gy/site/images/standards/aog---forensic-audit-manual.pdf>
- OAG. (2020). Annual Corporate Report 2020-2021. Office of the Auditor-General of Kenya. Retrieved from <https://www.oagkenya.go.ke/wp-content/uploads/2022/04/Annual-Corporate-Report-2020-2021.pdf>
- OAG. (2022). Annual Corporate Report 2022-2023. Office of the Auditor-General of Kenya. Retrieved from <https://www.oagkenya.go.ke/wp-content/uploads/2024/01/ACR-2022-23-1.pdf>
- OECD. (2017). Mexico's National Auditing System-Strengthening Accountable Governance. Retrieved from <http://www.oecd.org/gov/ethics/mexico-s-national-auditing-system-9789264264748-en.htm>
- OECD. (2018). Progress Report on the Implementation of Mexico's National Auditing System-Roadmap for Strengthening Accountable Governance. Retrieved from http://www.oecd.org/governance/ethics/WEB_ASF%20Progress%20report%20ENGLISH.pdf
- OECD. (2022). Strengthening Analytics in Mexico's Supreme Audit Institution. Retrieved from https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/10/strengthening-analytics-in-mexico-s-supreme-audit-institution_ae05f9d6/d4f685b7-en.pdf
- PASAI. (2020a). Financial Audit Manual 2020. Pacific Association of Supreme Audit Institutions. Retrieved from <https://static1.squarespace.com/static/57019a6db6aa607cbb909ab2/t/6021e5f88a9aeb6c4fdc542a/1612834335915/Regional+Financial+Audit+Manual+2020.pdf>
- PASAI. (2020b). Performance Audit Manual 2020. Pacific Association of Supreme Audit Institutions. Retrieved from <https://static1.squarespace.com/static/57019a6db6aa607cbb909ab2/t/600759b6b393ae621008ca03/1611094480090/PASAI+Performance+Audit+Manual+2020.pdf>
- P.K.Tiwari, K. S. (2015). Audit to Detect Fraud and Corruption: Evaluation of the Fight against Corruption and Money Laundering. *10th ASOSAI Research Project*. SAI India. Retrieved from <https://slideplayer.com/slide/6004293/>
- PONDOC, R. C. (2023a). MANILA BULLETIN. Retrieved from Commission on Audit: The conduct of fraud audit, Part 1. Retrieved from https://mb.com.ph/2023/10/23/commission-on-audit-the-conduct-of-fraud-audit#google_vignette
- PONDOC, R. C. (2023b). MANILA BULLETIN. Retrieved from Commission on Audit: The conduct of fraud audit, Part 2. Retrieved from <https://mb.com.ph/2023/11/6/commission-on-audit-the-conduct-of-fraud-audit-1>
- Raiss Shaghghi, S. (2023). Current Anti-Corruption Status in China. *Management, Economics, and Accounting*. Retrieved from <https://www.dpublication.com/wp-content/uploads/2023/05/14-1742.pdf>
- SAO. (2024). สรุปสาระสำคัญจากการเข้าร่วมอบรมออนไลน์ เรื่อง การใช้ทักษะการตรวจสอบทางบัญชีนิติวิทยาเพื่อเสริมสร้างประสิทธิภาพการตรวจสอบเบื้องต้น. Retrieved from <https://www.audit.go.th/sites/default/files/files/article/%E0%B8%81%E0%B8%B2%E0>

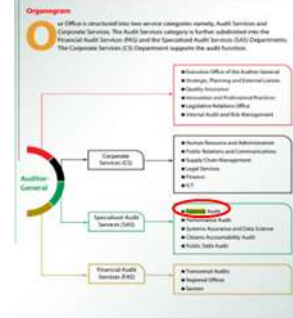
%B8%A3%E0%B9%83%E0%B8%8A%E0%B9%89%E0%B8%97%E0%B8%B1%E0
 %B8%81%E0%B8%A9%E0%B8%B0%E0%B8%81%E0%B8%B2%E0%B8%A3%E0
 %B8%95%E0%B8%A3%E0%B8%A7%E0%B8%88%E0%B8%AA%E0%B8%AD%E
 0%B8%9A%E0%B8%97%E0%B8%B2%E0%B8%87%E0%B8%9A%E0%B8%B1%E
 0%B8%8D%E0%B8%8A%E0%B8%B5%E0%B8%99%E0%B8%B4%E0%B8%95%E
 0%B8%B4%E0%B8%A7%E0%B8%B4%E0%B8%97%E0%B8%A2%E0%B8%B2%E
 0%B8%AF.pdf

- Sina, F. E. (2023). NAOT FORENSIC AUDIT FACILITY IS NOW OPERATIONAL: DOCUMENTING THE JOURNEY AND FUTURE PROSPECTS. *The Auditor General*, 1(1), 14-17. National Audit Office of Tanzania. Retrieved from https://www.nao.go.tz/uploads/CAG_AUDITOR_JOURNAL_JANUARY_-_APRIL_2023.pdf
- Šnjegota, D., & Šnjegota, B. M. (2017). Forensic accounting in function of prevention and fight against corruption in the public sector. *Challenges in Modern Corporate Governance*, 83-89. doi:10.15308/finiz-2017
- Susanto, H., Azis, H. A., Mulyani, S., & Sukmadilaga, C. (2019). The level of fraud detection affected by auditor competency using digital forensic support. *Utopia Y Praxis Latinoamericana*, 24(Esp.5), 252–267. <https://www.redalyc.org/journal/279/27962050029/html/>
- MISMANAGEMENT. the 12th UN/INTOSAI Seminar on Government Auditing, DEPARTMENT OF DEVELOPMENT SUPPORT AND MANGEMENT SERVICES. Vienna: INTOSAI. Retrieved from <http://www.intosai.org/uploads/3vn1996e2.pdf>
- Vasudevan, S. (2004). FORENSIC AUDITING. *Journal of the Institute of Chartered Accountants of India*, 53(3), 359-364. Retrieved from https://www.icaai.org/post.html?post_id=2804
- Veronika, V., & Simanjuntak, B. H. (2022). IMPLEMENTASI ISO 27037 DALAM PEMERIKSAAN INVESTIGATIF DENGAN TEKNIK FORENSIK DIGITAL UNTUK MEMPEROLEH BUKTI AUDIT DI BADAN PEMERIKSA KEUANGAN (BPK). *Jurnal Magister Akuntansi Trisakti*, 9(2), 89–104. <https://doi.org/10.25105/jmat.v9i2.13343>
- WGFACML. (2019). Minutes of the 13th Meeting of INTOSAI Working Group on Fight Against Corruption and Money Laundering, Nanjing – China (25-26 April 2019). Retrieved from https://wgfacml.asa.gov.eg/EN/meeting2019/13th_meeting_minutes.pdf
- WGFACML. (2024). About of WGFACML. Retrieved from https://wgfacml.asa.gov.eg/index_files/about_us.htm


Appendix

1. Details of SAIs that have Forensic Audit Experience

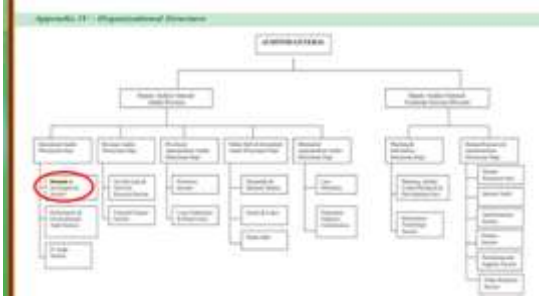
1.1 SAI Mexico - OLACEFS	
(1) Investigative Power	<ul style="list-style-type: none"> • Article 79 of the Mexico Constitution and Article 17 of the Federation's Audit and Accountability Act grant SAI Mexico the authority to investigate suspected cases of fraud or corruption. • Article 17 of the Federation's Audit and Accountability Act defines the powers of SAI Mexico as follows: <ul style="list-style-type: none"> ○ Oversee public resources allocated by the federal government. ○ Investigate actions or omissions that indicate irregularities, illegal activities, or administrative offenses. ○ Conduct on-site inspections and request relevant documents. ○ Interview and hold meetings with individuals or government officials. ○ Summon third parties to provide information.
(2) Special Audit Unit	<p>Department Name: Special Audit of Financial Compliance (AECF).</p> <p>Divisions:</p> <ul style="list-style-type: none"> • General Directorate of Forensic Audits (DGAF) • General Directorate of Audit of Information and Communications Technology (DGATIC) <p>Missions of DGAF:</p> <ul style="list-style-type: none"> • Detect corruption cases found during annual financial audits. • Conduct forensic audits to assess processes, facts, and evidence to detect and investigate irregularities or illegal activities. <p>Audit Approaches: Proactive Role and Reactive Role</p>
(3) Special Audit Team Qualification	The team consists of experts in various fields, including forensic accounting, law, public administration, accounting, and information technology (IT). These specialists collaborate in the Forensic Laboratory to analyze and investigate corruption cases.
(4) Tools for Audit	The Forensic Laboratory is responsible for handling and securing evidence following the Chain of Custody principles, ensuring proper collection, analysis, and safe storage of forensic evidence.

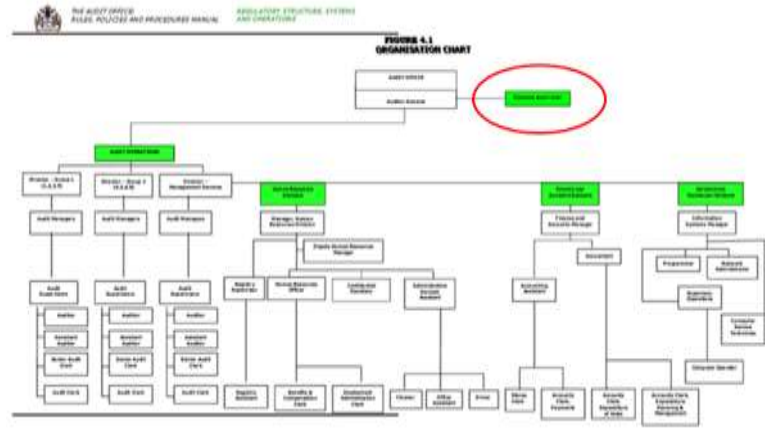
(5) Standard/Manual for Audit	N/A
(6) Receiving Case from Inside/Outside Sources	<ul style="list-style-type: none"> • Internal: Cases are referred from regular internal audit units or assigned by the Auditor General or Parliament through the Auditor General. • External: Reports can be submitted via the Ethical Line for Complaints (LED).
(7) Reporting Cases to Authorities	Audit reports are submitted to Parliament and law enforcement agencies for further legal action.
Source:	<ul style="list-style-type: none"> • OECD (2017); OECD (2018); ASF (2019); WGFACML (2019); (OECD, 2022)
1.2 SAI Kenya - AFROSAI-E	
(1) Investigative Power	<ul style="list-style-type: none"> • Article 29 of the 2010 Constitution of Kenya grants the Auditor-General the authority to conduct financial, operational, and compliance audits for all entities receiving public funds. • Article 37 of the Public Audit Act No.34 of 2015 allows the Auditor-General to conduct forensic audits upon request by Parliament to investigate corruption and financial irregularities.
(2) Special Audit Unit	<p>The Specialized Audit Service (SAS) Department consists of five divisions: (1) Forensic Audit (2) Performance Audit (3) Systems Assurance and Data Science (4) Citizens Accountability Audit (5) Public Debt Audit</p> <p>Name of Forensic Audit Division: Forensic Audit</p> <p>Missions:</p> <ul style="list-style-type: none"> • Investigate corruption and financial irregularities. • Identify those responsible for misuse of public funds. <p>Audit Approach: Proactive Role and Reactive Role</p> 
(3) Special Audit Team	Forensic audits are conducted by specialists in forensic accounting and IT, with expertise in technical investigations


Qualification	and extensive audit experience.
(4) Tools for Audit	N/A
(5) Standard/Manual for Audit	Forensic Audit Manuals
(6) Receiving Case from Inside/Outside Sources	<ul style="list-style-type: none"> • Internal: Cases are referred from internal audit units within the Supreme Audit Institution (SAI) or by directive of the Auditor-General. • External: Cases are initiated upon requests from Parliament or other agencies.
(7) Reporting Cases to Authorities	Audit reports are submitted to Parliament or the requesting agency for further action.
Source:	<ul style="list-style-type: none"> • Gichure & Nabwana (2017); OAG (2020); OAG (2022) • https://www.oagkenya.go.ke/about-us/
1.3 SAI Tanzania – AFROSAI-E	
(1) Investigative Power	<ul style="list-style-type: none"> • Article 27(1) of the Public Audit Act 2020 – Requires auditors to report suspected fraud or irregularities to the Auditor-General for further investigation. • Article 82 of the Public Audit Regulations 2009 – Grants the Auditor-General the authority to conduct forensic audits in ministries, independent agencies, government offices, local authorities, state-owned enterprises, and other public institutions.


(2) Special Audit Unit	<p>Department Name: Forensic Audit Unit</p> <p>Missions:</p> <p>Gather evidence related to criminal proceedings by evaluating:</p> <ul style="list-style-type: none"> • Motivation and opportunity for fraud. • Collusion among multiple suspects in fraudulent activities. • Physical evidence at the crime scene. • Statements from suspects during interviews or upon arrest. • Attempts to destroy fraud-related evidence. <p>Serve as expert witnesses in court, explaining audit findings and investigative methods.</p> <p>Audit Approach: Proactive Role and Reactive Role</p> 
(3) Special Audit Team Qualification	<p>Certified Public Accountants (CPAs), procurement specialists, civil engineers, lawyers, IT experts, valuation experts, and Certified Fraud Examiners (CFEs).</p>
(4) Tools for Audit	<p>The Digital Forensic Laboratory was established to enhance forensic audit capabilities by investing in high-tech equipment and software.</p> <ul style="list-style-type: none"> • Phase 1 (2014-2019) – Constructed the forensic lab on the 2nd floor and acquired the first set of forensic tools and software. • Phase 2 (2022) – Procured additional high-tech equipment, software, and office infrastructure. <p>Software:</p> <ul style="list-style-type: none"> • Forensic Toolkit (FTK), Forensic Explorer, EnCase – Forensic data analysis. • CaseWare IDEA – Data extraction and fraud detection. • ABBYY FineReader – Optical Character Recognition (OCR) software. <p>Hardware:</p> <ul style="list-style-type: none"> • FRED SR – High-performance forensic data analysis computer. • FRED Laptops – Portable forensic auditing devices.

	<ul style="list-style-type: none"> • Tableau Forensic Imager TX1 – Data collection hardware.
(5) Standard/Manual for Audit	<ul style="list-style-type: none"> • Forensic Audit Manual • Adaptation of the ACFE Fraud Examiners Manual
(6) Receiving Case from Inside/Outside Sources	<ul style="list-style-type: none"> • Internal: Cases are referred by internal audit units or the Auditor-General's directive. • External: Cases can be reported via SAI Tanzania's website ("Report Fraud").
(7) Reporting Cases to Authorities	<ul style="list-style-type: none"> • Sent to the requesting agency or other agencies as directed by the Auditor-General. • Copies provided to law enforcement agencies, such as the Anti-Corruption Bureau, Criminal Investigation Department, and Attorney General's Office.
Source:	<ul style="list-style-type: none"> • Sina (2023); NAOT (2024) • https://www.nao.go.tz/services • Survey Data
1.4 SAI Zambia – AFROSAI-E	
(1) Investigative Power	<ul style="list-style-type: none"> • Article 250 (1) of the Constitution of Zambia (Amendment) Act No. 2 of 2016 – Grants the Auditor-General the authority to conduct financial, value-for-money, forensic, and other audits on budget-funded projects. • Article 73 (1) of the Public Finance Management Act No. 1 of 2018 – Empowers the Auditor-General to: <ul style="list-style-type: none"> ○ Access financial data and documents of audited entities. ○ Conduct on-site inspections at appropriate times. ○ Request financial management information from responsible officials. ○ Access ICT systems used for financial management within audited entities.
(2) Special Audit Unit	<p>The Specialized Audit Service Department consists of three divisions: (1) Forensic & Investigations Section (2) Performance & Environmental Audit Section (3) Information Technology Audit Section</p> <p>Name of Forensic Audit Division: Forensic & Investigations Section</p>

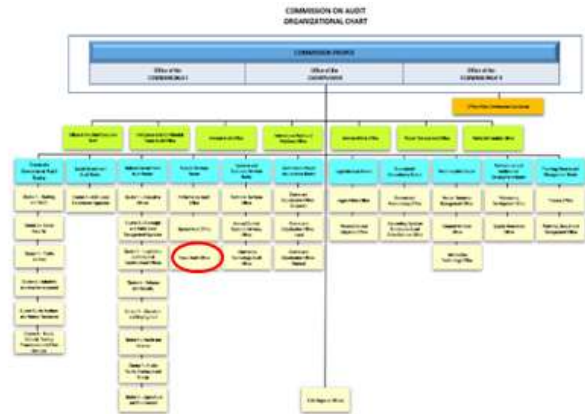
	<p>Missions:</p> <ul style="list-style-type: none"> • Conduct forensic audits to investigate financial misconduct across ministries, provinces, and budget-funded agencies. • Address fraud cases such as asset misappropriation, financial statement fraud, corruption, money laundering, and related offenses. • Serve as expert witnesses in legal proceedings to explain audit findings and forensic methodologies. <p>Audit Approach: Proactive Role and Reactive Role</p> 
(3) Special Audit Team Qualification	N/A
(4) Tools for Audit	<p>Advanced Technology Used:</p> <ul style="list-style-type: none"> • FTK (Forensic Toolkit) – Forensic data analysis and digital investigations. • ACL (Audit Command Language) – Advanced audit analytics for fraud detection and data integrity verification.
(5) Standard/Manual for Audit	Forensic Audit Manual
(6) Receiving Case from Inside/Outside Sources	<ul style="list-style-type: none"> • Internal: Cases referred from internal audit units within the Supreme Audit Institution (SAI) or initiated by the Auditor-General's directive • External: Cases submitted via the Hotline by the Zambia Information Technology Authority (ZICTA).
(7) Reporting Cases to Authorities	Audit Reports are forwarded to law enforcement agencies and used as evidence in court proceedings.
Source:	<ul style="list-style-type: none"> • WGFACML (2019); https://www.ago.gov.zm/?page_id=5235

1.5 SAI Guyana – CAROSAI	
(1) Investigative Power	<ul style="list-style-type: none"> • Articles 30–34 of the 2004 Guyana Audit Act – Grants the Auditor-General the authority to conduct special investigative audits and access information from federal, local government agencies, and other state-controlled entities. • Section 8 of the 2005 Audit Act Regulations, under Article 11 of the 2004 Guyana Audit Act, mandates the establishment of a Forensic Audit Unit within the Supreme Audit Institution (SAI) of Guyana.
(2) Special Audit Unit	<p>Department Name: Forensic Audit Unit</p> <p>Missions:</p> <ul style="list-style-type: none"> • Conduct comprehensive forensic investigations and submit reports with recommendations to the Auditor-General. • If criminal offenses are detected, cases are referred to the Director of Public Prosecutions, with a copy sent to the Commissioner of Police for further action. <p>Audit Approach: Proactive Role and Reactive Role</p> <p>Note: The Forensic Audit Unit was established to address the lack of expertise within law enforcement in handling fraud and corruption cases in government agencies.</p>  <p>The organizational chart, titled 'FIGURE 4.1 ORGANISATION CHART', shows the structure of the Auditor General's Office. At the top is the Auditor General, followed by the Deputy Auditor General. Below them are several departments: Administration, Finance, Information Systems, and Legal Services. The Forensic Audit Unit is shown as a specialized unit within the Information Systems department, highlighted in green and circled in red. Other units shown include the Audit Department, the Department of External Audit, and the Department of Internal Audit.</p>
(3) Special Audit Team Qualification	Specialists in investigative auditing and forensic accounting.
(4) Tools for Audit	Utilization of Computer-Assisted Audit Techniques (CAATs) with advanced forensic software and hardware to support forensic investigations

(5) Standard/Manual for Audit	Forensic Auditing Manual 
(6) Receiving Case from Inside/Outside Sources	<ul style="list-style-type: none"> • Internal: Cases are referred from internal audit units or initiated by the Auditor-General's directive. • External: Government entities and the general public can directly report fraud cases to the Auditor-General.
(7) Reporting Cases to Authorities	If sufficient evidence is found to support a criminal investigation and prosecution, the case is referred to the police and relevant judicial authorities.
Source:	<ul style="list-style-type: none"> • AOG (2004); AOG (2019); AOG (2024)
1.6 SAI US – No Region	
(1) Investigative Power	Under the Budget and Accounting Act of 1921, the Government Accountability Office (GAO) is granted authority in the following areas: <ul style="list-style-type: none"> • Investigations – GAO can examine all matters related to the receipt, disbursement, and use of federal funds (31 U.S.C. § 712). • Program and Activity Evaluations – GAO assesses the outcomes of government programs and activities under existing laws, either upon request from an authorized congressional committee, assignment from either house of Congress, or at the Comptroller General's discretion (31 U.S.C. § 717). • Access to Records and Information – GAO has broad authority to obtain records and data from federal agencies, including all information necessary regarding an agency's functions, powers, activities, organization, and financial transactions. GAO also has the legal authority to enforce its access rights through the courts (31 U.S.C. § 716).

(2) Special Audit Unit	<p>Department Name: Forensic Audits and Investigative Service (FAIS)</p> <p>Missions:</p> <p>The Forensic Audits and Investigative Service (FAIS) operates across three main areas:</p> <ul style="list-style-type: none"> • Forensic Auditing – Analyzing fraud cases using data matching, data mining, internal control evaluations, and statistical sampling. • Security and Vulnerability Assessments – Evaluating risks in financial systems and procurement processes. • Special Investigations – Investigating fraud, corruption, misconduct, procurement irregularities, conflicts of interest, and ethical violations. <p>FAIS follows an Integrated Audit Approach, combining forensic auditing and investigative techniques:</p> <ul style="list-style-type: none"> • Forensic Auditing – Utilizes data analysis, internal control assessments, and statistical sampling to detect fraud. • Investigations – Involves covert testing and witness interviews to gather evidence. <p>Audit Approach: Proactive Role and Reactive Role</p> 
(3) Special Audit Team Qualification	<ul style="list-style-type: none"> • Forensic audit teams consist of: Analysts, Financial Auditors, Forensic Auditors, Fraud Examiners • Essential Skills: Communication, Critical Thinking, IT Proficiency
(4) Tools for Audit	Software: IDEA
(5) Standard/Manual for Audit	<p>Auditing Standards:</p> <ul style="list-style-type: none"> • Generally Accepted Government Auditing Standards (GAGAS), also known as the Yellow Book • Quality Standards for Investigation Build (Council of the Inspectors General on Integrity and Efficiency - CIGIE)
(6) Receiving Case from	<ul style="list-style-type: none"> • Internal: Referred from internal audit units or assigned by the Auditor-General or Parliament.

Inside/Outside Sources	<ul style="list-style-type: none"> • External: Submitted via FraudNet.
(7) Reporting Cases to Authorities	<ul style="list-style-type: none"> • Audit Reports are sent to law enforcement agencies, including the Office of Inspector General (OIG) and the Department of Justice (DOJ). • High-Risk List Reports, assessing agencies and projects for fraud risks, mismanagement, or urgent reforms, are submitted to Congress.
Source:	<ul style="list-style-type: none"> • ALSAI (2018); GAO (2019) • https://www.gao.gov/assets/2023-02/gao-org-chart.pdf • https://www.gao.gov/about/careers/our-teams/FAIS
1.7 SAI Philippines – ASOSAI	
(1) Investigative Power	<ul style="list-style-type: none"> • Article IX-D, Section 2(2) of the 1987 Philippines Constitution – Grants the Commission on Audit (COA) exclusive authority to: <ul style="list-style-type: none"> ○ Define audit scope and methods. ○ Establish accounting and audit regulations. ○ Implement measures to prevent and disallow irregular, unnecessary, excessive, extravagant, or unreasonable expenditures and misuse of public funds and assets. • Section 40 of Presidential Decree No. 1445 (Government Auditing Code of the Philippines) – Empowers COA to: Conduct investigations and inquiries, and Impose penalties for contempt. • COA Resolution No. 2012-016 (December 7, 2012) – Established the Fraud Audit Office (FAO) to specialize in forensic auditing and fraud investigations.
(2) Special Audit Unit	<p>The Special Service Sector consists of three divisions: (1) Performance Audit Office (2) Special Audit Office (3) Fraud Audit Office</p> <p>Name of Forensic Audit Division: Fraud Audit Office</p> <p>Missions:</p> <ul style="list-style-type: none"> • Assessment – Evaluate complaints, reports, or audit requests related to fraud. • Fraud Investigation – Conduct forensic audits, compile audit reports with supporting evidence, and track compliance with recommendations.

	<ul style="list-style-type: none"> Legal Action – Ensure sufficient evidence for civil, administrative, and/or criminal prosecution against offenders. <p>Audit Approach: Proactive Role and Reactive Role</p> 
(3) Special Audit Team Qualification	Lawyers, Accountants, Engineers
(4) Tools for Audit	N/A
(5) Standard/Manual for Audit	COA Memorandum No. 2020-014 dated September 30, 2020
(6) Receiving Case from Inside/Outside Sources	<ul style="list-style-type: none"> Internal: Cases are referred from internal audit units or assigned by the Auditor-General or Parliament. External: Submitted via the Citizens' Desk Reporting System (CDRS).
(7) Reporting Cases to Authorities	Audit Reports are forwarded to law enforcement agencies, specifically the Office of the Ombudsman (OMB), for prosecution of identified offenders.
Source:	<ul style="list-style-type: none"> COA (2023); PONDOC (2023a); PONDOC (2023b) www.coa.gov.ph Survey Data
1.8 SAI Indonesia – ASOSAI	

	<ul style="list-style-type: none"> • Digital Forensic Auditors – Experts in forensic IT investigations: <ul style="list-style-type: none"> ○ Cellebrite Certified Physical Analyst (CCPA) ○ Computer Hacking Forensic Investigator (CHFI) ○ EnCase Certification ○ Certified Ethical Hacker (CEH)
(4) Tools for Audit	<p>The Digital Forensics Laboratory (LFD) supports investigative audits and state loss calculations using advanced forensic tools.</p> <p>Key Forensic Tools:</p> <ul style="list-style-type: none"> • Data Analytics Tools – Detect financial anomalies, fraud risks, and suspicious trends by analyzing historical data and behavioral patterns. • Optical Character Recognition (OCR) – Convert physical documents into searchable digital formats. • Audit Trail Creation – Uses OneDrive-based internal portals to automatically log and track all audit activities for transparency and verification. • Digital Forensics Software – Includes EnCase, FTK, Magnet, Cellebrite, and Oxygen for file recovery, digital evidence analysis, and cybercrime investigations related to fraud. • Data Visualization Software – Tools like Power BI help identify fraud patterns, clusters, and anomalies through graphical representation.
(5) Standard/Manual for Audit	<ul style="list-style-type: none"> • SAI Indonesia Regulation Number 1 of 2020 – Governs investigative audits, state loss calculations, and expert witness testimony in court. • SAI Indonesia Regulation Number 2 of 2020 – Establishes administrative procedures for investigative audits, state loss calculations, and expert witness roles. • Standard Operating Procedures for Digital Forensics – Includes guidelines, manuals, work procedures, and standard forms for forensic audits.
(6) Receiving Case from Inside/Outside Sources	<ul style="list-style-type: none"> • Internal: Cases referred from internal audit units or initiated by the Auditor-General or Parliament. • External: Submitted via the BPK Hotline and Citizen Helpdesk.
(7) Reporting Cases to Authorities	<p>Audit Reports are sent to law enforcement agencies for further action.</p>

Source:	<ul style="list-style-type: none">• Susanto et al. (2019); BPK (2020); Nasution & Cahyowati (2022); Veronika & Simanjuntak (2022); BPK (2023)• www.bpk.go.id• Survey Data
----------------	--

2. Survey

2.1 Results of Survey

- The questionnaire was sent via email to eight randomly selected Supreme Audit Institutions (SAIs) from the following countries:
Mexico, Kenya, Tanzania, Zambia, Indonesia, Philippines, Guyana, and the United States.
- Responses were received from three countries: Tanzania, Philippines, and Indonesia.

2.2 Questionnaire

(1) Does your SAI conduct forensic audits? (If yes, please answer the following questions.)

.....

(2) Does your SAI have the investigative power to conduct forensic audits? (Please reference the relevant law)

.....

(3) Is conducting forensic audits under a separate unit, or is it part of another unit? What is the mission of this unit?

.....

(4) What type of forensic audits does your SAI conduct: proactive or reactive?

.....

(5) What tools does your SAI use for conducting forensic audits?

.....

(6) What standards or manuals must forensic auditors comply with? If possible, please share any relevant documents.

.....

(7) What qualifications does your SAI require to conduct forensic audits?

.....

