ARTICLE 10

Integrating AI and Machine Learning Technique in IT Audit for Public Sector Auditing: Lessons from CAG Reports and Global Best Practices

Ashish Kumar Shukla*
Rimpa Mukherjee*

Received: 13 January 2026 **Accepted: 29 April 2026**

Abstract

India's public sector increasingly relies on digital systems for service delivery in defense, energy, transportation, and taxation. However, CAG audits often reveal vulnerabilities like data fragmentation and weak controls. This article examines IT Audit's role in addressing these challenges and explores how AI and ML can enhance auditing effectiveness through predictive analytics and anomaly detection, thereby strengthening the integration of IT Audit with advanced AI/ML techniques. It draws on CAG reports, including the Indian Navy's ILMS (Integrated Logistics Management System, an ERP based Inventory Management) (CAG, 2017), ONGC's SAP ERP PM Module (CAG, 2024a), GSTN (CAG, 2021a), and UIDAI (CAG, 2021b). The analysis covers service sectors such as defense logistics, energy maintenance, transportation payroll, fiscal services, and identity management. International perspectives from INTOSAI (2019; 2020a; 2023a) and ASOSAI (2023), along with peer-reviewed scholarship (Genaro-Moya et al., 2025; INTOSAI, 2025a), inform the discussion. The article addresses governance, ethics, and capacity building, advocating phased adoption to strengthen SAI India's accountability in a digital era.

Keywords

IT Audit, Artificial Intelligence, Machine Learning, Public Sector Auditing, Comptroller and Auditor General of India, Supreme Audit Institutions, INTOSAI, ASOSAI, Data Analytics, Cybersecurity and Ethical AI.

10.1 Introduction

In the contemporary landscape of public administration, the proliferation of IT systems has revolutionised service delivery across India's governmental entities. From defense logistics to energy asset management and railway payroll processing, these systems facilitate vast data handling, enabling efficiency gains and transparency (CAG, 2025a). Nevertheless, the complexity of these infrastructures introduces multifaceted risks, including cybersecurity threats, data inaccuracies, and operational inefficiencies, as evidenced in numerous CAG audits (CAG, 2024b). Traditional auditing methodologies, reliant on sampling and manual verification, are increasingly inadequate for scrutinising the scale and velocity of digital transactions.

IT Audit emerges as a critical discipline, systematically evaluating information systems to ensure asset safeguarding, data integrity, and alignment with organisational objectives (CAG, 2024c). Complementing this, AI and ML technologies offer transformative potential by automating pattern recognition, forecasting risks, and detecting anomalies in large datasets (INTOSAI, 2019). The CAG's Artificial Intelligence Strategy Framework (2025b) underscores this synergy, positioning AI/ML as tools to audit AI-driven government applications while enhancing audit efficacy.

*Senior Audit Officer, O/o Director of Audit (Navy), Mumbai, Maharashtra
Email: ashishkrs.def@cag.gov.in

*Assistant Audit Officer, O/o PAG (Audit-I), Mumbai, Maharashtra

The term "integrating IT Audit with AI/ML" as used in this article has a dual meaning: (i) using AI/ML tools to augment IT Audit processes such as risk-based audit planning, automated anomaly detection, and continuous control monitoring within the GUID[1] 5300 framework; and (ii) applying established IT Audit methodology to audit AI/ML-powered government systems, examining algorithmic governance, training data integrity, access controls, and explainability. This dual scope distinguishes the article from a general data analytics discussion and positions it squarely within the IT Audit discipline. The Government of India's NITI Aayog Responsible AI for All framework (2021) and CAG's own AI Strategy Framework (2025b) provide the regulatory backdrop for both dimensions.

This scholarly examination synthesises insights from CAG reports to elucidate IT Audit's contributions and AI/ML's prospective applications. Case studies focus on service sectors: defence (national security services), energy (resource maintenance services), revenue (financial services) and identity management services. Global perspectives from INTOSAI (2020a) and ASOSAI (2023) enrich the discourse, highlighting cross-jurisdictional learnings. The article posits that integrating AI/ML with IT Audit not only addresses extant deficiencies but also propels SAI India toward proactive, data-centric assurance, aligning with constitutional mandates under Article 149[2].

10.2 Theoretical and Conceptual Framework of IT Audit in the Public Sector

IT Audit constitutes a specialised subset of public sector auditing, grounded in standards such as INTOSAI's International Standards of Supreme Audit Institutions (ISSAI) 5300 (INTOSAI, 2020b). It encompasses assessments of general IT controls (e.g., access management, change control) and application-specific controls, ensuring compliance with governance frameworks like India's National Cyber Security Policy (CAG, 2024c).

IT Audit operates within a risk-based paradigm, identifying vulnerabilities that could undermine public service integrity (World Bank, 2022). CAG reports consistently document challenges: for instance, fragmented databases erode data reliability, while weak validation mechanisms facilitate errors or fraud (CAG, 2017). The advent of AI/ML introduces a paradigm shift, leveraging supervised and unsupervised learning algorithms to process unstructured data and predict outcomes (INTOSAI, 2023a). ML models, such as neural networks, can classify transactions for risk scoring, while AI enables natural language processing (NLP) for contract analysis.

10.3 Expanded Case Studies from CAG Audits: IT Vulnerabilities and AI/ML Interventions

This section delves into CAG audits, expanding on AI/ML case studies to illustrate practical applications. Each case highlights systemic issues uncovered through IT Audit and proposes AI/ML solutions, drawing on real-world implementations where feasible.

10.3.1 Defence Logistics Services: Inventory Management in the Indian Navy

The Indian Navy's ILMS, operational since 1993 guided by Material Planning Manual 1995 and upgraded in 2008, automates inventory provisioning for stores and spares. CAG Report No. 20 of 2017 scrutinised expenditures totaling ₹6,731.75 crore from 2010-11 to 2015-16, revealing profound inefficiencies rooted in IT deficiencies (CAG, 2017).

10.3.1.1 Key Audit Findings:

- Data Fragmentation: ILMS lacked seamless integration with dockyards, ships, and Material Organisations (MOs), impeding real-time asset visibility. This resulted in discontinuous information flows, exacerbating procurement duplications.
- Absence of Real-Time Monitoring: Manual interventions dominated, with no centralised dashboard for inventory oversight, leading to inaccurate demand projections.
- Inadequate Controls: Multiple vendor codes and insufficient data validation at entry points permitted errors, including algebraic flaws in provisioning formulas in-built into ILMS system for providing provisional Procurement Quantity, which projected inflated requirements of 3-6 years' consumption.

[1]GUID 5300 is a "Guideline on IT Audit", it falls under INTOSAI Framework for Professional Pronouncement (IFPP), in GUID (Guidance) Series (formerly part of ISSAI 5300 Series).

[2]Article 149 of the Indian Constitution defines the Duties and Powers of the Comptroller and Auditor-General (CAG), mandating that the CAG performs functions related to the accounts of the Union, States, and other bodies as prescribed by Parliament, ensuring financial accountability and transparency, acting as the guardian of public funds, making the CAG crucial for financial oversight.

- Forecasting Deficiencies: The system failed to incorporate dynamic variables, culminating in overstocking valued at ₹7,359 crore, obsolescence costs of ₹46.92 crore, and annual carrying expenses of ₹588.75 crore.

These findings underscore IT Audit's efficacy in diagnosing systemic lapses beyond procedural anomalies, impacting national security services.

10.3.1.2 AI/ML Expansion

In a hypothetical yet feasible AI/ML application, time-series forecasting models (e.g., ARIMA or LSTM neural networks) could analyse historical consumption data to predict spare parts demand with 85-95% accuracy, as demonstrated in similar defense logistics by the U.S. Government Accountability Office (GAO, 2023). Unsupervised ML clustering (e.g., K-means) could identify stock discrepancies across depots, flagging anomalies like excess holdings. A real-world parallel is SAI Thailand's use of ML for risk based inventory audits under ASOSAI guidance (ASOSAI, 2023), reducing overstock by 20%. For ILMS, AI-driven anomaly detection could integrate with existing ERP, using graph neural networks to map inter-unit relationships and prevent duplications. Pilot studies in CAG's forensic audits have already unearthed fraud through ML pattern recognition (Murthy, 2025a), suggesting scalability to defence contexts.

A critical prerequisite for deploying ML models in defence logistics is the availability of clean, complete, and representative training data. Given that ILMS data has historically suffered from fragmented records across dockyards and Material Organisations, algebraic errors in provisioning formulas, and duplicate vendor codes, any ML model trained on this historical data risks inheriting and amplifying these flaws. From an IT Audit perspective, the IT auditor must therefore: (a) assess the quality, completeness, and lineage of training datasets before ML deployment; (b) verify that model validation protocols include cross-validation on holdout datasets drawn from diverse depots and time periods; (c) examine whether systematic biases in historical procurement records (e.g., decades of overstocking caused by the flawed ILMS formula) have been identified and corrected prior to model training; and (d) ensure that a documented and tested retraining schedule is in place to prevent model drift as consumption and procurement patterns evolve post-ILMS Version 2.0 upgrade. Without these data governance safeguards, AI/ML-generated demand forecasts may reproduce—at speed and scale—the very inefficiencies the CAG audit exposed.

10.3.1.3 The Legacy ILMS follows a Linear and Manual Flow

- Procurement Requests → Indent Processing → Material Planning → Procurement → Receipt/Issue

Transforming Navy Inventory Management with AI/ML: Figure 10.1 presents a comparative visualisation of the Indian Navy's Inventory Management System (ILMS), contrasting the legacy procurement flow with a proposed AI/ML-enhanced framework. It highlights systemic inefficiencies identified by the CAG (2017) and illustrates how artificial intelligence can address these challenges through predictive analytics and intelligent automation.

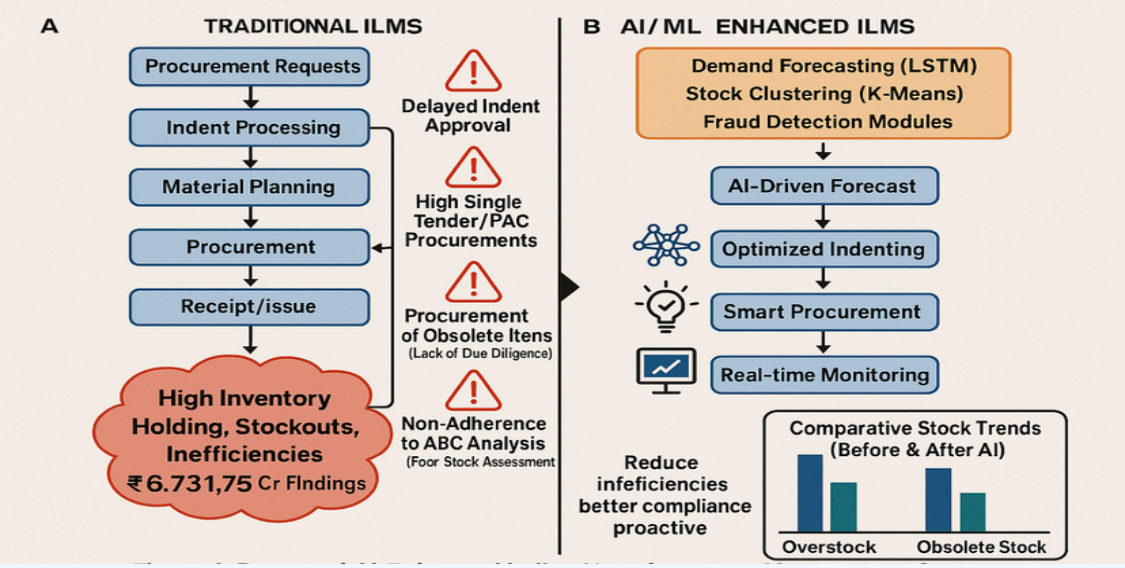

Figure 10.1: ILMS Flowchart with AI layers for Forecasting and Detection

Improved Flow: AI-Driven Forecast → Optimised Indenting → Smart Procurement → Real-Time Monitoring

Outcome: This intelligent system reduces inefficiencies, enhances compliance, and enables proactive decision-making across the supply chain.

Strategic Implication: This transformation aligns with global best practices and audit-driven reforms, offering a scalable blueprint for modernizing defense logistics. By embedding AI into ILMS, the Navy can shift from reactive procurement to predictive, data-driven inventory management.

Acceptance of Audit Recommendations by Navy: Based on the audit recommendation, the following actions have been taken in 2024-2025 by the Naval Headquarters/Ministry of Defence, which brought perceptible improvements in processes and systems:

- Revision of the Previous Material Planning Manual 1995, the Procurement Manual 1995, the Warehousing manuals 1995 and the latest version of the above manuals issued in 2025.
- Incorporation of Modified ABC/VED Classification as per Pareto's law based on audit recommendations.
- Revision of procurement formula in-built into the ILMS system with the technical assistance of IIT, Madras

Audit Impact: Performance Audit on "Inventory Management of Naval Stores, Equipment and Spare Parts in the Indian Navy" (CAG Report No. 20 of 2017) went beyond routine checks and challenged entrenched practices by identifying an inherent algebraic flaw in the provisioning formula of the Integrated Logistics Management System (ILMS), which had remained uncorrected for nearly two decades in Material Planning Manual 1995.

This pathbreaking finding not only questioned the status quo but also directly led to the development and implementation of ILMS Version 2.0, incorporating a dynamic provisioning model for accurate forecasting, minimising manual interventions, and ensuring transparency and accountability in defence logistics. Audit initiative epitomises the values of innovation, transparency, and good governance, and makes a significant contribution towards the mission of the Comptroller and Auditor General of India in promoting accountability and efficiency in public resource management, and act as a model case of how excellence in public auditing can drive systemic improvements in governance.

10.3.2 Energy Maintenance Services: SAP ERP Plant Maintenance Module in ONGC

ONGC's SAP ERP, deployed under Project ICE (Information consolidation for Efficiency) for a ₹81.50 crore investment, incorporates a Plant Maintenance (PM) Module for equipment servicing. CAG Report No. 2 of 2024 evaluated its efficacy, noting that PM orders accounted for only ₹99.22 crore against total maintenance expenses of ₹1,281.16 crore in 2020-21 (CAG, 2024a).

10.3.2.1 Key Audit Findings:

- Master Data Incompleteness: Critical fields like asset numbers (97.86% blank) and warranties (100% blank) undermined system utility and integration.
- Transactional Inefficiencies: Delays in report generation (up to 84 days), misclassified maintenance orders, and prolonged open statuses (88% exceeding 365 days) highlighted procedural gaps.
- Control Weaknesses: Absence of duty segregation (users with up to 30 roles) and non-mandatory root cause fields facilitated errors.
- Data Integrity Issues: Retired assets remained active, distorting KPIs; manual interventions rendered reports unreliable.
- Implementation Shortfalls: Logbooks were underutilised in 50 plants, and static equipment lacked mapping to maintenance plans.

These vulnerabilities risked operational disruptions in energy services, with backlogs spanning one day to two years.

10.3.2.2 AI/ML Expansion:

Predictive maintenance via AI could leverage sensor data (e.g., vibration, temperature) from integrated SCADA systems, employing ML algorithms like random forests to forecast failures with 90% precision, akin to Petrobras' AI implementations in Brazil (INTOSAI, 2023b). For fraud detection, anomaly models could scrutinise claims, identifying outliers in expense patterns—mirroring CAG's AI-driven revelations of billions in irregularities in state schemes (Times of India, 2025). ASOSAI's case study on SAI Indonesia's ML for energy audits demonstrates a 25% efficiency gain (ASOSAI, 2023). In ONGC, generative AI could automate root cause analysis from textual logs, reducing manual efforts by 40%, as per EUROSAI's generative AI guidelines (EUROSAI, 2025).

When a mature ERP like SAP PM is enhanced with AI/ML capabilities (predictive maintenance, generative root cause analysis), the IT auditor's focus must evolve beyond traditional application control testing. The following five dimensions define the changed audit approach:

(a) Audit of AI/ML Model Logic: Verify that the predictive maintenance model is trained on validated sensor data (vibration, temperature, SCADA readings), that the algorithm's outputs are explainable to maintenance engineers using techniques such as SHAP values, and that all human overrides of AI recommendations are logged, reviewed, and approved by an authorised officer. The IT auditor should review model documentation, including feature selection rationale, training data sources, and validation accuracy metrics.

(b) Shift from Sample-Based Testing to Continuous Monitoring: Traditional IT Audit tests a sample of transactions against defined controls. In an AI/ML-augmented ERP, the IT auditor should assess whether the AI system itself performs continuous control monitoring, and evaluate the reliability of AI-generated anomaly flags as audit evidence—verifying that these flags are investigated, resolved, and documented rather than silently overridden.

(c) Segregation of Duties in AI-Automated Workflows: The CAG audit already noted that users had up to 30 conflicting roles. When AI automation generates work orders or approves maintenance actions, the risk compounds: assess whether AI-generated outputs bypass segregation-of-duties controls, and whether emergency override privileges are time-bound and audit-logged.

(d) Cybersecurity Risks Specific to AI/ML: The IT auditor must assess adversarial attack risks — whether malicious inputs to sensors or data feeds could manipulate AI outputs to mask equipment failures in safety-critical energy infrastructure. Model poisoning (corruption of training data) and data exfiltration from ML pipelines are cybersecurity threats unique to AI-augmented systems that require specific audit procedures beyond standard network security testing.

(e) Compliance with GoI AI Guidelines: The IT auditor should verify that the AI/ML deployment within ONGC's SAP PM complies with NITI Aayog's Responsible AI for All (2021) framework, particularly the principles of accountability, safety and reliability, and fairness and non-discrimination, as well as CAG's own AI Strategy Framework (2025b) which mandates XAI (Explainable AI) for LLM-based audit tools.

Figure 10.2 on PM lifecycle diagram with AI interventions on the next page illustrates the transformation of ONGC's SAP Plant Maintenance (PM) lifecycle by juxtaposing legacy audit findings from CAG Report No. 2 of 2024 with targeted AI interventions. The circular lifecycle diagram maps the standard SAP PM process, while red callouts highlight systemic failures and blue overlays propose AI solutions aligned with global Supreme Audit Institution (SAI) practices.

Strategic Alignment: The proposed AI model aligns with INTOSAI's 2023b guidance and mirrors SAI Indonesia's use of big data in energy sector audits. It demonstrates how machine learning can enhance ERP systems by embedding intelligence into routine workflows — a scalable model for other public sector enterprises.

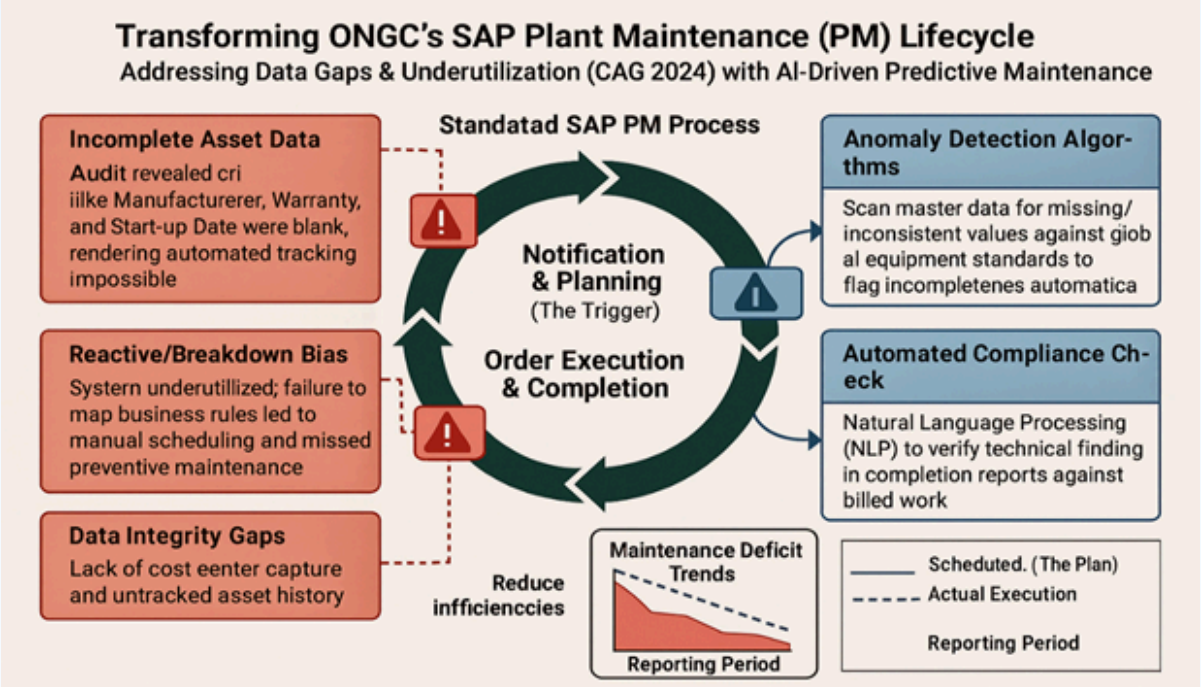

Figure 10.2: Operational Audit of ONGC's SAP ERP Plant Maintenance module

10.3.3 Identity Management Services: Functioning of Unique Identification Authority of India (UIDAI)

The 2021 CAG Performance Audit of UIDAI (CAG, 2021b) identified IT control gaps in Aadhaar issuance: biometric validation weaknesses leading to duplicate enrolments, inadequate access controls over the Central Identities Data Repository (CIDR), and insufficient audit trails for data access by enrolment agencies. From an IT Audit standpoint (GUID 5300), key focus areas are access management, segregation of duties in enrolment agency oversight, and data integrity controls. AI/ML can strengthen IT Audit of UIDAI through: ML-based deduplication combining facial recognition with fingerprint clustering, anomaly detection in grievance redressal response patterns, and NLP-based review of enrolment agency compliance documentation. Critically, any AI deployment must comply with the Aadhaar act 2016/amendment act 2019 and India's Digital Personal Data Protection Act (DPDPA) 2023, and the IT auditor must verify that privacy-by-design principles are embedded in the AI system architecture and that algorithmic decisions affecting Aadhaar status are explainable and appealable.

10.3.4 AI/ML-Enabled Remote IT Audit: Continuous Control Monitoring in Revenue, Infrastructure, and Local Government Digital Systems

Remote IT Auditing, as described in this section, is fully consistent with the IT Audit definition, which encompasses assessments of general IT controls (access management, change control, data integrity) and application-specific controls. All of these can be evaluated remotely through secure, standards-compliant data access arrangements. The AI/ML layer enhances these core IT Audit functions: ML anomaly detection replaces manual sampling in application control testing; NLP automates review of system access logs and change management records; and predictive risk models support risk-based audit planning consistent with ISSAI 3000/5300.

10.3.4.1 Fiscal Services: IT Audit of GST Network (GSTN) Phase II and the Shift towards Remote, AI-Enabled Auditing

The Comptroller and Auditor General's (CAG) Audit of the Goods and Services Tax Network (GSTN) Phase II (CAG, 2021a) underscored both the strategic importance and inherent risks of large-scale digital public financial platforms. The audit revealed significant control deficiencies, including inadequate system validations leading to erroneous GST refunds exceeding ₹1,000 crore, weak access controls exposing sensitive taxpayer data, and incomplete integration with State tax systems. These findings highlight the limitations of traditional audit approaches when applied to complex, real-time, IT-driven ecosystems.

In this context, remote auditing through IT Audit frameworks, augmented by Artificial Intelligence (AI) and Machine Learning (ML), emerges as a critical enabler for future public sector audits. Given that revenue administrations—GST, Income Tax, Customs, and Central Excise—operate almost entirely on digital platforms, remote audits allow auditors to securely access and analyse vast volumes of transactional data off-site. Data analytics and AI driven risk assessment can support audit planning by identifying high-risk taxpayers, refund claims, and systemic vulnerabilities, while virtual interactions enable continuous audit engagement without physical presence. This approach enhances audit efficiency, expands coverage of risk-prone areas, reduces cost and time overruns, and ensures audit continuity during disruptions, subject to robust safeguards for data security, legal admissibility, and auditor capacity building.

The potential of AI/ML in GST audits is particularly significant. Machine learning–based anomaly detection models can identify fraudulent Input Tax Credit (ITC) claims, circular trading, and refund manipulation, drawing parallels with the Supreme Audit Institution of the Netherlands' use of AI in tax audits (INTOSAI, 2023a). CAG's ongoing AI pilot initiatives have already demonstrated the feasibility of detecting similar fraud patterns within GST data streams (The Hindu, 2025), with international experience suggesting recovery potential of 15–20 per cent of revenue leakages.

Beyond GST, AI/ML-enabled remote auditing has broad applicability across other major audit domains. In the Railway Audit, AI tools can analyse procurement, contracts, inventory, web-based IPAS (Integrated Payroll & Accounting System), and project execution data to flag anomalies, duplicate payments, and cost escalations, while predictive analytics can identify projects at risk of delays or overruns. Natural Language Processing (NLP) can assist auditors in reviewing complex contracts, tender documents, and policy guidelines at scale, enabling more focused field verification.

Similarly, audits of Local Government Bodies can be strengthened through AI/ML-driven risk profiling of budgets, expenditures, grants-in-aid, and utilisation certificates. Anomaly detection can identify irregular payments and duplicate beneficiaries in welfare schemes, while geo-tagged data and satellite imagery can remotely verify the existence and progress of infrastructure assets such as roads, drains, and public buildings. NLP tools can further support the review of council resolutions, tenders, and compliance reports, improving audit coverage and transparency.

Overall, the integration of remote IT auditing with AI and ML represents a paradigm shift in public sector auditing, enabling CAG to move towards a continuous, risk-based, and technology-assisted audit model. While professional judgment remains central, AI/ML tools act as force multipliers—enhancing audit effectiveness, strengthening accountability, and aligning Indian public sector audits with global best practices.

10.4 International Comparative Perspectives: AI/ML Case Studies from INTOSAI and ASOSAI

The global auditing community, led by INTOSAI and ASOSAI, has actively integrated AI and ML into public sector auditing. Comparative case studies from other Supreme Audit Institutions (SAIs) offer valuable lessons, best practices, and transferable strategies for SAI India (CAG).

(i) Framework for Auditing AI/ML Systems: INTOSAI's 2020 White Paper on Auditing ML Algorithms (INTOSAI, 2020a), (co-authored by SAIs of Finland, Germany, Netherlands, Norway, and the U.K.) provides the foundational audit framework, covering risk assessment, bias evaluation, and explainability requirements. INTOSAI's INCOSAI 2025 Theme II Discussion Paper extends this to building SAI capacity to audit AI systems themselves. These documents define the global standard against which CAG's AI audit methodology should be benchmarked.

(ii) AI as an Audit Efficiency Tool – Proven Cases: Several SAIs have demonstrated significant efficiency gains viz. SAI UK (NAO) achieved a 25% reduction in fraud detection time using ML for irregular welfare payments. SAI Canada reduced manual fieldwork by 40% using ML on satellite data for environmental compliance audits. SAI Indonesia increased audit coverage by 25% using predictive models in energy audits (ASOSAI, 2023). SAI Thailand detected procurement bidding anomalies 30% faster using AI risk-based models. These results are directly transferable to CAG's defence, energy, procurement and revenue audit domains.

(iii) Governance and Ethical AI in Audit Context: SAIs have successfully addressed governance challenges in production environments. SAI Germany implemented differential privacy in ML models to anonymise audit data. SAI Brazil used NLP on procurement contracts to detect overbilling. These cases illustrate that AI governance (explainability, privacy protection, bias mitigation) is not a theoretical concern but an operational requirement.

(iv) Capacity Building – Structured Knowledge Transfer: ASOSAI's 2022–2027 strategic plan and IDI's 2025 high-level dialogue emphasise multidisciplinary teams, hybrid training, and structured knowledge sharing as prerequisites for sustainable AI adoption. SAI India's participation in INTOSAI working groups positions it to adopt these frameworks systematically rather than in isolation.

In summary, international practice validates a governance-first, phased approach to establish the audit framework for AI systems, pilot AI audit tools in high-impact areas, build explainability and bias governance, and scale through structured capacity building.

10.5 Governance, Ethical Considerations, and Risks in AI/ML Adoption

Empirically, SAI India's adoption of AI aligns with global trends; INTOSAI's Working Group on Big Data advocates for AI in enhancing auditor competencies (IDI, 2025). However, integration demands robust governance to mitigate biases and ensure explainability (ASOSAI, 2023).

AI/ML integration raises ethical dilemmas, including algorithmic bias and opacity (MDPI, 2025). The adoption of AI and ML in public sector auditing necessitates robust governance structures to address ethical dilemmas and mitigate risks. This section elaborates on these aspects, drawing from academic papers and international guidelines to provide a comprehensive analysis.

Central to governance is ensuring transparency and explainability in AI systems. Genaro-Moya et al. (2025) argue that opaque algorithms can undermine audit credibility, as decisions influenced by "black-box" models may lack justification. For instance, in SAI UK's ML pilots, explainable AI (XAI) techniques like SHAP values were employed to interpret model outputs, ensuring auditors could trace decisions back to data inputs (NAO, 2020). CAG's strategy framework mandates similar XAI for its LLM tools (CAG, 2025b).

Ethical challenges include algorithmic bias, where training data reflecting historical inequalities perpetuates discrimination. A systematic review on bias in AI auditing highlights risks in fairness and accountability (ScienceDirect, 2024a). In public auditing, biased models could skew risk assessments, disproportionately flagging certain demographics in welfare audits. The emergence of AI ethics auditing, as discussed in Schiff, D. S. and others (2024), calls for robust stakeholder involvement and external reporting to counter this.

Data privacy emerges as a critical risk, particularly under India's Data Protection Act. AI systems processing sensitive public data must comply with GDPR[3] -like standards. SAIs like SAI Germany have implemented differential privacy techniques in ML models to anonymise data during audits.

Accountability for AI-influenced decisions is another concern. Who bears responsibility if an AI-flagged anomaly leads to erroneous audit findings? ResearchGate's paper on ethical AI auditing advocates for organisational transparency and compliance mechanisms (ResearchGate, 2025). INTOSAI (2023a) stresses human oversight, with auditors retaining final judgment.

Robustness and reliability pose technical risks; adversarial attacks could manipulate ML models. ScienceDirect (2024a) notes these in auditing contexts, recommending regular model retraining. For SAI India, this means developing policies for bias audits and privacy impact assessments, aligning with ASOSAI's ethical AI guidance (ASOSAI, 2023).

In conclusion, governance must encompass legal, technical, and ethical dimensions, ensuring AI enhances rather than undermines public trust.

10.6 Capacity Building and Institutional Readiness

Capacity building is foundational to AI/ML adoption in SAIs, requiring investments in human capital, infrastructure, and knowledge ecosystems. This expanded section details strategies, programs, and challenges, informed by global and academic insights. The following competency framework is proposed, specific to IT auditors:

(a) ML Model Auditing: IT auditors should be able to review and critically assess model documentation, validation reports, performance metrics (accuracy, precision, recall), and bias test results. They do not need to code models but must understand what these metrics mean for audit reliability and whether the model is fit for purpose in a specific audit context.

[3]General Data Protection Regulation, EU 2016/679

(b) AI Governance and Regulatory Compliance Auditing: Familiarity with NITI Aayog's Responsible AI for All (2021) framework, India's Digital Personal Data Protection Act 2023, CAG's AI Strategy Framework (2025b), and INTOSAI's guidance on auditing ML algorithms (2020a). The IT auditor must be able to assess whether AI deployments in government systems comply with these frameworks, particularly regarding accountability, explainability, and human oversight requirements.

(c) Cybersecurity Audit for AI-Specific Threats: Understanding of adversarial machine learning attacks (model poisoning, data injection, evasion attacks), AI-specific data exfiltration risks, and supply chain vulnerabilities in pre-trained models. IT auditors reviewing AI-augmented ERP systems, identity platforms, or logistics systems must be able to assess these risks beyond standard cybersecurity audit checklists.

(d) Training Data and Data Pipeline Auditing: Ability to assess data lineage documentation, labelling quality and methodology, dataset representativeness, and the existence of data governance policies covering training data curation and version control. This skill is central to evaluating whether AI/ML outputs are reliable as audit evidence.

(e) Explainability Assessment Using XAI Tools: Practical familiarity with SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations) at the output-interpretation level, enabling the IT auditor to verify that AI model decisions in government applications are interpretable, traceable to input data, and documentable as audit evidence. CAG's AI Strategy Framework (2025b) already mandates XAI for its LLM audit tools; IT auditors must be equipped to evaluate compliance with this mandate.

(f) AI Ethical Audit Checklist for IT Auditors: The following checklist is proposed for IT auditors reviewing AI/ML deployments in government systems: (1) Is the AI system's purpose, scope, and decision logic documented and approved by a competent authority? (2) Has a bias audit been conducted on training data, and are results documented? (3) Are model outputs explainable to non-technical stakeholders and auditable? (4) Is there a documented human oversight mechanism for AI-generated decisions with significant consequences? (5) Does the system comply with India's DPDP Act 2023 and applicable sector regulations? (6) Is there a model version control register and a tested retraining/rollback protocol? (7) Have cybersecurity risks specific to the AI/ML pipeline been assessed and mitigated? (8) Is there a grievance redressal mechanism for individuals adversely affected by AI-driven decisions?

CAG's initiative to train 5,000 auditors in AI/ML exemplifies proactive readiness (Mint, 2025). Collaborations with IITs for custom LLMs further build expertise (The Hindu, 2025).

INTOSAI's high-level dialogues advocate multidisciplinary teams and emphasises competency development through hybrid training (IDI, 2025). Challenges include skill gaps and resistance to change. ScienceDirect (2024b) assesses institutional readiness in developing countries, recommending multidisciplinary teams (ScienceDirect, 2024b).

For SAIs, ASOSAI promotes knowledge sharing (ASOSAI, 2023). SAI Russia's WGITA Summit in 2025 discussed AI training (INTOSAI Russia, 2025)
.
Institutional readiness involves infrastructure; CAG's infra building for AI (Economic Times, 2025a). Overcoming barriers requires sustained funding and partnerships. In essence, capacity building is iterative, blending training, collaboration, and adaptation to ensure SAIs like CAG are AI-ready.

10.7 Pathways Forward for SAI India

A strategic roadmap for AI/ML adoption in SAI India should be phased, risk-managed, and aligned with global standards. This section outlines detailed steps.

Phase 1: Assessment and Piloting (0-12 months). Conduct readiness audits as per ScienceDirect (2024b). Pilot AI in high-impact areas like GSTN fraud detection (CAG, 2021a), using ML for anomaly spotting.

Phase 2: Integration and Scaling (12-24 months). Integrate AI into audit workflows, as in INTOSAI's Theme II (INTOSAI, 2025a). Scale to defense and energy, incorporating predictive models.

Phase 3: Governance and Evaluation (24+ months). Establish ethical oversight committees, per Genaro-Moya et al. (2025). Evaluate impacts through KPIs, refining models iteratively.

A calibrated approach involves piloting AI in high-impact areas (e.g., GSTN fraud detection), bolstering IT controls, and establishing ethical oversight. Alignment with INTOSAI's emerging technologies working group ensures global interoperability (INTOSAI, 2023b).

Addressing barriers: Secure funding, mitigate biases via diverse data, and foster cultural acceptance through training.

This pathway positions SAI India as a leader, enhancing audit relevance in a digital state.

10.8 Conclusion

The integration of IT Audit with AI/ML marks a transformative era for public sector auditing in India. CAG reports on ILMS, SAP, IPAS, GSTN, and UIDAI reveal systemic vulnerabilities amenable to AI solutions (CAG, 2017; 2024a; 2022a; 2021a; 2021b). Expanded international perspectives from INTOSAI and ASOSAI underscore global best practices, from SAI UK's fraud detection to SAI Indonesia's efficiency gains (INTOSAI, 2025a; ASOSAI, 2023).

Ethical governance is paramount, addressing biases and privacy as per academic insights (Genaro-Moya et al., 2025; ScienceDirect, 2024a). Capacity building through training and partnerships will equip auditors (IDI, 2025). The phased pathway ensures sustainable adoption, promising enhanced accountability and public trust in an AI-driven future, this integration fortifies SAI India's role in a digitised polity, ensuring accountable service delivery.

Data Availability

No new data has been introduced.

Ethics Statement

This article is a conceptual and documentary analysis based on publicly available secondary sources, and it does not involve human participants, animals or primary field experiments requiring prior ethical approval. No sensitive personal data was collected, processed or reported, and no procedures with potential physical, psychological or social risk to individuals or communities were undertaken.

Funding

None

Conflict of Interest

The authors declare no conflict of interest.

References

1. Comptroller and Auditor General of India (CAG). (2017). Report No. 20: Compliance Audit Union Government (Defence Services) – Navy and Coast Guard.
2. CAG's Report No. 1 of 2021 (2021a). IT Audit of GSTN Phase II.
3. CAG's Report No 24 of 2021(2021b). Performance Audit on Functioning of UIDAI
4. CAG's Report No. 2 of 2024 (2024a): Information Systems Audit of Plant Maintenance Module of SAP ERP in ONGC.
5. CAG's (2024b). Audit Reports Overview. https://cag.gov.in/en/audit-report
6. CAG's Manual on Information System (IS) Audit 2024, (2024c).
7. CAG's Artificial Intelligence Strategy Framework, (2025b).
8. Asian Organization of Supreme Audit Institutions (ASOSAI). (2023). Prepared during SAI Thailand's ASOSAI Chairmanship 2021–2024.
9. Economic Times. (2025a). CAG pushes AI, digital tools to detect frauds in audits.
10. EUROSAI. (2025). Generative AI for External Audit: Scope, Strategies, Use Cases.
11. Government Accountability Office (GAO). (2023). AI in Defense Logistics (Internal reference; analogous to public reports on AI accountability).
12. The Hindu. (2025). CAG to launch AI system for auditing and efficiency.
13. INTOSAI Development Initiative (IDI). (2025). Building Auditor Competencies to use AI and Technology.
14. Schiff, D. S., Kelley, S., & Camacho Ibáñez, J. (2024). The emergence of artificial intelligence ethics auditing. Big Data & Society, 11(4). https://doi.org/10.1177/20539517241299732 (journals.sagepub.com)
15. International Organization of Supreme Audit Institutions (INTOSAI). (2019).
16. GUID 5100: Guidance on the Use of Data Analytics in Audits. INTOSAI (2020a). Auditing ML Algorithms: A White Paper for Public Auditors.
17. INTOSAI (2020b). ISSAI 5300: IT Audit Standards revised as GUID 5300 under IFPP.
18. INTOSAI (2023a). INTOSAI Journal Science and Technology Q2 2023.
19. INTOSAI (2023b). Applications in Developing and Maintaining Expertise within SAIs.
20. MDPI. (2025). Artificial Intelligence and Public Sector Auditing for SAIs by Genaro Moya
21. Mint. (2025). CAG building infra & processes to harness AI&ML.
22. Times of India. (2025). CAG push for digital audits: AI tool unearth fraud cases
23. National Audit Office (NAO). (2020). Investigation into the Use of Data Analytics in Audit.
24. Bias and ethics of AI systems applied in auditing – A system review (ScienceDirect, 2024a)
25. Ethical Auditing of AI: Org Transparency & Compliance (ResearchGate, December 2025)