2025

Generative AI for External Audit: Scope, Strategies, Use Cases, Challenges and Future Outlook

A Handbook for Supreme Audit Institutions

Sivré, Vincent

25/06/2025

FOREWORD

Generative AI transforms Supreme Audit Institutions by enhancing every audit phase—from risk profiling to reporting—through data analysis, summarisation, and automation. Yet its adoption demands ethical safeguards, human oversight, and transparent governance. When responsibly implemented, AI empowers auditors to uphold independence, boost quality, and reinforce public accountability in the digital age.

This advanced training course is designed to apply generative AI across all phases of the audit process—from risk profiling and legal analysis in the pre-audit stage, to drafting scoping documents and detecting anomalies during planning, to summarising complex documentation and generating tailored interview guides during fieldwork. In the analysis and reporting phases, generative AI can structure large datasets, perform sentiment analysis, and produce multilingual, audience-specific reports. In the post-audit stage, AI supports automated follow-ups and stakeholder engagement, while enhancing training through simulation.

The course, delivered by Vincent Sivré, is intended for professionals from Supreme Audit Institutions (SAIs), equipping them with practical skills to enhance their audit work through the effective use of AI.

Vincent Sivré brings a robust and versatile set of competencies that enable him to design and lead specialised training sessions on generative artificial intelligence (GenAI) for audiences such as auditors from supreme audit bodies. As a senior auditor, he possesses deep expertise in public financial oversight, governance, and accountability frameworks—insight that allows him to adapt AI training to the specific needs and challenges faced by auditors in the public sector.

His academic background includes studies at esteemed institutions such as Sciences Po Paris, the École nationale d'administration (ENA), Sorbonne University, and the École normale supérieure de Paris-Saclay. This solid educational foundation supports his ability to communicate complex GenAI concepts clearly and effectively to professional audiences.

Mr Sivré places strong emphasis on the measurement and realisation of productivity gains in AI projects, advocating for the use of analytical indicators and prioritising tangible improvements in operational efficiency. This pragmatic approach ensures that his training is not only conceptually sound but also directly applicable to the day-to-day activities of auditors.

In summary, Vincent Sivré combines high-level expertise in AI and data, extensive knowledge of public sector auditing, and refined pedagogical skills. This unique blend positions him to design and deliver impactful training programmes on generative AI, precisely tailored to the needs of auditors in supreme audit institutions.

TABLE DES MATIÈRES

SYNTHESYS

Generative AI represents a watershed moment for Supreme Audit Institutions (SAIs), offering transformative potential across the audit lifecycle. Unlike traditional AI systems that rely on fixed outputs, generative models such as GPT-4, Claude, and LLaMA produce nuanced, context-sensitive content. These capabilities allow auditors to navigate unstructured data, streamline report drafting, and review policies with unprecedented speed and accuracy.

Throughout every audit phase, generative AI has meaningful applications. In the pre-audit stage, it enhances risk assessment and legal analysis. During planning, it supports the drafting of scoping documents and the identification of anomalies. In fieldwork, auditors can rely on AI to summarise complex documents and generate tailored interview guides. For analysis and reporting, it can structure large datasets, conduct sentiment analysis, and produce multilingual reports tailored to diverse stakeholders. Post-audit, AI facilitates automated follow-ups, deepens stakeholder engagement, and enriches training through simulation-based learning.

Yet, the promise of generative AI must be tempered by rigorous governance. These tools should complement—not supplant—human judgement, aligning with INTOSAI standards and core principles of transparency, reproducibility, and accountability. Ethical foundations such as contestability and subsidiarity are essential. A robust governance framework—featuring human-in-the-loop protocols, data stewardship, model auditability, and oversight bodies—is critical to responsible integration.

A hybrid implementation strategy, combining proprietary and open-source models, provides SAIs with flexibility and control. Phased adoption allows institutions to test feasibility, mitigate risk, and cultivate internal trust. While many European SAIs remain in early stages of AI maturity, practical use cases in fraud detection and continuous monitoring illustrate clear, measurable gains.

Importantly, AI integration is not merely a technical upgrade but a strategic and cultural shift. Anchored in institutional values and public service ethics, generative AI enables SAIs to evolve from retrospective compliance checks to forward-looking mechanisms of accountability. However, serious challenges remain. Issues such as algorithmic bias, data privacy, model opacity, and AI "hallucinations" demand careful mitigation through interdisciplinary oversight and technical tools like SHapley Additive exPlanations (SHAP). Human-centred design, transparent procurement, and GDPR-compliant data handling are non-negotiable.

Success hinges on skilled, adaptable auditors—professionals fluent in both audit principles and algorithmic thinking. With strategic partnerships, targeted training, and thoughtful innovation, SAIs can uphold democratic governance while embracing a future shaped by intelligent systems. In doing so, they affirm their enduring role as guardians of public trust in the digital age.

RECOMMENDATIONS

Recommendation n° 1 : Embrace AI as a Strategic Enabler, Not Just a Tool

Auditors must understand the rationale for adopting AI within the public sector—strengthening transparency, efficiency, and accountability in a digital age. AI should be aligned with SAI mandates and broader national digital governance strategies.

Recommendation n° 2 : Develop AI Literacy Across Audit Teams

Invest in continuous training on AI fundamentals, including differences between traditional and generative AI, large language models (LLMs), and prompt engineering. Every auditor should be able to critically engage with AI outputs and understand their implications.

Recommendation n° 3 : Integrate AI Thoughtfully into Audit Workflows

Identify audit processes most suited for generative AI (e.g., document review, report drafting, risk profiling). Start with clear use cases and integrate AI tools in phases, guided by feasibility, pilot testing, and institutional capacity.

Recommendation n° 4 : Uphold Ethical and Legal Standards

Ensure AI applications comply with data protection laws, ISSAI principles, and public interest obligations. Mitigate bias, enforce explainability, and maintain traceability of all AI-generated content. Human oversight must remain non-negotiable.

Recommendation n° 5 : Establish a Robust AI Governance Framework

Design clear policies for AI procurement, use, and auditability. Define accountability lines for AI decisions, embed human-in-the-loop protocols, and regularly assess model performance, bias, and drift.

Recommendation n° 6 : Build Data Infrastructure for AI Readiness

Audit value depends on data quality. Prioritise structured, digitised, and well-governed data sources. Collaborate with government entities to standardise and prepare datasets for future AI integration.

Recommendation n° 7 : Use AI to Enhance but Not Replace Auditor Judgment

Generative AI can support tasks such as anomaly detection, image analysis, or sentiment mapping, but the final professional judgment, especially in findings and recommendations, must always lie with the auditor.

Recommendation n° 8 : Foster Cross-Functional and External Partnerships

Collaborate with legal, technical, and academic stakeholders to co-develop AI tools, assess algorithmic fairness, and exchange best practices. SAIs must also build networks with international peers for joint innovation and learning.

Recommendation n° 9 : Prepare for Tomorrow: Experiment, Learn, Adapt

Audit innovation is iterative. Pilot RPA-AI integrations, explore multimodal auditing, and simulate audit scenarios using synthetic data. Future readiness depends on a culture of experimentation, adaptability, and strategic foresight.

INTRODUCTION: THE GENERATIVE IMPERATIVE IN PUBLIC SECTOR AUDITING

The advent of generative artificial intelligence heralds a transformative epoch for Supreme Audit Institutions (SAIs), demanding not merely technological accommodation but a fundamental recalibration of audit philosophy. This technology, distinguished from traditional AI by its capacity to synthesise original content—text, code, imagery—through large language models (LLMs), diffusion architectures, and prompt engineering, transcends conventional analytical functions. Where traditional systems excel at pattern recognition within constrained parameters, generative AI exhibits emergent creative and interpretive faculties, thereby redefining the auditor's role from analyst to orchestrator of synthetic intelligence.

The public audit landscape, governed by sacrosanct principles of probity, accountability, and constitutional fidelity, now confronts a dual mandate: to harness generative AI's potential for unprecedented efficiency gains while safeguarding the inviolable tenets of audit legitimacy. LLMs such as GPT-4, Claude, and open-source alternatives like LLaMA offer profound capabilities—ingesting decades of audit precedents in moments, drafting evidential narratives with jurisprudential precision, and distilling complex regulatory frameworks into actionable insights. Yet these very capacities necessitate rigorous governance, lest efficiency compromise ethical imperatives.

This guide contends that generative AI, judiciously deployed, may elevate public sector auditing from retrospective compliance to anticipatory stewardship. It enables SAIs to navigate the deluge of unstructured data—contracts, correspondence, multimedia evidence—that increasingly characterises modern governance while preserving the methodological rigour demanded by INTOSAI standards. However, its integration demands more than technical proficiency; it requires institutional wisdom to discern where algorithmic synthesis augments human judgment and where it risks undermining the adversarial scrutiny that underpins public trust.

The following chapters furnish a structured pathway for this transformation. Commencing with a taxonomy of generative AI's applicability across financial, compliance, and performance audits, we proceed to strategic frameworks for ethical integration, explore concrete use cases across the audit lifecycle, and confront the governance quandaries intrinsic to synthetic content generation. Our discourse culminates in pragmatic roadmaps for implementation—acknowledging that the auditor of the future must be both sceptic and technologist, upholding the timeless values of public accountability through the most advanced tools of our age.

In this endeavour, we anchor every precept to the non-negotiable trinity of public audit: that the process remains independent in judgment, transparent in execution, and constitutionally faithful in purpose. For in the marriage of artificial intelligence and audit integrity lies not merely efficiency, but the reaffirmation of democracy's safeguards.

1 SCOPE OF GENERATIVE AI IN EXTERNAL AUDIT

The landscape of external audit, traditionally grounded in rigorous methodology and meticulous human judgment, now stands at the threshold of profound transformation. The advent of **generative artificial intelligence (AI)**—a class of algorithms capable not merely of pattern recognition but of language generation, document synthesis, and conceptual reasoning—invites a reconsideration of how public sector audits are conceived, planned, and executed. For **Supreme Audit Institutions (SAIs)**, which hold a constitutional mandate to safeguard accountability and transparency in the stewardship of public resources, this technological juncture presents both an opportunity and an obligation: an opportunity to enhance efficiency and depth, and an obligation to harness innovation responsibly and judiciously. This chapter seeks to delineate the scope of generative AI within the domain of external audit by exploring its applicability across audit types, the internal processes most amenable to AI augmentation, the varieties of data with which auditors routinely engage, and the foundational technologies underpinning this emergent field.

1.1 Audit Typologies and Generative AI Use Cases

Public sector audits are broadly categorised into **financial**, **compliance**, and **performance audits**, each with its own objectives, evidentiary standards, and analytical techniques. Within each of these domains, generative AI presents distinct avenues for contribution—some already accessible, others promising near-future potential.

In **financial audits**, the primary objective is to determine whether an entity's financial statements are free from material misstatement and prepared in accordance with applicable accounting frameworks. The challenge of scale—reviewing thousands of transactions and multiple systems—has long compelled auditors to sample data selectively. Generative AI offers a complementary alternative: automating the preliminary analysis of voluminous financial documentation, flagging anomalies in accounting entries, and assisting in the drafting of audit findings. For instance, AI can extract and summarise the notes to financial statements, compare them with previous years, and flag inconsistencies that merit human scrutiny. Similarly, AI-driven classification models can categorise expenditures according to risk indicators, allowing auditors to focus their efforts more strategically.

Compliance audits, which assess whether public entities adhere to laws, regulations, and internal controls, stand to benefit from the language-understanding capabilities of large language models (LLMs). These models can parse legal texts, identify obligations, and detect deviations between stipulated norms and actual practice. An illustrative use case lies in the review of procurement procedures: AI can rapidly analyse a corpus of tender documents, contracts, and correspondence, identify deviations from procurement law, and draft preliminary compliance assessments. Moreover, AI can assist in preparing questionnaires and interview frameworks tailored to the statutory context of each audit.

In **performance audits**, which examine the economy, efficiency, and effectiveness of public interventions, the potential of generative AI is particularly striking. These audits often involve complex evaluative judgments, informed by qualitative and quantitative evidence, stakeholder interviews, and contextual knowledge. AI models can synthesise public policy documents, summarise social programme evaluations, and assist in correlating expenditure data with policy outcomes. Consider, for example, an audit of a national school feeding programme: AI could summarise academic studies on nutritional impact, analyse government expenditure trends, extract key performance indicators from ministerial reports, and generate hypotheses for field validation by audit teams.

1.2 Audit Processes Amenable to Generative AI

While the conceptual reach of generative AI spans the full audit cycle, its most immediate utility lies in augmenting discrete processes within the audit methodology. Chief among these are **data ingestion**, **document review**, **text summarisation**, **analysis**, and **report drafting**.

Data ingestion—the process of collecting, cleansing, and organising audit-relevant information—is an area where generative AI can vastly reduce the burden on auditors. In the context of a large-scale infrastructure audit, for example, AI models can extract contract values, completion dates, change orders, and clauses from dozens of procurement documents, converting unstructured text into structured data suitable for risk analysis.

Similarly, AI models trained or fine-tuned on domain-specific corpora can perform **semantic clustering**, grouping similar documents or paragraphs across a large volume of audit evidence. This capability enables auditors to quickly identify themes—e.g., recurring causes of procurement delay—and trace their evolution across cases and time periods.

In the **report drafting phase**, generative AI can offer what may be termed "synthetic scaffolding": the generation of preliminary text for findings, observations, or background sections based on structured audit evidence. While human review and validation remain essential, the time saved in constructing the first draft is substantial. Furthermore, the model's ability to adjust tone and structure depending on the audience—be it Parliament, civil society, or the audited entity—adds communicative flexibility to audit outputs.

1.3 Data Types and Sources in Audit Practice

To assess the suitability of generative AI in an audit context, one must consider the nature of the data upon which it operates. In practice, SAIs deal with a blend of **structured data** (e.g., financial records, databases, time series) and **unstructured data** (e.g., contracts, policies, email communications, meeting minutes). Traditional data analytics tools have long served auditors well in the realm of structured data; however, the vast and growing corpus of unstructured data has often proven more elusive to systematic review.

It is precisely in this terrain that generative AI excels. LLMs, trained on internet-scale corpora, are capable of interpreting and generating text that is coherent, context-aware, and often surprisingly nuanced. When paired with retrieval-augmented generation (RAG) architectures or fine-tuned on institution-specific data (e.g., previous audit reports, legal codes), these models can retrieve relevant passages, summarise lengthy documents, and generate hypotheses for audit testing.

Consider the challenge of reviewing internal emails during a fraud investigation. Whereas manual review might require weeks of effort, an AI system could identify conversations indicative of conflicts of interest or bypassing of controls, clustering them by relevance and sentiment for auditor follow-up. Similarly, in performance audits, where impact evaluations are often buried in dense, academic reports, AI can summarise findings and extract methodological assumptions in a fraction of the time.

1.4 Technological Foundations

At the heart of these capabilities lie **large language models**—massive neural networks trained to predict text based on vast datasets. Among the most prominent are **OpenAI's GPT models** (notably GPT-4), **Anthropic's Claude series**, **Meta's LLaMA models**, and a rapidly evolving ecosystem of **open-source alternatives**, including Mistral, Falcon, and others.

Each model architecture carries trade-offs in terms of performance, transparency, adaptability, and data governance. Proprietary models such as GPT-4 tend to exhibit superior performance out of the box, benefiting from extensive commercial training resources. Conversely, open-source models offer greater control and customisability, particularly when deployed within sensitive institutional environments such as national audit offices, where data privacy and localisation are paramount.

One emerging best practice is the use of **hybrid deployments**, in which open-source models handle routine tasks on-premises, while secure API calls to commercial models are reserved for high-complexity natural language generation. Another is the **fine-tuning or prompt engineering** of models using audit-specific data, allowing for context-aware performance aligned with institutional norms and expectations.

In sum, the scope of generative AI in external audit is both broad and deep. It spans all major audit types, supports multiple processes within the audit lifecycle, and thrives on the kinds of unstructured data that increasingly characterise modern public administration. Its technological foundations are robust and evolving, yet their responsible application requires discernment, oversight, and a commitment to public service ethics. As we proceed through this handbook, we shall explore not only the promise of generative AI but also the principles, constraints, and safeguards necessary to ensure that its adoption strengthens, rather than supplants, the human judgment at the heart of public audit.

2 STRATEGIC INTEGRATION OF AI INTO AUDIT PRACTICE

The digital transformation of public sector auditing necessitates not merely technological adoption but a deliberate strategic alignment with institutional governance, international standards, and ethical imperatives. Supreme Audit Institutions (SAIs) must navigate this evolution whilst preserving audit independence, methodological rigour, and public trust. This chapter delineates a structured approach to integrating artificial intelligence (AI) into audit practice, anchored in INTOSAI standards, maturity assessment frameworks, and actionable implementation roadmaps.

2.1 Alignment with INTOSAI Principles and Standards (ISSAIs)

At the heart of strategic integration lies the imperative to align AI practices with the International Standards of Supreme Audit Institutions (ISSAIs). These standards, promulgated under the auspices of INTOSAI, enshrine the principles of legality, impartiality, transparency, and due process in public audit.

Incorporating AI into audit processes must in no wise compromise these cardinal values. As emphasised in the Moscow Declaration (INTOSAI, 2019), AI ought to be harnessed to enhance the independence, capacity, and impact of SAIs. This necessitates that audit judgments remain human-led, even when augmented by predictive or generative AI tools, ensuring automation never obscures accountability. Methodological rigour must be preserved through codified AI workflows mirroring traditional audit practices, particularly in evidence triangulation and quality assurance. Transparency, moreover, must be inviolably upheld via comprehensive model documentation and audit trails elucidating AI's influence on findings and risk assessments.

Thus, AI must be construed not as a surrogate for auditor discretion but as an instrument enhancing analytical precision and procedural efficiency—perpetually tempered by professional scepticism.

2.1.1 Foundational Compliance

The ISSAIs constitute the bedrock of ethical and effective auditing. AI integration must fortify—not erode—these principles. Under INTOSAI-P 12 **(Value and Benefits of SAIs)**, AI should amplify audit impact beyond mere process automation. Illustratively, the European Court of Auditors (2021) employs AI to predict budgetary inefficiencies, thereby advancing ISSAI's mandate for proactive fiscal stewardship. Concurrently, INTOSAI-P 20 **(Principles of Transparency and Accountability)** mandates independent validation of AI tools to ensure accuracy, exemplified by the GAO's AI Accountability Framework (2021), which requires third-party algorithmic testing prior to deployment.

2.1.2 Ethical and Legal Guardrails

ISSAI 130 **(Code of Ethics)** obligates AI systems to eschew bias, safeguard confidentiality, and ensure human accountability. The controversy surrounding Australia's Centrelink AI audit system (2021), censured for algorithmic bias, underscores the imperative of ethics-by-design (Brookings, 2021). Similarly, ISSAI 100 **(Fundamental Auditing Principles)** demands transparency and reproducibility of AI-generated findings. Brazil's tax authority (Receita Federal, 2021) adheres to this standard by publishing methodological notes for its machine learning models.

Proposed Amendments to the French Court of Accounts Code of Ethics Concerning the Use of Artificial Intelligence

1. The Financial Jurisdictions (FJ) recognize the benefits of using artificial intelligence (AI) to improve the efficiency and scope of their work, in accordance with the missions assigned by the legislature. To be legitimate, this use must be carried out within a rigorous framework that respects the principles of this charter in order to strengthen public trust in the institution.

2. The use of tools or techniques based on artificial intelligence cannot replace the independent exercise of professional judgment, nor undermine the independence, impartiality, or integrity of the persons concerned. The data processed and the results produced must be interpreted with the required critical distance, respecting the adversarial principle, the rights of the parties being audited, and the requirements of professional secrecy.

3. Any use of artificial intelligence must be rigorously documented, allowing for the tracing of its objectives, parameters, data sources, as well as technical and methodological limitations. Data subjects must ensure that processing is reproducible, verifiable, and compliant with applicable data protection and information security regulations.

4. Financial jurisdictions must ensure that individuals likely to use artificial intelligence tools receive appropriate training, covering both the technical aspects and the ethical and legal issues surrounding these technologies.

Key Principles Underpinning the Amendments:

- **Subsidiarity**: AI as an augmentative—not substitutive—instrument in audit practice.
- **Contestability**: Guaranteed recourse to human oversight for algorithmic determinations.
- **Institutional Vigilance**: Proactive governance to mitigate emergent risks of automation bias or opacity.

Drafted in accordance with INTOSAI standards and the EU's Ethics Guidelines for Trustworthy AI (2019).

2.2 Governance Framework for AI Integration in SAIs

AI governance within SAIs demands a multi-layered institutional architecture ensuring control, accountability, and ethical application. A mature governance model integrates oversight structures, risk registers, transparency mechanisms, and escalation protocols.

Essential components include an **AI Oversight Board**—a standing body with cross-functional representation responsible for approving use cases, monitoring risks, and validating outputs. **Model Documentation and Auditability** must accompany all AI systems via model cards detailing function, training data, limitations, and biases. A robust **Data Governance Framework** is indispensable, assuring data lineage, integrity, and quality as audits increasingly rely on structured and unstructured data. Crucially, **Human-in-the-loop Assurance** mandates that every AI-augmented output be verified and endorsed by an accountable auditor, ensuring legal defensibility and alignment with ISSAI 140 (Quality management for SAIs).

2.2.1 Institutional Oversight Structures

Effective AI adoption requires unambiguous governance. **AI Audit Committees**, as advocated by the OECD (2020), should comprise multidisciplinary experts (auditors, data scientists, legal advisors) to oversee projects—exemplified by Canada's Phoenix payroll audit system (2021). Concurrently, **Risk Management Protocols** (per KPMG, 2021) must classify AI tools by risk level (e.g., high-risk for fraud detection, low-risk for document review).

2.2.2 Policy and Procurement Considerations

Vendor Neutrality is paramount to avoid lock-in; Singapore's Smart Nation Programme achieves this through open-source AI frameworks. **Data Sovereignty** requires cloud-based AI tools to comply with jurisdictional data laws, notably the EU's GDPR, mandating citizen data storage within territorial boundaries.

2.3 AI Maturity Model for SAIs

Recognising SAIs' heterogeneous readiness, AI deployment must be undergirded by a **Maturity Model**—a diagnostic tool assessing institutional capacity and guiding capability development. A five-tiered continuum is proposed:

Tableau n° 1 : AI Maturity Model for SAIs

Maturity Level	Key Characteristics	Case Example
Awareness	Conceptual recognition; no operational deployments	
Experimentation	No formal AI strategy; experimental pilots	Early trials in Mexico's SAI (2020)

Maturity Level	Key Characteristics	Case Example
Operationalisation	Defined use cases (e.g., anomaly detection)	French Court of Accounts (2017, Payroll)
Institutionalisation	AI embedded in core audit workflows	Smart Nation Singapore (2021) ?
Transformative	AI drives predictive and prescriptive auditing	?

Maturity assessments enable SAIs to calibrate training, policy development, and infrastructure investment to institutional realities.

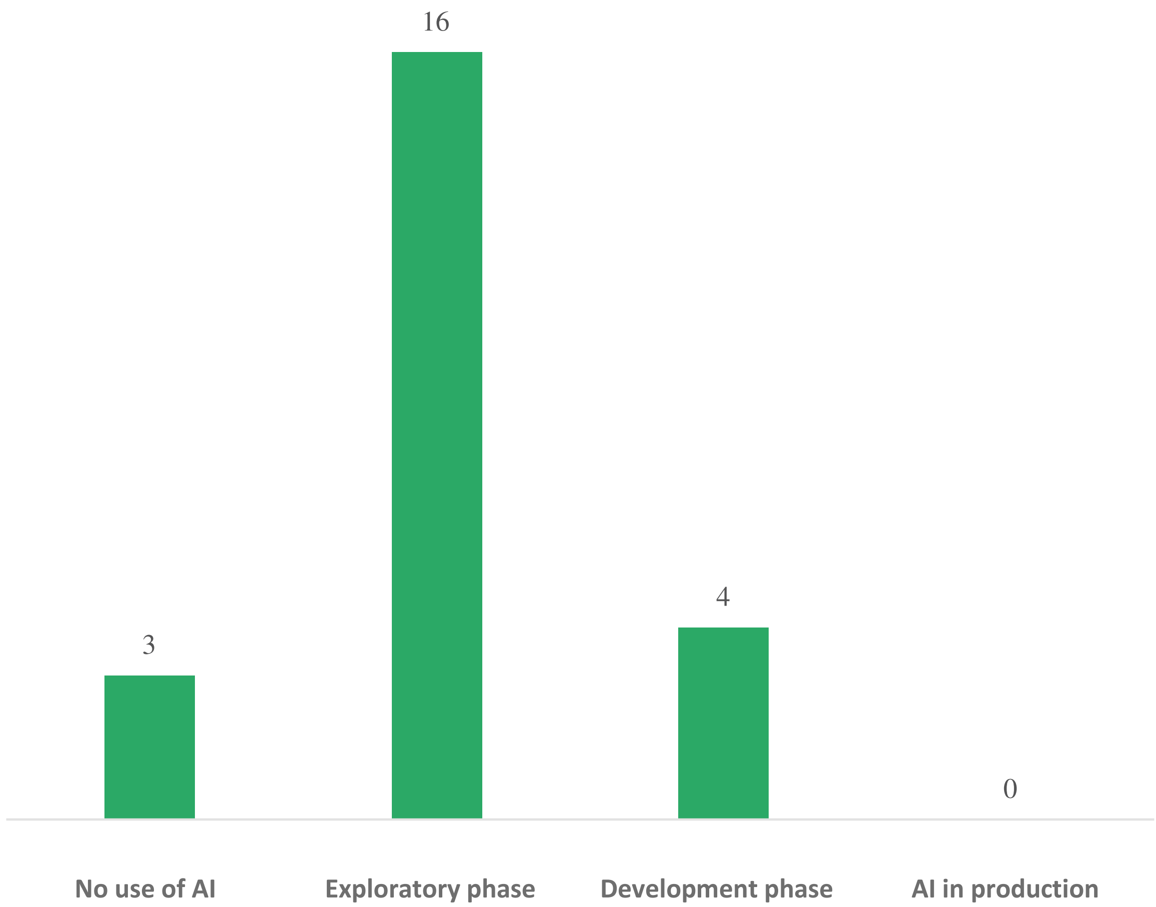
2.4 Benchmarking Progress

2.4.1 Benchmarking with EU Supreme Audit Institutions

In February 2024, the European Court of Audit (ECA) launched a survey to the 27 SAIs to gather an overview of how they are approaching AI. ECA received 23 replies, which provide a representative picture of the current state of play.

Sixteen of the surveyed SAIs (70 %) are currently in the exploratory phase, four (18 %) are developing some AI tools and no SAI yet has AI tools in production (see ***graphique 1***).

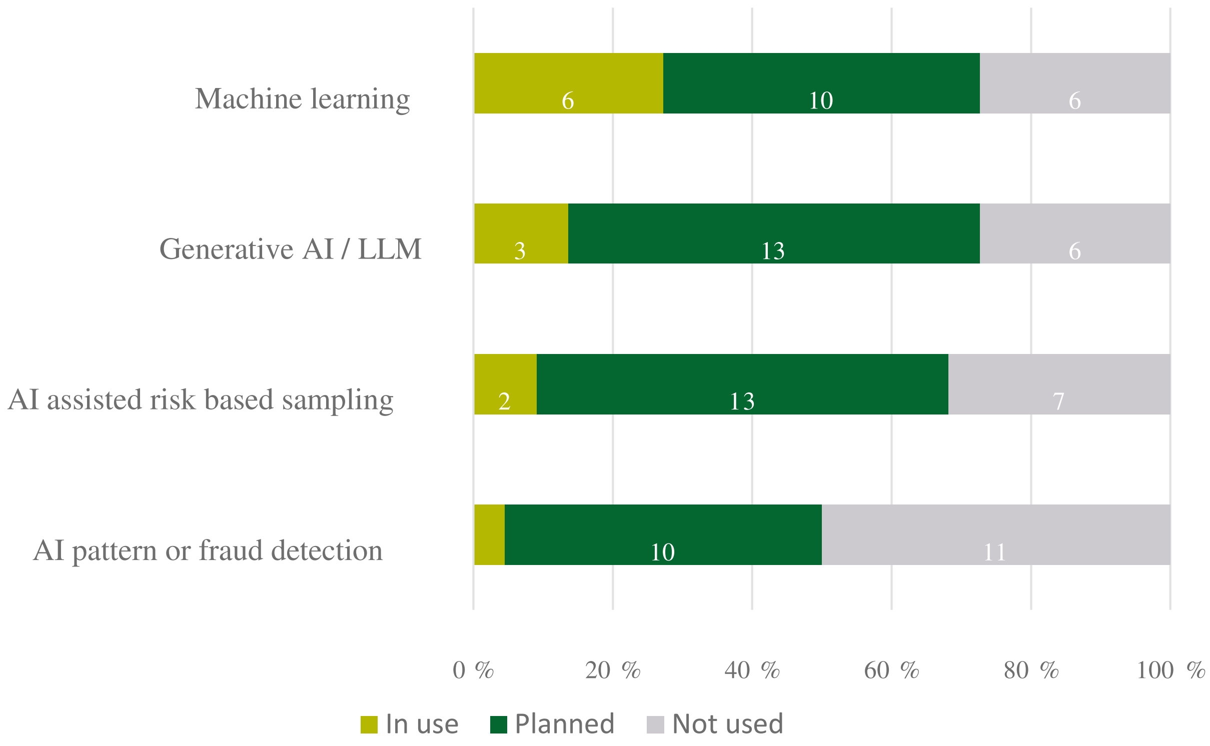
Graphique n° 1 : EU SAIs' self-assessment on the status of AI implementation



Source: ECA survey.

Eight SAIs stated that they are making already some use of AI technologies. Most SAIs are planning to use these technologies in the future (see ***graphique 2***). As an example, one respondent mentioned that they are using generative AI to assist in writing computer code.

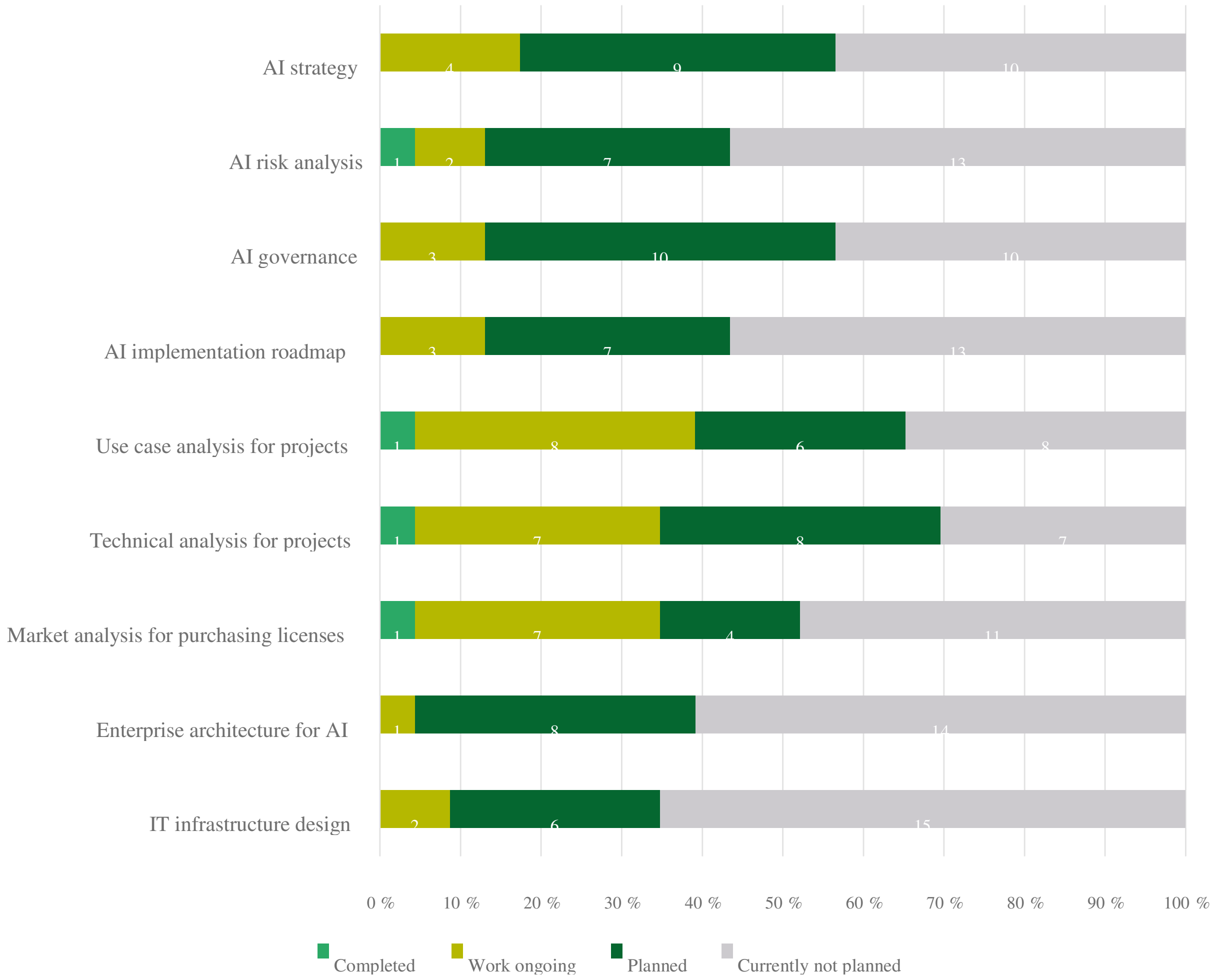
Graphique n° 2 : SAIs using or planning to use specific AI technologies



Source: ECA survey.

When introducing AI in the work practice, organisations can opt for a top-down approach, i.e. starting with strategic documents and moving down to technical analyses, or a bottom-up approach, i.e. consolidating technical experience and pilots into a formalised roadmap. Based on the replies concerning the status of key documents, ECA were not able to identify a dominant approach among SAIs (see ***graphique 3***).

Graphique n° 3 : Status of key documents concerning AI activities



Source: ECA survey.

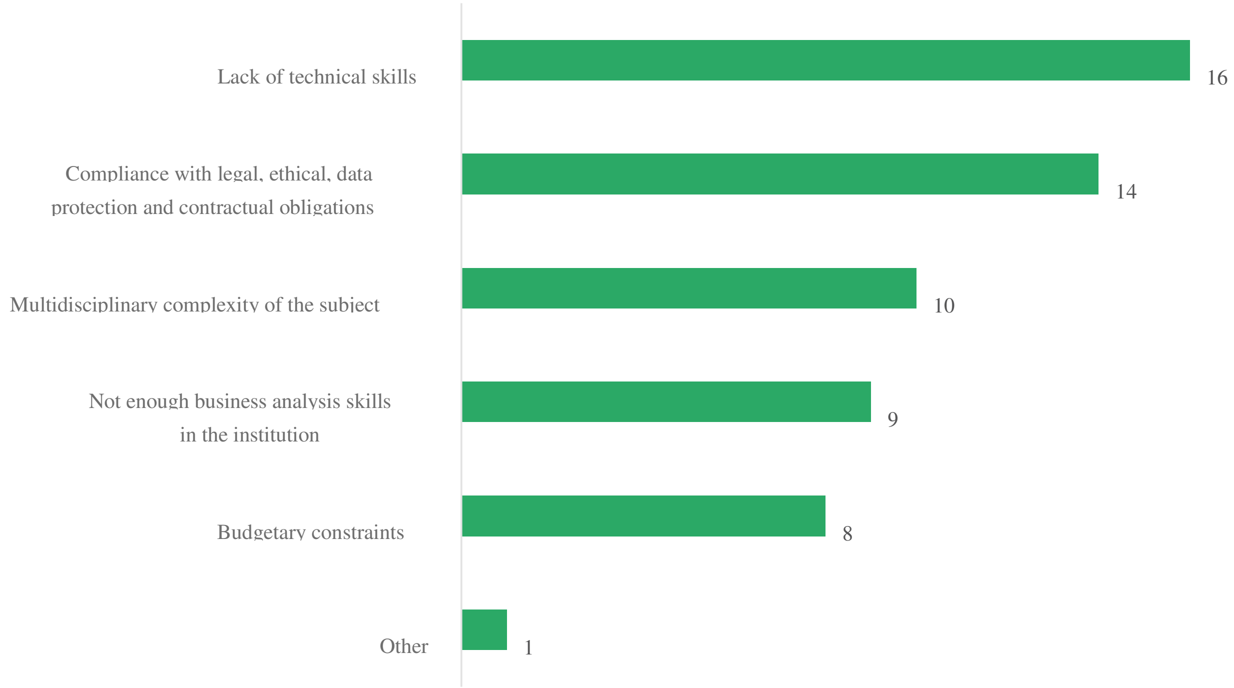
ECA asked SAIs whether they would be interested in cooperating with the ECA on AI. Three SAIs (17 %) replied that they are not interested due to practical reasons (e.g. lack of resources). The others would be most interested in cooperating with ECA in:

- the identification and exploration of use cases;
- sharing knowledge, documentation, code about experiments; and
- sharing user feedback on prototypes.

Interestingly, most SAIs are interested in sharing the analysis of the audit-related aspects of artificial intelligence, an aspect the ECA started much earlier to formalise.

ECA last question concerned the challenges that SAIs face in implementing AI in their organisation. Their replies are summarised in ***graphique 4***.

Graphique n° 4 : Most mentioned challenges to AI implementation



Source: ECA survey.

During official visit of EU SAIs and participation in working groups ECA gathered some additional feedback:

- in several cases, their staff started experimenting with AI at personal level, received general training, and expressed the need for guidance on practical applications;
- in some cases SAIs have started investigations on how to use LLMs to support their audit activities, but they do not have enough resources to create a specific AI task force;
- they expressed their interest in receiving ECA documents and training session.

2.4.2 Other non-EU audit institutions

In the context of the various INTOSAI working groups, the ECA has periodic exchanges with non-EU audit institutions. ***Table 2*** lists some relevant information regarding AI activities.

Tableau n° 2 : Examples of AI activities in non-EU audit institutions

US GAO	o The Government Accountability Office is very active in the field of AI; they also communicate activities and progress on their public website. o The GAO AI Accountability Framework was finalised in 2021; it identifies key accountability practices, centred around the principles of governance, data, performance, and monitoring, to help US federal agencies and others use AI responsibly. o The GAO Innovation Lab, set up in 2019 and currently comprises around 12 experts, is part of the broader "Science, Technology Assessment, and Analytics" team (STAA). As of September 2023, the STAA team has 156 employees[1]. o They recently published a very interesting list of current audit scenarios under analysis and prototyping.
TCU and CGU Brazil	o At the 4th Annual Meeting of the Working Group on Impact of Science and Technology on Auditing (Abu Dhabi, November 2023), the Tribunal de Contas da União presented how they use AI to enhance risk-based sample selections and the use of AI chatbots to analyse documents. o At the OECD Tech & Analytics Community of Practice of 17.11.2023, the Comptroller General of the Union presented "Generative AI for Integrity", showing how they have finetuned a Language Model (Llama2-7B) to improve its fluency in Portuguese, and how they use it to extract data from invoices.

Source: ECA.

2.5 Developing an AI-Audit Strategy Roadmap

A strategic roadmap is indispensable for aligning AI adoption with institutional priorities. It must articulate **Vision and Mission Alignment** (defining AI's role in public accountability), **Use Case Prioritisation** (selecting high-impact, low-risk domains like procurement anomaly detection), **Capability and Gap Assessment** (mapping IT infrastructure, staff competencies, and data quality), **Capacity Building** (integrating AI literacy into professional development), **Change Management Strategy** (fostering staff

[1] See also: Testimony before the Committee on House Administration, House of Representative.

confidence via transparent pilot evaluations), and **Monitoring and Evaluation** (employing metrics to refine deployments).

2.5.1 Prioritising Use Cases

SAIs should initially target high-impact, low-complexity applications: **Fraud Detection**, where the IMF (2020) cites AI's ROI in identifying benefit fraud (e.g., Australia's Centrelink), and **Contract Compliance**, wherein Microsoft (2021) documents a 70% reduction in manual review time.

Schéma n° 1 : AI Use Cases in Auditing: Reshaping Audit Practices

Source: Rajeev Sharma, AI Use Cases in Auditing: Reshaping Audit Practices, markovate.com

	Key Application Area	Primary Benefits/Function	Illustrative Example
1	**Data Analytics**	Enables rapid & accurate analysis of vast structured/unstructured data, revealing hidden patterns for deeper insights & improved audit quality.	AI algorithms identify patterns in revenue sources or expense disparities, providing strategic business enhancement suggestions.

	Key Application Area	Primary Benefits/Function	Illustrative Example
2	**Fraud Detection**	Uses ML & NLP to analyze large datasets & unstructured data, detecting anomalies signaling fraud efficiently.	ML models identify unusual transaction spikes or suspicious vendor payments for timely investigation.
3	**Predictive Analysis**	Forecasts future outcomes (revenue, expenses, risks) based on historical data for proactive risk management & strategic advice.	Analyzes past trends to forecast revenue dips/increases, advising on risk mitigation or growth opportunities.
4	**Planning & Resource Allocation**	Optimizes audit resource deployment using historical data, prioritizing high-risk areas for efficiency & effectiveness.	Assesses past audits to identify high-risk areas, prompting focused resource allocation in future audits.
5	**Continuous Monitoring**	Provides real-time transaction tracking & anomaly detection, offering ongoing assurance (vs. periodic traditional audits).	AI-driven solutions scan systems continuously, instantly alerting on unusual transactions or fraud indicators.
6	**Risk Assessment**	Analyzes historical data & trends to identify/predict high-risk areas, ensuring comprehensive audit coverage.	Evaluates past audits, transactions, and trends to highlight fraud/compliance/financial risks, enabling adjusted audit strategies.
7	**Document Processing**	Automates scanning, categorization & data extraction from documents (e.g., invoices) using OCR, reducing manual effort & errors.	OCR processes thousands of invoices, extracts financial data accurately, and flags missing/mismatched information.
8	**Anomaly Detection**	Identifies irregularities across entire datasets (vs. samples), flagging potential errors, non-compliance, or fraud early.	Detects abnormal patterns like frequent round-dollar transactions or rapid vendor payments signaling potential fraud.
9	**Journal Entry Testing**	Enables full-population testing (vs. sampling) to rapidly identify suspicious/unusual entries indicative of fraud.	Analyzes millions of entries to detect unusually high or round-number entries, focusing auditor effort on high-risk transactions.
10	**Audit Reporting**	Generates insightful reports with enhanced visualization, trend analysis, and forward-looking predictive recommendations.	Integrates predictive insights into reports, offering stakeholders actionable recommendations based on current data.

Source: Rajeev Sharma, AI Use Cases in Auditing: Reshaping Audit Practices, markovate.com

2.5.2 Implementation Phases

Implementation should proceed thus: **Pilot Testing** (small-scale deployments like automated invoice checks), **Scale-Up** (integration into financial/performance audits), and **Institutionalisation** (updating audit manuals per Deloitte, 2021).

2.5.3 Measuring Success

Success metrics encompass **Quantitative** indicators (e.g., reduced audit cycle time, as in Canada's Phoenix system, 2021) and **Qualitative** measures (stakeholder trust in AI outputs, per EY, 2021).

2.6 Policy, Procurement, and Privacy Considerations

2.6.1 Regulatory Compliance

Algorithmic Transparency Laws (e.g., the EU AI Act, 2024) require disclosure of AI logic for high-risk applications. **Procurement Standards** (per PwC, 2021) should mandate explainability features in vendor contracts.

2.6.2 Privacy-Preserving AI

Federated Learning (promoted by the World Bank, 2021) enables decentralised AI training to protect sensitive data, while **Anonymisation Techniques** (e.g., differential privacy mandated by GAO, 2021) safeguard confidentiality.

***

The integration of AI into public sector auditing transcends mere technical adaptation; it constitutes a governance imperative. SAIs must anchor AI in INTOSAI standards to preserve audit legitimacy, adopt tiered maturity models to ensure scalable progress, and prioritise ethics and privacy in procurement and policy.

As McKinsey (2021) contends, the future belongs to auditors who harness AI as a strategic ally—not a disruptive force. By wedding innovation to institutional integrity, SAIs may redefine public accountability for the digital age.

Subsequent chapters shall explore these insights' practical applications across the audit lifecycle, affirming that strategic AI integration is less a destination than a voyage—one demanding diligence, expertise, and unwavering constitutional fidelity.

3 KEY USE CASES IN EXTERNAL AUDIT

The application of generative artificial intelligence (AI) within the external audit landscape offers a transformational potential that is both immediate and enduring. As Supreme Audit Institutions (SAIs) seek to address increasingly complex public sector realities, generative AI provides a suite of tools that can augment, streamline, and elevate each phase of the audit lifecycle. In this chapter, we examine the principal use cases for generative AI across six critical stages of the audit process: the pre-audit phase, audit planning, fieldwork and evidence collection, audit analysis, reporting, and post-audit activities. Each section draws upon practical scenarios, evidentiary examples, and reflections from contemporary audit environments.

3.1 Pre-Audit Phase

3.1.1 Risk Profiling and Selection of Auditees

Generative AI models can analyse vast datasets—including past audit findings, financial disclosures, procurement data, and open-source intelligence—to help auditors prioritise auditees based on risk exposure, anomaly frequency, and contextual relevance. These models can synthesise risk indicators from unstructured data, such as news articles, public complaints, or whistle-blower reports, generating dynamic risk profiles for public entities.

3.1.2 Automated Review of Laws, Policies, and Regulations

The pre-audit phase often involves scoping the legal and regulatory landscape. Generative models can assist by summarising statutory texts, highlighting compliance obligations, and identifying key thematic shifts over time. For example, models like GPT or Claude can parse hundreds of pages of updated budgetary laws and synthesise the implications for auditors in a few succinct paragraphs.

3.1.3 Summarisation of Budget Documents and Expenditure Frameworks

AI can rapidly summarise complex budget documents and public expenditure frameworks. This functionality is especially valuable in large federal or decentralised states, where thousands of pages of financial planning documents must be digested swiftly. Generative models can extract core narratives, flag significant allocations, and align expenditure lines with performance objectives.

3.2 Audit Planning

3.2.1 Drafting Scoping Documents and Planning Memos

Drafting well-calibrated scoping documents and planning memoranda is a labour-intensive task. Generative AI can be employed to create initial drafts based on prior audits, risk profiles, and applicable standards. These drafts can then be reviewed and contextualised by senior auditors, accelerating turnaround without compromising quality.

3.2.2 Risk-Based Sampling Supported by AI-Driven Anomaly Detection

AI can improve the statistical rigour of sampling methodologies by identifying anomalies in financial data or transactions. Generative AI models can interface with structured data analytics to produce justifications for sampling strategies, flagging patterns that warrant closer scrutiny based on historical irregularities or predictive assessments.

3.2.3 Translation and Summarisation of Historical Audits or Financial Reports

In multilingual jurisdictions or in cross-border performance audits, generative AI can provide rapid translations and concise summaries of past audits or financial statements. This capacity fosters institutional memory, promotes knowledge sharing, and ensures consistency across audit teams.

3.3 Fieldwork and Evidence Collection

3.3.1 Document Review and Summarisation (Contracts, Emails, Invoices)

Field auditors are often overwhelmed by the volume of documents requiring review. Generative AI can automate the extraction of critical clauses, identify deviations from norms, and summarise the salient features of complex documentation. This capability is particularly impactful in contract audits or compliance assessments.

3.3.2 AI-Generated Interview Protocols Tailored to Audit Objectives

When designing fieldwork interviews, generative AI can create protocols tailored to specific audit themes, drawing upon both the objectives of the audit and the institutional profile of the interviewee. This allows for more precise and insightful engagements, especially in performance audits where qualitative data is pivotal.

3.3.3 Code Generation and Testing for IT Audits

In IT and cybersecurity audits, generative AI can support the generation of scripts and code to test systems for security flaws, compliance issues, or operational inefficiencies. By automating repetitive technical tasks, auditors can focus on interpreting results and providing strategic recommendations.

3.3.4 Image/Video Analysis for Infrastructure Audits

In combination with vision AI, generative models can assist in analysing images or drone footage related to public infrastructure projects. AI can detect inconsistencies, measure progress, and generate structured commentary on the state of roads, schools, or hospitals. This is particularly useful in geographically remote or conflict-affected areas.

3.4 Audit Analysis

3.4.1 Extracting and Structuring Insights from Massive Datasets

Auditors frequently contend with vast repositories of data. Generative AI can automate the structuring of such data, classifying transactions, tagging entities, and summarising statistical outliers. This can be instrumental in social programme audits, where data may span multiple agencies and sectors.

3.4.2 Large-Scale Sentiment or Opinion Analysis on Stakeholder Feedback

In participatory audits or evaluations of service delivery, AI can perform sentiment analysis on citizen feedback, parliamentary debates, or social media discourse. Generative models can synthesise these insights, providing auditors with a more nuanced understanding of public concerns and expectations.

3.4.3 Classification of Findings Using AI-Assisted Tagging

As findings emerge, AI can assist in categorising them according to standardised audit themes (e.g., procurement irregularities, HR mismanagement, financial impropriety). This streamlines report writing and facilitates consistency across multi-auditor teams.

3.5 Reporting

3.5.1 Drafting Audit Observations, Narratives, and Executive Summaries

Perhaps the most obvious use case for generative AI is in the drafting of written content. AI can transform bullet points or data tables into well-structured paragraphs, tailored to audit style guides and ISSAI-based formats. Auditors retain full editorial control, but benefit from first drafts that reduce cognitive and temporal load.

3.5.2 Tailoring Reports for Parliament, Civil Society, and the Media

Different stakeholders require different levels of detail and emphasis. Generative AI can generate multiple versions of the same report—an executive summary for Parliament, a data-driven infographic for media outlets, or a public-friendly FAQ for civil society. This adaptive communication enhances the reach and resonance of audit findings.

3.5.3 Visualisation Generation with AI for Charts and Dashboards

Generative AI tools can be integrated with data visualisation platforms to automatically create charts, graphs, and dashboards. These visual assets clarify complex findings and make reports more digestible for non-technical audiences. This is particularly relevant in audits involving longitudinal data or comparative metrics.

3.6 Post-Audit

3.6.1 Q&A Bots Trained on Audit Reports to Support Stakeholder Inquiries

Post-audit engagement can be significantly enhanced through AI-powered bots trained on the content of audit reports. These bots can answer stakeholder questions, direct users to relevant sections, and provide clarifications. This democratises access to audit insights and extends their utility beyond publication.

3.6.2 Training Junior Auditors Using Simulated AI-Driven Audit Environments

Generative AI can help simulate realistic audit scenarios for training purposes. Junior auditors can interact with dynamic datasets, conduct mock interviews, and draft sample observations—all guided by AI-generated prompts. This experiential learning accelerates competence and confidence.

3.6.3 Automatic Generation of Follow-Up Tracking Reports

Tracking the implementation of audit recommendations is a critical but often neglected task. Generative AI can cross-reference management responses, implementation updates, and field verification notes to generate draft follow-up reports. This ensures continuity, accountability, and institutional memory.

***

In conclusion, generative AI is not a panacea, but a powerful enabler. Its value lies in its ability to amplify human judgment, accelerate routine processes, and deepen analytical capacity. When deployed responsibly and strategically, generative AI can transform external audit from a primarily retrospective exercise to a forward-looking, real-time instrument of public sector accountability. Future chapters will further explore how to build the competencies, safeguards, and infrastructures necessary to unlock this potential sustainably and ethically.

4 IMPLEMENTATION ROADMAP

The integration of generative AI into external audit practice must be guided by a clear, pragmatic roadmap that accounts for the organisational readiness, technical capacity, legal frameworks, and strategic imperatives of Supreme Audit Institutions (SAIs). Implementing AI in a public auditing context demands both vision and caution, as audit offices operate under rigorous standards of independence, accountability, and transparency. This chapter presents a phased implementation model, introduces essential tools and platforms, and examines the policy and operational considerations for effective, ethical, and sustainable AI integration.

4.1 Phased AI Integration Model

A deliberate, staged approach allows SAIs to test and refine AI use cases, build institutional confidence, and mitigate risks.

4.1.1 Phase 1: Feasibility and Experimentation

In this initial phase, SAIs assess internal needs, define objectives, and experiment with generative AI tools in low-risk environments. The focus is on:

- Identifying relevant audit processes for augmentation (e.g., document summarisation, memo drafting).
- Creating AI literacy among staff through training and exploratory workshops.
- Establishing a cross-functional AI task force (auditors, data scientists, legal advisors).
- Conducting proofs of concept using open-source models or trial licences.

- Reviewing legal frameworks for data privacy and model usage.

4.1.2 Phase 2: Pilots and Limited-Scale Deployment

Having established feasibility, SAIs move to pilot deployments. Use cases such as automated planning memos or summarisation of audit histories are deployed in select departments:

- Measurable KPIs and audit quality benchmarks are defined.
- Human-in-the-loop oversight is enforced to ensure reliability.
- Technical assessments on latency, performance, and bias are conducted.
- Stakeholder feedback, particularly from line auditors, is gathered.
- Partnerships with academic institutions or audit peers are formalised.

4.1.3 Phase 3: Scaled Adoption with Integrated Workflows

In the final phase, successful use cases are embedded into organisational workflows:

- AI becomes a standard layer within audit management systems.
- APIs link generative models to audit databases and planning tools.
- Institutional governance policies and audit manuals are updated.
- Continuous monitoring systems are installed to track accuracy, fairness, and unintended effects.

Throughout all phases, emphasis must be placed on audit quality, replicability, and compliance with international standards.

4.2 Key Tools and Platforms

Several commercial and open-source generative AI platforms are emerging as valuable assets for SAIs:

- **ChatGPT Enterprise (OpenAI)**: Offers robust security, customisation, and integration capabilities. Particularly suited for drafting reports, generating interview questions, and assisting with communication strategies.
- **Claude (Anthropic)**: Known for its alignment with ethical safety norms and large context windows, making it suitable for reviewing extensive legislative or financial documents.
- **Meta's LLaMA and Open-Source Models (Mistral, Falcon, etc.)**: These can be fine-tuned for local languages and regulatory contexts. They offer transparency and control over model behaviour but require more technical overhead.

- **Microsoft Copilot and Google Duet AI**: Useful for embedding generative AI within common office applications like Excel, Word, and email systems, thereby supporting day-to-day audit tasks.

SAIs must match the tool to the use case, balancing performance, cost, interpretability, and auditability.

4.3 Procurement, Licensing, and Open-Source Considerations

Procurement in the public sector is governed by strict regulatory frameworks. When acquiring generative AI solutions, SAIs must:

- Ensure procurement criteria include explainability, security, and audit trail capabilities.
- Prefer models with strong localisation features (language, legal domain).
- Negotiate licensing terms that allow for internal retraining, monitoring, and safe sandboxing.
- Evaluate open-source alternatives for their transparency and customisation potential, especially for sensitive audits where data sovereignty is paramount.
- Conduct vendor risk assessments and consider exit strategies in case of tool discontinuation or vendor non-compliance.

A hybrid strategy—using commercial models for generic tasks and in-house or open-source models for sensitive domains—can often provide the optimal balance.

- ## 4. Data Preparation and Model Fine-Tuning

Generative AI relies heavily on the quality and availability of training and inference data. SAIs should undertake the following actions:

- **Data Governance**

  - Conduct a full data inventory: identify audit reports, financial statements, legal texts, and stakeholder feedback.
  - Classify data by sensitivity and establish access controls.
  - Implement anonymisation protocols for personal or classified data.

- **Data Cleaning and Structuring**

  - Convert legacy documents into machine-readable formats.
  - Use natural language processing (NLP) tools to structure unstructured text.
  - Create labelled datasets for fine-tuning, such as annotated audit findings or categorised risk indicators.

- **Model Fine-Tuning**

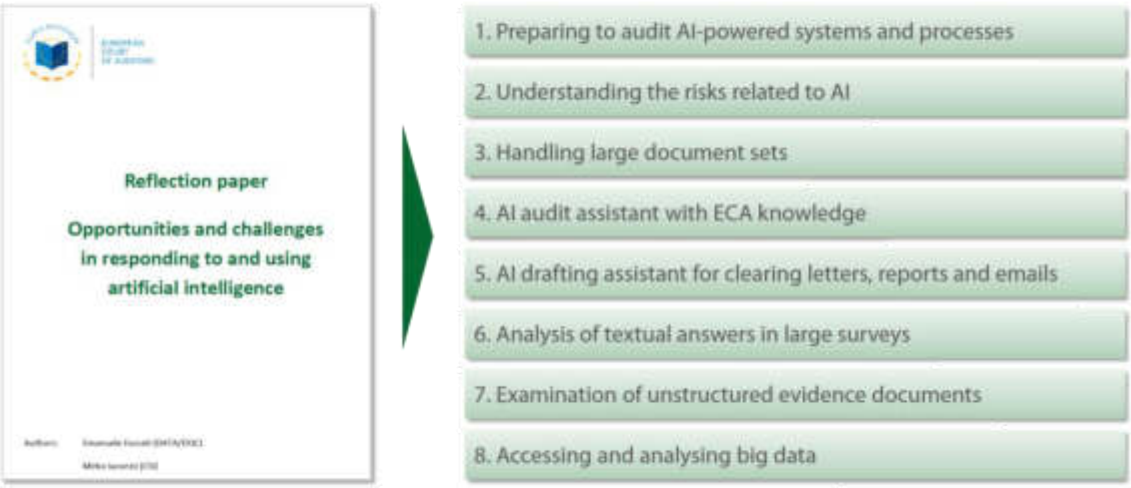
- Fine-tune models on historical audits, audit standards (ISSAIs), and local policy contexts.
- Monitor outputs for hallucinations, factuality errors, or discriminatory patterns.
- Conduct validation cycles with experienced auditors to evaluate model responses.

In doing so, SAIs not only improve the accuracy of AI tools but also preserve institutional knowledge in scalable digital form.

4.4 The European Court of Audit Proposal for an AI roadmap

In the reflection paper “Opportunities and challenges in responding to and using artificial intelligence”, The European Court of Audit (ECA) listed in 2023 a series of audit needs and practical use cases related to AI (see ***graphique 5***).

Graphique n° 5 : Audit needs and use cases related to AI



Source: ECA, DEC 113/23.

To address these needs and also enable the implementation of future use cases, ECA must establish a clear and coherent AI framework. This includes setting up a competence centre with appropriate governance, providing a specific training path, preparing technical infrastructure and IT tools, enhancing the services provided by the DATA team and the Directorate for Information, Workplace and Innovation (DIWI), and creating a portfolio of project proposals. In addition, ECA should foster interinstitutional cooperation and exchange of knowledge and practices. In the following paragraphs, ECA describe the proposed actions to achieve the three strategic goals.

Tableau n° 3 : Summary of proposed actions

Action	Description	Related to need described in the reflection paper	Strategic goal	Estimated completion
1	Create and followup a detailed communication plan	1, 2	1, 2, 3	Q2/2024
2	Create an AI training path for ECA staff	1, 2	1, 2	2024, then regular updates
3	Enhance the DATA services offered	3, 6, 7, 8	1, 2, 3	2025
4	Propose a portfolio of projects for new or enhanced tools	3, 4, 5, 6, 7	1	2024
5	Creation of an AI competence centre at the ECA and related governance	All	1	2024
6	Foster interinstitutional cooperation	All	1, 2, 3	2024, then regular updates

Source : ECA, 2023.

Some actions involve activities that are already ongoing in various directorates. ECA include them here to create a comprehensive document that reflects all aspects of AI. Other actions will require dedicated projects to be established, involving mostly DIWI and managed by the existing ECA governance bodies. The deployment roadmap is based on two principles:

- ECA prioritise solutions that it can acquire on the market or from the open-source community (subject to the data protection officer's approval), or that are developed by other institutions or interinstitutional working groups; and
- ECA develop its own AI solutions when it need to apply them to very specific activities, or when the sensitivity of data and information requires a strict control over the tool.

In preparing the document, ECA have not been in the position to estimate the required budget and resources for IT projects and for the actions detailed below, because it did not yet have sufficiently detailed specifications and analysis. In any case, an accurate estimation could only be obtained when ECA will launch individual project proposals and subject them to the usual IT processes. These project proposals, once received, will be analysed by DIWI for resource allocation and prioritisation. DATA team's resources involved in AI-related activities have been budgeted for in the 2024 work programme of the Directorate of the Audit Quality Control Committee (DQC).

As a quick and non-exhaustive reminder, the general process ECA follow to launch IT activities starts with customer relationship management (CRM) requests, that are filtered and assessed by DIWI management. The approved ones become short innovation projects (SIPs) or full IT projects, and follow the related processes and governance.

To move ahead quickly, ECA propose to use the SIP approach, i.e. the short innovation projects introduced by DIWI in 2022 to facilitate the process of innovation with tangible results. The SIPs should be used when the technology proposed is still not mature and/or requires some experimentation to assess the technical feasibility, evaluate the overall complexity and to provide a general estimation of the final costs and realistic delivery timing. SIPs are well defined smaller projects with specific goals and duration, and involve a pre-defined and controlled set of resources (example: one professional for three months and software purchase for €40 000). The SIP is run by a business project manager (for example, an auditor) supported by an IT project manager. The expected outcomes of a SIP are a completed Proof of Concept (or a minimum viable product[2]) and a documented analysis of what it takes in terms of resources and time to put in place or create the final product (tool and/or service).

***

The implementation of generative AI in external audit is both a technical journey and a cultural transformation. The phased model presented here—spanning experimentation, piloting, and scaled integration—provides a structured pathway that respects audit independence while embracing innovation. By selecting the right tools, ensuring ethical procurement, and preparing high-quality data, SAIs can unlock powerful efficiencies and insights. Above all, the roadmap must remain adaptive, ensuring that generative AI serves the enduring mandate of public audit: to safeguard accountability, integrity, and the public interest in an age of rapid digital change.

[2] An MVP is a development technique in which a new product or website is developed with sufficient features to satisfy early adopters. The final, complete set of features is only designed and developed after considering feedback from the product's initial users. This concept allows developers and companies to test their product hypotheses with minimal resources and to efficiently integrate user feedback to iterate and improve the product.

5 ETHICAL, LEGAL AND GOVERNANCE CHALLENGES IN AI-POWERED PUBLIC SECTOR AUDITING

The integration of artificial intelligence (AI) into public sector auditing presents transformative opportunities—enhancing efficiency, reducing fraud, and improving fiscal accountability. However, its adoption also introduces profound ethical, legal, and governance challenges. Governments and auditors must navigate dilemmas surrounding **integrity, bias, privacy, and explainability** to ensure AI systems uphold democratic values and public trust. This chapter examines these challenges through the lens of **transparency, fairness, and accountability**, drawing upon global case studies and regulatory frameworks.

5.1 Integrity, Transparency, and Accountability in AI Systems

5.1.1 The Imperative of Algorithmic Integrity

AI-driven audits must adhere to the same **rigorous ethical standards** as traditional audits. Unlike deterministic rule-based systems, AI models—particularly generative AI—operate probabilistically, raising concerns about **consistency and reliability**. For instance, the **GAO's AI Accountability Framework (2021)** emphasizes that agencies must ensure AI outputs are **verifiable, reproducible, and free from manipulation**.

- **Case Study**: Singapore's Smart Nation Programme employs AI for **contract compliance audits**, ensuring procurement transparency by cross-referencing vendor data with historical fraud patterns (Microsoft, 2021). However, if training data is incomplete, the system risks **false positives**, undermining trust in automated audits.

5.1.2 Transparency as a Governance Requirement

Public sector AI must be **explainable to non-technical stakeholders**, including legislators and citizens. The **OECD (2020)** advocates for **"algorithmic impact assessments"**—mandating disclosures on how AI models reach decisions.

- **Best Practice**: The **European Court of Auditors (2021)** requires AI tools used in budget compliance to provide **audit trails**, ensuring human auditors can trace decision logic.

5.1.3 Accountability in AI Decision-Making

When AI errors occur—such as misclassifying legitimate welfare claims as fraudulent—**clear accountability structures** must exist. The **Australian Centrelink scandal**

(2021) demonstrated the dangers of **over-reliance on AI without human oversight**, where faulty algorithms wrongly accused thousands of welfare recipients.

- **Regulatory Response**: The **EU's AI Act (2024)** classifies high-risk AI applications (e.g., fraud detection) as requiring **human-in-the-loop safeguards**.

5.2 Bias, Fairness, and Hallucinations in Generative AI

5.2.1 Systemic Bias in Training Data

AI models trained on historical audit data can inadvertently perpetuate existing societal biases, leading to discriminatory outcomes. Several public sector case studies illustrate how such biases manifest:

5.2.1.1 France's Welfare Fraud Detection Algorithm

The French government's use of algorithms to identify welfare payment errors has been legally challenged by human rights organizations[3]. The lawsuit alleges that the system discriminates against disabled individuals and single mothers by assigning risk scores based on personal data, leading to biased and intrusive investigations. This case underscores the importance of ensuring that AI tools do not reinforce existing societal disparities.

5.2.1.2 Denmark's Welfare Surveillance System

Denmark's Public Benefits Administration implemented a data mining initiative using machine learning algorithms to detect welfare fraud[4]. However, the system has been criticized for incorporating variables like nationality, leading to accusations of ethnic profiling. Such practices highlight the ethical challenges of using AI in public sector surveillance.

These examples underscore the critical need for transparency, ethical oversight, and continuous evaluation of AI systems in the public sector to prevent the perpetuation of historical biases and ensure equitable outcomes for all citizens.

[3] Algorithms Policed Welfare Systems For Years. Now They're Under Fire for Bias | WIRED.
[4] How Denmark's Welfare State Became a Surveillance Nightmare | WIRED

5.2.2 Fairness in AI-Driven Audits

The **IMF (2020)** highlights that AI must balance **fraud detection** with **equitable treatment**. Brazil’s tax compliance system (Receita Federal, 2021) uses **anomaly detection** but includes **socioeconomic filters** to prevent over-penalizing small businesses.

The International Monetary Fund (IMF) underscores the necessity of balancing fraud detection with equitable treatment in the deployment of artificial intelligence (AI) within public finance systems. In its 2024 publication[5], the IMF emphasizes that while AI can significantly enhance the detection of anomalies and fraudulent activities, it must be implemented with a strong ethical framework to prevent reinforcing existing biases or disproportionately affecting vulnerable populations. The IMF advocates for AI systems that respect data privacy, promote equitable access to services, and include robust oversight mechanisms to monitor AI's performance and impact.

In Brazil, the Receita Federal (Federal Revenue Service) has integrated AI-driven anomaly detection into its tax compliance system to identify irregularities and potential fraud. Recognizing the risk of over-penalizing small businesses and low-income groups, the system incorporates socioeconomic filters designed to mitigate such outcomes. These filters adjust the AI's risk assessments by considering the socioeconomic context of taxpayers, thereby aiming to prevent the disproportionate targeting of disadvantaged groups. This approach reflects a commitment to fairness and equity in tax enforcement, aligning with the IMF's recommendations for ethical AI deployment in public finance.

These examples illustrate the critical importance of integrating ethical considerations into AI systems used for fraud detection in the public sector. By incorporating safeguards such as socioeconomic filters and oversight mechanisms, governments can leverage AI's capabilities while upholding principles of fairness and equity.

5.2.3 Hallucinations and Fabricated Outputs

Generative AI models like LLMs can "hallucinate"—generating plausible but false audit findings. For instance, an AI might invent fictitious transactions if trained on insufficient data. Hybrid auditing is recommended, where AI flags anomalies but human auditors verify evidence.

Exemple of fabricated data : Artificial Intelligence AI and Machine Learning ML in Public Auditing Opportunities and Challenges SAI Algeria - Asian Journal of Government Audit (some references of article are fictional, for instance : Shukla, A., Sharma, P., & Verma, S. (2022). Algorithm Transparency in Machine Learning for Public Sector Auditing. Journal of Audit Methodologies, 14(1), 73-88.

[5] blog-pfm.imf.org, Unleashing the Power of AI in Public Finance.

5.3 Privacy and Confidentiality in Sensitive Government Data

5.3.1 Data Protection Risks

AI auditing requires access to **citizens' financial, health, and employment records**, raising **GDPR and** [Health Insurance Portability and Accountability Act](#) **(HIPAA) compliance** concerns. The **GAO (2021)** warns that **predictive auditing** in healthcare (e.g., Medicare fraud detection) must **anonymize data** to prevent breaches.

5.3.2 Secure AI Architectures

The **World Bank (2021)** advocates for **federated learning**, where AI models train on **decentralized data** without direct access to sensitive records.

For example, Estonia's **X-Road system** allows auditors to analyze encrypted datasets without exposing individual identities.

Estonia's X-Road system, also known as X-tee, is a cornerstone of the nation's digital infrastructure, enabling secure and efficient data exchange between various public and private sector entities. This decentralized platform ensures that data remains within its originating system, allowing authorized access without the need for centralized storage, thereby enhancing data security and privacy.

For auditors, X-Road offers significant advantages. By facilitating encrypted data exchanges, auditors can access necessary information across different databases without exposing individual identities. Each transaction on X-Road is digitally signed, time-stamped, and logged, ensuring data integrity and providing a transparent audit trail. This system aligns with the "once-only" principle, reducing redundancy and minimizing the risk of data breaches.

The platform's architecture is designed to prevent unauthorized access. Only registered and authenticated members can participate in data exchanges, and all data transfers are encrypted. This ensures that sensitive information remains confidential and is only accessible to entities with the appropriate permissions.

In summary, Estonia's X-Road system exemplifies how a well-structured digital infrastructure can facilitate efficient auditing processes while upholding the highest standards of data privacy and security.

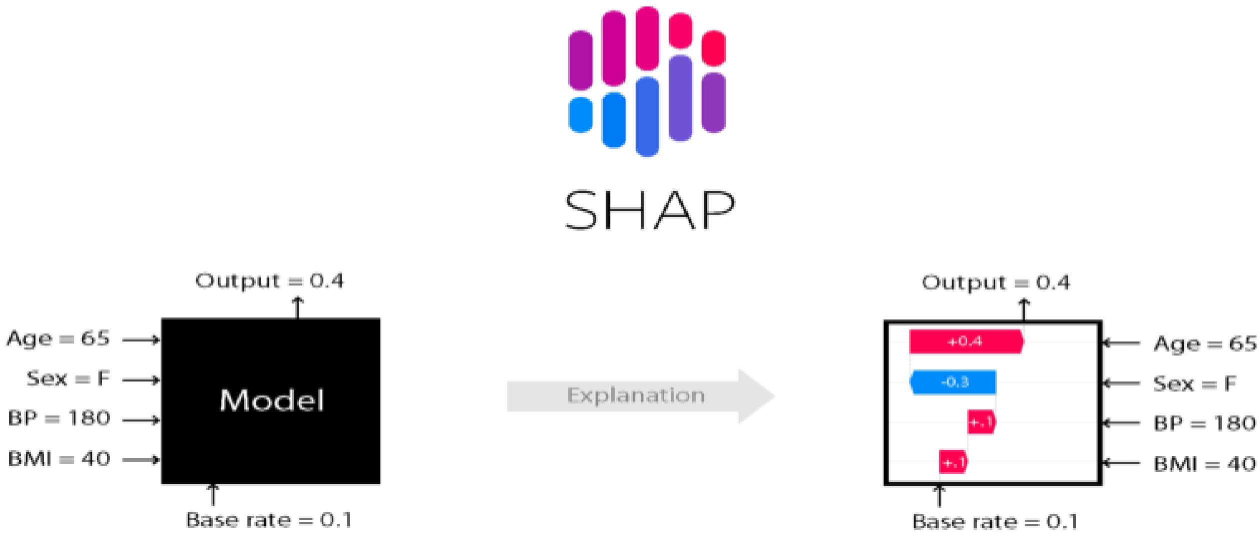
5.4 Explainability and Traceability of AI-Generated Outputs

Many AI models (e.g., deep learning) lack **intuitive explainability**, complicating compliance with **legal due process**. The **ACCA (2020)** argues that auditors must **document model logic** to defend findings in court. PwC (2021) uses **SHAP (Shapley Additive Explanations)** values to break down AI decisions in public sector audits. It is a game theoretic approach to explain the output of any machine learning model. It connects optimal credit allocation with local explanations using the classic Shapley values from game theory and their related extensions (see papers for details and citations).

5.4.1 What does SHAP do?

SHAP assigns each input feature a **"SHAP value"**, which represents how much that feature contributed to the difference between the model's prediction for a specific input and the average prediction across all inputs. It's based on **Shapley values** from cooperative game theory, which ensure a fair distribution of "credit" among features.

Graphique n° 6 : SHapley Additive exPlanations



Source: Welcome to the SHAP documentation — SHAP latest documentation

5.4.2 Why is SHAP useful?

- **Transparency**: It makes black-box models (like gradient boosting or deep learning) more interpretable.
- **Fairness**: Helps identify bias or unfair treatment by showing which features drive decisions.
- **Debugging**: Helps developers understand why a model made a certain prediction and whether it aligns with domain knowledge.

5.4.3 How does SHAP work?

- It computes the average marginal contribution of a feature across all possible combinations of features.

- This is computationally intensive, so SHAP uses approximations or model-specific optimizations (e.g., for tree-based models like XGBoost or LightGBM).

5.4.4 Example

Suppose an AI model predicts whether a loan should be approved. SHAP might show that:

- Income contributed +0.3 to the approval score
- Credit history contributed +0.2
- Age contributed -0.1
  This lets you see not just the final prediction, but *why* the model reached that conclusion.

In the context of **auditing and public governance**, SHAP is especially valuable because it supports **explainability and accountability**—both key principles when deploying AI in sensitive or regulated environments.

***

To harness AI's potential while mitigating risks, public sector auditors should adopt:

1. **Human Oversight**: Maintain **human review** of AI-generated findings.
2. **Bias Audits**: Regularly test models for **discriminatory patterns**.
3. **Transparency Protocols**: Disclose **data sources, logic, and limitations**.
4. **Privacy-by-Design**: Use **encryption and anonymization** techniques.
5. **Legal Compliance**: Align AI tools with **GDPR, AI Act, and GAO standards**.

As **McKinsey (2021)** notes, AI in auditing is not about replacing humans but **augmenting judgment**—ensuring technology serves **public interest above all**.

6 RISKS AND MITIGATION STRATEGIES IN AI-POWERED PUBLIC SECTOR AUDITING

The integration of artificial intelligence into public sector auditing represents both a remarkable opportunity and a considerable responsibility. While AI systems offer unprecedented capabilities in fraud detection, anomaly identification, and predictive analysis, their deployment introduces complex risks that demand equally sophisticated mitigation strategies. Supreme Audit Institutions must navigate these challenges with both technical precision and institutional wisdom, ensuring that technological adoption enhances rather than compromises the quality and integrity of public financial oversight.

6.1 Model Drift and the Challenge of Outdated Training Data

One of the most insidious risks in AI-powered auditing emerges from model drift, wherein the statistical properties of the target variable change over time, rendering once-reliable algorithms increasingly inaccurate. This phenomenon proves particularly problematic in public sector contexts where economic conditions, regulatory frameworks, and patterns of financial behavior evolve continuously. The Australian Centrelink case study (2021) demonstrated how welfare fraud detection models trained on pre-pandemic data failed to account for subsequent changes in unemployment patterns, resulting in both false positives and systemic inequities.

Mitigating this risk requires implementing robust model monitoring protocols. The European Court of Auditors (2021) has established a framework where predictive algorithms undergo quarterly performance assessments against updated validation datasets. Furthermore, the GAO's Accountability Framework (2021) recommends the creation of "temporal buffers" - maintaining parallel systems trained on different time horizons to detect and quantify drift. Perhaps most crucially, SAIs must resist the temptation to view AI models as static solutions; as the OECD (2020) emphasizes, these systems demand the same ongoing professional skepticism that auditors apply to financial statements.

6.2 Security Vulnerabilities and Adversarial Prompt Engineering

As Large Language Models become integrated into audit workflows, they introduce novel security considerations that traditional IT systems never faced. The phenomenon of "jailbreaking" - wherein carefully crafted inputs can subvert an AI's intended constraints - presents particular concern for SAIs handling sensitive fiscal data. Recent demonstrations have shown how seemingly innocuous prompts can induce models to bypass confidentiality protocols or generate inappropriate outputs.

The Singapore Smart Nation Programme (2021) offers instructive safeguards, implementing multi-layered validation for all AI-generated audit content. Their approach combines syntactic pattern recognition (flagging known adversarial prompt structures) with semantic analysis (evaluating output plausibility) before any findings enter official workflows. Microsoft's work with government auditing (2021) further demonstrates the value of "red teaming" exercises, where security specialists systematically attempt to compromise systems during development. These practices align with the World Bank's guidance (2021) on maintaining "defensive AI architectures" in public financial management.

6.3 The Perils of Inappropriate Automation

Not all audit functions benefit equally from AI augmentation, and discerning where automation adds value versus where it introduces risk represents a critical judgment for SAIs. The Canadian Phoenix payroll system audit (2021) revealed how excessive reliance on machine learning for complex exception handling actually exacerbated errors in benefit calculations.

Similarly, the IMF (2020) cautions against using predictive models for inherently qualitative assessments, such as evaluating the intent behind financial transactions.

Developing institutional wisdom about when not to deploy AI requires establishing clear suitability criteria. PwC's framework (2021) proposes three key considerations: the availability of high-quality training data, the ability to clearly define success metrics, and the existence of human fallback mechanisms. The Brazilian tax authority's implementation (Receita Federal, 2021) demonstrates this principle effectively, using AI for initial risk scoring while reserving human judgment for final compliance determinations. As KPMG's research (2021) underscores, the most effective audit functions will be those that view AI as a powerful but limited tool - one that supplements rather than supplants professional expertise.

6.4 Human-in-the-Loop Protocols as a Foundational Safeguard

The concept of human oversight takes on renewed importance in AI-augmented auditing. Robust Human-in-the-Loop (HITL) systems serve not merely as quality control measures but as essential components of procedural legitimacy. The EU's predictive auditing framework (European Commission, 2021) mandates that all algorithmic findings undergo human validation before affecting decisions, with particular scrutiny for high-impact determinations.

Designing effective HITL systems requires more than simply inserting human reviewers into automated workflows. Deloitte's implementation guidance (2021) emphasizes the need for specialized interface design that surfaces the most relevant information for human judgment, along with the model's confidence metrics and alternative interpretations. The ACCA (2020) further recommends that audit teams include members with dedicated training in AI interpretation, creating what McKinsey (2021) terms "bilingual" professionals fluent in both auditing standards and machine learning outputs.

6.5 Toward Responsible AI Adoption in Public Audit

The path forward for SAIs lies not in avoiding AI's risks but in managing them with the same rigor applied to financial risks. This requires viewing AI systems not as infallible black boxes but as complex instruments requiring continuous calibration and oversight. The EY framework (2021) proposes treating significant AI implementations as auditable entities themselves, subject to the same standards of evidence and documentation as the programs they evaluate.

Ultimately, as the Brookings Institution's research (2021) concludes, the measure of successful AI integration in public auditing won't be technological sophistication alone, but rather enhanced public trust. By implementing these mitigation strategies - combating model drift, securing against adversarial attacks, exercising automation restraint, and maintaining meaningful human oversight - SAIs can harness AI's potential while upholding their foundational commitments to accountability and good governance. The digital transformation of public audit need not compromise its essential character; rather, thoughtfully implemented, it can extend and enhance auditing's vital role in democratic society.

7 SKILLS AND CAPACITY BUILDING FOR AI-AUGMENTED PUBLIC SECTOR AUDITING

The transformative potential of artificial intelligence in public sector auditing remains fundamentally constrained not by technological limitations, but by human capital readiness. As Supreme Audit Institutions navigate the Fourth Industrial Revolution, cultivating a workforce capable of harnessing AI's analytical power while preserving auditing's core ethical tenets becomes paramount. This evolution demands nothing less than a renaissance in professional development—one that transcends technical upskilling to forge auditors equipped as sophisticated interpreters of algorithmic governance.

7.1 Reimagining the Audit Profession's Competency Architecture

Traditional audit competencies—financial acuity, regulatory knowledge, and investigative rigor—now require augmentation by three cardinal capabilities: algorithmic literacy, prompt craftsmanship, and ethical foresight. The GAO's Accountability Framework (2021) rightly identifies AI fluency not as a specialist niche but as a foundational requirement for all audit personnel. This manifests practically in auditors' ability to interrogate AI outputs with the same professional skepticism applied to financial statements. Singapore's Smart Nation Programme (2021) exemplifies this integrated approach, where auditors routinely validate machine learning predictions against ground-truth samples while maintaining epistemological vigilance regarding training data provenance.

7.2 Structured Learning Pathways for the Digital Auditor

Effective training transcends tool-specific instruction to cultivate conceptual mastery. The European Court of Auditors (2021) has pioneered a tiered curriculum progressing from awareness (understanding AI's capabilities and limitations) through interpretation (decoding model outputs and confidence metrics) to co-creation (collaborating with data scientists on audit-relevant algorithms). Crucially, as KPMG's research (2021) emphasizes, such programs must embed ethical reasoning throughout—challenging auditors to anticipate how bias might manifest in welfare fraud detection systems or how explainability deficits could undermine due process in tax compliance audits.

The emerging discipline of prompt engineering represents a particularly nuanced skill frontier. Brazil's Receita Federal (2021) demonstrates how carefully architected prompts transform generic large language models into specialized audit assistants capable of synthesizing regulatory frameworks with case-specific evidence. Mastery here demands linguistic precision, contextual awareness, and iterative refinement—skills more akin to legal drafting than conventional IT proficiency.

7.3 The Tripartite Collaboration Imperative

AI-augmented auditing dissolves traditional silos between audit, legal, and technical domains. Canada's Phoenix payroll audits (2021) reveal how effective AI implementation requires continuous dialogue: auditors define operational requirements, data engineers ensure algorithmic fairness, and legal advisors scrutinize compliance with evolving regulations like the EU AI Act. The OECD (2020) advocates formalizing this collaboration through embedded liaison roles—legal experts within audit teams and "audit translators" within data science units. Such integration ensures technical solutions remain anchored to public sector auditing's constitutional role.

7.4 Strategic Knowledge Partnerships

Closing the AI skills gap necessitates looking beyond institutional boundaries. Forward-thinking SAIs are cultivating symbiotic relationships with academia and technology communities. Australia's collaboration with university data ethics labs provides continuing education on bias mitigation techniques used in Centrelink welfare audits, while Microsoft's partnership with Singapore (2021) establishes joint innovation labs for developing audit-specific AI tools. The World Bank (2021) further documents how "technology stewardship programs" that second auditors to AI research centers accelerate organizational learning.

These alliances yield reciprocal benefits: universities gain access to real-world audit datasets for research (subject to rigorous anonymization protocols), while SAIs acquire early exposure to emerging techniques like federated learning for privacy-preserving data analysis. Crucially, as the Brookings Institution notes (2021), such partnerships must maintain strict governance to preserve audit independence—establishing clear intellectual property frameworks and conflict-of-interest safeguards.

7.5 Towards the Bilingual Auditor

The ultimate objective is developing what McKinsey (2021) terms the "bilingual professional"—auditors equally conversant in evidentiary standards and algorithmic logic. This manifests in practitioners who can articulate how a neural network identified contract irregularities while simultaneously assessing whether its methodology satisfies ISSAI evidentiary requirements. The ACCA's global certification initiative (2020) represents a significant stride toward formalizing this dual competency, blending technical modules on machine learning with rigorous examinations on professional ethics.

7.6 Institutionalizing Continuous Adaptation

Capacity building must evolve from episodic training to embedded organizational capability. The IMF (2020) recommends establishing Centers of Excellence within SAIs that serve both as internal consultancies on complex AI audits and as observatories tracking technological evolution. The European Commission's digital competency framework (2021) further mandates annual skills gap analyses and personalized development plans—recognizing that AI proficiency requires perpetual renewal.

In this transformative journey, SAIs would do well to recall Francis Bacon's adage: knowledge is power. By strategically cultivating human capabilities alongside technological infrastructure, public audit institutions can ensure artificial intelligence amplifies rather than undermines their mission to safeguard public resources and uphold democratic accountability. The future belongs not to algorithms alone, but to auditors who wield them with wisdom, discernment, and unwavering commitment to the public trust.

8 SAIS USE CASE STUDIES ON ARTIFICIAL INTELLIGENCE IN AUDIT

The integration of Large Language Models into public audit workflows represents a paradigm shift in governmental accountability. Choosing the right GenAI strategy for external audits depends on the SAI's specific needs, resources, and strategic objectives. Each option offers different levels of control, customization, and complexity, making it essential to consider the best fit to align with goals and compliance requirements.

Tableau n° 4 : Generative AI use cases for external audits

Audit Risk Assessment and Planning	Audit Plan Development	Engagement and Readiness Planning	Execution	Reporting
• Supports auditor research and risk understanding for specific industries.	• Enhances auditor research-business processes and control expectations.	• Supports auditor research for a deeper understanding of risk and business processes.	• Facilitates data analysis through natural language processing and advanced querying	• Generates initial audit reports and conducts thorough reviews.
• Guides audit design and process structuring.	• Recommends audits based on evaluated risk levels.	• Suggests control objectives and testing procedures for identified risk areas.	• Guides the creation of interview questions and assesses risk in control descriptions	• Summarizes audit findings for audit committee presentations.
• Identification and categorization of various audit areas.	• Allocates resources optimally based on availability and audit requirements.	• Outlines data sources and methods for extracting and analyzing data.	• Produces initial drafts of workpapers and summarizes audit evidence.	• Customizes communication styles for different stakeholders and enables report translations.

Source: ZBrain.

This chapter presents a diverse panorama of AI applications in audit practices across supreme audit institutions (SAIs) worldwide. These case studies reflect both the potential and challenges of integrating AI into public sector audits. Several countries, including China, India, Indonesia, Mexico, and Korea, have employed machine learning (ML), optical character recognition (OCR), graph theory, and business intelligence tools to enhance procurement oversight, detect anomalies, and prevent fraud in social programmes.

China pioneered with OCR to digitise archival data and detect collusion in procurement. India has leveraged AI in detecting scholarship fraud, circular trading, and forged images—demonstrating the granular capabilities of AI in detecting systemic irregularities. Indonesia, Mexico, and Korea showcased scalable solutions, such as anomaly detection in social assistance or job-matching systems. Other notable approaches included audit of AI algorithms themselves (Netherlands), and standardisation efforts to support AI readiness (Russia).

Crucially, these case studies not only illustrate AI's role in bolstering transparency and accountability but also foreground the need for ethical governance, algorithmic auditability, and capacity-building within SAIs. As AI becomes increasingly embedded in governance, the role of auditors in ensuring its responsible use is ever more vital.

Tableau n° 5 : Summary Table of SAI Use Case Studies

Case	Title / Focus	Country	AI Technique(s)	Audit Objective
A1	AI-based Archives & OCR	China	OCR	Digital archival of audit documents

Case	Title / Focus	Country	AI Technique(s)	Audit Objective
A2	Collusion in Procurement	China	AI	Detect bid rigging
A3	Circular Trading in Tax	India	ML, Rule-based	Detect circular transactions
A4	Image Similarity Detection	India	AI, Image Matching	Detect reuse of identical photos
A5	Non-existent Schools	India	AI/ML	Detect fraudulent scholarship claims
A6	Watermark Reading	India	AI	Extract hidden image metadata
A7	Ineligible Scholarship Quotas	India	AI/ML	Validate quota eligibility
A8	Graph Theory in Procurement	India	Graph Analysis	Detect bidder collusion
A9	Anomalies in Spending	Indonesia	AI	Budget misuse detection
A10	Auditing Procurement	Indonesia	AI	Automated procurement audit
A11	Social Assistance Fund	Indonesia	AI	Fraud detection in welfare
A12	ML in Sampling	Mexico	ML	Intelligent audit sampling
A13	Audit of AI Algorithm	Netherlands	Algorithmic Audit	Evaluate fairness/transparency of AI
A14	Payroll IT Audit	Nigeria	IT Audit Tools	Review integrated payroll system
A15	Anti-Corruption via Digital Tech	Oman	AI/BI Tools	Combat systemic corruption

Case	Title / Focus	Country	AI Technique(s)	Audit Objective
A16	Job-Matching AI Audit	Korea	AI, Algorithm Review	Audit KEIS matching system
A17	Welfare Blind Spot Detection	Korea	AI	Find citizens lacking access to welfare
A18	Records Digitisation	Russia	AI-readiness	Prepare archives for AI analysis
A19	Violation Auto-detection	Russia	AI	Flag public sector irregularities
A20	BI Software "VERA"	Türkiye	Business Intelligence	Improve audit efficiency & targeting

Source : India Compendium on Responsible Artificial Intelligence, 2023 (G 20).

8.1 Digitisation and Data Extraction: Building AI-Ready Infrastructures

Several case studies underscore the importance of foundational data work as a precursor to sophisticated AI analytics. The National Audit Office of China, for instance, utilised Optical Character Recognition (OCR) to create searchable digital archives. While this may appear rudimentary compared to more advanced applications, it is in fact a critical first step—transforming static records into analysable data sets. Similarly, Russia's efforts to standardise and digitise government records represent a long-term investment in AI-readiness, laying the groundwork for future audits powered by machine learning (ML) and natural language processing.

This recognition—that AI systems are only as capable as the data they ingest—runs as a leitmotif throughout the compendium. It reveals a shared understanding among SAIs: that responsible AI begins not with flashy algorithms, but with careful curation, structuring, and governance of data.

8.2 AI in Fraud Detection: From Pattern Recognition to Predictive Modelling

A dominant theme across the case studies is the use of AI to uncover fraudulent activity and irregular practices, particularly in the realms of public procurement and welfare distribution. India presents several striking examples. One case explores the detection of "circular trading" in tax filings—a practice whereby firms falsely inflate revenues through interconnected transactions. Here, AI models were trained to identify anomalous patterns and transactional loops that would elude manual inspection.

In another case, Indian auditors used image comparison algorithms to expose multiple applicants using identical photographs to claim scholarships, as well as identifying ghost schools fraudulently drawing state funds. These use cases highlight the micro-level acuity of AI systems when applied judiciously: capable of detecting inconsistencies that reside not in the substance of a transaction but in its structure, frequency, or metadata.

The Indonesian Audit Board took a similar approach to social assistance audits. By deploying AI to detect anomalies in spending, they uncovered discrepancies that traditional audits had failed to flag. The net result is an audit function that is no longer merely reactive, but increasingly pre-emptive—able to scan vast datasets in real-time and alert auditors to deviations as they occur.

8.3 Auditing the Algorithms: Ensuring AI Accountability

A particularly sophisticated contribution comes from the Netherlands, which conducted a direct audit of an AI algorithm itself. This meta-auditing—auditing the algorithm rather than the process or outputs it governs—marks an essential evolution in oversight thinking. As governments increasingly deploy algorithmic decision-making in welfare, immigration, and employment systems, the need for rigorous evaluation of these systems' fairness, transparency, and performance becomes paramount.

The Netherlands' case raises profound ethical and epistemological questions: How do we ensure that AI does not replicate or exacerbate social biases? Who bears responsibility for algorithmic errors? What standards of accountability are applicable to non-human decision-making agents? These questions, once theoretical, now demand concrete responses from SAIs, and the Dutch example offers a valuable prototype.

South Korea's audit of KEIS's AI-powered job-matching system echoes these concerns. The audit scrutinised the logic of the matching algorithm, finding that it recommended jobs even when matching scores were low and geographic preferences were disregarded. The implications are dual: first, algorithmic optimisation must reflect user-centric criteria; second, the audit function must evolve to interrogate the assumptions and threshold logic embedded within such systems.

8.4 The Architecture of Collaboration: Graph Theory and Network Analysis

Some of the most innovative techniques described in the compendium draw from graph theory and network science. India's use of graph analytics to detect collusion in government procurement represents a compelling blend of computational rigour and forensic investigation. By mapping the relationships among bidders and identifying tightly knit clusters suggestive of cartel-like behaviour, auditors were able to trace anti-competitive practices with unprecedented precision.

Such methods exemplify the shift from linear audit trails to multidimensional analysis. Auditors are no longer confined to tracing individual transactions; they are now capable of visualising entire ecosystems of activity, flagging emergent patterns of risk or corruption, and intervening proactively. This ability to "see the whole system" is perhaps the most revolutionary contribution of AI to public audit.

8.5 Challenges and Caveats: The Ethics of Automation

Yet for all its promise, the adoption of AI in audit is not without complications. Many of the case studies acknowledge the challenges of building in-house AI capabilities, training auditors in data science, and managing ethical dilemmas inherent in automated decision-making. Moreover, transparency in AI is not guaranteed. Black-box algorithms, especially those developed by third parties, can hinder auditability.

Hence, responsible AI in the public sector must rest upon a trinity of principles: explainability, accountability, and inclusivity. SAIs must develop not only technical competencies but also ethical frameworks to govern the use of AI. This includes protocols for bias testing, mechanisms for human oversight, and avenues for public redress.

***

In sum, the India compendium offers a kaleidoscopic view of how nations are integrating AI into audit, shaped by local needs, technological maturity, and institutional capacity. From rudimentary OCR to complex network analysis, each use case contributes to a shared global project: reimagining the audit function for the digital age.

Yet what unites these disparate efforts is not merely technological innovation but a renewed commitment to democratic governance. In deploying AI to scrutinise state functions, SAIs are reaffirming their constitutional role as guardians of the public trust. And in doing so, they offer a vital lesson: that in an age of machines, the enduring values of accountability, fairness, and justice remain profoundly human.

9 FUTURE OUTLOOK AND INNOVATION TRENDS

As the landscape of public sector auditing evolves at an unprecedented pace, the convergence of generative artificial intelligence (AI) and advanced automation technologies heralds a new era for supreme audit institutions. The integration of generative AI with robotic process automation (RPA), the advent of continuous and real-time AI-driven monitoring, the rise of multimodal auditing, the deployment of AI for stakeholder engagement, and the prospective use of synthetic data for audit simulation collectively signal a profound transformation in the audit profession. This chapter explores these innovation trends, elucidating their implications for the future of external audit in the public sector.

The integration of generative AI with RPA marks a pivotal shift from rule-based automation towards intelligent, adaptive audit processes. Traditionally, RPA has excelled in automating repetitive, structured tasks—such as data extraction, document classification, and workflow management—thereby enhancing operational efficiency and ensuring regulatory compliance through consistent audit trails

However, the addition of generative AI enables these automated systems to learn from data patterns, adapt to evolving scenarios, and make contextually informed decisions. This synergy empowers audit bots not only to execute routine tasks but also to generate nuanced insights, draft narrative reports, and even simulate complex scenarios, thus elevating the sophistication and value of automated audit functions. The result is a dynamic audit environment where efficiency is coupled with adaptability, allowing auditors to focus on higher-order analysis and strategic advisory roles.

A second, equally transformative trend is the emergence of continuous audit and AI-driven real-time monitoring. In contrast to traditional periodic audits, continuous auditing leverages AI to monitor transactions, controls, and compliance indicators as they occur, providing near-instantaneous detection of anomalies, risks, or policy breaches.

Generative AI models, trained on historical data and regulatory frameworks, can flag irregularities, prioritise high-risk cases, and even suggest remedial actions. This real-time vigilance not only enhances the timeliness and relevance of audit findings but also fosters a culture of proactive risk management within public sector organisations. As audit cycles become more dynamic and ongoing, the role of the auditor evolves from retrospective reviewer to real-time risk advisor, necessitating new skills in data analytics, AI oversight, and strategic communication.

The future of audit will also be characterised by the proliferation of multimodal auditing, wherein text, video, image, and speech analysis converge to offer a holistic view of organisational activities. Generative AI's capacity to analyse unstructured data—ranging from written correspondence and financial records to surveillance footage and audio recordings—enables auditors to uncover patterns, detect inconsistencies, and validate findings across multiple modalities. For instance, AI-driven image recognition can verify the physical existence of assets, while natural language processing can scrutinise contracts for compliance risks. The integration of such diverse data streams not only enriches the evidentiary base of audits but also enhances the robustness and credibility of audit conclusions. This multimodal approach is particularly salient in the public sector, where the complexity and breadth of operations often defy conventional audit techniques.

Another frontier is the application of AI to stakeholder engagement and participatory audit. Public sector audit institutions are increasingly called upon to foster transparency, accountability, and citizen trust. Generative AI can facilitate this mandate by enabling interactive platforms that solicit stakeholder input, analyse public submissions, and synthesise feedback into actionable insights. AI-powered chatbots and virtual assistants can demystify audit processes, answer stakeholder queries, and disseminate audit findings in accessible formats. Moreover, AI can identify emerging concerns or sentiments within stakeholder communities, allowing auditors to tailor their focus and communication strategies accordingly. This participatory dimension not only enhances the legitimacy of audits but also aligns audit priorities with societal expectations and democratic values.

Looking further ahead, the prospective use of synthetic data for audit simulation represents a paradigm shift in audit methodology. Synthetic data—artificially generated datasets that mimic the statistical properties of real-world data—enables auditors to test controls, validate algorithms, and simulate fraud scenarios without compromising sensitive information. Generative AI models can create realistic yet anonymised datasets, facilitating rigorous stress-testing of audit procedures and systems. This approach is particularly valuable in the context of emerging risks, such as cyber threats or novel financial instruments, where historical data may be scarce or incomplete. By harnessing synthetic data, audit institutions can enhance their preparedness, refine their methodologies, and ensure the resilience of their audit frameworks in the face of uncertainty.

The cumulative impact of these innovation trends is profound. The automation of routine audit activities, the acceleration of real-time analytics, the expansion into multimodal evidence, the deepening of stakeholder engagement, and the adoption of synthetic data collectively redefine the audit function. Auditors are thus liberated from the constraints of manual data processing and empowered to deliver deeper, more timely, and more strategic insights. At the same time, these advancements necessitate a recalibration of audit methodologies, a commitment to ethical standards, and an ongoing investment in skills development. As generative AI outputs may not always be independently verifiable, robust human oversight and transparent governance frameworks become indispensable to manage risks and uphold public trust.

The journey towards intelligent, adaptive, and participatory audit is not without its challenges. Integrating generative AI and automation technologies requires careful management of organisational change, comprehensive staff training, and vigilant attention to data privacy and regulatory compliance. Yet, for those institutions willing to embrace this transformation, the rewards are substantial: enhanced audit accuracy, operational efficiency, and the capacity to anticipate and respond to emerging risks in real time.

***

In conclusion, the future outlook for external audit in the public sector is defined by innovation, integration, and intelligence. Generative AI, in concert with RPA and other advanced technologies, is poised to revolutionise the audit profession, positioning supreme audit institutions at the vanguard of public accountability and good governance. By harnessing these trends, auditors will not only safeguard the integrity of public administration but also contribute to the broader societal mission of transparency, equity, and trust in public institutions.

ANNEXES

1 APPENDICES

1.1 Sample Prompts and Templates for Auditors

Effective engagement with generative AI begins with well-crafted prompts and structured interaction. Below are tailored prompts and templates external auditors can use across various phases of the audit lifecycle.

1.1.1 Pre-Audit Risk Identification Prompts

"Analyze historical audit findings for [Ministry/Agency] to identify recurring risk themes."

"Summarize the main regulatory requirements for public procurement in [Jurisdiction]."

1.1.2 Audit Planning Prompts

"Draft a scoping memo for a performance audit on digital service delivery in [Department]."

"Generate a risk-based sampling plan based on anomalies in last year's expenditure report."

1.1.3 Evidence Collection Prompts

"Summarize the following contractual document for key obligations and risks."

"Identify any inconsistencies in these financial transactions: [Upload dataset]."

1.1.4 Findings and Analysis Prompts

"Draft audit observations based on the following flagged anomalies."

"Categorize the following stakeholder feedback by sentiment and theme."

1.1.5 Reporting Prompts

"Write an executive summary of the audit findings on public health service delivery."

"Create charts and dashboards summarizing audit results for legislative briefings."

1.1.6 Post-Audit Prompts

"Generate a follow-up report template for tracking implementation of audit recommendations."

"Create a Q&A chatbot outline based on the last three performance audits."

1.2 Risk Matrix for Generative AI in Audits

Risk Category	Risk Description	Likelihood	Impact	Mitigation Measures
Data Privacy	Exposure of sensitive government data in AI tools	Medium	High	Use anonymization, deploy on-premise models, secure data within confidential enclaves
Hallucinations	AI generating plausible but false information	High	High	Establish human-in-the-loop validation, implement strict model constraints
Bias and Discrimination	Disparate outcomes arising from systemic biases in training data	Medium	High	De-bias datasets, use fairness auditing and adversarial testing tools
Over-Reliance	Excessive deferral by auditors to AI-generated outputs	Medium	Medium	Provide auditor training, require mandatory peer review for AI-assisted conclusions
Legal Non-Compliance	Breach of GDPR or national data protection regulations due to AI tool misuse	Low	High	Ensure legal vetting, enforce procurement due diligence, implement clear usage policies
Vendor Lock-In	Dependence on proprietary AI systems lacking interoperability or portability	Medium	Medium	Use open-source alternatives, develop multi-vendor procurement strategies
Traceability Deficiency	Lack of transparency in AI decision-making processes	High	High	Require detailed documentation, enable audit trails and explainability protocols

Risk Category	Risk Description	Likelihood	Impact	Mitigation Measures
Technical Failure	Model errors causing audit delays or incorrect findings	Low	High	Maintain redundancy, apply rigorous automated testing, and define fallback mechanisms
Skill Gaps	Inadequate AI literacy among auditors hindering effective oversight	High	Medium	Launch continuous training programmes, establish AI literacy benchmarks

1.3 AI Tools Comparison

Tool	Type	Strengths	Limitations	Recommended Use Cases
ChatGPT Enterprise	Commercial	Secure, scalable, customizable, integrates with MS tools	Licensing cost, opaque architecture	Reporting, summarization, content drafting
Claude (Anthropic)	Commercial	Constitutional AI, more aligned and steerable responses	Limited availability, less integration	Dialogue-based analysis, memo drafting
LLaMA 3	**Open-source**	High performance, modifiable, strong community	Requires infrastructure, risk of misuse	On-premise document review, evidence analysis
GPT-4 via Azure	Commercial	Compliant with data residency laws, robust performance	Limited customization, vendor dependency	Secure audits, government-specific deployments
Falcon LLM	**Open-source**	Lightweight, suitable for fine-tuning	Lower performance on complex queries	Department-specific automation
BLOOM	**Open-source**	Multilingual support, transparent governance	Slower inference, lower availability	Localized audits, translation, summarization
Azure OpenAI Studio	Platform	Visual interface, logging, API orchestration	Azure dependency, some services limited by geography	Workflow integration, testing, prototyping

Another benchmark: [Comparatif Interactif IA 2025 | Claude]

1.4 Policy Templates for AI Use Governance

1.4.1 AI Use Policy Template for Supreme Audit Institutions (SAIs)

- **Purpose:** To define the principles, roles, and procedures governing the responsible use of AI in public sector audits.

- **Scope:** Applies to all SAI employees, contractors, and external partners using AI tools.

- **Key Principles:**
  - Transparency: All AI-generated content must be clearly attributed and documented.
  - Human Oversight: AI shall support, not replace, auditor judgment.
  - Privacy Protection: AI systems must comply with all applicable data protection laws.
  - Explainability: Users must be able to interpret AI-generated recommendations.
  - Bias Mitigation: Regular testing and documentation must be performed to detect and mitigate bias.

- **Permitted Uses:**
  - Drafting reports, memos, and summaries.
  - Document review and analysis.
  - Data pattern detection and anomaly identification.

- **Prohibited Uses:**
  - Final decision-making without human review.
  - Training AI with sensitive data unless privacy controls are in place.
  - Sharing outputs with unauthorised third parties.

- **Training Requirements:**
  - Mandatory induction training on AI ethics and governance.
  - Ongoing technical upskilling opportunities.

- **Audit and Oversight:**
  - Quarterly review of AI usage logs.
  - Annual audit of model performance and outcomes.

1.4.2 AI Vendor Assessment Checklist

- **Protection**: Does the vendor offer on-premise deployment or sovereign cloud options?
- **Security:** Is the model trained using differential privacy or secure multi-party computation?
- **Explainability:** Are output rationales and model logs accessible to users? | | Bias Mitigation | Does the vendor disclose datasets and allow independent fairness testing?
- **Legal Compliance:** Is the tool GDPR compliant?
- **Contractual Terms:** Are SLAs included for model reliability and uptime?
- **Ethical Certification:** Is the system certified by third-party bodies or ethical review boards?
- **Integration Capability:** Can it be embedded into existing audit and data platforms? |

1.4.3 Audit Team AI Usage Declaration

Team Name: ______________________________

Audit Name: ______________________________

Date: ___________________________________

AI Tools Used:

Purpose of Use:

Review and Validation Process:

AI outputs reviewed by: _____________________

Peer review conducted on: _____________________

Declaration:

I hereby confirm that all AI-assisted work has been conducted in accordance with the SAI's governance policy.

Signed: _______________________ Date: _______________________

2 REFERENCES AND FURTHER READING

2.1 Bibliography

- INTOSAI. (n.d.). *Documents – Open access*. Retrieved from https://www.intosai.org/en/documents/open-access.html

- International Organization of Supreme Audit Institutions. (2023). *Science and technology in audit. The International Journal of Government Auditing*, *50*(2). Retrieved from :

  https://www.intosai.org/fileadmin/downloads/about_us/IJGA_Issues/2023/EN_Q2_2023_v50n2.pdf
- SIGMA (Support for Improvement in Governance and Management). (2024). *Increasing the impact of supreme audit institutions through external engagement* (SIGMA Paper No. 69). OECD. Retrieved from: https://one.oecd.org/document/GOV/SIGMA(2024)2/en/pdf
- World Bank. (2021). *Supreme audit institutions' use of information technology globally for more efficient and effective audits*. EFI Insight-Governance. Retrieved from : https://documents1.worldbank.org/curated/en/461071634537328252/pdf/Supreme-Audit-Institutions-Use-of-Information-Technology-Globally-for-More-Efficient-and-Effective-Audits.pdf
- McKinsey & Company. (2023, January). *The economic potential of generative AI: The next productivity frontier*. Retrieved from: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#introduction
- European Court of Auditors. (2024). *Artificial intelligence initial strategy and deployment roadmap, 2024–2025*. European Union. Retrieved from :

  https://www.eca.europa.eu/ECAPublications/ECA-AI-Strategy-2024-2025/ECA-AI-Strategy-2024-2025_EN.pdf
- Comptroller and Auditor General of India. (2023). *Compendium on responsible artificial intelligence*. Retrieved from :

  https://sai20.org/storage/app/uploads/public/679/c97/4b0/679c974b0954d084882913.pdf
- Adelakun, B. O., Onwubuariri, E. R., Adeniran, G. A., & Ntiakoh, A. (2024). Enhancing fraud detection in accounting through AI: Techniques and case studies. *Finance & Accounting Research Journal*, *6*, 978–999. https://doi.org/10.51594/farj.v6i6.1232
- Amirizaniani, M., Yao, J., Lavergne, A., Okada, E. S., Chadha, A., Roosta, T., & Shah, C. (2024). *LLMAuditor: A framework for auditing large language models using human-in-the-loop*. https://doi.org/10.48550/arXiv.2402.09346

2.2 Further reading

These strategy roadmaps offer guidance and inspiration for any tech leader driving AI, automation, or enterprise transformation. They're practical, high-impact resources from top consulting firms, tech giants, and respected professional associations.

1) Accenture – The Art of AI Maturity

2) Amazon – AWS Cloud Adoption Framework for Artificial Intelligence, Machine Learning, and Generative AI

3) Bain – Transforming CX with AI

4) Booz Allen – Securing AI

5) Microsoft – CIO's GenAI Playbook

6) PMI – DS/AI Project Playbook

7) PwC – Agentic AI Playbook

8) Scaled Agile – AI-Augmented Workforce

9) World Economic Forum – AI C-Suite Toolkit

-