



OFFICE OF THE STATE
COMPTROLLER AND
OMBUDSMAN OF ISRAEL

Artificial Intelligence in Public Sector Auditing

Dr. B. R. Ambedkar Lecture Series

Office of the Comptroller and Auditor General of India

New Delhi, June 2026

Matanyahu Englman

State Comptroller of Israel

& EUROSAI President



Top AI Risks

-  **Out of control**
-  **True or false - manipulation**
-  **Autonomic weapon in wrong hands**
-  **The employment market**
-  **Lack of transparency ("Blackbox")**
-  **Bias and discrimination**
-  **Data privacy**
-  **Information security**
-  **Fraud detection**
-  **Accountability & legal responsibility
(due to lack of human oversight)**
-  **Lack of professional human capital**
-  **Finance markets**

Recent Audits on Cyber and IT



OFFICE OF THE STATE COMPTROLLER
AND OMBUDSMAN OF ISRAEL



Examples of Cyber & IT Audits from 2024-2025



Information Systems and
Cyber Protection in Municipal
Elections



Information Security of
Collection Systems in Local
Authorities



Operation of Surveillance
Cameras by Local Authorities in
Public Spaces



Information Systems at the
Israel Postal Company and
the Postal Bank



Government Risk
Management in the ICT



Supply Chain Cyber Risk
Management in the ICT Sector



National Preparedness
in the Field of Artificial
Intelligence (AI)



Information Security and
Cyber Protection at the National
Insurance Institute



AI and Information Systems Audits

ARTIFICIAL INTELLIGENCE

- National Preparedness in the Field of Artificial Intelligence (November 2024)
- Parallel international audit in the field of artificial intelligence (published in March 2026)
- Cross-cutting questionnaire for 90 government ministries and public bodies on the implementation of the technology (October 2025; official findings to be published shortly)

INFORMATION SYSTEMS AND DIGITAL TECHNOLOGIES

- Information Systems and Cybersecurity at the Ministry of Foreign Affairs (2026)
- Document Authentication at the Ministry of Foreign Affairs – Apostille (February 2026)
- Implementation of the Government Policy for Providing Online Services to the Public (2022; 2024)
- ICT Systems for National Management of Information and Support for Evacuees During Operation Swords of Iron (February 2026)



OFFICE OF THE STATE COMPTROLLER
AND OMBUDSMAN OF ISRAEL



Cybersecurity and Civilian Infrastructure Audits



OFFICE OF THE STATE COMPTROLLER
AND OMBUDSMAN OF ISRAEL

CYBER AND INFORMATION SECURITY

- Cybersecurity in Remote Work (June 2026)
- Physical and Environmental Protection of Server and Communications Rooms (not yet published)
- Cybersecurity in Local Elections (May 2025)
- Penetration Testing in Government Ministries (e.g. May 2023)
- Cyber Protection and Business Continuity in the Automated Processing Service Unit at the Tax Authority (2022)
- Cyber Protection of Medical Devices and the Security of the Information Stored Therein (2022)
- Cyber Security in the Israel Electric Corporation Ltd. (2022)

Challenges in Conducting Cybersecurity Audits

- Establishment of two departments within the Office of the State Comptroller
- Incorporation of cyber reports in the workplan
- Intra-organizational qualifications (CISA)
- Internal training (CISA)
- Engagement with hacker service providers
- Development by the office of methodology for conducting penetration tests
- Development by the office of methodology for incorporating AI tools



OFFICE OF THE STATE COMPTROLLER
AND OMBUDSMAN OF ISRAEL



The Government's Handling of Foreign Influence in the Digital Space

- Identifying the threat in the world and in Israel
- Gaps in providing an inter-organizational government response
- Monitoring foreign influence - gaps and challenges
- Coping - deleting content
- Coping - public education and outreach
- Foreign influence during an election period



Election Period - Escalation of the Threat

United Kingdom

The UK Parliament's Intelligence and Security Committee expressed concerns regarding Russian interference in British politics, including in democratic processes such as the 2016 Brexit referendum.

United States

The Department of Homeland Security noted that foreign actors would almost certainly seek to influence democratic processes at all levels of government - federal, state and local - and identified efforts by Iran to influence the electorate and undermine confidence in the electoral process.

European Union

Russian attempts to interfere in the 2024 European Parliament elections were identified.

World Economic Forum

In 2025, it ranked the risk of disinformation at the top of the short-term risk list, noting that it was a key tool used by foreign actors to influence voters' intentions.

**Fueling
social
divisions**

**Undermining
citizens'
confidence in
the voting
results**

**Influencing
voters and
manipulating
election results**

**Undermining
public trust
in the
electoral
system**

**Creating
chaos on
election
day**

**Undermining
the
democratic
process**



Responding to Cyber Incidents During the Emergency Situation



The State Comptroller
and Ombudsman of Israel

PART 1

Examines the level of protection and resilience of the Israeli economy - the extent to which its various sectors are prepared to prevent, detect and respond to significant cyberattacks - as presented by the Israel National Cyber Directorate and the Israel Security Agency, each within its respective area of responsibility, and how this information was communicated to the political echelon before and during the emergency situation

PART 2

Examines the measures taken by state regulatory authorities before and during the emergency situation to strengthen the resilience of entities in the economy

PART 3

Examines the preparedness of 21 key entities in the economy - including critical national infrastructure entities, government ministries, essential bodies, institutions of higher education, local authorities and special entities that operate under self-regulation in the cyber field - to deal with cyberattacks before and during the emergency situation

Key Findings



The State Comptroller
and Ombudsman of Israel

"National Preparedness for Artificial Intelligence" November 2024

**Only NIS 1 billion
has been approved
in two tranches,
but the utilization
has been slow
and partial**

**Gaps in the central
governmental body
responsible for
leading a national
program**

**Gaps in the
approved
national program
and strategy**

**Failure to include the
education system in
the national program**



National Preparedness in the Field of Artificial Intelligence



The State Comptroller
and Ombudsman of Israel



OFFICE OF THE STATE COMPTROLLER
AND OMBUDSMAN OF ISRAEL

National Preparedness in the Field of Artificial Intelligence

November 2024

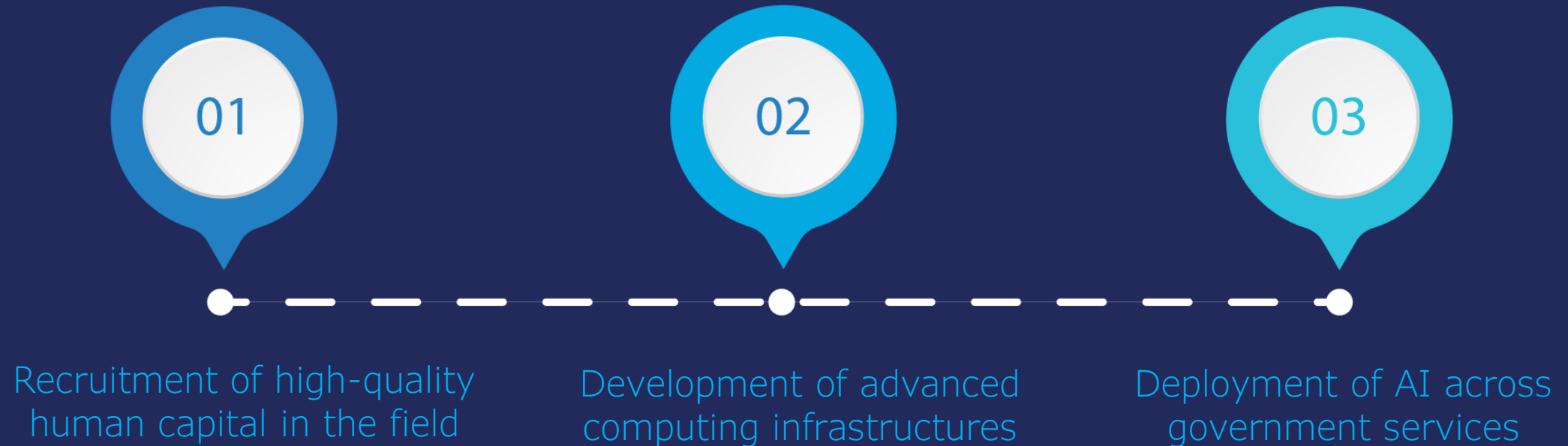
Governments Resolution 3375 – National AI Headquarters



The State Comptroller
and Ombudsman of Israel

- Establishment of a support unit in the Prime Minister's Office, with an initial budget of NIS 120 million (2025-2026)
- **Core mandate:** Formulation of a multi-year national AI plan within 120 working days

THREE MAIN AXES



Appointment of Chief of Staff with experience in military intelligence and digital transformation

Ministry of Education Declares 2025 as the Year of AI



The State Comptroller
and Ombudsman of Israel

The Ministry of Education developed teacher training and innovative lesson plans to make AI accessible to all students and teachers across Israeli society

Over 400 leading tech companies (including Google, Microsoft, Apple, and Nvidia) partnered with the ministry to train ~3,000 mentors who supported schools in implementing AI tools

New tools include: Q (AI coaching bot), Bina (secure Gemini-based chat), **Magic school** (lesson planning and assessment), and **Minecraft** adapted for younger students



Summary



The State Comptroller
and Ombudsman of Israel

In 14 months (Nov 2024-Jan 2026), Israel moved from no approved AI strategy to concrete government decisions, including a lead body and initial budget.

With key recommendations in place, the focus now shifts to implementation: strengthening engineering capacity, advancing legislation, and securing long-term funding.

Nov 24
State Comptroller's
Report

Nov 24
Nagel Committee
Report

Sep 25
Resolution 3375

Dec 25 - Jan 26
Expected formulation of
a multi-year plan

Parallel Audit on Artificial Intelligence

12 Countries



9 Topics

Plan

Strategic Plan
Budgets
Regulation

Prepare

Infrastructure
Digital Maturity
Information Security

Deliver

Governmental
Projects
Human Capital
NLP

89%

identified **clear governance and strategy** as key to AI success

90%

prioritize an **AI ecosystem** for cross-sector coordination

91%

set goals to boost public awareness and understanding of AI

92%

see human capital shortages as the main barrier to AI adoption



Parallel Audit on AI

Coordinated by SAI Israel | March 2026

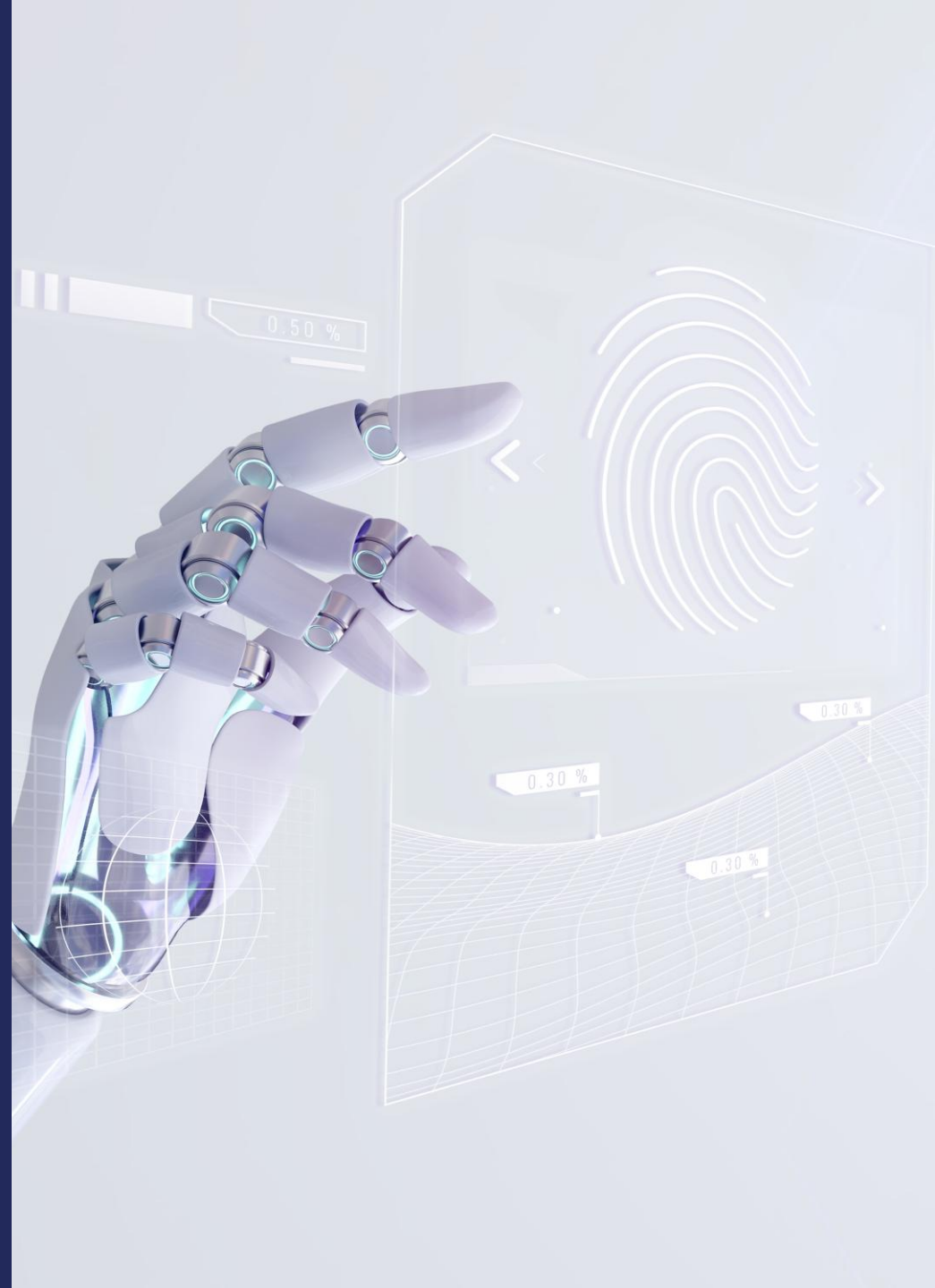


OFFICE OF THE STATE COMPTROLLER
AND OMBUDSMAN OF ISRAEL



The State Comptroller
and Ombudsman of Israel

Activities of European SAIs in the Field of AI Deployment and Cybersecurity



EU Artificial Intelligence Act



OFFICE OF THE STATE COMPTROLLER
AND OMBUDSMAN OF ISRAEL

ARTICLE 15: ACCURACY, ROBUSTNESS AND CYBERSECURITY

SUMMARY

1. High-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle.
2. To address the technical aspects of how to measure the appropriate levels of accuracy and robustness set out in paragraph 1 and any other relevant performance metrics, the Commission shall, in cooperation with relevant stakeholders and organisations such as metrology and benchmarking authorities, encourage, as appropriate, the development of benchmarks and measurement methodologies.
3. The levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall be declared in the accompanying instructions of use.
4. High-risk AI systems shall be as resilient as possible regarding errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems. Technical and organisational measures shall be taken in this regard. The robustness of high-risk AI systems may be achieved through technical redundancy solutions, which may include backup or fail-safe plans. High-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way as to eliminate or reduce as far as possible the risk of possibly biased outputs influencing input for future operations (feedback loops), and as to ensure that any such feedback loops are duly addressed with appropriate mitigation measures.
5. High-risk AI systems shall be resilient against attempts by unauthorised third parties to alter their use, outputs or performance by exploiting system vulnerabilities. The technical solutions aiming to ensure the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks. The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set (data poisoning), or pre-trained components used in training (model poisoning), inputs designed to cause the AI model to make a mistake (adversarial examples or model evasion), confidentiality attacks or model flaws.



Reports by European SAIs



European Court of Auditors



Special Report: “EU Artificial Intelligence Ambition - Stronger governance and increased, more focused investment essential going forward” (2024)

Aim of the audit:

- To assess the effectiveness of the European Commission's contribution to the development of the EU's AI ecosystem.
- To assess the implementation of EU-funded initiatives supporting medium-sized enterprises (SMEs) and AI research.

Special Report: “EU Artificial Intelligence Ambition - Stronger governance and increased, more focused investment essential going forward”

Key Findings:

- Poor coordination of AI measures across the EU due to lack of governance tools.
- EU AI investment lagging behind global leaders.
- Infrastructure support for SMEs is timely but slow in delivering results.
- EU-funded AI research spending is rising, but contributions to developing an EU AI ecosystem are insufficient.

Recommendations for the Commission:

- Re-evaluate EU AI investment targets with member states.
- Assess the need for an EU-funded support system for AI-innovative SMEs.
- Ensure coordinated functioning of EU-funded AI infrastructure.
- Strengthen efforts to exploit results from EU-funded AI research



National Audit Office of Lithuania



“Management of Artificial Intelligence in the Public Sector” (2025)

Aim of the audit:

To assess whether the public sector has the necessary preconditions for effective AI management, focusing on:

- **Development readiness** - Are enabling conditions in place for AI development?
- **Governance & risk**: Is AI regulation sufficient to mitigate potential risks?
- **Resources and capacity**: Are the resources required for the functioning of AI properly managed?

“Management of Artificial Intelligence in the Public Sector”

Key Findings:

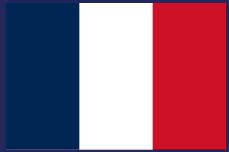
- Weak enabling conditions for AI in the public sector
- Insufficient legal and governance framework for AI
- Inadequate management of AI-related resources

Key Recommendations for the relevant bodies:

- Establish a national AI strategy for the public sector
- Promote knowledge-sharing and good practices
- Develop core data and language resources
- Strengthen methodological guidance, computing capacity and data governance
- Provide training and support to build institutional competences
- Enhance AI risk management and cybersecurity



French Court of Accounts



“Evaluation of the National Artificial Intelligence Research Strategy (NSAI)” (2023)

Goals:

- Evaluate whether the national AI research strategy (launched 2018, updated 2022-2025) strengthened France’s scientific and ecosystem position.
- Examine effectiveness and coherence of national funding and strategic priorities in AI research, training, and centers of excellence.
- Assess whether ethical, trust, and coordination mechanisms are embedded in the strategy’s implementation.



French Court of Accounts

“Evaluation of the National Artificial Intelligence Research Strategy (NSAI)”

Key findings:

- France has maintained a strong research base, remaining top in Europe and improving in global rankings.
- The strategy’s research and excellence components are largely implemented, but impact measurement is weak.
- Funding is fragmented across programs with no consolidated reporting mechanism to track results comprehensively.
- Coordination across public policies remains dispersed and undertracked.

Recommendations:

- Establish systematic monitoring & impact measurement of the AI research strategy outcomes.
- Improve governance coherence and long-term steering structures across universities, research institutes, and ministries.
- Enhance integration of ethical and trust considerations into research and training programs.
- Strengthen linkages between research excellence centers to avoid silos and boost international visibility.



Romanian Court of Audit



Romanian Court of Accounts Digital Strategy 2023–2028 (2023)

Goals:

- Establish a comprehensive digital transformation framework for the Romanian Court of Accounts through 2028.
- Enhance IT capacity, automation, and data-driven audit processes, including emerging technologies like AI, machine learning and analytics.
- Improve audit quality, efficiency, and interoperability across government via digital systems.
- Strengthen audit institution's transformation to a digital, data-centric audit organization.



Romanian Court of Audit

Romanian Court of Accounts Digital Strategy 2023–2028

Key findings:

- RCA aims to integrate digital technologies to modernize audit processes.
- The strategy acknowledges the need to automate repetitive tasks and transition to *data-driven auditing*.
- Current systems and skills require significant improvement to support advanced analytical tools and emerging tech-like AI.
- Interoperability and data exchange between RCA systems and audited entities is essential for future digital maturity.

Recommendations / Strategic Priorities:

- Implement a legislative framework to support digital and AI integration.
- Enhance staff digital skills and competency in data analysis and tech tools.
- Boost interoperability and secure data exchange among audit and public sector systems.
- Monitor and adapt the *digital transformation trajectory* with performance indicators through 2028.



National Audit Office of Estonia



“Overview of the development of AI solutions in public sector organisations” (2025)

Goals:

- Provide a national overview of how Estonian public sector organisations develop and use AI solutions.
- Assess the readiness of public authorities to adopt AI in a responsible, secure, and effective manner.
- Identify key enablers and obstacles affecting AI development and implementation in the public sector.

Scope:

- Covers the period 2016-2024

Based on:

- A survey of 48 public sector organisations
- Analysis of national AI strategies and digital policy documents
- Interviews with key ministries and agencies

Contributes to a EUROSAI international joint audit on AI readiness, to be completed in 2026.

“Overview of the development of AI solutions in public sector organisations” (2025)

Key findings:

- AI adoption is growing, but most solutions are still in testing or early-use phases.
- Fewer than 30 AI solutions are actively used, and tangible benefits (cost savings, faster decisions) remain limited.
- Main obstacles identified: poor data quality and limited data availability; insufficient AI knowledge and skills among public sector staff; legal and data protection constraints; lack of long-term funding and dedicated IT infrastructure.
- Most organisations do not yet have an AI strategy or action plan aligned with national objectives.

Key Recommendations:

- Strengthen data governance and data quality management as a prerequisite for AI.
- Invest in capacity building and AI literacy across public sector organisations.
- Provide clear legal guidance and national regulation to support compliant AI use.
- Improve strategic planning, coordination, and sustainable funding for AI solutions.
- Ensure risk assessment, transparency, and security in line with the EU AI Act.

**State Audit Office
of the Republic of
Latvia**



“Introduction and Use of Artificial Intelligence in Latvia” (2025)

Aim of the audit:

- To summarize the situation regarding the introduction and use of artificial intelligence in Latvian public administration.
- To provide information to each ministry and state institution as a potential implementer, user and developer of AI solutions in its sector, including for the formation of sectoral policy.

“Introduction and Use of Artificial Intelligence in Latvia”

Findings:

- Limited use of AI in public administration
- Lack of overall information and evaluation
- Unidentified infrastructure and resources
- Fragmented strategy and policy framework
- AI not clearly addressed in planning documents
- Insufficient legal and ethical framework



Netherlands Court of Audit



“Focus on AI in the Dutch Central Government” (2024)

Aim of the audit

To provide an initial insight into the AI allegedly used by central government, the opportunities government organizations expect AI to deliver and how they evaluate and mitigate the risks.



Netherlands Court of Audit

“Focus on AI in the Dutch Central Government”

Key Findings:

- Most of the 70 audited bodies use multiple AI systems (3+ per organization).
- AI is mainly applied to internal processes (data retrieval, application processing), with limited direct impact on citizens.
- AI is seen as tool for efficiency gains, while uptake is constrained by:
 - Skills and expertise gaps
 - Legal and regulatory uncertainty
 - Unsuitable infrastructure
 - High compliance burden
- Risk assessments are lacking or inconsistent; there is no government-wide assessment instrument.
- Organizations report no unacceptable risks, but some uncertainty remains regarding prohibited AI uses.



National Audit Office of Norway



“The Use of Artificial Intelligence in the Central Government” (2024)

Audit focus areas:

Service delivery- Is AI used to improve efficiency and quality of public services?

Ethics and responsibility - Are ethical principles applied in AI development and use?

Governance and coordination – Does central coordination (Ministry of Digitalization and Public Governance) promote responsible AI adoption across government?

“The Use of Artificial Intelligence in the Central Government”

Key Findings:

- AI adoption across government is uneven and limited.
- Key requirements for broader AI adoption are still lacking.
- Ethical AI practices vary between agencies; oversight is insufficient.
- Weak AI coordination across the public sector, falling short of national AI ambitions.

Key Recommendations (Ministry of Digitalization and Public Governance):

- Strengthen policy instruments for responsible AI:
 - Digital infrastructure & shared solutions
 - Access to high-quality data
 - Interdisciplinary expertise
- Provide regulatory clarity and consistent interpretation of AI-related legislation.
- Promote a common ethical framework with practical guidance for AI development and use.



UK National Audit Office



“Use of Artificial Intelligence in Government” (2024)

Aim of the Audit:

To examine how effectively the government has organized itself to maximize the opportunities of AI in providing public services, while mitigating the risks.

“Use of Artificial Intelligence in Government”

Findings:

- AI has strong potential to transform public services and boost productivity across government.
- A government-wide AI strategy and implementation plan is still pending.
- AI adoption is still early-stage – limited operational use.
- Clear ownership and accountability are essential to ensure value for money.
- Achieving impact requires business process redesign and workforce changes, not just new technology.
- Success depends on an ambitious strategy backed by:
 - Skills and capacity
 - Sustainable funding
 - Enabling conditions
- Structural (legacy, IT systems, limited data access and sharing, etc.) must be addressed.



Executive Summary

Key Insights from the Reports of European SAIs

- **Governance and coordination are the main bottlenecks**

AI strategies, responsibilities, and oversight are fragmented across the EU and within public administrations, leading to uneven adoption, weak risk management, and limited accountability.

- **Investment is increasing, but impact is lagging**

EU funding and infrastructure for AI are growing, yet delivery is slow and poorly aligned with operational needs—especially for SMEs and public-sector users—leaving Europe behind global leaders.

- **AI use is narrow and internally focused**

Public bodies mainly apply AI to internal efficiency gains, with limited citizen-facing impact. Adoption is constrained by skills shortages, legacy systems, data access issues, and compliance burdens.

- **Legal, ethical, and risk frameworks are incomplete and inconsistent**

Regulatory uncertainty, uneven ethical practices, and the absence of standardized risk assessment tools undermine trust, scalability, and responsible AI deployment.

- **Transformation requires systemic change, not just technology**

Meaningful AI impact depends on clear ownership, redesigned processes, skilled workforces, high-quality data, shared infrastructure, and sustained funding—supported by an ambitious, coordinated strategy.



Other Initiatives



“Intelligent Auditor in an Artificially Intelligent State?”

Hybrid seminar (24-25 September 2024) - “Intelligent Auditor in an Artificially Intelligent State?”.

Organized for all INTOSAI members, in the framework of the 17th Meeting of the EUROSAI IT Working Group.

Dual focus:

Auditing AI-based solutions
Levering AI within SAIs

Included SAI presentations and expert insights and addressed opportunities, risks and practical use cases of AI.

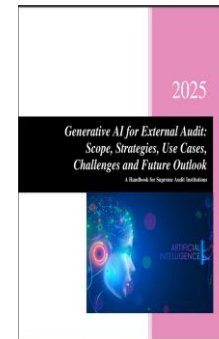
State Audit Office of the Republic of Croatia



“Generative AI for External Audit: Scope, Strategies, Use Cases, Challenges and Future Outlook” - Handbook

In 2025, the State Audit Office of the Republic of Croatia published a handbook for Supreme Audit Institutions titled: "Generative AI for External Audit: Scope, Strategies, Use Cases, Challenges and Future Outlook".

The handbook constitutes an advanced training course aimed at applying 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 summarizing complex documentation and generating tailored interview guides during fieldwork" - and in the post-audit stage.





Auditing AI Systems - Guidance for Public Sector Auditors

- A practical international guidance paper developed collaboratively by multiple SAls: Finland, Germany, Netherlands, Norway, UK and Brazil.
- Designed to support public auditors in examining AI and machine learning systems used by government entities.
- Provides an auditable framework, risks catalogue and audit methodology to assess AI systems throughout their lifecycle.

Goals

- Help SAls build capacity and consistent approaches for auditing AI systems.
- Offer a structured audit catalogue covering areas such as governance, data quality, development, deployment and evaluation.
- Include an audit helper tool to tailor audit tests to specific contexts.



Auditing AI Systems - Guidance for Public Sector Auditors

Key Features

- Focus on project management & governance, data handling, model development and production, and ongoing evaluation.
- Highlights AI-specific risks such as fairness, transparency, privacy, accountability and compliance issues.
- Accompanies methodology with recommended audit questions and controls, adaptable to different types of AI systems.

Why this matters

- Supports convergence of AI audit practices across SAs internationally.
- Helps auditors evaluate whether AI systems deliver public value, manage risk, and comply with legal and ethical requirements.



OFFICE OF THE STATE COMPTROLLER
AND OMBUDSMAN OF ISRAEL

Thank you!