PARALLEL AUDIT ON AI

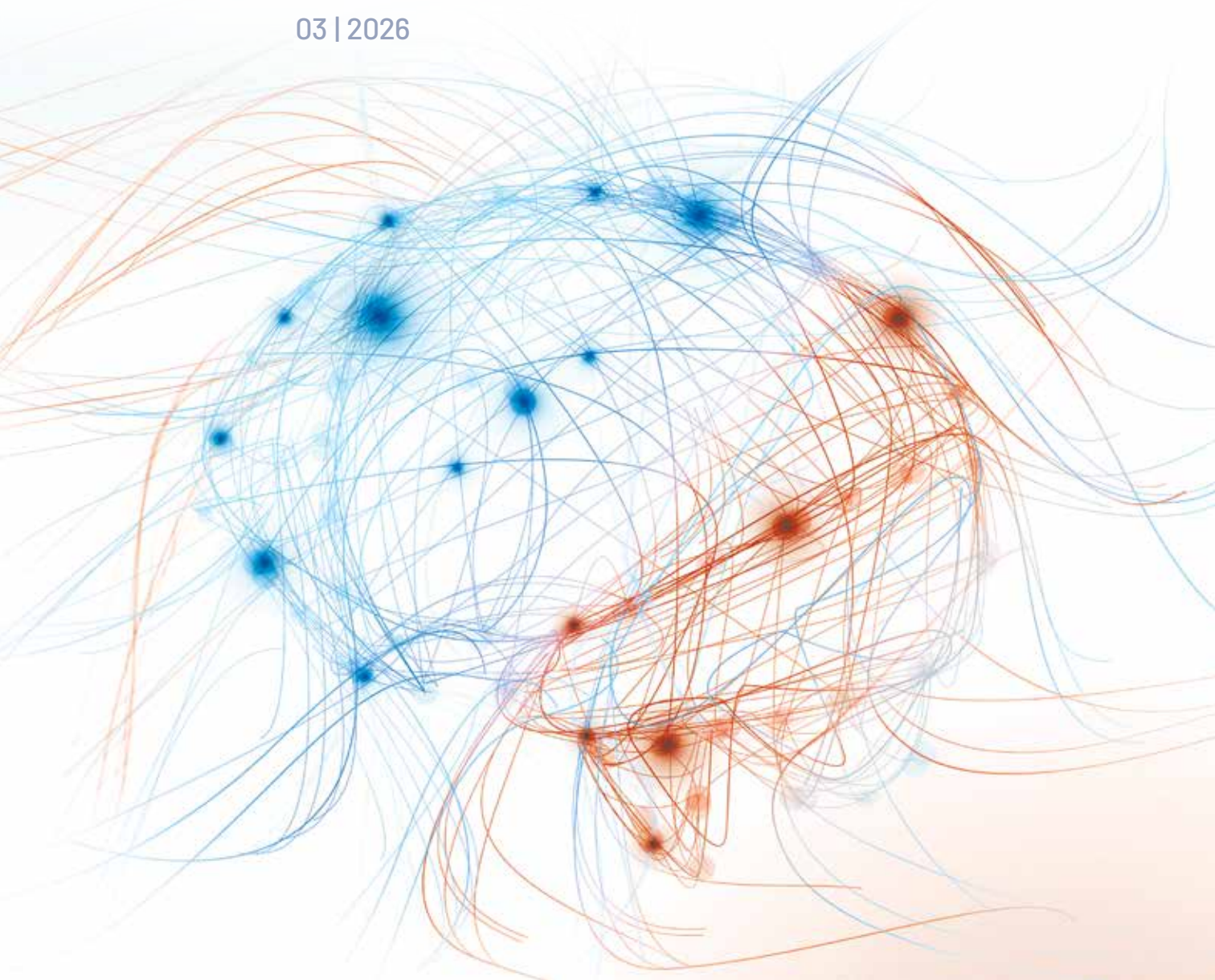
03 | 2026

EUROSAI

The State Comptroller
and Ombudsman of Israel

PARALLEL AUDIT ON AI

03 | 2026



Catalogue Number ISSN 2026-S-007
0793-1948

EUROSAI PRESIDENCY FOREWARD

Artificial Intelligence is no longer a distant prospect – it is rapidly becoming part of the everyday machinery of European governments. Public authorities across Europe are moving from pilot initiatives to full-scale implementation, embedding AI in public services, internal workflows, and decision-support systems. This momentum can deliver better outcomes for citizens and more effective public administration – but it also brings significant responsibilities concerning legality, security, privacy, transparency, and public trust.

At this pivotal moment, the EUROSAI Presidency is proud to present this Parallel Audit on Artificial Intelligence – a clear demonstration that Supreme Audit Institutions (SAIs) choose cooperation over fragmentation. Coordinated by SAI Israel, this initiative brought together twelve participating SAIs: Albania, Estonia, France, Israel, Italy, Latvia, Lithuania, North Macedonia, Poland, Romania, Slovakia, and Switzerland. Together, they examined governmental preparedness for a technology that permeates every layer of the state, from national strategic planning to concrete cross-sectoral projects. This initiative reflects EUROSAI Strategic Goal 1 in action: supporting effective, innovative, and relevant audits by promoting and strengthening professional cooperation.

As AI systems expand across audited entities, auditors will increasingly encounter these technologies "from within" – in procurement processes, data governance frameworks, cybersecurity controls, human resources management, and frontline service delivery. A key added value of this Parallel Audit lies in the shared understanding it has fostered: SAIs must be equipped to audit AI with confidence, possessing the skills, methodologies, and tools necessary to assess how such systems are designed and deployed, how risks are identified and mitigated, and how public value is created and safeguarded.

The technological landscape ahead will be faster, more automated, and increasingly language-driven. European governments will require clear strategies, robust governance frameworks, and skilled professionals to keep pace with rapid technological change. By learning together, developing common approaches, and strengthening our collective capabilities, SAIs can help guide AI adoption toward transparency, resilience, accountability, and tangible results for citizens.

On behalf of the EUROSAI Presidency, I extend my sincere appreciation to the Members of EUROSAI, colleagues, and experts who contributed to this important project. Your dedication and expertise have been instrumental in shaping a shared vision for AI adoption that is transparent, accountable, and beneficial to society. Your collective effort has further strengthened cooperation among EUROSAI members and will continue to support responsible AI governance across Europe.

Matanyahu Englman,
EUROSAI President
State Comptroller and
Ombudsman of Israel

EXECUTIVE SUMMARY

AI is no longer a "future policy" topic - it is already changing how governments work, how services are delivered, and how public trust is earned or lost. This Parallel Audit shows that many countries are moving quickly from ambition to action, but that readiness is still uneven: progress accelerates where strategy, funding, governance, data, skills, and controls move together, and it stalls where they advance separately.

Led by the Office of the State Comptroller and Ombudsman of Israel (SAI Israel) under EUROSAI Strategic Goal 1, this multinational Parallel Audit brought together 12 SAIs (Albania, Estonia, France, Israel, Italy, Latvia, Lithuania, North Macedonia, Poland, Romania, Slovakia and Switzerland). Conducted between May 2024 and December 2025, the audit used a shared analytical framework of 9 topics and more than 92 structured questions to compare national preparedness across strategic, infrastructural, and implementation dimensions.

National Strategic Plan. The audit found that countries are pursuing different paths: some have government-approved AI strategies, while others rely on broader digital strategies, standalone initiatives, or draft strategies without formal adoption. Where governance ownership and cross-ministry coordination are clear, strategies translate more effectively into action and public-facing trust measures, including strong emphasis on public awareness. The chapter concludes that strategic direction matters most when it is paired with implementation ownership and measurable goals. It recommends periodic strategy reviews to ensure the chosen model still supports an ecosystem approach, real coordination, and sustained delivery.

National AI Budgets. Funding is a decisive test of seriousness, and the audit found that many countries still struggle with visibility. Less than half reported a clearly defined AI budget, while others embed AI spending in broader digital or sectoral envelopes, making it harder to track whether resources match strategic priorities. The chapter concludes that fragmented budgeting weakens oversight and slows coherent scaling. It recommends improving transparency by distinguishing direct AI project funding from enabling investments (especially infrastructure), consolidating visibility across ministries, and coordinating external funding streams through clear ownership and multi-year planning.

Regulatory Guidelines. Regulatory readiness is developing, but not consistently. Roughly half of countries reported published AI guidelines, even though all reported a dedicated body responsible for oversight. The EU AI Act is already acting as a powerful catalyst, yet countries anticipate heavy implementation demands and capacity constraints. The chapter concludes that institutional ownership is ahead of operational guidance, and that ethics often remains a principles-level commitment without consistent, testable assurance. It recommends publishing practical guidelines, treating EU AI Act preparation as whole-of-government execution (not

only legal transposition), and strengthening enforceable mechanisms such as defined accountability, traceability, and pre-deployment checks where appropriate.

Infrastructure. Many countries are investing in AI infrastructure, especially compute capacity, but implementation is still in progress and cross-country comparability is limited by uneven measurement. National cloud environments are common, yet every country relies on third-party providers, reinforcing that hybrid delivery is the norm. The chapter concludes that infrastructure enables everything else, but it can also become a bottleneck when governance, demand forecasting, and accountability in hybrid environments are unclear. It recommends mapping capacity and forecasting demand across national and contracted resources, and strengthening hybrid governance to manage security, cost, resilience, and supplier concentration risks.

Information Security. The audit found strong awareness of AI security risks, especially data leakage and unauthorized access, but weaker baselines for enforceable practice. Mandatory cybersecurity protocols and AI-specific privacy policies were not consistently reported, and incident experience remains limited - which makes prevention and preparedness even more critical. The chapter concludes that AI security is as much a governance challenge as a technical one. It recommends establishing baseline requirements and role-based training, improving traceability and documentation, and adopting lifecycle security practices that apply consistently across ministries and suppliers.

Digital Maturity. Data foundations remain a decisive constraint on scalable AI. While all countries reported some form of data sharing policy, operational barriers persist - especially regulatory and governance friction, interoperability gaps, and uneven data readiness. External benchmarking reinforces a recurring pattern: policy and platforms can advance faster than proven impact. The chapter concludes that governments often have "rules to share data," but not always the operational conditions to share it efficiently, safely, and at scale. It recommends strengthening governance clarity, streamlining processes, improving interoperability and data quality practices, and building auditability so lawful reuse can be demonstrated, not just declared.

Government Projects. AI is already producing practical use cases across government, particularly in high-volume operational domains, and many countries report productivity improvements. Yet monitoring and evaluation mechanisms are not consistently embedded, and KPIs are often concentrated on efficiency rather than a balanced view of service quality, model performance, sustainability, reuse, and risk. The chapter concludes that implementation is advancing faster than governments' ability to prove and compare impact. It recommends establishing consistent portfolio visibility, adopting balanced evaluation frameworks, and standardizing minimum reporting so scaling decisions are evidence-based and risk remains visible.

Human Capital. Talent is the most universal constraint: every country reported a shortage of AI experts, and many also reported a shortage of researchers. Upskilling is underway in many places, but not yet universal, and retention of critical

stewardship roles remains a vulnerability that can deepen reliance on external providers. The chapter concludes that AI readiness rises or falls on people - not just technology. It recommends integrated workforce strategies that combine education pipelines, role-based training, enablement structures (centers of expertise and knowledge-sharing), and stronger recruitment and retention for key oversight and delivery roles.

Natural Language Processing (NLP). Most countries are developing local-language NLP capability, but the dominant delivery model is external or hybrid, which raises long-term dependency and lifecycle governance questions. The chapter concludes that language capability is foundational for scalable AI in government services and internal operations, but it must be sustainable and governable over time. It recommends treating NLP as a reusable shared capability, and where vendors are central, enforcing clear responsibilities for maintenance, monitoring, documentation, updates, and risk management.

Overall, the audit's message is clear: governments are building momentum, and many of the right building blocks are already in motion. The next leap forward is to connect them - turning strategies into governed delivery, turning investment into transparent portfolios, turning principles into enforceable safeguards, and turning pilots into measurable public value at scale.

KEY TERMS AND FACTS

1 | **AIGO** - AI Governance Observatory
2 | **AI** - Artificial Intelligence
3 | **CPU** - Central Processing Unit
4 | **DoS** - Denial of Service
5 | **ERDF** - European Regional Development Fund
6 | **EU** - European Union
7 | **EU AI Act** - European Union Artificial Intelligence Act
8 | **EuroHPC** - European High-Performance Computing Initiative
9 | **EUROSAI** - European Organisation of Supreme Audit Institutions
10 | **GII** - Global Innovation Index
11 | **GPAI** - Global Partnership on Artificial Intelligence
12 | **HPC** - High-Performance Computing
13 | **HR** - Human Resources
14 | **ICT** - Information and Communication Technology
15 | **IT** - Information Technology
16 | **InvestEU** - InvestEU programme
17 | **LLM** - Large Language Model
18 | **NLP** - Natural Language Processing
19 | **ODM** - Open Data Maturity
20 | **OECD** - Organisation for Economic Co-operation and Development
21 | **OECD.AI** - OECD AI policy observatory
22 | **PPP** - Public-Private Partnership
23 | **RAM** - Random Access Memory
24 | **R&D** - Research and Development
25 | **RDI** - Research, Development and Innovation
26 | **RRF** - Recovery and Resilience Facility
27 | **SAI** - Supreme Audit Institution
28 | **SG1** - Strategic Goal 1 (EUROSAI Strategic Goal 1)
29 | **SME** - Small and Medium-sized Enterprise
30 | **STEM** - Science, Technology, Engineering and Mathematics
31 | **ToR** - Terms of Reference

TABLE OF CONTENTS

INTRO

Artificial Intelligence (AI) is fundamentally reshaping the modern landscape, accelerating its activity in recent years due to digital transformation processes and the rapid increase in the scope and quality of databases across all sectors. This revolutionary technology holds immense potential for the government sector, specifically for achieving economic savings, improving public services, and enhancing the overall effectiveness of government actions.

Image contains AI generated elements

However, this rapid penetration presents significant challenges, including obstacles related to cooperation and the pooling of information, and the urgent need to adjust existing legislation and regulation to enable data sharing while abiding by laws concerning information security and privacy protection requirements.

OECD

"An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

Different AI systems vary in their levels of autonomy and adaptiveness after deployment."

According to the 2023 OECD definition

Given the transformative nature and widespread relevance of AI, the Office of the State Comptroller and Ombudsman of Israel (SAI Israel) initiated this project to conduct a Parallel Audit on AI, focusing on governmental preparedness for this technological shift. The 12 participating Supreme Audit Institutions (SAIs) included: **Albania, Estonia, France, Italy, Latvia, Lithuania, North Macedonia, Poland, Romania, Slovakia, Switzerland, and the Lead SAI, Israel,** who acted as the coordinator of the process from planning through to publication.

This cooperative endeavor is linked to the EUROSAI Strategic Goal 1: Supporting effective, innovative and relevant audits by promoting and brokering professional cooperation.

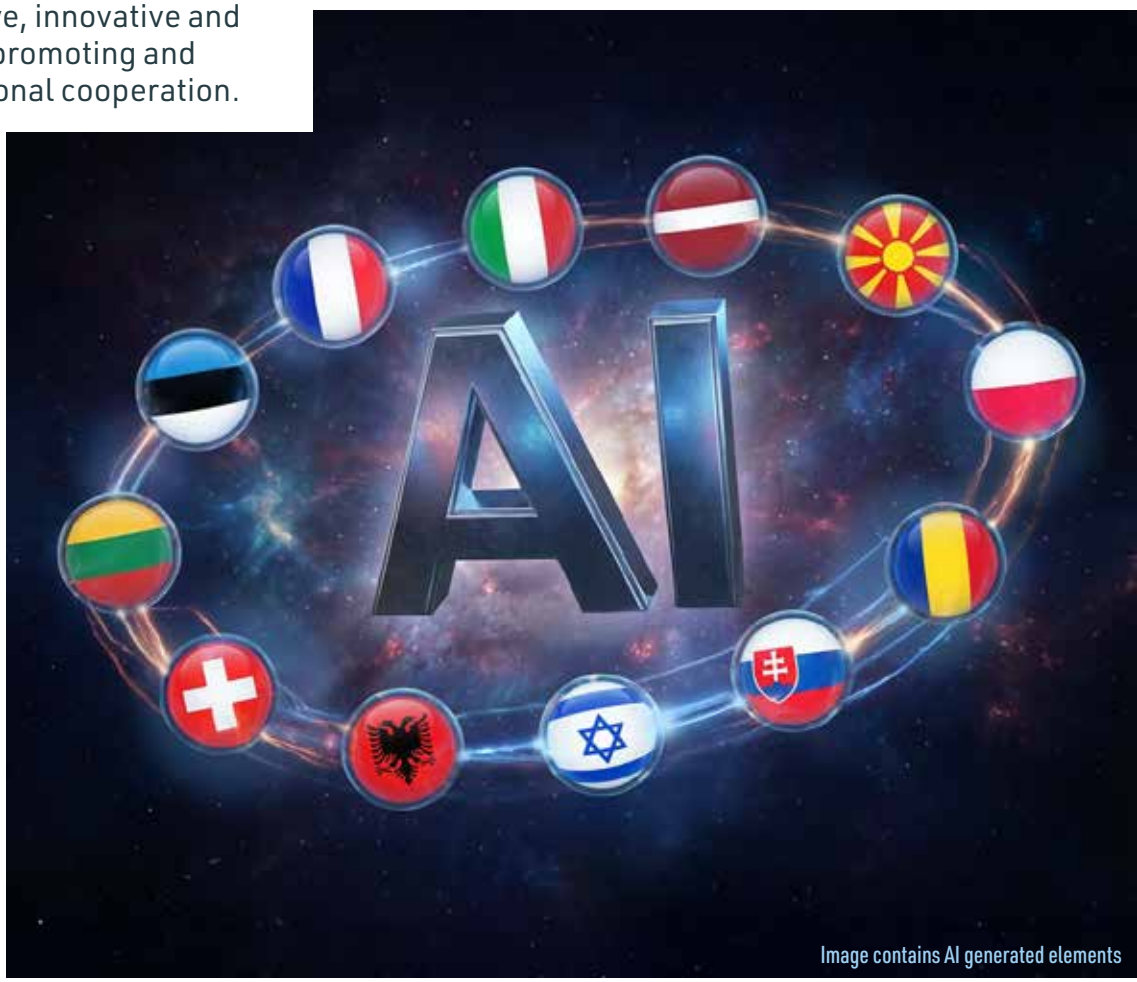


Image contains AI generated elements

COORDINATING A PARALLEL AUDIT
NAVIGATING A MULTINATIONAL AUDIT LANDSCAPE

Comparing the preparedness of multiple jurisdictions presented a substantial analytical challenge, particularly given that this audit examines a wide-spread technology that permeates every layer of government. AI influences strategic national planning at the top level, while simultaneously shaping operational implementation through concrete AI projects across diverse ministries and sectors. As a result, the audit required a cross-cutting perspective that could capture both the high-level policy environment and the practical realities of adoption on the ground.

Each participating SAI operates within a distinct administrative, legal, and institutional landscape, adding further complexity to any comparative assessment. These differences span key factors such as SAI mandates, hierarchies of audit bodies, and federal versus regional divisions of responsibility. A common pattern among several participants (e.g., **Albania, Estonia, Latvia, Lithuania, Slovakia, and Israel**) is a largely centralized public administration, where SAI mandates can cover both central government and local authorities - though in practice, parts of the parallel audit focused mainly on central-government bodies, shaping how "whole-of-government" readiness is interpreted.

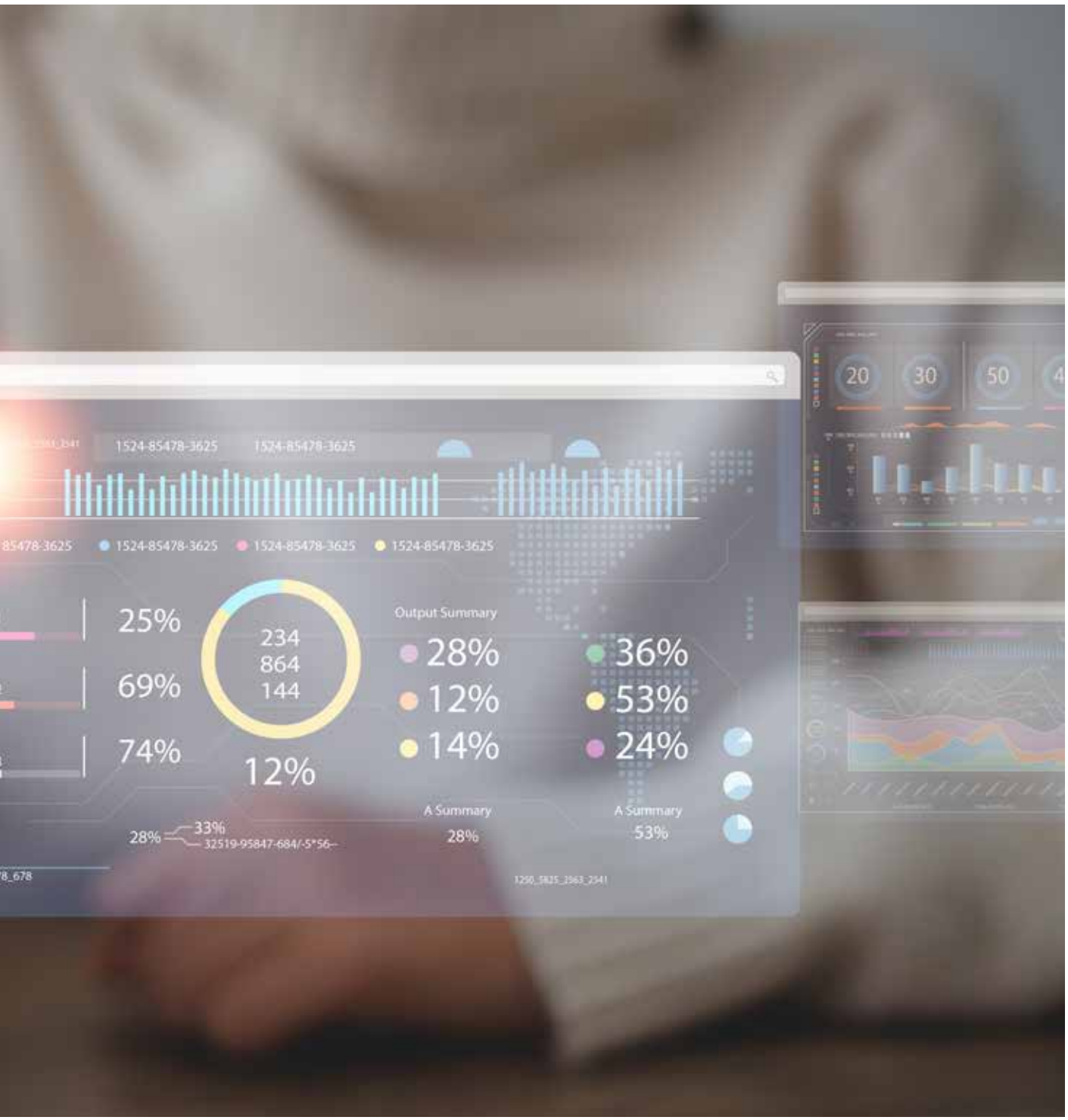
By contrast, **Italy** combines a wide mandate with a territorially distributed audit structure of regional chambers and multiple central audit functions, alongside an ongoing organizational reform. **Switzerland** raises a different consideration: in a federal context, AI strategy may be framed at the Federal Administration level rather than as a single "national" strategy, requiring comparisons to account for governance level and terminology. Coordinating such diverse contexts, timelines, definitions, and levels of digital maturity required a harmonized analytical approach. To address this, we invested in comprehensive audit-question planning.

ANALYTICAL METHODOLOGY
HOW WE BUILT A UNIFIED ANALYTICAL APPROACH

The audit topics were selected through a coordinated voting process in which each SAI voted for its priority areas using a shared online form. Once the topics were finalized, we expanded each into a structured set of yes/no, quantitative, and open-ended audit questions. This structure was chosen to support a more consistent analysis, given the differences in terminology, scope, and measurement used by each SAI. For the open-ended responses, answers were grouped under unified analytical terms to enable coherent and comparable interpretation across all participating institutions.

The audit addressed a detailed framework comprising **9 core topics** - Strategical (National Strategic Plan, Government Budgets, Regulatory Guidelines), Infrastructural (Infrastructure, Digital Maturity, Information Security), and Implementational (Government Projects, Human Capital, NLP). These domains were analyzed through **over 92 specific audit questions**[1], though not all participants were able to obtain responses to every question.

1 Appendix A.


20
30
50
1524-85478-3625
1524-85478-3625
1524-85478-3625
1524-85478-3625
1524-85478-3625
25%
69%
74%
234
864
144
12%
Output Summary
28%
12%
14%
36%
53%
24%
A Summary
28%
A Summary
53%
28%
33%
32519-95847-684/-5*56

AUDIT TIMELINE

The Parallel Audit on AI was carried out between May 2024 and December 2025 and covered the full audit cycle, including planning, fieldwork, data collection, analysis, and preparation of this consolidated report. Throughout the process, we held ten meetings that provided ongoing updates on the audit's progress as well as professional lectures on key AI topics.

2024

MAR

SG1 Meeting
Initiative & ToR
Presentation

MAY

1st Meeting

Brainstorming
audit topics

Starting the voting
process on audit
topics

JUN

Expanding 9
selected audit
topics into
92 audit questions

JUL

2nd Meeting

Kickoff
audit work

STKI
(business
technologies
market research
and strategic
analyst firm)
AI Powered World
Presentationon
audit topics

2025-2026

JAN

7th Meeting

Oxford insights
governmental
AI readiness
index presentation

JAN

Database
normalization
and analysis

FEB

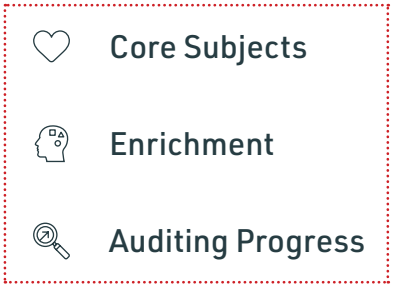
8th Meeting

Dr. Roey Tzezana
futurist and
researcher in
futures studies
(TAU)
discussing AI's
influence on
governments,
corporations,
and society

MAR

9th Meeting

Prof. Sefidanis
Associate
Professor, former
Vice-Rector
for Science and
founder and CEO
of "SEFIDANIS"
R&D center
exploring AI
adoption in North
Macedonia



SEP

3rd Meeting

Expanded topics Roundtables

Introduction to AI tools for auditors

OCT

4th Meeting

Small-group Roundtables

Additional AI tools for auditors

NOV

5thMeeting

Presentations on national AI Strategies & Regulation

DEC

First Findings Uploaded

DEC

6th Meeting

Sharing Initial Findings

Ms. Carolin Prabhu (SAI Norway) Performance audit on the use of AI in the Norwegian central government

Mr. Marco Schreyer (SAI Switzerland) AI Agentic Auditing research

OCT

Last Submissions Received

NOV

10th Meeting

Discussing First Draft: intro, first topic, overall Structure and findings representation

NOV

Finalizing Audit Chapters

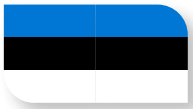
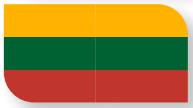
JAN

Circulation of the full draft report to the participating SAIs for comments

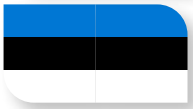
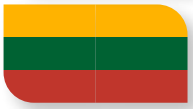
MAR

Publication of the full report

FINDINGS SUBMISSIONS TIMELINE

SAI	Date
	March 2025
	May 2025
	
	June 2025
	
	
	September 2025
	
	October 2025
	
	

INDIVIDUAL AUDIT REPORTS PUBLISHING DATES[2]

SAI	Date
	April 2023 November 2025
	November 2024
	May 2025
	June 2025
	July 2025
	July 2025
	To be published by the last quarter of 2026
	Publication not confirmed
	Publication not confirmed
	Publication not confirmed
	Publication not confirmed
	Publication not confirmed

2 Appendix B.

THE NATIONAL STRATEGIC PLAN

In today's rapidly evolving digital landscape, a national strategic plan for AI is a key foundation for effective, responsible, and future-ready AI adoption. While some countries have adopted formal, government-approved strategies, others rely on separate initiatives or emerging frameworks - each reflecting a different approach to coordination, priority-setting, and ecosystem development.

This chapter examines whether such strategies exist, their scope and structure, and the extent to which they align with international best practices such as the OECD's AI principles. It explores whether governments have defined clear goals, governance structures, timelines, and mechanisms to overcome barriers, and whether strategic plans reflect a broader vision or a siloed, sector-specific focus. International benchmarks are also reviewed to understand how countries measure progress and whether improving their global standing is a stated objective.

Image contains AI generated elements

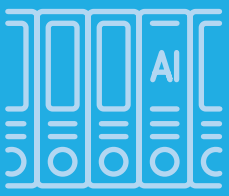
AI PLANNING LANDSCAPE

A key starting point for assessing national readiness in AI is determining whether a country has formally committed to a strategic direction. This includes not only the existence of a government-approved AI plan but also the presence of alternative policies or initiatives guiding AI development in its absence. The structure and scope of these frameworks - whether broad ecosystem strategies or targeted sectoral efforts - offer insight into each country's engagement, coordination, and long-term vision for AI.

Countries have adopted several strategic models to guide the development and adoption of AI, each with its own level of comprehensiveness, coordination, and institutional backing[3].

Dedicated AI Strategies

This is the most structured approach, involving a formal, government-approved document that defines the long-term vision and goals for AI at the national or federal level. These strategies typically include specific implementation mechanisms, governance structures, dedicated budgets, and clear performance indicators. They reflect a high degree of political commitment and often address cross-sectoral applications, regulatory frameworks, talent development, and international cooperation.



Broader Digital Strategies with AI Components

In some countries, AI is integrated into a wider digital transformation strategy. These strategies usually emphasize general modernization goals, such as broadband expansion, e-government, data economy, and digital inclusion, with AI positioned as one of many technologies contributing to that transformation. While this approach supports broad policy coherence, it may lack focused attention on AI-specific challenges and opportunities.

3 It is also important to note that in countries with federal or multi-layered administrative structures, strategic plans may apply primarily to the federal government and not automatically extend to regional or state authorities, which can influence the scope and interpretation of the national strategy.

Standalone AI Initiatives

A third model involves implementing individual AI initiatives or programs without a cohesive national strategy. These efforts are often guided by government resolutions, which define specific objectives or assign responsibilities to certain ministries or agencies. While this approach allows for agility and targeted progress in priority areas, it often lacks overarching coordination, long-term vision, and strategic integration across sectors. As a result, implementation may be fragmented, and alignment with broader national goals or international frameworks can be limited.

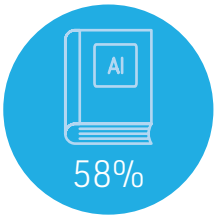
Drafted but Unapproved Strategies

Finally, there are cases in which countries have prepared comprehensive AI strategies, but these were not formally adopted at the government level.

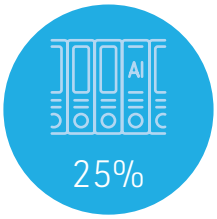
Without official approval, such strategies may remain aspirational, lacking the authority and resources needed to influence policy, budget planning, or national coordination efforts.

Among the 12 participating countries, six - Estonia, France, Italy, Poland,Romania and Switzerland[4] - have approved **dedicated AI strategies,** while Albania is drafting one. Latvia, North Macedonia and Slovakia have integrated AI goals into **broader digital strategies,** and Israel is advancing through a **standalone initiative.** Lithuania reported drafting a strategy in 2019 that was not officially approved by the government and did not become a planning document.

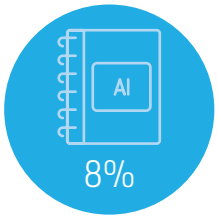
These differences reflect varied levels of political commitment, strategic clarity, and institutional coordination.



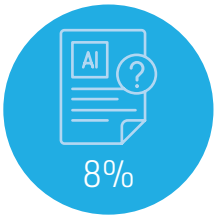
Dedicated AI Strategies



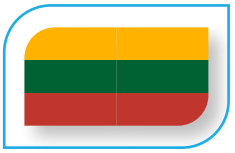
Broader Digital Strategies



Standalone AI Initiative



Drafted but Unapproved Strategies



Each model carries strengths and trade-offs.

Dedicated strategies provide focus, consistency, and international visibility, but require long-term governance and investment.

Broader digital strategies encourage integration but may overlook AI-specific needs.

Standalone initiatives allow flexibility and quick implementation but often lack scale and coordination.

Most countries appear to be balancing long-term planning with the need for adaptable implementation models.

4 The AI strategy was developed by the Federal Administration. Details can be found in the appendix B on page 151.

Another finding relates to public engagement. 91% of participating countries reported having specific goals to increase public awareness and understanding of AI, reflecting growing recognition that public trust and informed participation are essential for successful AI adoption.

Several countries already point to concrete, public-facing actions: **France** is funding public campaigns alongside AI-focused education pathways; **Italy** is planning broad media outreach (TV and radio segments, newspaper and magazine columns), public service ads on AI risks and opportunities, and dedicated websites and social media content; **Lithuania** links engagement to public debate on AI and the ethics of its use; **Romania** is promoting citizens' right to information when interacting with AI, including through a public "Catalog of AI applications used in public administration"; **Slovakia** reported a national popularization campaign; and **Switzerland** emphasized structured dialogue with the population.

Awareness efforts - through education, transparency, and dialogue - support responsible use and help prepare society for AI-related change.

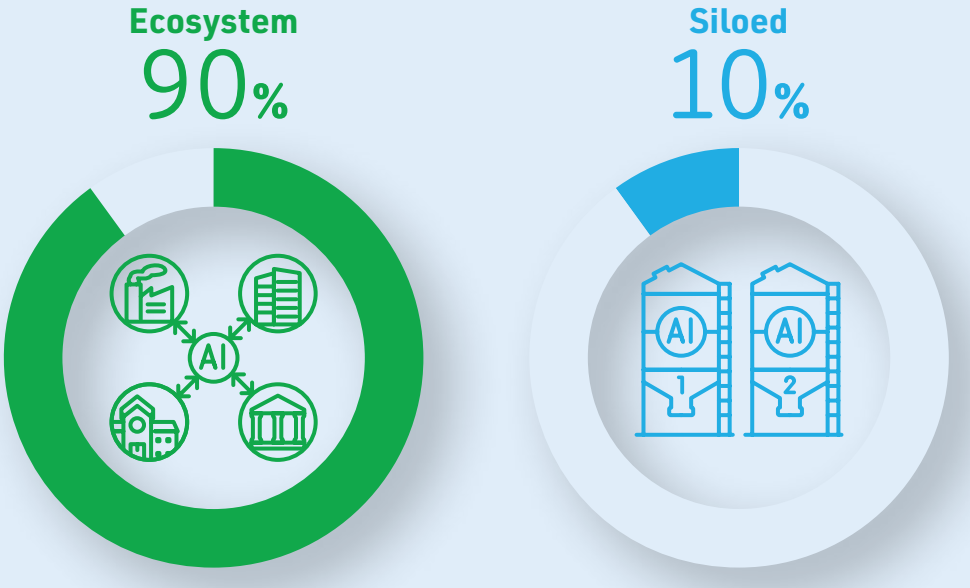
91%

of participating countries reported having specific goals to increase public awareness and understanding of AI.

According to 12 Responses

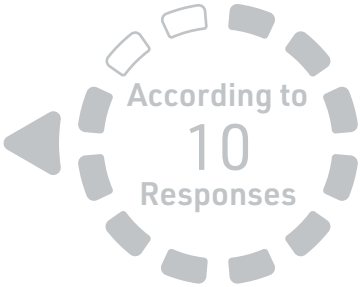
Image is AI generated

The audit also examined whether countries are pursuing an **ecosystem** or **siloed** approach to AI implementation. An ecosystem approach fosters collaboration between government, academia, industry, and civil society, aiming for systemic coordination across sectors. A siloed approach, by contrast, focuses on isolated projects with limited integration, which may constrain long-term impact.



Around 90% of countries prioritize an **AI ecosystem model,** promoting cross-sector coordination and shared infrastructure.

These states view AI as a national effort requiring broad engagement. In contrast, one country, operating a standalone initiative, follows a more siloed path, focusing on targeted government-led projects.



Recommendation

As countries continue to refine their approaches, it may be useful for them to periodically review whether their chosen model - dedicated strategy, integrated digital plan, or initiative-based approach - continues to support effective coordination, meaningful public engagement, and an ecosystem perspective that can sustain AI development over time.

GOVERNANCE STRUCTURE

An essential component of any national AI strategy is a clear governance structure that defines who is responsible for leading and coordinating implementation. Without defined ownership and oversight, strategic plans risk fragmentation, delays, or inconsistent execution. Assigning responsibility to specific governmental entities helps ensure accountability, policy coherence, and alignment across sectors. This subchapter examines the institutional arrangements adopted by countries to manage AI implementation and the range of ministries and agencies involved.

The audit found that 90% of responding countries have explicitly assigned overall responsibility for implementing the national AI strategy in the public sector **to a specific governmental authority.** In eight of these cases, the lead role was given to a designated body - most often a digital government authority (four cases), followed by regional development authorities (two cases), an economy authority (one case), and, in one case, a dedicated national AI coordinator. In three countries, overall implementation is coordinated primarily through an **inter-ministerial committee** (two governmental and one external).

Designated Authorities to Oversee AI Strategy Implementation:

Digital

Regional Development

Economy

National AI Coordinator

Inter-Ministerial Committees

Implementation is not limited to a single lead body. Countries involve a wide range of authorities, depending on their strategic priorities.

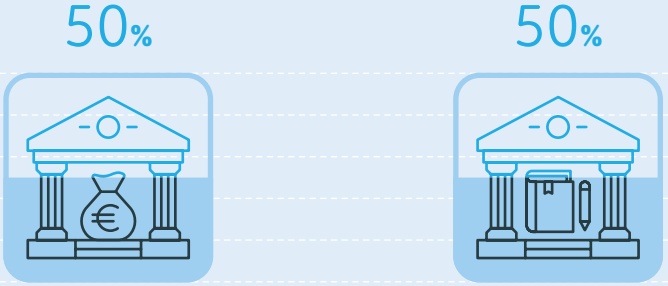
The most commonly involved authorities are those responsible for economic development and education, each cited by 6 countries. Ministries of defense and innovation were mentioned by 5 countries (42%). Other actors include ministries of technology (3 countries, 25%), as well as health, justice, statistics, labor, finance and general government bodies, each cited by 2 countries (17%).

Ministries of communications, foreign affairs, interior, and digital transformation were each mentioned by one country (8%).

In 2 cases (17%), countries reported that each ministry is responsible for its own AI implementation, highlighting a more decentralized model.

This diversity reflects the cross-cutting nature of AI and the need for coordinated, multi-sector governance structures.

Most Commonly Involved Entities in Strategy Implementation:



Ministry of Economic Development

Ministry of Education

42%

Ministry of Defense

42%

Ministry of Innovation

25%

Ministry of Technology

These findings suggest that most countries have taken steps to institutionalize responsibility for AI at the national level.

Digital government or IT ministries and ministries of economy often lead due to their roles in digital infrastructure and innovation policy, while education ministries are involved in talent development.

The inclusion of sectors like defense, justice, and labor shows that AI is being addressed not only as a technological issue but also in terms of security, ethics, workforce transformation, and public service delivery.

The variation in structures - between centralized ministries, national coordinators, and inter-ministerial bodies - reflects differing administrative cultures and levels of strategic centralization.

However, the shared practice of involving multiple ministries signals an understanding that **effective AI governance requires cross-government collaboration**.

Countries that establish both a clear lead entity and strong inter-agency coordination mechanisms are likely to be better equipped to manage complex implementation challenges and align AI development with national priorities.

Image is AI generated

Recommendation

Going forward, periodically reviewing mandates and coordination arrangements may help ensure that governance structures remain fit for purpose as AI policies and use cases evolve.

Image is AI generated

CONTENT OF PLANS

Beyond the existence of a national AI strategy, its content plays a critical role in determining its effectiveness. A well-designed plan must go beyond high-level aspirations and provide a clear roadmap for action, including priorities, implementation structures, and areas of focus.

The strength of the strategy lies not only in its ambition but in the concrete elements that support execution - governance, funding, infrastructure, and collaboration.

Understanding the substantive content of national plans provides insight into how governments translate AI visions into operational commitments.

Top Elements of the Strategic Plan that are Most Crucial for Its Successful Execution

As part of the audit work, participating SAIs identified the elements (one or more) they consider most critical for the successful execution of national AI strategies.

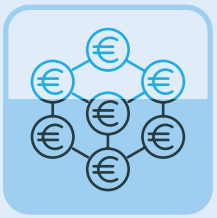
The most frequently cited was **governance and strategic management,** including leadership, coordination, implementation, and evaluation, reported by eight countries (89%). **Financial frameworks,** including budgeting and sustainable funding, and **infrastructure and data capabilities** were each highlighted by five countries (55%). **Human capital development** was noted as a critical requirement by four countries (44%), while two countries (22%) emphasized building a **strong public–private ecosystem,** including **ethical and legal frameworks** and collaboration with external stakeholders.

These responses represent what the auditing institutions themselves view as the core building blocks needed to ensure strategies translate into operational results.

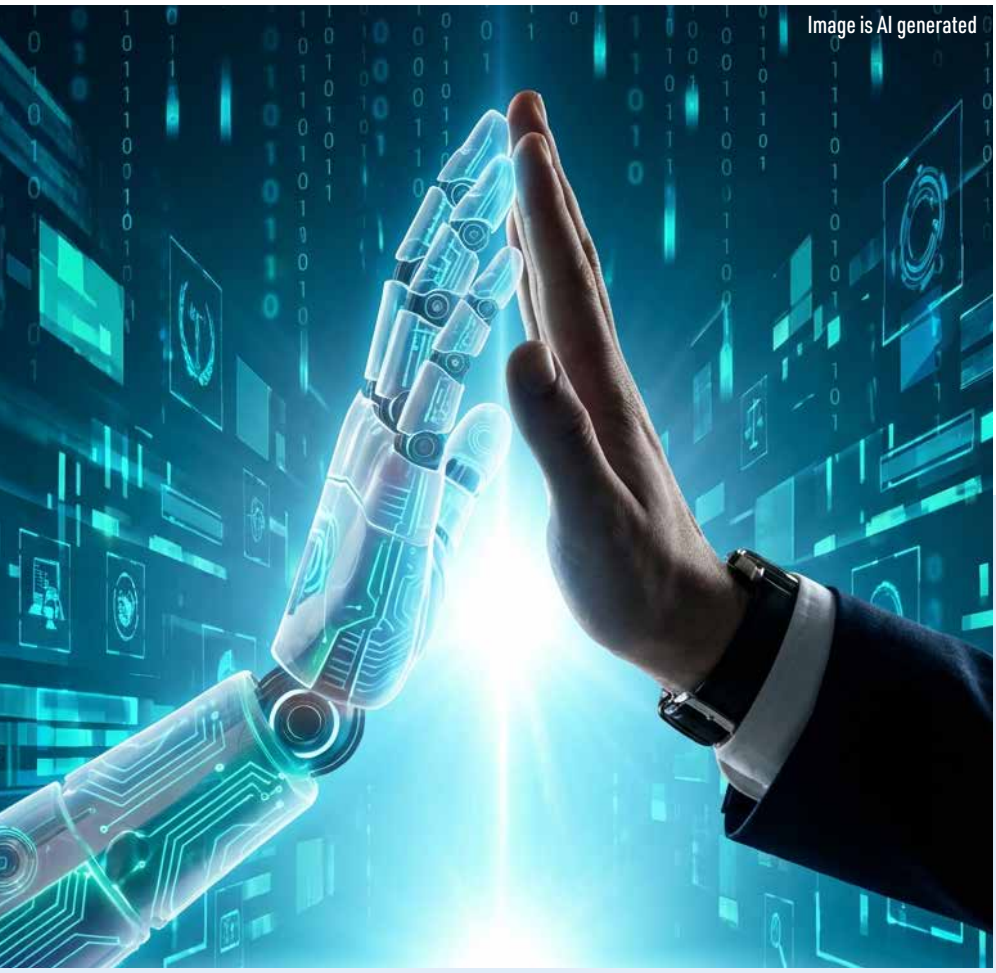
89%

Governance and Strategic Management

55%



Financial Frameworks



According to 10 Responses

55%

Infrastructure and Data Capabilities

44%

Human Capital Development

22%

Building a Strong Public-Private Ecosystem

22%

Collaboration with External Stakeholders

In contrast to these critical elements, the audit also examined the actual focus areas that appear within the national strategies and plans.

The most common focus areas were **human capital and education** and **AI adoption and sectoral deployment,** each reported by nine countries (82%). These include public-sector and private-sector adoption, workforce preparation, training programs, and public awareness.

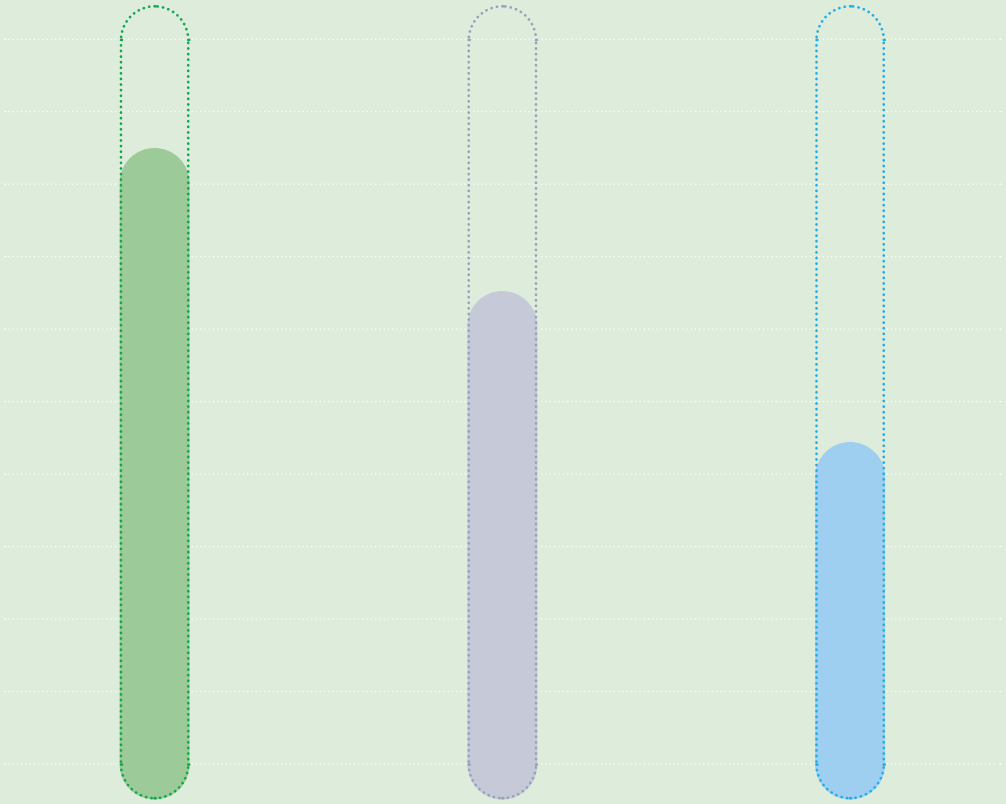
Governance, regulation, and trust, as well as research and innovation, were each referenced by seven countries (64%), reflecting an emphasis on responsible AI and the strengthening of research ecosystems. Infrastructure and core technologies, including data, computing capabilities, and NLP, were explicitly included in five strategies (45%).

These focus areas represent the substantive pillars shaping the content of national plans.

According to 11 Responses

Image is AI generated

Top Actual Focus Areas That Appear Within the National Strategies and Plans



82%

- Human Capital
- Education
- AI Adoption
- Sectoral Deployment

64%

- Governance, Regulation and Trust
- Research
- Innovation

45%

- Infrastructure
- Core Technologies

While countries differ in their strategic priorities, the audit findings highlight a shared understanding of what underpins effective AI strategy execution.

The strong emphasis on governance and strategic management reflects recognition that leadership, coordination, and monitoring are essential to ensure that strategic plans move beyond paper and translate into measurable outcomes. Similarly, identifying financial frameworks as a critical element underscores the need for long-term investment.

The repeated reference to infrastructure, data, and human capital indicates that countries view these enablers as structural foundations for success. The inclusion of a public–private ecosystem reflects awareness of the need to integrate legal, ethical, and collaborative components early in implementation.

A comparison of the critical elements identified by SAIs with the focus areas embedded in the strategies shows a high degree of alignment.

Human capital, for example, appears both as a core requirement for execution and as a central focus area, reinforcing its pivotal role in national AI readiness. Likewise, the recognition of infrastructure and data as essential enablers corresponds with the inclusion of core technologies and ICT in many plans. Governance and trust frameworks appear consistently across both categories, demonstrating an understanding that coordinated oversight and ethical safeguards are vital to responsible AI deployment.

This alignment suggests that countries with a clear understanding of what drives successful implementation are embedding those drivers directly into their strategic focus areas - a sign of increasing coherence and maturity in national AI planning.

Recommendation

As countries update or revise their AI strategies, it may be useful for them to ensure that these critical execution elements remain explicitly reflected in the content of their plans, and that focus areas continue to balance enabling conditions with concrete, applied outcomes.

STRATEGIC GOALS

A well-formulated AI strategy not only defines broad ambitions but also sets **measurable goals and timelines** to track progress and guide implementation.

The inclusion of concrete indicators enables governments to assess what has been achieved, identify challenges, and adjust priorities over time.

Structuring plans across defined phases, supported by relevant metrics, strengthens strategic accountability and increases the likelihood of real-world impact. This subchapter examines how national strategies are framed in terms of **timeframe, key objectives,** and **quantifiable outcomes.**

According to 11 Responses

Among eleven countries with strategies or initiatives, (Estonia, France, Israel, Italy, Slovakia, North Macedonia and Poland) have adopted **multi-phase plans** (64%), typically structured around three-year cycles, allowing for evaluation and adjustment between phases.

The remaining four (36%) - Albania, Latvia, Romania and Switzerland - follow a **single-phase structure**, though Romania and Switzerland launched their plans only recently, in 2023 or 2024, and are still in the implementation stage of the current plan.

These varying approaches reflect different levels of strategic maturity and planning depth.

64% adopted a multi-phase plan

36% follow a single-phase structure

Across the participating states, **five recurring focus areas** emerged in relation to strategic goals and performance indicators. The most prominent is **human capital and skills development,** cited by nine countries (82%), with goals such as expanding AI-related education, aligning training with labor market needs, and growing the AI workforce. Indicators include numbers of AI graduates, participants in training programs, and national talent targets.

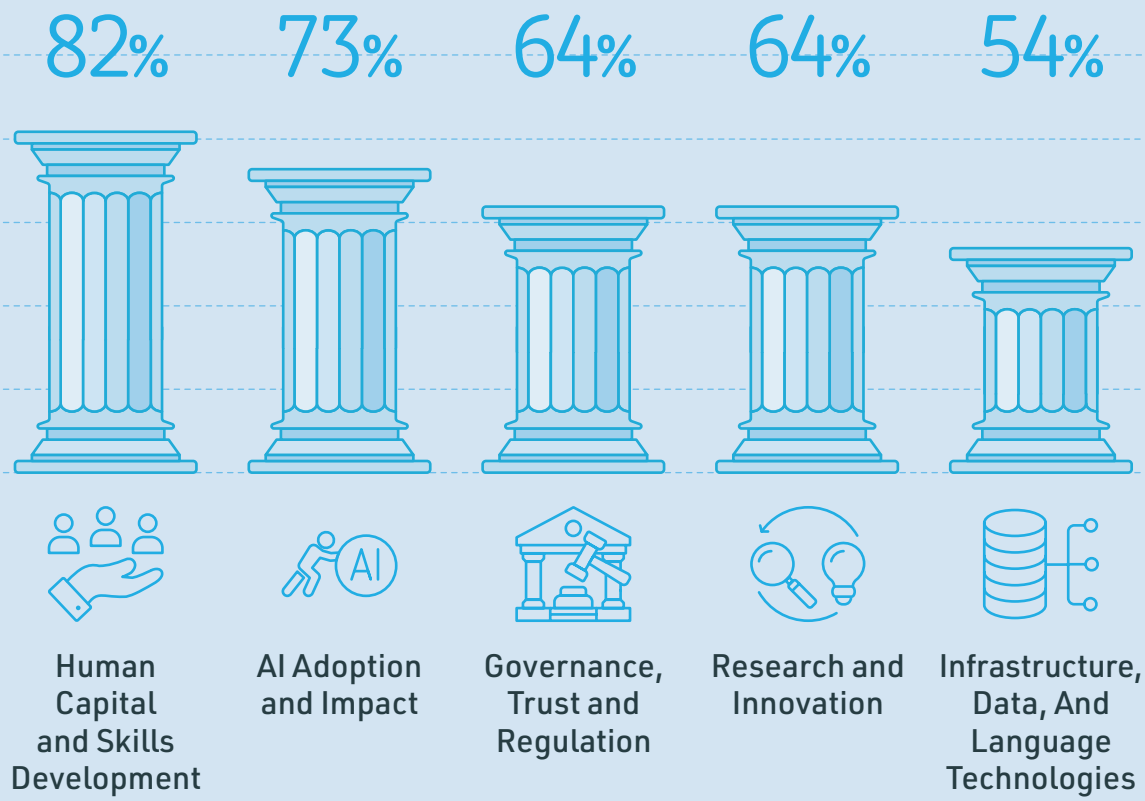
The second major focus is **AI adoption and impact,** mentioned by eight countries (73%). Goals include increasing the use of AI in public services and businesses, improving efficiency, and boosting productivity. Common indicators involve reductions in manual work, adoption rates in SMEs, and the number of AI-enabled government services.

Governance, trust, and regulation were cited by seven countries (64%), reflecting efforts to ensure safe and ethical AI use through legal frameworks, oversight bodies, and participation in international governance structures. **Research and innovation** goals, also mentioned by seven countries (64%), include expanding applied and fundamental AI research, supporting excellence centers, and increasing collaboration. Six countries (54%) emphasized **infrastructure, data, and language technologies,** such as investments in computing power, open data maturity, and the development of local NLP or foundational models.

The findings indicate a broad consensus on the strategic priorities for national AI development. Most countries emphasize **talent development, responsible AI governance, sectoral adoption,** and **research excellence** as pillars for success.

The presence of specific indicators, often with numeric targets, demonstrates a shift from high-level vision to results-oriented planning. Countries that include clearly defined metrics and multi-year structures are better positioned to monitor progress, allocate resources effectively, and adjust policies as needed.

Pillars for Success Emphasized by the Countries



The alignment between focus areas and associated indicators also signals an increasing sophistication in how countries approach AI strategy. For example, goals in education are tied to measurable outcomes such as graduation rates and training volumes. Infrastructure objectives are tracked through open data scores or foundational model milestones. This integrated approach reflects a recognition that **strategic vision must be supported by operational clarity,** and that measurement is key to translating policy into practice.

Recommendation

As strategies evolve, countries may benefit from periodically reviewing whether their indicators remain aligned with emerging priorities and whether data systems are robust enough to support meaningful monitoring and evaluation.

OECD ALIGNMENT

The OECD's AI Principles are among the most widely recognized international standards for the responsible development and use of AI. They provide a values-based framework that promotes innovation while ensuring safety, transparency, accountability, and respect for human rights.

For countries developing national AI strategies, alignment with these principles serves not only as a benchmark of ethical and trustworthy AI governance, but also as a means to support international cooperation, policy consistency, and public trust. The audit examined whether countries refer to these principles in their national strategies and how they engage with broader OECD best practices. **80% of member states reported that their plans refer to all five of the OECD's AI values-based principles** [5].

Values-Based Principles

- Inclusive growth, sustainable development and well-being
- Human rights and democratic values, including fairness and privacy
- Transparency and explainability
- Robustness, security and safety
- Accountability

Recommendations for Policymakers

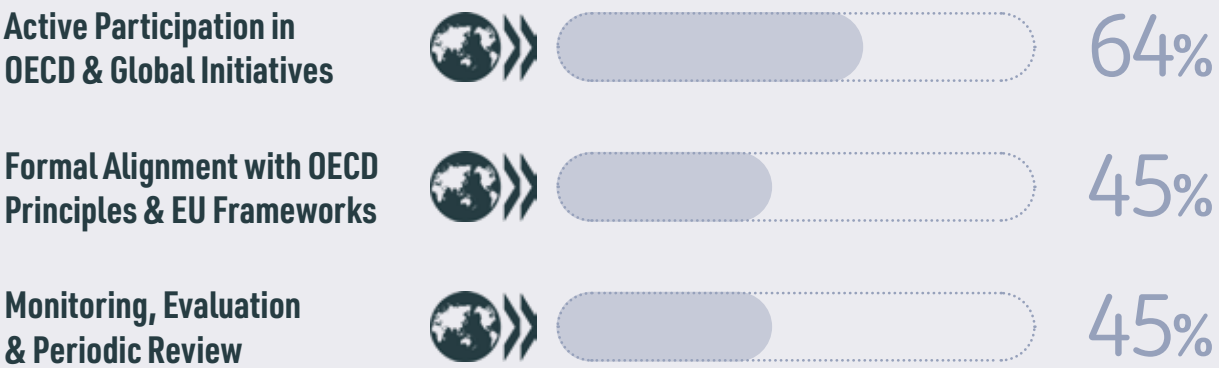
- Investing in AI research and development
- Fostering an inclusive AI-enabling ecosystem
- Shaping and enabling interoperable governance and policy environment for AI
- Building human capacity and preparing for labour market transformation
- International co-operation for trustworthy AI

5 https://oecd.ai/en/ai-principles

Beyond formal references, many countries demonstrate active engagement with OECD-related processes. 64% of member states participate in **international forums and working groups,** including OECD.AI[6], AIGO[7], and GPAI[8]. 45% reported explicit policy alignment with the OECD principles or the EU's AI framework, as well as conducting monitoring and evaluation activities such as periodic reviews and the designation of oversight bodies. A further 27% noted multi-stakeholder collaboration, involving domestic working groups and partnerships with academia, civil society, and industry.

According to 11 Responses

Ways to Ensure Alignment with OECD Best Practices



6 OECD.AI is an online interactive platform dedicated to promoting trustworthy, human-centric artificial intelligence (AI) launched by the OECD in 2020.

7 OECD Working Party on Artificial Intelligence Governance.

8 International initiative currently consisting of 44 member countries that promotes the responsible development and use of artificial intelligence (AI).

These findings indicate a strong collective effort to **anchor national AI efforts in globally recognized frameworks.** The widespread reference to OECD principles suggests that ethical and responsible AI is not viewed as optional, but as a core element of strategic planning.

Moreover, the combination of formal alignment, international participation, and structured evaluation reflects a growing institutional capacity to engage in **ongoing governance,** not just one-time compliance. Countries that actively review progress, involve diverse stakeholders, and adapt their policies through international collaboration appear better positioned to ensure that AI development remains accountable, inclusive, and aligned with democratic values.

The audit also suggests that **OECD engagement contributes to policy maturity and legitimacy.**

States that align their strategies with OECD and EU frameworks often use them as a foundation for internal governance models, monitoring systems, and cross-border cooperation.

Participation in OECD and global forums enables countries to **learn from best practices,** benchmark their progress, and refine their regulatory approaches. While the degree of alignment and participation varies, most member states view OECD frameworks not only as guiding principles but as **practical tools** for building trusted and resilient AI systems.


Image is AI generated

Recommendation

Looking ahead, countries may wish to periodically revisit their strategies and governance arrangements in light of evolving OECD guidance, ensuring that alignment remains substantive and that lessons from international cooperation are effectively integrated into national practice.

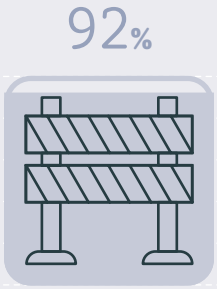
BARRIERS TO ADOPTION

Despite growing commitment to AI strategy, many governments face significant **practical challenges** in turning plans into action. These barriers often stem from limitations in **capacity, resources, and coordination,** which can slow or complicate implementation efforts. Identifying these challenges is key to understanding where targeted interventions are needed and how strategies can be adjusted to close gaps. This subchapter presents the most common barriers reported by member states and the areas they are prioritizing to address them.

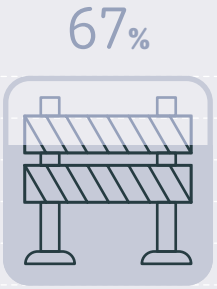
Image is AI generated

Main Barriers in Promoting AI in Public Sector

92% of countries cited the barrier of shortage of human capital and digital skills. 67% reported insufficient infrastructure and technological capacity, as well as financial and budgetary constraints. 50% pointed to governance and coordination issues, legal and regulatory gaps, and lack of trust, awareness, and cultural resistance. Data availability and sharing limitations were also noted by 33%.



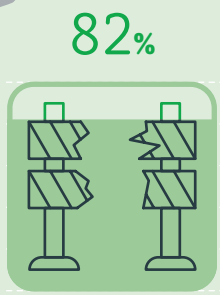
Human Capital and Skills Shortage



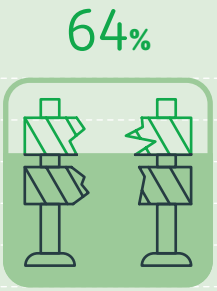
Infrastructure and Technological Capacity

Ways to Overcome Those Barriers

To address these challenges, most countries (82%) identified strengthening governance and strategic coordination as a priority. 64% see the promotion of research, development, and innovation (RDI), improvements in data governance and digital infrastructure, and investment in human capital development as key focus areas. 55% reported efforts to expand funding mechanisms and enhance legal and regulatory frameworks. Other targeted measures include promoting public awareness and an innovation culture (45%), in one case (9%) developing language technologies.



Governance and Strategic Coordination



Research, Development, and Innovation (RDI) Promotion

67%

Financial and Budgetary Constraints

50%

Governance and Coordination Challenges

50%

Legal and Regulatory Gaps

50%

Trust, Awareness, And Cultural Resistance

64%

Data Governance and Infrastructure Improvement

64%

Human Capital Development and Skills Enhancement

55%

Financial Investment and Funding Mechanisms

55%

Regulatory and Legal Framework Development

These findings confirm that while national strategies are in place, implementation depends heavily on overcoming structural and capacity-related barriers. The widespread skills shortage indicates a pressing need for education and workforce transformation, particularly in the public sector.

Financial constraints highlight the importance of long-term investment planning, while gaps in infrastructure and data systems limit the ability to deploy AI at scale. Governance and regulatory weaknesses further complicate inter-ministerial coordination and trust in AI systems.

Importantly, the areas prioritized to address these barriers reflect a proactive and balanced approach. Countries are not only investing in technical enablers such as infrastructure and RDI but are also recognizing the importance of organizational readiness, legal clarity, and cultural change.

The combination of internal capacity-building and broader ecosystem development suggests that member states are moving beyond strategy formulation toward building the institutional foundations necessary for sustained AI adoption.

Image is AI generated

Recommendation

Going forward, countries may benefit from continuing to align their capacity-building, funding, and regulatory efforts with the specific barriers they have identified, ensuring that limited resources are directed toward the constraints that most significantly hinder effective implementation.

INTERNATIONAL BENCHMARKING

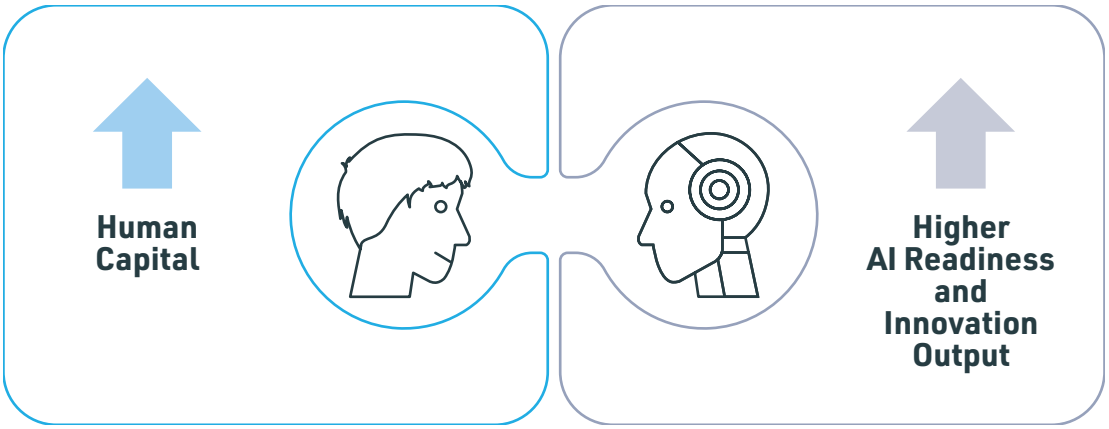
Global benchmarking plays a critical role in helping governments understand how their AI readiness compares internationally. Comparative indexes provide insights into strengths and weaknesses across key pillars such as talent, infrastructure, governance, and innovation.

For audit purposes, they offer a valuable external lens to validate national progress and guide future priorities. This subchapter summarizes cross-index findings and outlines strategic takeaways based on comparative data from sources like the **Oxford AI Readiness Index, Tortoise Global AI Index,** and the **Global Innovation Index (GII).**[9]

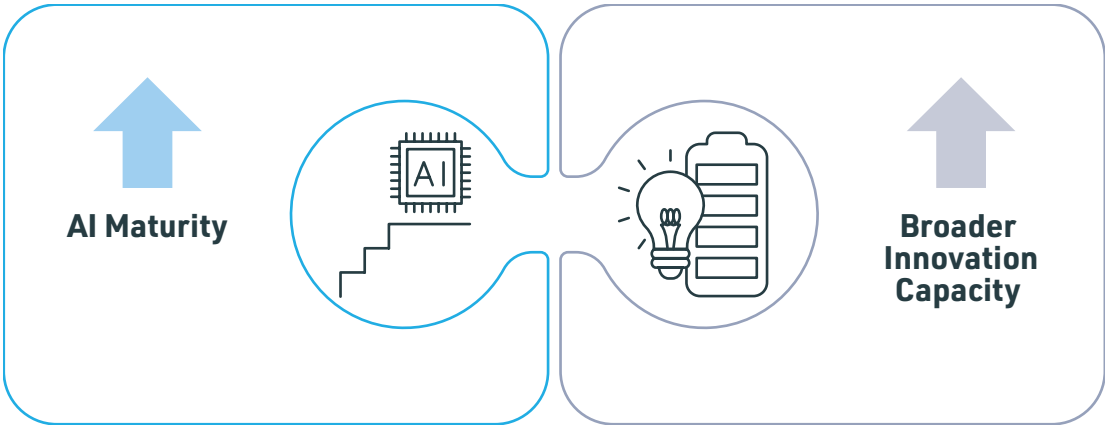
9 Appendix C.

The analysis found[10] strong alignment across indexes, especially in how **human capital** consistently correlates with **higher AI readiness and innovation output.** Countries such as **Switzerland, France, and Israel** ranked well across multiple indexes, indicating a coherent innovation ecosystem. The findings emphasize that **business sophistication** plays a bridging role between education and commercialization, and that **AI maturity often mirrors broader innovation capacity.** Cross-index validation also indicates that high-performing countries tend to combine strength in **talent, infrastructure, governance,** and **market dynamics.** However, countries investing heavily in infrastructure without parallel development in **business or research** saw limited AI impact.

Human Capital Consistently Correlates with Higher AI Readiness and Innovation Output



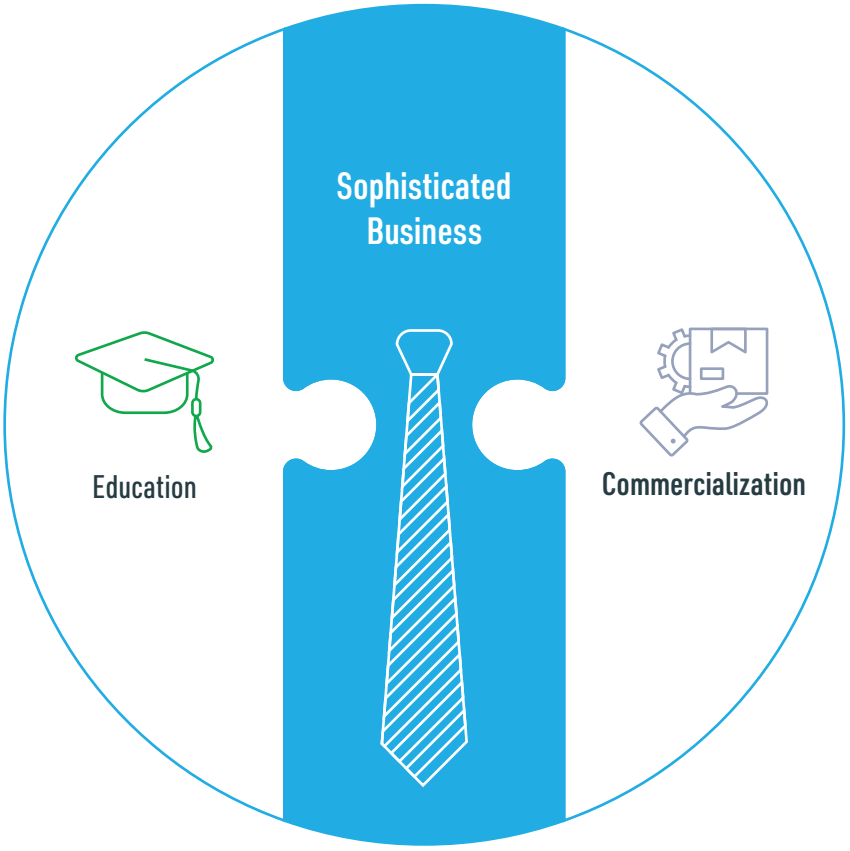
AI Maturity Often Mirrors Broader Innovation Capacity



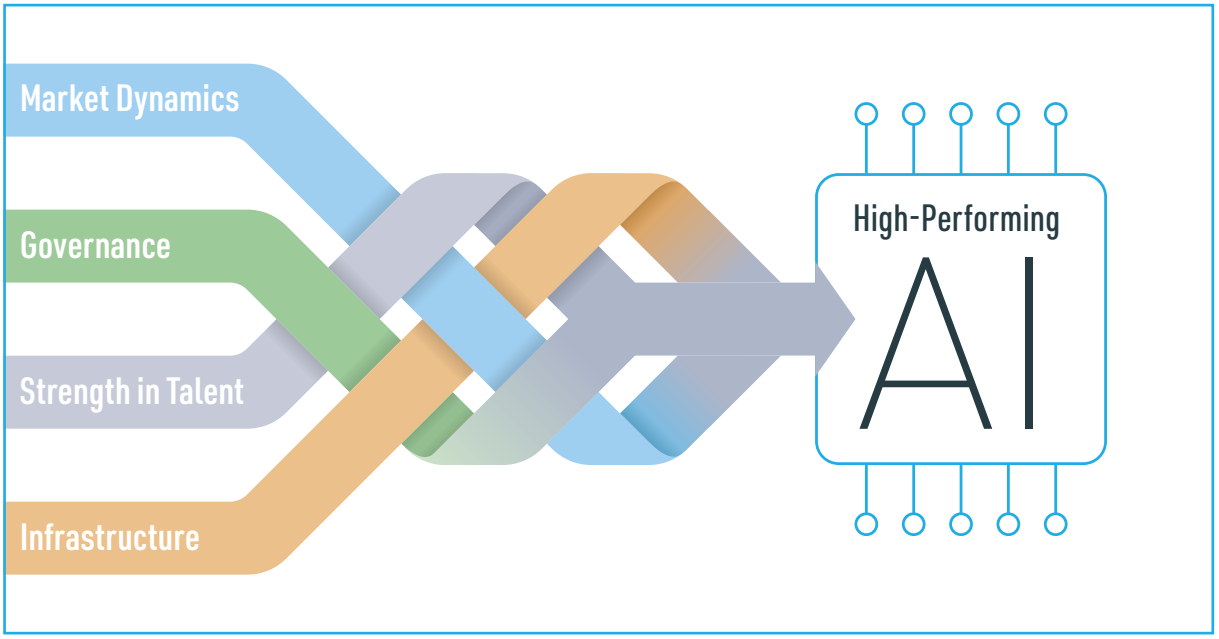
10 See full methodology and calculations in appendix D.

According to
12
Responses

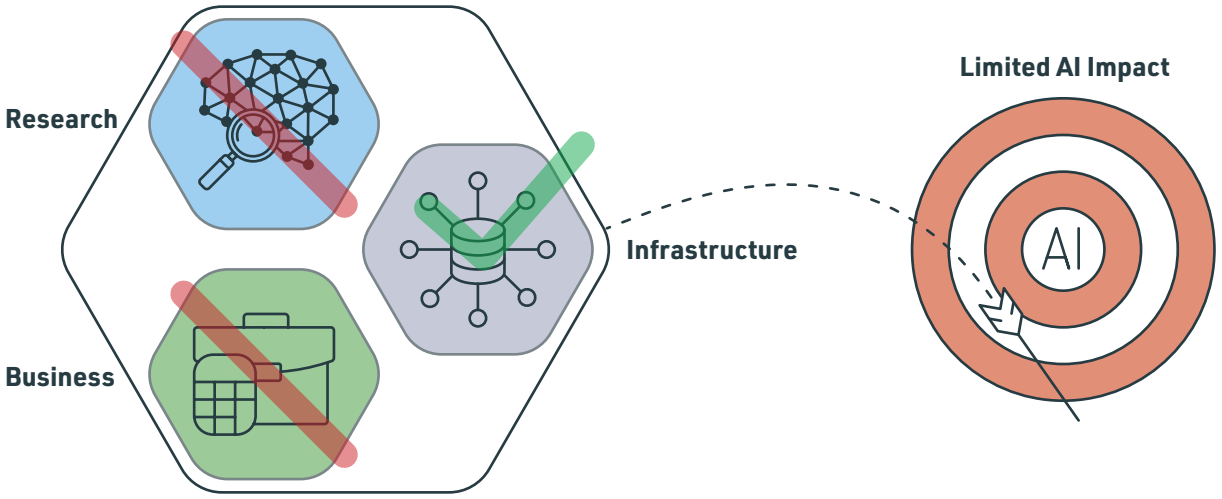
Business Sophistication Plays a Bridging Role Between Education and Commercialization



High-Performing Countries Tend to Combine Market Dynamics, Governance, Strength in Talent and Infrastructure



Countries Investing Heavily in Infrastructure Without Parallel Development in Business or Research Saw Limited AI Impact



These insights point to several strategic conclusions. First, **human capital is the foundation** of national AI capacity - driving both supply (skills, research) and demand (adoption, innovation). Second, **business sophistication and market readiness** enable investment and tech transfer, and can be reinforced through policies such as R&D tax incentives and public-private partnerships. Third, **infrastructure is essential but not sufficient;** its impact depends on the presence of skilled labor, effective governance, and innovation ecosystems. Lastly, countries that align their AI strategies with broader innovation and education policies tend to perform better across multiple benchmarks.

The audit also highlights **directions for policymakers** based on international evidence. These include sustained investment in STEM and AI education, strengthening industry-academic collaboration, and improving access to finance for AI ventures. National strategies tend to be more effective when they are well-funded, cross-sectoral, and coordinated across government entities. Closing the **research-to-commercialization gap** and promoting **AI for public value** - for example, through use cases in health, environment, and mobility - are also essential for driving adoption and building trust. A coordinated, ecosystem-based approach that integrates AI into broader innovation planning is vital for long-term competitiveness and resilience.

Recommendation

While institutional contexts differ, using these international benchmarks as a reference point may help countries prioritize actions that strengthen both AI readiness and their overall innovation systems.

CONCLUSIONS

A comprehensive picture emerges across all subchapters: most participating countries are gradually moving from declarations toward practical implementation of AI strategies. Where progress is strongest, it tends to be supported by a close alignment between clear institutional leadership, cross-government coordination, multi-year planning with measurable targets, and reference to international frameworks such as the OECD AI Principles and leading benchmark indexes. By contrast, gaps are more evident where these links are weaker - for example, when investment in digital infrastructure is not matched by talent development, when isolated pilot projects are not anchored in a broader strategy, or when ambitions for data sharing are not supported by adequate legal and institutional foundations. The comparative indexes point in the same direction: human capital is the central driver of performance, business sophistication forms a bridge between education and commercialization, and infrastructure on its own cannot deliver impact without effective governance and a culture of experimentation, learning, and measurement.

On this basis, several strategic directions for public sector planners can be inferred from the audit evidence. A consistent starting point is people - broad AI literacy across the civil service, accompanied by specialized expertise and strengthened managerial capability. Building on this, countries benefit from a stable governance architecture: a clear lead body with an appropriate mandate and budget, cross-ministerial coordination mechanisms, and systematic measurement aligned with ethical and legal standards. Around this, many of the more advanced approaches are developing a shared layer of national infrastructure - data governance and standards for secure sharing, high-quality open data, secure cloud and compute environments, and local language capabilities. Within such a framework, it becomes easier to promote value-driven adoption, focusing on high-impact public sector use cases developed in controlled experimental environments and supported by results-oriented procurement, with successful solutions scaled once value is demonstrated. Throughout this process, governments may wish to continue measuring outcomes rather than inputs, deepening collaboration with academia and industry, and embedding risk management, privacy, and information security into planning. Taken together, these elements can help shift AI from a scattered set of initiatives toward a more stable and accountable driver of public sector transformation.

NATIONAL AI BUDGETS

Smart AI strategies only become real when the resources follow the vision. Following the previous chapter on national strategic plans, this chapter examines how governments translate ambition into concrete financial commitments. While strategies define priorities and set long-term goals, budget decisions determine the pace, scope, and credibility of AI implementation across the public sector. Without clear and sustained funding, even the most sophisticated AI roadmap risks remaining a declarative document rather than a practical instrument for change.

The following chapter reviews how governments back AI ambitions with financial commitments, including whether AI-related budgets are set out clearly or absorbed into broader digital and sector budgets. It also considers how spending is structured across major investment areas and what this suggests about implementation priorities. In addition, the chapter examines how countries use external funding sources and partnerships to supplement public resources and sustain AI efforts over time.

Image is AI generated

BUDGET ALLOCATION AND BREAKDOWN

A key element in assessing how governments move from AI ambition to delivery is understanding how resources are allocated and how those allocations are structured.

Budget allocation and breakdown provide a practical signal of prioritization - revealing whether AI is treated as a distinct investment area or absorbed into broader digital and sectoral spending, and whether funding is coordinated across government or dispersed among individual institutions.

The way budgets are broken down across foundations such as infrastructure, research, skills, and implementation also shed light on the balance between building long-term capacity and supporting near-term deployment of AI solutions in the public sector.

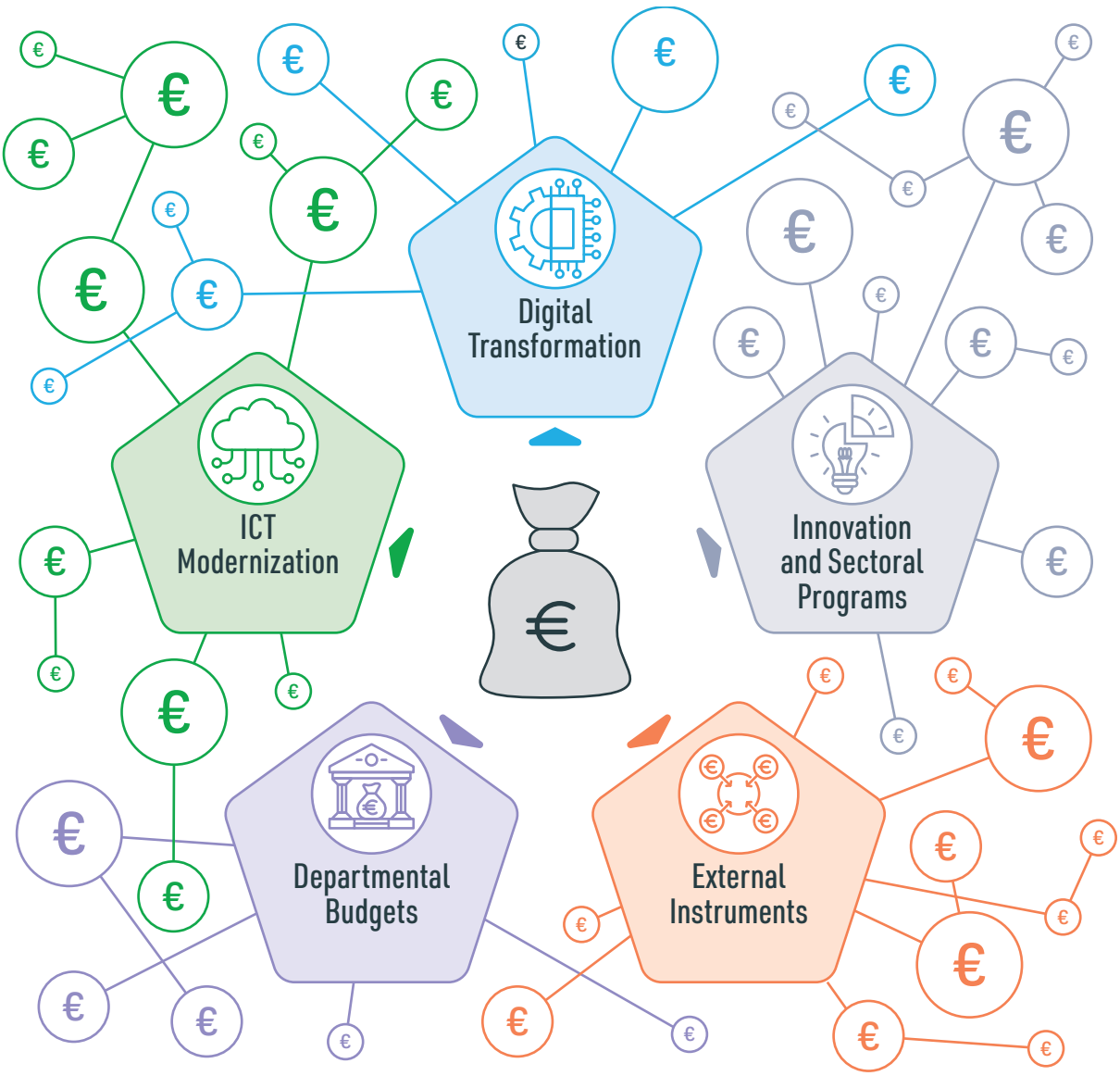
Only 45% of countries reported a clearly defined budget dedicated specifically to AI, while 55% indicated that no separate, consolidated AI budget exists.

In many of the latter cases, AI spending is embedded within broader envelopes for digital transformation, ICT modernization, innovation, or sectoral programs, rather than tracked as a standalone line item.

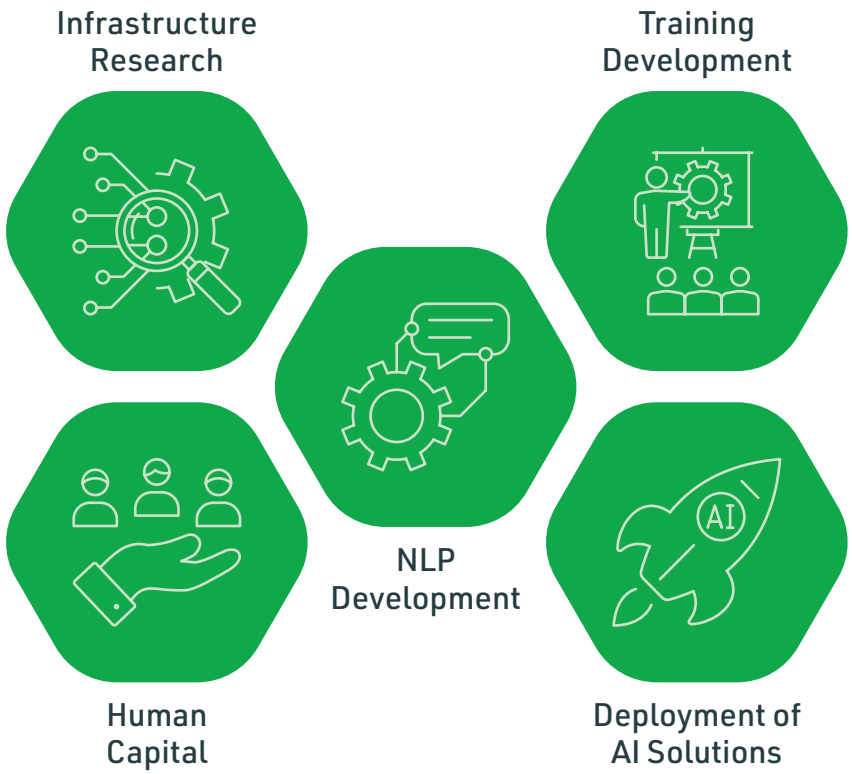
Several respondents noted that even when AI activities are explicitly planned, funding is often distributed across multiple ministries and agencies, financed through ordinary departmental budgets or external instruments such as EU funds, which limits visibility over total national AI investment and makes it harder to monitor implementation against strategic objectives.

According to
11
Responses

Funding Is Often Distributed Across Digital Transformation, ICT Modernization, Innovation and Sectoral Programs, Departmental Budgets and External Instruments such as EU Funds



Across five responses, budget breakdowns are presented through a mix of thematic categories and allocation logic rather than a consistent structure. Most descriptions cluster spending into recurring lines, including **enabling infrastructure** (often framed around compute capacity and related foundations), **research and development, NLP** as a distinct investment area, **human capital and training,** and the **development and deployment of AI solutions** in practice. A common pattern is the separation between direct AI project funding and broader, enabling or "non-direct" digital investments where AI is expected to be used, with this enabling investment often described as the dominant component.



Where allocations are quantified, infrastructure and compute capacity frequently receive the largest shares (including examples such as 49% directed to HPC and 83% classified as non-direct AI support linked to HPC, alongside reference to more than €61 million of HPC projects being implemented through a national recovery and resilience plan under the RRF. Mid-tier allocations tend to support research and innovation and, in some cases, separately funded technical domains such as NLP, while some breakdowns also report substantial portions directed to wider national priorities such as the economy and defense or security-related areas.

By contrast, regulation and governance and narrower public-sector lines such as higher education and public sector transformation are typically reported as smaller budget items when explicitly tracked.

Taken together, these findings indicate that AI financing is still often managed as a dispersed set of allocations rather than as a clearly defined, transparently tracked investment portfolio.

In over half of the countries, AI-related spending is embedded within broader digital or sectoral budgets and split across multiple institutions, which reduces visibility over total national effort and complicates monitoring against strategic objectives. Where countries do report budget breakdowns, they tend to use different classification approaches, but a recurring picture emerges in which enabling foundations - especially infrastructure and compute capacity - dominate, while investment in governance and regulatory capacity is comparatively limited when explicitly budgeted.

Recommendation

As countries continue to refine their budgeting approaches, it may be useful for them to periodically review whether their current funding structure provides sufficient transparency and strategic steer - including a consistent way to distinguish direct AI project funding from enabling investments, to consolidate AI-related spending across institutions and major external funding streams, and to ensure that foundational investments are balanced with adequate resourcing for implementation and oversight.

ALTERNATIVE FUNDING MODELS

These alternative streams fall into three broad categories:

EU and International Public Funding Programs

EU instruments - Horizon Europe, ERDF, Digital Europe, and the RRF - form the backbone of public AI finance, providing multi-year, cross-border resources that fuel national initiatives and research hubs (e.g., the €67.6 million Romanian AI HUB).

These flagship programs are now complemented by InvestEU, development banks, and bilateral donors, broadening the pool of international funding available for AI. Together, they enable collaboration across countries and sectors while advancing AI technologies in multiple domains.

Public-Private Partnerships (PPPs) and Joint Funding Models

Public-Private Partnerships are evolving into diversified, joint-funding frameworks that knit together government, academia, and industry. By blending private-sector innovation and capital with public oversight and societal objectives, PPPs have become a powerful, expanding vehicle for AI research, technology transfer, and implementation. New focal points – such as strategic industry alliances and Centers of Excellence co-funded with universities – translate publicly funded research into market-ready solutions while distributing cost and risk.

These models also facilitate international collaboration and shared financial responsibility, accelerating the global advancement of AI technologies and ensuring they remain aligned with public priorities.

Competitive and Collaborative Research Models

Grass-roots, incentive-based mechanisms - crowdfunding, collaborative research hubs, and prize or "grand-challenge" competitions - catalyze bottom-up innovation by inviting public participation, competition, and cross-sector partnerships.

These models diversify funding streams, draw in broad technical expertise, and create ecosystems where joint projects with universities and international research groups share knowledge globally. Together, they accelerate creative AI solutions and provide the agility to pivot quickly toward emerging technological challenges.

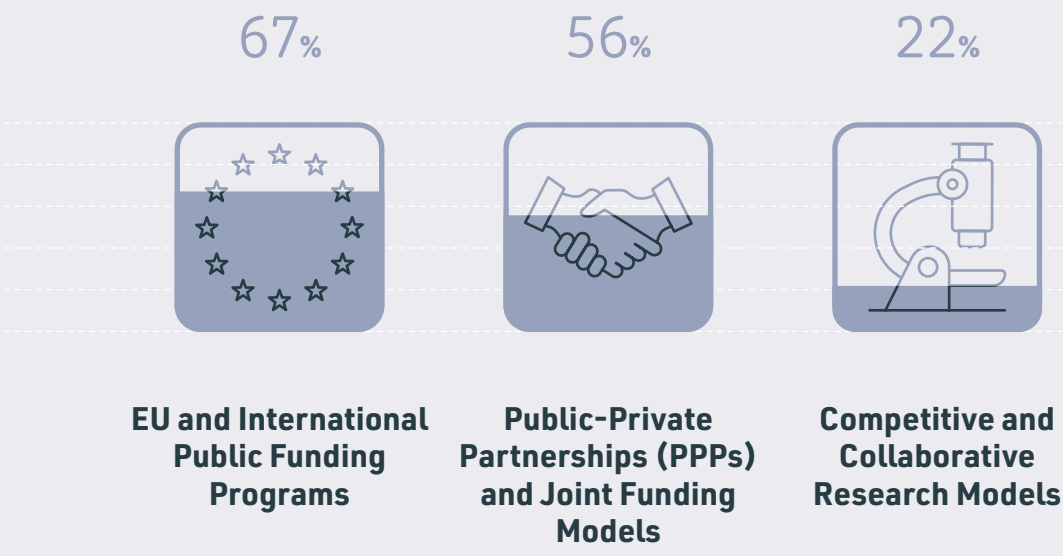
Together, these mechanisms expand the fiscal toolbox available to governments, but they also introduce coordination challenges and heighten the need for clear, multi-year financial planning. The following findings summarize how participating states are leveraging each category to supplement their AI budgets and where gaps in strategic alignment still persist.

Responses indicate that alternative AI funding models are largely anchored in EU and international public programs, referenced by roughly two-thirds of responses (67%). These sources include Horizon Europe, the Recovery and Resilience Facility and national recovery plans, ERDF and other EU digitization instruments, and additional mechanisms such as InvestEU, development banks, and bilateral donors, with some countries pointing to dedicated national vehicles that manage such financing and others illustrating scale through major multi-year programs and hub-style investments.

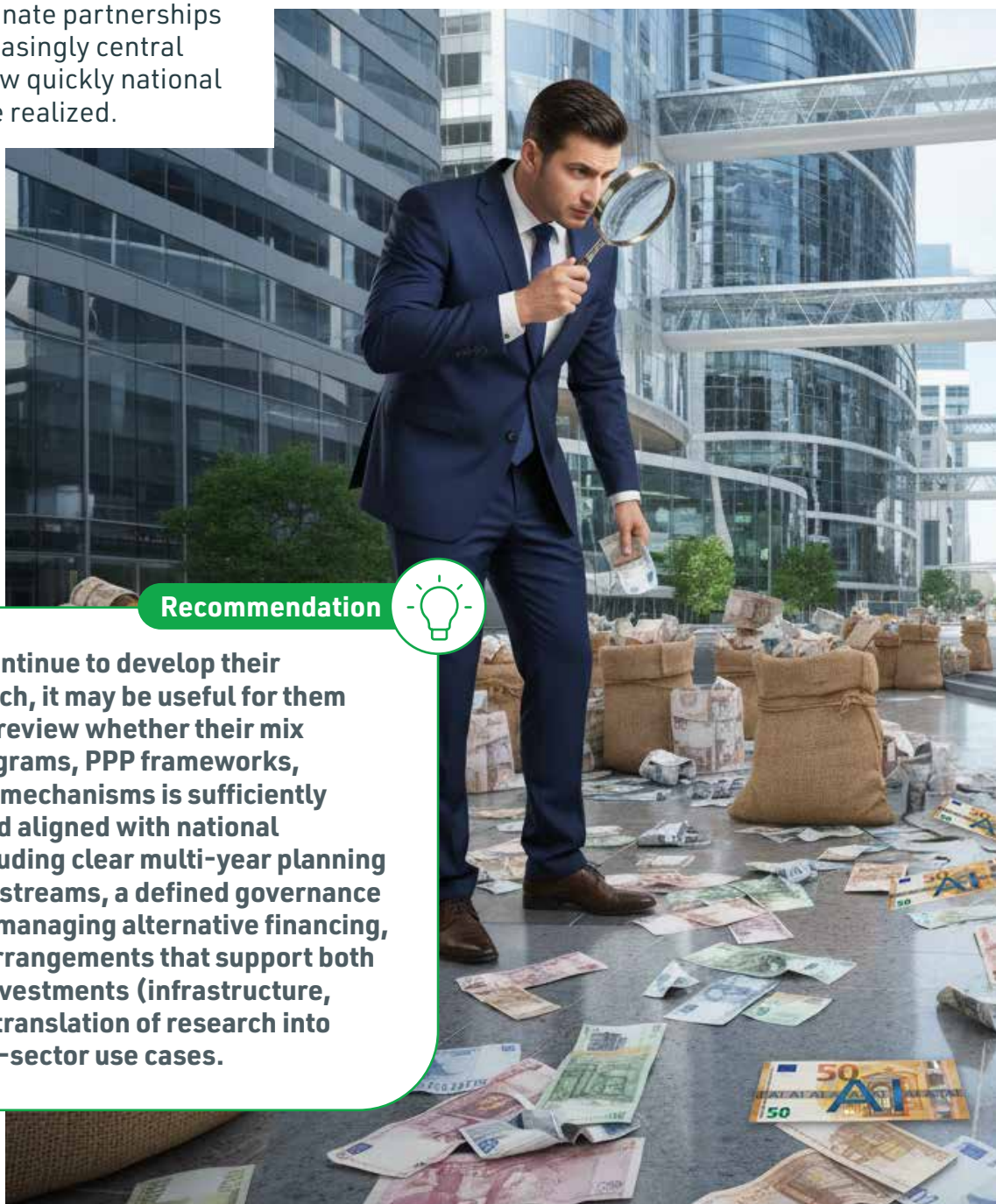
PPPs and joint funding models are also widespread (56%), typically linking government with universities and research centers and, in several cases, extending to industry collaboration models that support technology transfer, commercialization, and scaling.

Competitive and collaborative research models are mentioned less frequently (22%), but include prize-style challenges, collaborative hubs, and crowdfunding-type approaches intended to broaden participation and stimulate innovation.

Alternative Funding Models



Overall, the responses suggest that most countries seek to supplement national budgets through structured external channels, with EU and international instruments providing a primary backbone and PPPs serving as a key mechanism for converting research investment into deployable capabilities. At the same time, the distribution of approaches implies that access to external funding and the ability to coordinate partnerships are becoming increasingly central determinants of how quickly national AI ambitions can be realized.



Recommendation

As countries continue to develop their funding approach, it may be useful for them to periodically review whether their mix of external programs, PPP frameworks, and innovation mechanisms is sufficiently coordinated and aligned with national priorities - including clear multi-year planning across funding streams, a defined governance or "owner" for managing alternative financing, and practical arrangements that support both foundational investments (infrastructure, skills) and the translation of research into scalable public-sector use cases.

CONCLUSIONS

The chapter indicates that AI financing across participating states is still marked by fragmentation and uneven visibility. Less than half of countries report a clearly defined, dedicated AI budget, while most embed AI spending within broader digital, ICT, innovation, or sectoral envelopes and distribute responsibility across multiple ministries and agencies. This reduces the ability to consolidate national AI investment, compare funding levels over time, and monitor whether spending is aligned with strategic objectives.

Image contains AI generated elements

Where countries do report budget breakdowns, they reference broadly similar investment lines - enabling foundations such as infrastructure and compute capacity, research and innovation, human capital and training, and the development and deployment of AI solutions - yet classification approaches vary and the boundary between direct AI spending and enabling or "non-direct" support is not consistently defined.

At the same time, most countries seek to supplement national resources through external channels, with EU and international programs frequently serving as the main backbone and PPPs acting as a key mechanism for connecting government, academia, and industry.

Taken together, these findings suggest that the pace and credibility of AI implementation increasingly depend not only on the level of investment, but also on the coherence of budget structures, cross-government coordination, and the capacity to manage diverse funding streams over multiple years.

REGULATORY GUIDELINES

Clear and practical AI rules are increasingly important for governments seeking to adopt AI in a responsible and consistent way. Regulatory guidelines translate AI ambition into safeguards and accountability, helping public institutions manage risk while protecting rights and maintaining trust. While strategic plans define direction and budgets provide capacity, regulatory guidance helps determine what is permitted, how risks are addressed, and who is accountable when AI supports public services or administrative decisions.

This chapter examines how participating countries are shaping the rules and oversight for government AI. It reviews the status of national guidance and responsible bodies, the influence of the EU AI Act, and approaches to ethical risk management and public trust. It also considers key legal challenges that can affect implementation, including data protection, accountability, and fundamental rights.

Image is AI generated

OVERVIEW OF REGULATORY GUIDELINES

The establishment of clear and comprehensive regulatory guidelines is a crucial step in ensuring that AI technologies are adopted responsibly and ethically within government operations. Regulatory frameworks set expectations for transparency and accountability, define governance responsibilities, and provide a common basis for consistent implementation across ministries and agencies. In the public sector, where AI systems can affect rights, service access, and administrative decisions, guidance on acceptable use and oversight helps reduce legal uncertainty, strengthen internal controls, and support responsible innovation.

The regulatory landscape for AI within government operations remains uneven. Half of the responding countries (50%) reported that AI regulatory guidelines have been formally published, while the other half (50%) reported that no such guidelines have been issued. This variation suggests that, in several countries, AI implementation may still rely on broader digital, ICT, or sector-specific rules rather than dedicated AI guidance, which can create inconsistent practices across government.

According to 10 Responses

At the same time, all responding countries (100%) reported the existence of a dedicated agency or body responsible for overseeing the development and implementation of AI regulations. This indicates that institutional ownership is in place even where formal guidelines have not yet been published, and that countries are moving to assign clear responsibility for oversight, coordination, and compliance.

100%

report a Dedicated Body Responsible for AI Regulation

67%

report a framework or initiative in place in the public sector

Alignment with international standards is also reflected in the use of the OECD framework for trustworthy AI[11]. 67% of countries reported that a framework or initiative is in place to implement the OECD's principles within the public sector, while 33% reported that no such mechanism exists.

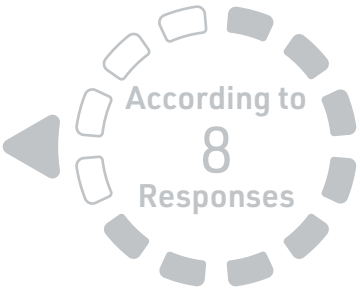
In addition, six countries reported that all OECD principles are explicitly referred to and adopted in their national strategies.

This indicates that, where adopted, OECD principles are often used not only as general values but as an organizing reference for governance expectations and responsible public-sector AI practices.

11 https://oecd.ai/en/ai-principles

The key principles and provisions outlined in the regulatory frameworks that have been published largely focus on **transparency and accountability** (75%), **human rights and human-centered safeguards** (75%), and **regulatory governance and approach** (62.5%).

Transparency and accountability are emphasized as crucial to ensuring that AI systems are visible and contestable, with mechanisms for traceability, explainability, and responsibility. Human rights and human-centered safeguards are equally prominent, ensuring that AI systems prioritize human autonomy, dignity, equality, and privacy, while avoiding harmful profiling and discrimination. Several countries also emphasize the importance of regulatory governance, including risk-based logic, technical interoperability, and multi-stakeholder processes for more inclusive regulation. In addition, **technical and operational safeguards,** such as security, safety, and quality assurance, are highlighted by 50% of the countries as essential to maintaining reliable and secure AI systems. Less frequently, countries include provisions on **international alignment and interoperability** (37.5%), ensuring that their AI regulations are consistent with global standards such as the EU AI Act and OECD principles. Finally, some countries mention **public value objectives** (25%), aiming to achieve benefits such as efficiency, better services, and innovation leadership through AI deployment in the public sector.



Key Principles in Regulatory Frameworks

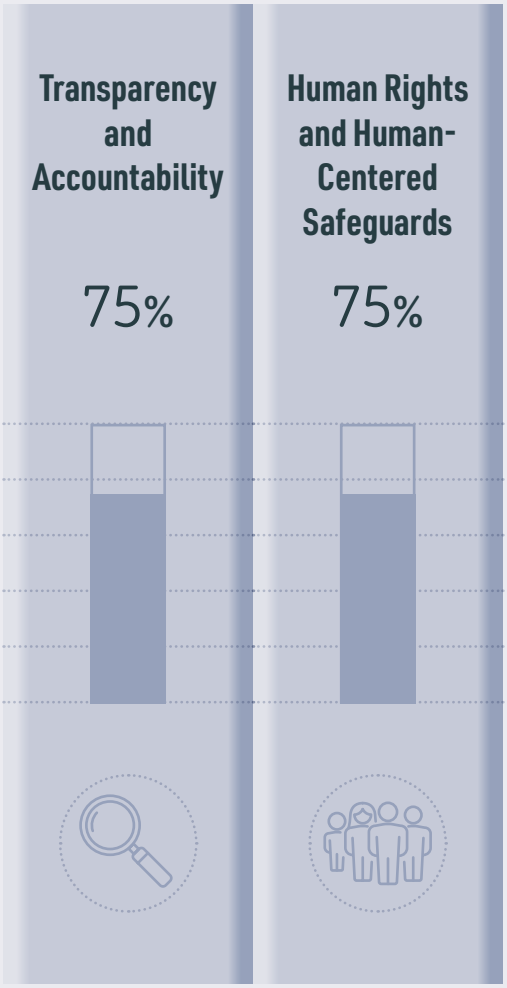
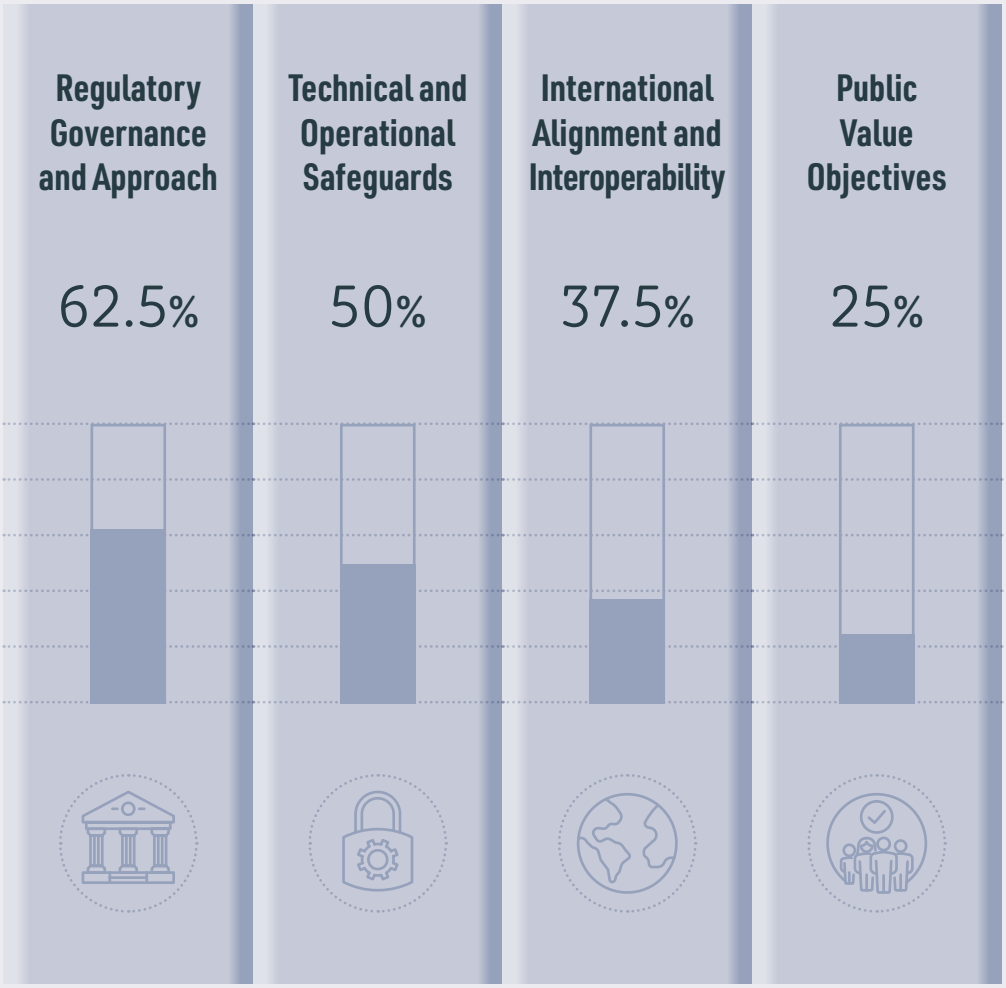


Image is AI generated



The content of existing frameworks reveals a clear focus on **transparency and accountability** and **human rights safeguards,** reflecting a growing recognition of AI's ethical implications. However, the relatively low emphasis on **international alignment** and **public value objectives** suggests that while the regulatory focus is on compliance and risk management, broader goals such as cross-border cooperation and societal impact may require further attention.

Image is AI generated

Countries may wish to consider publishing clear, operational AI regulatory guidelines to support consistent implementation across government. Strengthening coordination between central oversight bodies and sector regulators could help standardize expectations and compliance. Aligning national approaches with established international frameworks may also support interoperability and reduce fragmentation.

EU AI ACT

The EU AI Act is a major driver of how governments regulate, procure, and use AI in public services. By setting common expectations for risk management, compliance, and governance, it requires countries to translate a shared European framework into practical national rules, oversight arrangements, and operational guidance across ministries and agencies.

EU Artificial Intelligence Act

The EU AI Act[12] is the first comprehensive regulatory framework for AI, built around a risk-based approach. It assesses AI systems based on the risks they pose to individuals, society, and fundamental rights, taking into account their context and intended purpose. The Act defines four risk levels, with corresponding obligations:

* **Unacceptable risk (prohibited practices)** - Banned AI uses that pose a clear threat to safety or rights (e.g., certain forms of social scoring).

* **High-risk AI systems** - Permitted, but subject to strict requirements due to potential harm to health, safety, or fundamental rights (e.g., some systems used in critical infrastructure or education).

* **Limited-risk AI systems (transparency obligations)** - Mainly disclosure duties, especially where people interact with AI or where content is generated or altered (e.g., labelling deepfakes). Generative AI generally falls here, alongside related obligations (including copyright-related duties for providers).

* **Minimal or no risk** - No additional rules under the Act (e.g., spam filters or AI-enabled video games).

12 https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

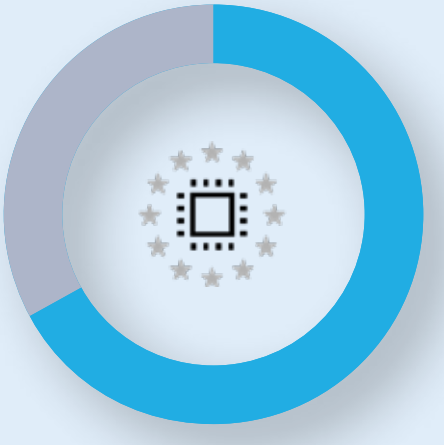
The Act is already influencing national regulatory activity. 60% of responding countries reported that **additional regulatory guidelines have been initiated** in connection with the Act, while 40% reported no additional guidelines at this stage. This indicates that, for many governments, the Act is acting not only as a future compliance requirement but also as a near-term catalyst for domestic preparation.

According to 10 Responses

Beyond the AI Act

60%

Initiated additional guidelines



40%

Did not initiate additional guidelines

In response to the question on the main challenges and opportunities presented by the EU AI Act for the country's AI development and regulatory landscape, the opportunities described framed the Act primarily as a standardization and compliance agenda that can strengthen regulatory clarity. About 33% emphasized **alignment with EU standards, legal harmonization,** and **a stronger binding regulatory basis** as key benefits. In addition, 17% highlighted **reinforcement of safe and ethical AI use,** and 17% cited **innovation and international funding opportunities** linked to compliance.

According to 6 Responses

EU AI Act - Opportunities

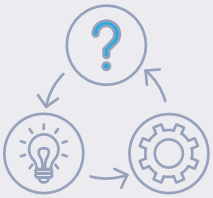
Harmonized regulatory environment

Safer, more ethical AI use

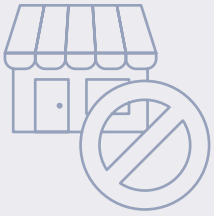
Innovation support and access to international funding

EU AI Act - Challenges

Keeping oversight aligned with fast-moving technology



Uncertainty around implementing and guidance



market-access barriers and reduced national business attractiveness

Coordinating EU rules with national governance

Talent shortages

Challenges were raised across all responses, reflecting the expected complexity of translating EU requirements into national practice. Specific issues included **keeping oversight current with rapid technological change** (17%), **managing friction between EU-level rules and multi-level national governance** (17%), and **near-term uncertainty linked to upcoming implementing acts and guidance** that may affect interpretation and obligations (17%). Capacity constraints were also noted, with 17% identifying difficulty **hiring highly qualified human resources** due to the specialized knowledge required for the AI Act and higher remuneration expectations than state administration salaries. In addition, 17% warned that failure to meet requirements could create **market-access barriers and reduce national attractiveness** as a business location.

Taken together, the findings suggest that countries view the EU AI Act as both an anchor and a stress test. Where additional guidance is being developed, governments appear to be using the Act to strengthen governance and clarify expectations for responsible AI. At the same time, the uniform emphasis on implementation challenges indicates that compliance is expected to be demanding due to rapid technological change, complex coordination requirements, and administrative burden. The attention to regulatory uncertainty and workforce constraints suggests that execution risks may be driven as much by capacity and timing as by the legal requirements themselves.

Recommendation

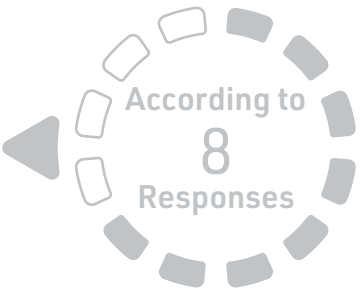
A practical approach is to treat EU AI Act preparation as a whole-of-government governance effort rather than a narrow legal exercise. Strengthening implementation capacity and early cross-ministry coordination could reduce fragmentation, while continued alignment with evolving EU guidance could help manage uncertainty and support more consistent application.

ETHICAL RISKS IN AI DEPLOYMENT

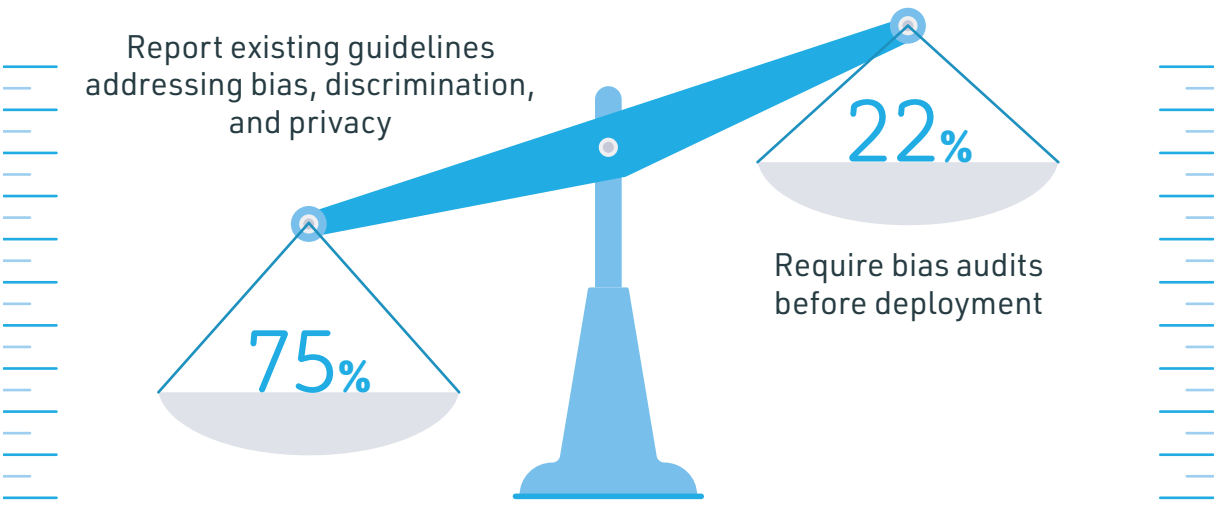
Ethical risks in government AI systems are not limited to technical errors - they can affect equality of access to services, procedural fairness, privacy protection, and the legitimacy of public decisions. Because public authorities can use AI in high-impact contexts, weak safeguards can translate into discriminatory outcomes, loss of trust, and legal exposure. Managing these risks requires more than general principles. It depends on operational tools that identify and reduce bias across the AI lifecycle, clear governance responsibilities, and mechanisms that allow decisions to be explained, reviewed, and corrected.

Across participating countries, formal requirements for bias audits before deployment remain uncommon. **Only 22% reported that developers of AI systems for public use are required to conduct bias audits prior to deployment, while 77% reported no such requirement.**

By contrast, ethical guidance is more widely established. **75% indicated that guidelines or regulations exist to address ethical concerns such as bias, discrimination, and privacy violations,** while 25% reported that such guidance is not in place.



Ethics Safeguards vs. Bias Audits



When describing how ethical risks such as bias and discrimination are handled, responses clustered around four equally common approaches. Measures supporting **transparency and accountability,** including explainability and traceability, were cited by 50%, alongside **risk management and continuous assurance tools** such as impact assessments, periodic audits, and maturity models (50%). **Fairness requirements and data quality safeguards** were also cited by 50%, reflecting controls aimed at reducing biased inputs and reinforcing non-discrimination principles. A further 50% emphasized **governance and enforcement mechanisms,** including binding rules, accountability arrangements, and cross-agency coordination. Capability building through **guidance and training** appeared in 33%, while **explicit human oversight** of AI-supported decisions was cited less often at 17%.

Measures for Ethical Risk Handling

50% Transparency and Accountability

50% Governance and Enforcement

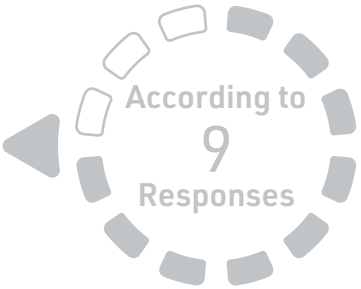
50% Risk Management and Ongoing Assurance

33% Guidance and Training

50% Fairness and Data Quality Safeguards

17% Explicit Human Oversight

Approaches to promoting public trust and transparency were more outward-facing and participatory. **Transparent communication and access to information** was the most frequent theme at 67%, focusing on clear explanations of AI use and publication of relevant information. **Public participation and dialogue** were cited by 56%, alongside **governance, compliance, and independent assurance mechanisms** such as audits, oversight bodies, and certification or conformity checks (56%). **Education and literacy** appeared less frequently, cited by 22%, mainly through public awareness and stakeholder training.



Approaches to Promoting Public Trust

67%

Transparent Communication and Access to Information

56%

Public Participation and Dialogue

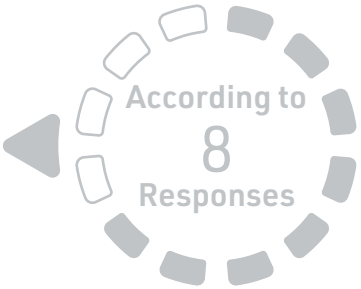
56%

Governance, Compliance, and Independent Assurance

22%

Education and Literacy

Measures to ensure compliance with ethical standards showed a strong emphasis on controls and oversight. **Legal and compliance safeguards,** including privacy, security, and alignment with standards, were cited by 57%. **Risk management and operational controls** were also cited by 57%, covering practical processes for identifying and mitigating risks during design and use. **Ethical governance and oversight mechanisms,** such as ethical review bodies and monitoring programs, were cited at the same rate (57%). **Capability building and responsible development** practices appeared less often at 14%, including training, awareness, and organizational practices intended to reduce ethical risk at the source.



Measures To Ensure Compliance with Ethical Standard

57%

Legal and Compliance Safeguards

57%

Risk Management and Operational Controls

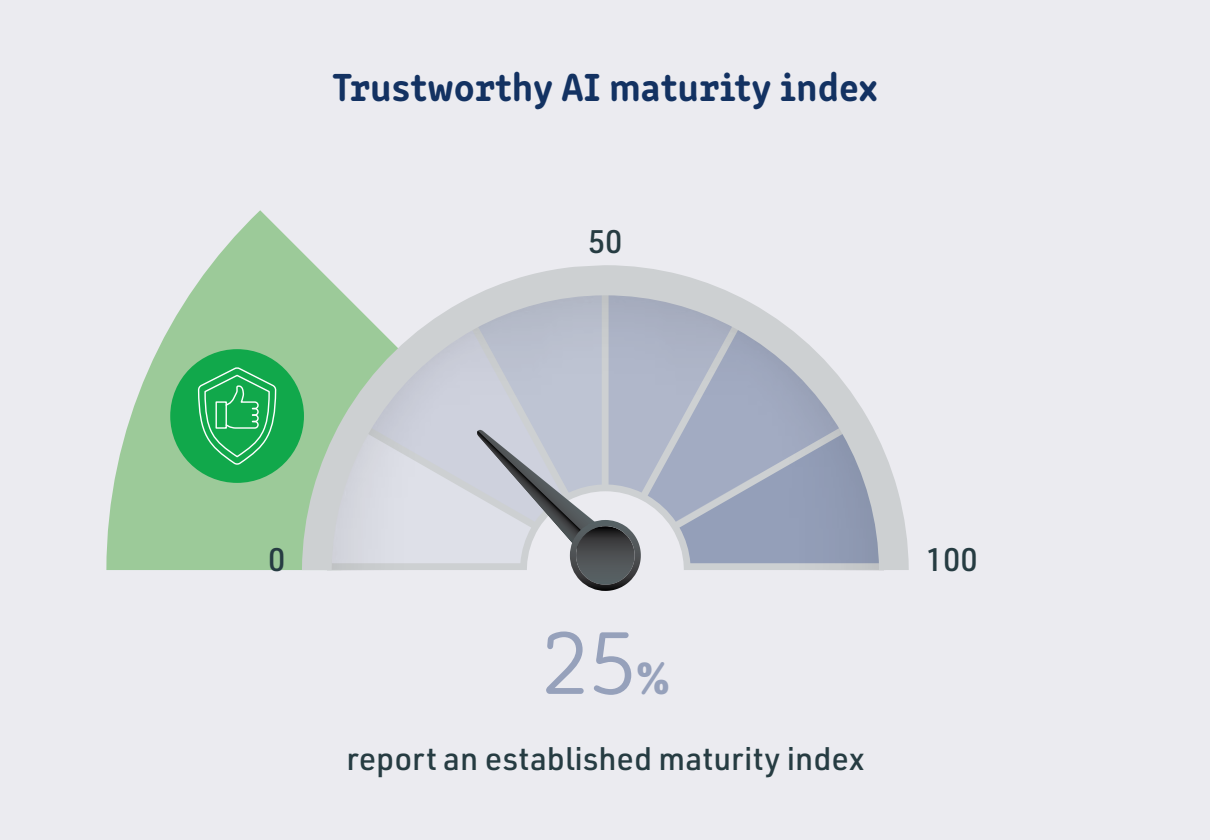
57%

Ethical Governance and Oversight Mechanisms

14%

Capability Building and Responsible Development

Beyond case-by-case risk controls, some governments seek to monitor trustworthy AI readiness across the public sector through a maturity index. Only 25% reported that **a maturity index for trustworthy AI has been established,** while 75% reported that no such index exists. This suggests that, in most countries, ethical assurance is still managed primarily through individual policies, guidance, or project-level processes rather than through a structured, comparable measurement tool that can track progress, identify gaps across ministries, and support more consistent governance and accountability over time.



Taken together, the findings suggest an imbalance between high-level ethical intent and enforceable assurance in practice. Countries appear to converge on a shared understanding of what responsible public-sector AI should include, with recurring emphasis on transparency and accountability, risk-based controls, fairness safeguards, and strong governance. However, the overall picture indicates that ethics is often treated as a framework-level commitment rather than as a consistently embedded, testable practice throughout development and deployment. Where safeguards remain primarily policy-based, implementation depends heavily on the maturity of internal controls and the ability to translate expectations into measurable assurance.

The findings also indicate that public trust is being pursued through a combination of visibility and accountability. Countries tend to link legitimacy to making AI use understandable to the public, supported by participatory mechanisms and independent assurance. At the same time, comparatively limited attention to capability building - including education and literacy - suggests that trust strategies may lean more toward communication and compliance than toward sustained institutional and societal understanding. This pattern points to the importance of stronger connections between ethical requirements, operational assurance mechanisms, and the internal capacity needed for consistent implementation across government.

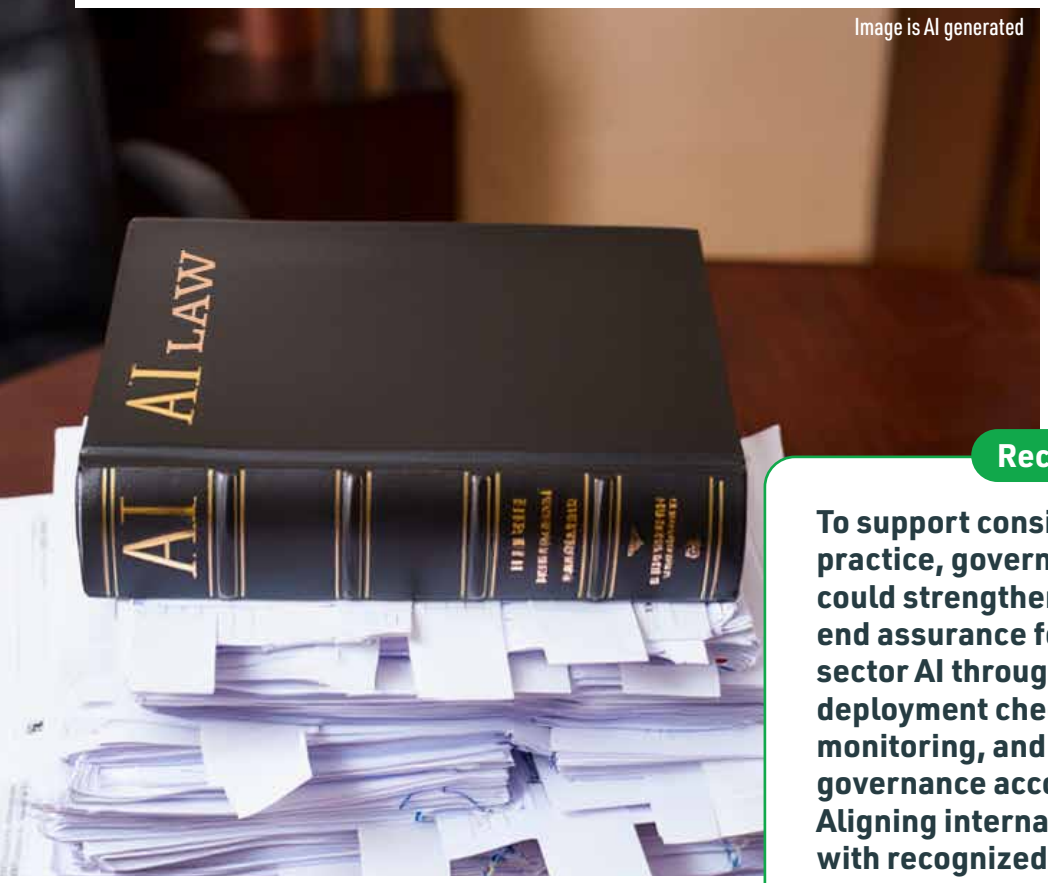


Image is AI generated

Recommendation

To support consistent ethical practice, governments could strengthen end-to-end assurance for public-sector AI through clear pre-deployment checks, ongoing monitoring, and defined governance accountability. Aligning internal practices with recognized frameworks and standards could help standardize implementation across ministries. Expanding training and practical guidance for developers, procurement teams, and decision-makers may also help translate ethical commitments into routine operational practice.

LEGAL RISKS AND LITIGATION IMPACTS

Legal clarity is a foundational condition for government AI adoption, particularly where systems influence entitlements, enforcement, or other high-impact administrative decisions. Public authorities must ensure that AI use is grounded in lawful data access and processing, protects fundamental rights, and enables accountability when outcomes cause harm or are challenged. Because government AI often relies on cross-sector data and complex procurement and outsourcing arrangements, legal risks can arise even when technology performs as intended. A coherent legal approach also supports consistent implementation across ministries by clarifying permissible uses, oversight responsibilities, and the standards that enable decisions to be explained, reviewed, and defended.

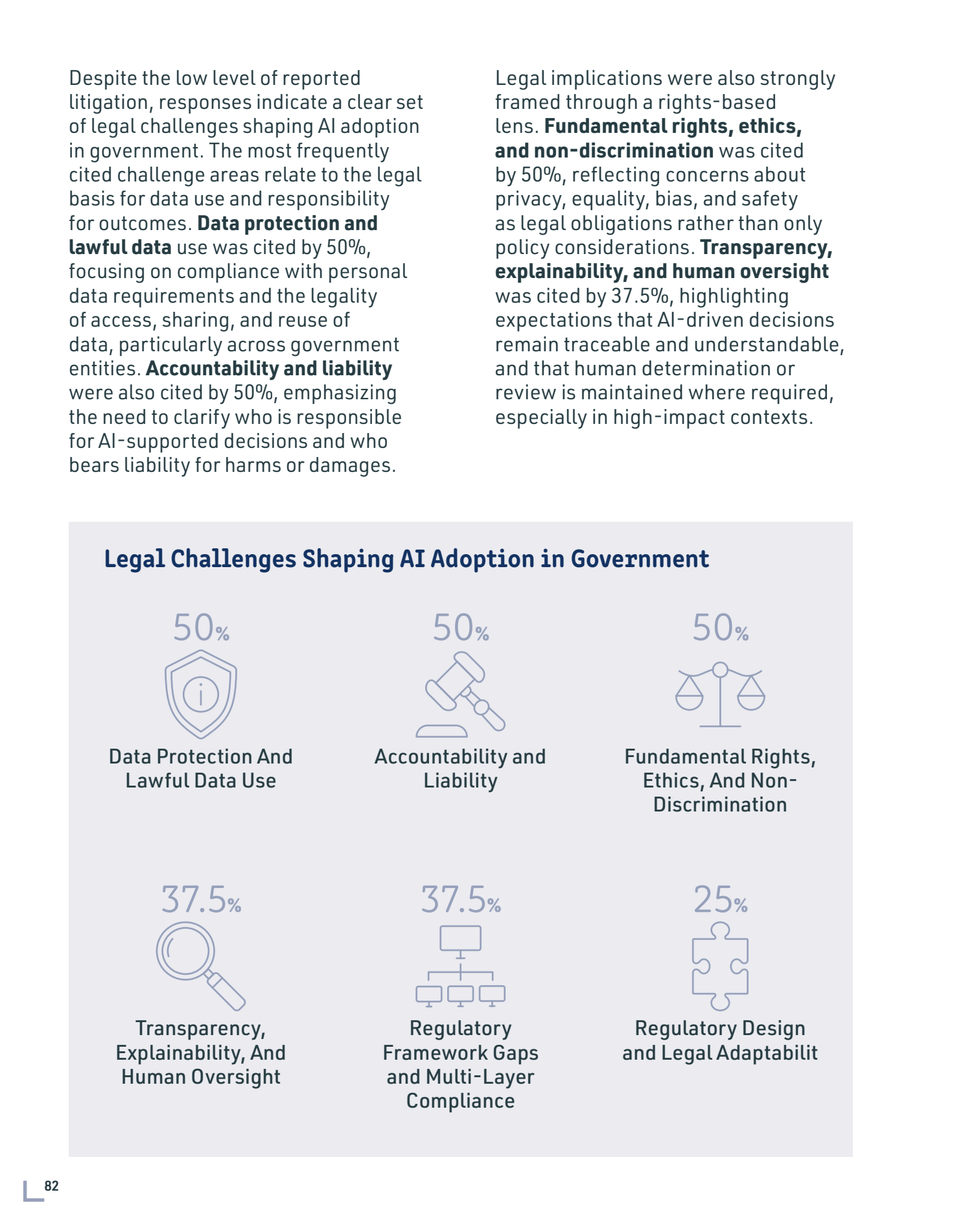
Reported litigation related to government AI use appears limited at this stage. Only 14% of countries reported litigation concerning AI, including issues such as liability, permissible uses, limits, and protections, while 86% reported no litigation. This suggests that most countries have not yet faced significant court-tested disputes linked directly to government AI deployment, or that such disputes are still emerging and not yet captured as a recurring pattern.


Image is AI generated

Despite the low level of reported litigation, responses indicate a clear set of legal challenges shaping AI adoption in government. The most frequently cited challenge areas relate to the legal basis for data use and responsibility for outcomes. **Data protection and lawful data** use was cited by 50%, focusing on compliance with personal data requirements and the legality of access, sharing, and reuse of data, particularly across government entities. **Accountability and liability** were also cited by 50%, emphasizing the need to clarify who is responsible for AI-supported decisions and who bears liability for harms or damages.

Legal implications were also strongly framed through a rights-based lens. **Fundamental rights, ethics, and non-discrimination** was cited by 50%, reflecting concerns about privacy, equality, bias, and safety as legal obligations rather than only policy considerations. **Transparency, explainability, and human oversight** was cited by 37.5%, highlighting expectations that AI-driven decisions remain traceable and understandable, and that human determination or review is maintained where required, especially in high-impact contexts.

Legal Challenges Shaping AI Adoption in Government



Regulatory structure and coherence challenges were also prominent. **Regulatory framework gaps and multi-layer compliance** was cited by 37.5%, reflecting the absence of dedicated AI rules in some settings and the need to align sector-specific laws with broader legal instruments and varying layers of hard and soft law. **Regulatory design and legal adaptability** were cited by 25%, emphasizing the difficulty of updating legal frameworks quickly enough to keep pace with technological change while avoiding over-regulation, fragmented national approaches, or slow harmonization processes.

Taken together, the findings suggest that legal risk in government AI deployment is currently driven more by unresolved structural questions than by litigation volume. The repeated emphasis on lawful data use, accountability, and rights protections indicates that many governments are still defining the conditions under which AI can be used legally and safely, and how responsibility is assigned when AI is part of decision-making. The presence of transparency and oversight themes further suggests that legal expectations increasingly overlap with operational controls, requiring institutions to demonstrate traceability, explainability, and human-centered safeguards in practice.

The findings also indicate that fragmented regulatory environments can amplify legal uncertainty. Where multiple legal layers apply simultaneously, compliance may become harder to operationalize across ministries, particularly when responsibilities for data governance, model oversight, and accountability are distributed. This pattern implies that legal readiness for AI depends not only on the existence of rules, but also on clear institutional interpretation, consistent application, and the ability to adapt legal instruments as AI systems and use cases evolve.

Recommendation

As AI use expands, clarifying legal responsibilities for AI-supported decisions - including data governance and liability - can help ensure that transparency and human oversight requirements are applied consistently in public-sector processes. Strengthening coordination across regulators and ministries could reduce fragmentation and support more uniform compliance. Aligning national approaches with established regional and international frameworks may also enhance legal certainty and interoperability.

CONCLUSIONS

Across the participating countries, the regulatory environment for government AI is developing unevenly, with a recurring gap between institutional arrangements and fully operational guidance.

Many countries have established responsible bodies and are articulating common safeguards, but published regulatory guidelines and standardized assurance mechanisms are not consistently in place.

Where frameworks exist, they tend to prioritize transparency and accountability, protection of rights, and risk-based controls, reflecting a shared orientation toward trustworthy AI. International frameworks - including the OECD principles and the EU AI Act - are widely used as reference points, supporting convergence around common expectations, even as national approaches differ in speed and depth.

At the same time, implementation capacity and legal complexity emerge as cross-cutting constraints. Countries commonly frame the EU AI Act as a harmonizing anchor while also anticipating significant execution challenges related to rapid technological change, multi-level governance, and near-term regulatory uncertainty as guidance evolves.

Ethical risk management is often addressed through principles, oversight, and communication measures, but fewer systems appear to rely on consistent, testable pre-deployment assurance or maturity measurement across the public sector.

Legal concerns - especially lawful data use, accountability, and fundamental rights - cut across all areas, indicating that regulatory readiness depends not only on formal rules but also on clear responsibilities, coordinated enforcement, and practical tools that can be applied consistently across ministries as AI use expands.

INFRASTRUCTURE

Infrastructure is the quiet foundation behind every successful government AI effort. It shapes whether agencies can move beyond pilots to reliable, secure, and scalable use, while supporting consistent safeguards for sensitive data and public services. In practice, infrastructure decisions influence what can be delivered, how quickly it can be deployed, and how confidently it can be governed. In that sense, infrastructure does not compete with strategy, budgets, or regulatory guidance - it enables them, and it can also become the main constraint when capacity, access, or oversight is unclear.

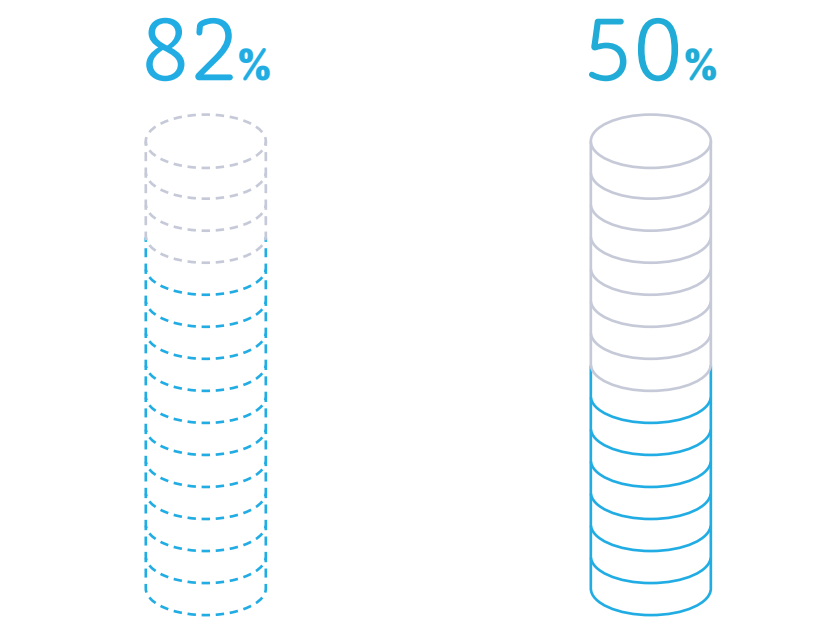
This chapter examines whether governments have launched national initiatives to develop **AI infrastructure** and what types of capability are being expanded. It also reviews whether a **national cloud** infrastructure exists, including reliance on third-party providers for cloud and computing services. Finally, it considers what the reported patterns imply for governance in hybrid environments and for cross-country comparability of infrastructure readiness.

Image is AI generated

About 82% of responders reported that the government **has launched national initiatives for AI infrastructure development,** while about 18% reported no such initiatives. Among responses that addressed implementation progress, the results indicate that, on average, about 50% of established AI infrastructure development projects have been implemented.

According to 11 Responses

AI infrastructure initiatives



Where respondents described the types of infrastructure being developed or expanded, **compute infrastructure** such as HPC and supercomputers was the most common category (about 78%). This category covered national or research-grade computing for AI and scientific workloads. **Data platforms** were mentioned by about 22% and referred to enabling data environments such as regional AI data-center hubs, storage capacity, and data lakes. **International/shared compute access** was also cited by about 22%, typically through arrangements such as EuroHPC membership or access pathways that extend national compute capacity. **Innovation and R&D facilities,** mentioned by about 22%, included labs and test environments supporting startups, experimentation, and applied R&D.

The results indicate that many governments are prioritizing high-end computing capacity as the most visible bottleneck for AI development, particularly for research and advanced training workloads. At the same time, the lower and equally distributed reporting of data platforms, shared access arrangements, and innovation facilities indicates that enabling layers of the ecosystem are less consistently developed or, in some cases, less consistently documented. The reported implementation rate, suggests that infrastructure programs are often still in delivery and that a significant share of planned capability has not yet translated into operational capacity.

Types of Infrastructure

78% Infrastructure

22% Data Platforms

22% International/Shared Compute Acces

22% Innovation And R&D Facilitie

The audit results also show that infrastructure development is closely tied to cloud strategy. About 64% reported having a **national cloud** infrastructure, while about 36% did not. Separately, all respondents (100%) reported using **third-party providers** for cloud and computing purposes, reinforcing that national capacity is commonly complemented by external services.

Taken together, these results indicate that cloud-based delivery models are central to government AI even where national platforms exist, and that national cloud infrastructure is often one element within a wider hybrid environment. Universal reliance on third parties may improve speed and scalability, but it also increases the importance of clear governance for procurement, security assurance, and operational accountability in outsourced or shared environments.

AI infrastructure initiatives

64%

Have a national cloud infrastructure

100%

Rely on third-party providers for it

Across both national AI infrastructure and national cloud environments, reported compute resources were unevenly quantified and difficult to compare. Where capacity figures were provided for overall infrastructure, some responses cited detailed performance or scaling statements, while others relied on qualitative descriptions such as "thousands of processor cores" or referenced compute capacity without metrics. In the national cloud context, quantification was generally weaker.

Where figures were reported, they were typically expressed through aggregate indicators such as total CPU cores and RAM, while many responses described cloud architectures and service models without specifying available processing capacity. This limits cross-country comparability and makes it harder to assess whether available capacity matches national AI ambitions or is sufficient for public-sector needs.

Image is AI generated

Image is AI generated

Recommendation

To support effective planning and oversight of AI infrastructure, governments could establish a **compute capacity mapping and demand-forecasting framework** that provides decision-makers with a current, consolidated view of available resources - across national cloud, data centers/HPC, and contracted services - and how this capacity aligns with national priorities and ministry-level needs. Such a framework can link priority use cases to **indicative technical requirements** (for example, GPU/accelerator needs, storage, network throughput, security tier, and availability targets), improving awareness of the typical scale of resources required for activities such as model development and training, NLP, data platform operations, and reliable AI-enabled service delivery.

Governments should ensure **clear governance for hybrid environments,** defining how national cloud capabilities are complemented by third-party providers, including workload classification, security and compliance responsibilities, and ongoing monitoring of utilization, performance, cost, resilience, and supplier concentration risks.

In parallel, countries may benefit from balancing targeted investments in high-end compute with **structured public-private collaboration,** such as testbeds and controlled experimentation environments that enable public institutions to validate, procure, and scale AI solutions safely and effectively.

INFORMATION SECURITY

Information security is increasingly central to how governments can adopt AI in ways that are responsible, resilient, and trusted. As public institutions expand AI use in decision support and service delivery, they also expand the range of digital risks that can affect sensitive information, service continuity, and public confidence. Strong information security helps ensure that AI systems remain reliable under real-world conditions, including in the face of misuse, error, or malicious interference. It also provides the safeguards that allow strategic priorities to be implemented without creating unacceptable exposure to risks or undermining trust.

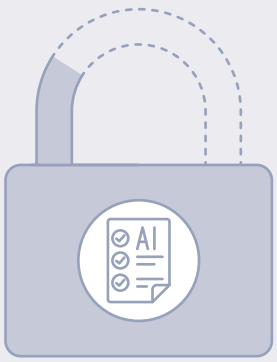
This chapter examines how governments are positioning information security and privacy within their AI efforts, with a primary focus on the risks and safeguards that shape real-world implementation. It briefly reviews whether baseline requirements are in place, and assesses the main information security risks governments associate with AI projects and the measures established to reduce them. The chapter also considers how incidents are detected, addressed, and used to strengthen controls over time.

Image is AI generated

FOUNDATIONAL SAFEGUARDS FOR SECURE AI

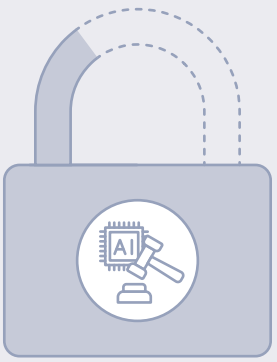
Baseline **cybersecurity** and **privacy** safeguards provide the minimum conditions for AI projects to be developed and operated consistently across government. When protocols, role-based training, and AI-relevant privacy requirements are clearly defined, institutions can apply common controls across the AI lifecycle, set consistent expectations for staff and suppliers, and reduce reliance on informal practices. Such baselines also support oversight by making responsibilities, required controls, and compliance expectations easier to verify, particularly where AI solutions are developed or operated with **third-party providers.**

Among respondents, only 30% reported that the government has mandatory **cybersecurity protocols** and **training** programs for personnel involved in AI projects. Similarly, only 40% indicated the existence of policies or regulations that specifically address **data privacy** concerns in AI applications.



30%

has mandatory cybersecurity protocols and training programs for personnel involved in AI projects.



40%

indicated the existence of AI data privacy policies or regulations.

Regarding **cybersecurity incidents,** five of six respondents reported zero incidents in the past year, while one respondent reported a single case involving a **denial of service** vulnerability in an **LLM** chat and attempted **prompt injection,** which was not deployed in production and was subsequently remediated.

According to 6 Responses

83%

reported zero cybersecurity incidents in the past year.

1

reported case involving a denial of service vulnerability in an LLM chat and attempted prompt injection.

Recommendation

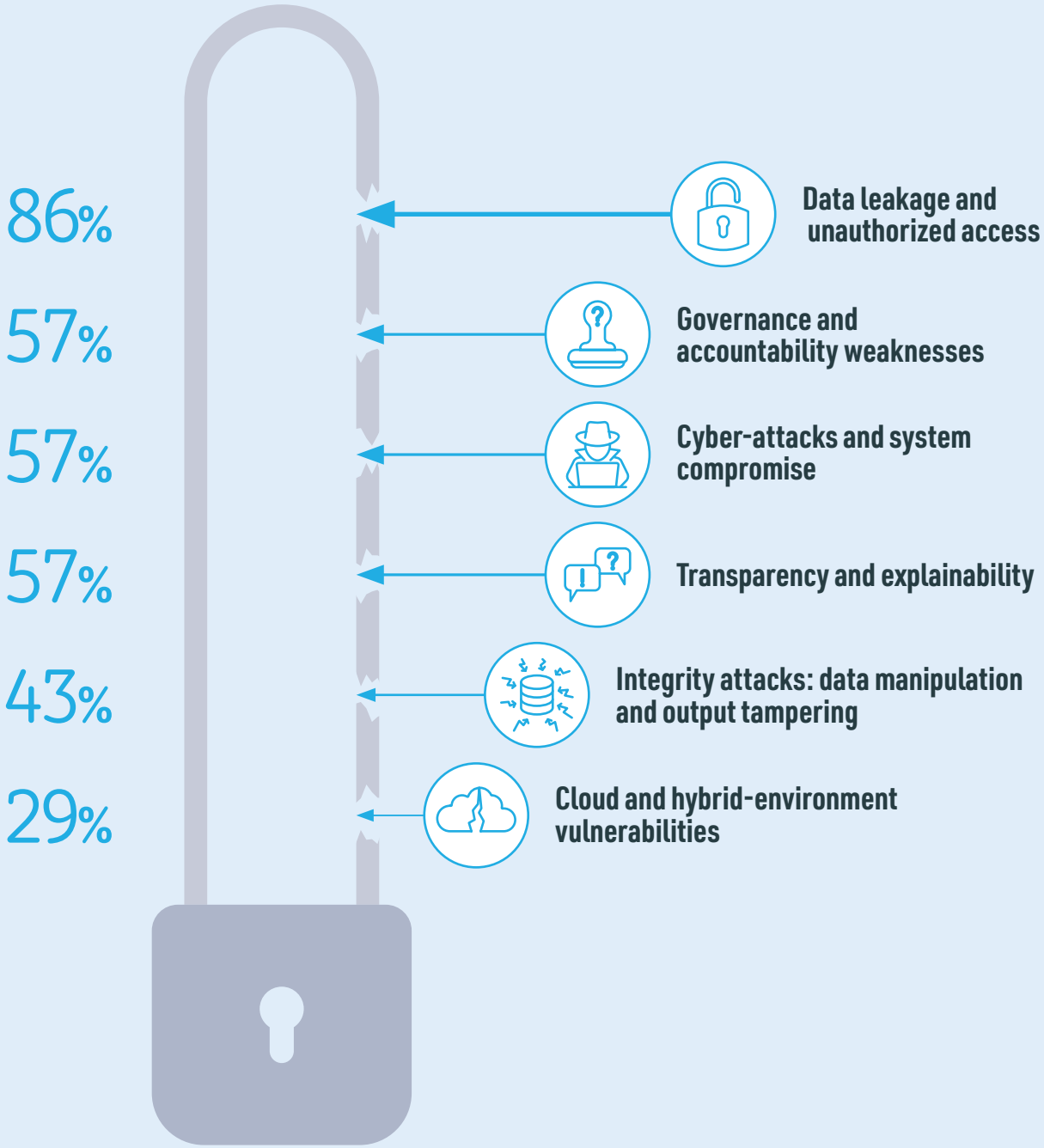
Countries may wish to consider setting a clear baseline of mandatory cybersecurity requirements and role-based training for personnel involved in AI projects, aligned with existing public sector frameworks. Strengthening governance could help define responsibilities and consistent expectations, including security testing, monitoring, and incident response. Clarifying AI-relevant privacy requirements within established data protection arrangements may further support consistent implementation and accountability.

TURNING AI RISKS INTO ENFORCEABLE SAFEGUARDS

AI can expand the reach and responsiveness of public services, but it also requires disciplined security practice to sustain trust and operational reliability. This subchapter provides context for assessing how governments identify information security and privacy risks in AI use and how they translate those risks into effective safeguards. It highlights the importance of addressing risks across the full lifecycle of AI systems, clarifying roles and responsibilities among involved actors, and ensuring that mitigation measures are measurable, auditable, and consistently applied. It also frames why this risk-to-control linkage matters for oversight, accountability, and continuous improvement as AI capabilities evolve.

AI-Related Security Risks

When asked about the main information security risks identified in government projects in the field of AI, the most frequently cited risk was **data leakage and unauthorized access** (86%), often linked to exposure or misuse of personal or sensitive data across training, processing, storage, and use. **Governance and accountability weaknesses** were also frequently cited (57%), reflected in unclear ownership of AI decisions, fragmented responsibilities, insufficient controls across the AI lifecycle, and skill gaps. **Cyber-attacks and broader system compromise** were cited at a similar rate (57%), including service disruption and data theft. **Transparency and explainability** gaps (57%) were highlighted as limiting traceability and assurance. Additional risks included **integrity threats such** as data manipulation and output tampering (43%), and vulnerabilities in **cloud** and **hybrid environments** (29%), including misconfiguration and shared-responsibility gaps.


86%
Data leakage and unauthorized access
57%
Governance and accountability weaknesses
57%
Cyber-attacks and system compromise
57%
Transparency and explainability
43%
Integrity attacks: data manipulation and output tampering
29%
Cloud and hybrid-environment vulnerabilities

The responses suggest that governments frame AI security as an end-to-end control challenge rather than a single technical issue. The prominence of **data exposure risks,** alongside repeated references to **governance and accountability weaknesses,** indicates that confidentiality concerns are closely linked to how responsibilities, access, and controls are managed across the AI lifecycle.

The simultaneous emphasis on **cyber-attacks and system compromise** implies that AI is largely understood as extending familiar ICT threat scenarios into new environments, often with added complexity from external components, accelerated iteration, and broader integration into service delivery. Concerns about limited **transparency, traceability, and explainability** highlight that assurance depends on the ability to understand and reconstruct how AI outputs were produced, especially when errors, anomalies, or incidents occur.

References to **integrity threats** and **cloud-hybrid** vulnerabilities further indicate awareness that manipulation, misconfiguration, and shared-responsibility gaps can undermine both model performance and operational reliability.

Regarding mitigation, responses most commonly emphasized **security engineering and technical controls** (57%), including sandboxed environments, network segmentation, encryption, access control, monitoring, and incident response measures. A smaller group highlighted **transparency and accountability** measures (43%), including traceability, disclosure duties where relevant, clear assignment of responsibilities, internal policies, and periodic risk or impact assessments. Fewer responses focused on **data protection and privacy** measures (29%), such as minimizing personal data use, purpose definition, retention rules, and privacy-enhancing techniques. Additional approaches mentioned with similar frequency (29%) included **lifecycle risk management** and operational assurance, meaningful **human oversight** to prevent over-reliance, and **organizational capability** building through training and internal expertise.

Ways to Reduce AI-Related Security Risks

57%

Security engineering and technical controls

43%

Transparency and accountability

29%

Risk management and operational assurance

29%

Human oversight and responsible use

29%

Data protection and privacy

29%

Organizational capability

The mitigation patterns suggest that respondents distinguish between controls that reduce immediate technical exposure and measures that make AI use governable over time. The greater emphasis on **technical safeguards** indicates a priority on containing attack surfaces, restricting risky functionality, and strengthening detection and response capabilities. At the same time, the recurring focus on **accountability,** traceability, and transparency reflects recognition that oversight depends on being able to evidence how systems operate, who is responsible, and how decisions can be reviewed when outcomes are contested or incidents occur. References to privacy-oriented measures and lifecycle risk management indicate movement toward preventive approaches that embed safeguards into design, procurement, and operations, rather than relying only on reactive security controls. The inclusion of human oversight and capability building further suggests that control effectiveness is shaped by institutional routines and skills, including how staff validate outputs, enforce procedures, and maintain controls throughout the system lifecycle.

This subchapter indicates that governments view AI security as **a combined technical and governance challenge** that must be managed across the full lifecycle of AI systems. The risks described extend from data exposure and service compromise to integrity threats and cloud-hybrid weaknesses, alongside recurring concerns about accountability and limited traceability. Mitigation approaches reflect a layered model that pairs technical controls and operational monitoring with institutional measures such as defined responsibilities, auditability, and risk-based assessments. Overall, the responses point to stronger assurance where technical safeguards are reinforced by clear governance arrangements that make AI use consistently manageable and reviewable across government.

Recommendation

To strengthen assurance over AI security risks, countries may wish to consider adopting an integrated lifecycle approach that links technical controls with clear **governance** and accountability. Establishing baseline requirements for secure design, testing, monitoring, and incident response could help reduce exposure to data leakage, system compromise, and integrity threats, including in **cloud** and hybrid settings. In parallel, strengthening **traceability** and documentation, including audit trails and defined decision rights, may improve the ability to investigate outcomes, learn from incidents, and enforce responsibilities across ministries and **third-party providers**. Targeted capability building and practical guidance for operational teams may further support consistent implementation and meaningful **human oversight** in routine use.

DIGITAL MATURITY

AI in government depends on high-quality, accessible data. When ministries cannot reliably find, access, trust, and legally reuse data across organizational boundaries, AI initiatives remains limited to pilots, delivers inconsistent outcomes, and introduce avoidable legal and security risks. Reliable AI applications - and even basic data-driven insights - also depend on data being cataloged, standardized, and maintained at sufficient quality so that datasets can be discovered, linked, and interpreted consistently across systems and agencies. In this chapter, **digital maturity is assessed primarily through data maturity:** how well governments govern, share, and reuse data as a common asset across ministries through shared direction, consistent rules, and platforms that enable secure access and trustworthy use, supported by quality data assurance over time. Strengthening these foundations also improves public services even before AI is introduced, by enabling more data-informed operations, faster learning from evidence, and more consistent delivery across agencies.

This chapter examines how governments are strengthening the data foundations that support digital maturity, focusing on the presence and direction of national data strategies, the design and practical functioning of cross-ministry data sharing arrangements, and barriers that limit effective exchange. To contextualize these findings, it references the **2025 Open Data Maturity (ODM)** assessment as an external benchmark - particularly the gap that can persist between publication and demonstrated impact. The chapter also reviews initiatives to consolidate data through government-wide data lakes, including expected benefits and implementation challenges that may affect sustainable reuse and AI-enabled delivery at scale.

Image is AI generated

DATA STRATEGY AND DATA SHARING FOUNDATIONS

A national data strategy and a workable data sharing framework are core instruments for turning data from fragmented administrative holdings into a reusable resource across government.

They set a common direction for how data should be catalogued, standardized, protected, and reused, and they clarify how ministries are expected to exchange information while meeting legal, privacy, and security obligations. Because cross-ministry sharing often involves multiple systems, competing mandates, and sensitive datasets, these instruments also function as coordination mechanisms - defining roles, decision rights, and the operational conditions that make reuse feasible.

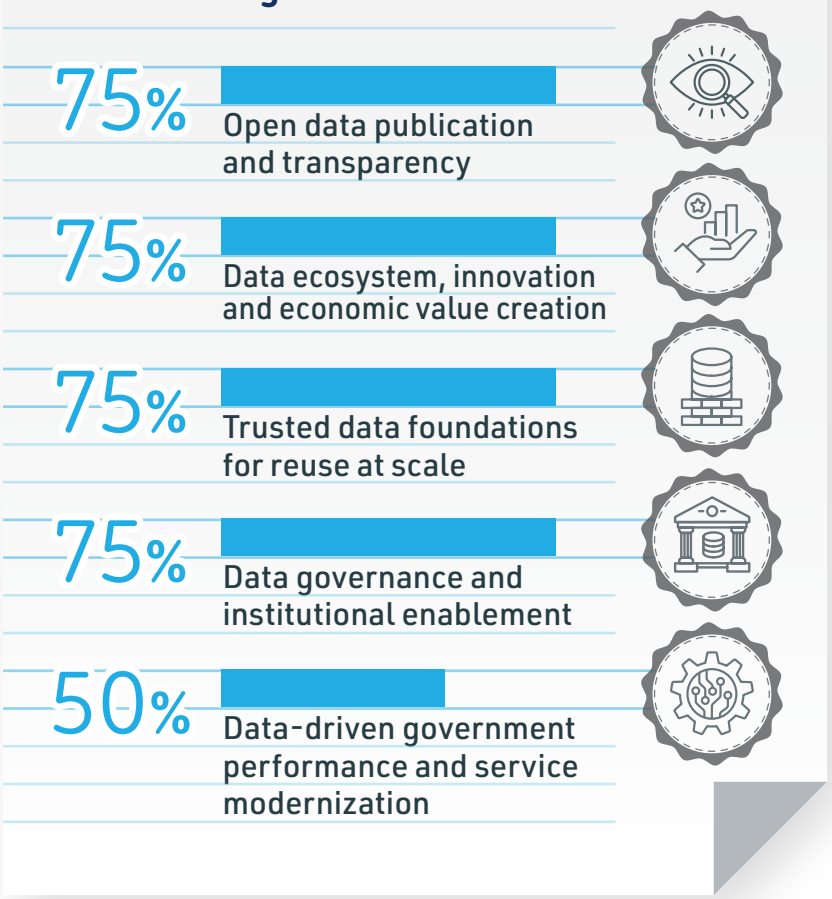
Regarding the existence of a governmental data strategy, 50% reported having a formal strategy in place. In the remaining cases, participants described decentralized or in-progress arrangements, such as ministry-led strategies, reliance on fragmented initiatives that involve quality, maturity and availability goals, or partial coverage through related instruments (e.g., legal requirements for open, machine-readable publication or standalone strategies for specific data domains).

50%

reported having a formal data strategy in place

Among respondents who described strategic priorities in detail, there was strong convergence around enabling themes. 75% referenced **open data publication and transparency,** including mechanisms to release datasets and improve access and reuse. The same share highlighted **data ecosystem development and innovation-oriented value creation,** including collaboration across stakeholders to stimulate new services and economic value. Responses also show that 75% prioritized **trusted data foundations for reuse at scale,** including interoperability, standardization, and improvements in data quality. In addition, 75% addressed **data governance and institutional enablement,** including legal frameworks, coordination arrangements, and capability building within government. By comparison, 50% referenced explicit objectives linked to **data-driven government performance and public service modernization,** including using data to improve services and strengthen decision-making.

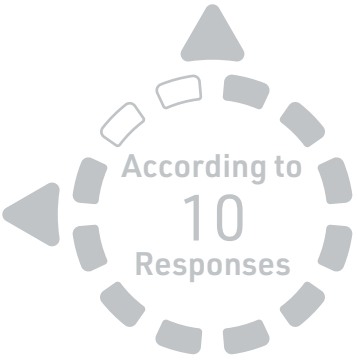
Key Objectives in Governmental Data Strategies



Overall, many strategies appear to focus first on building the conditions for sustainable data use - transparency, ecosystem growth, interoperability, and institutional capability - rather than directly anchoring data as a management tool for service outcomes. This sequencing is consistent with governments strengthening foundational layers before scaling advanced applications. At the same time, the lower emphasis on performance and service modernization may signal slower progress on measurement, operational integration, and service redesign, which can reduce the tangible public value that data reforms are expected to deliver.

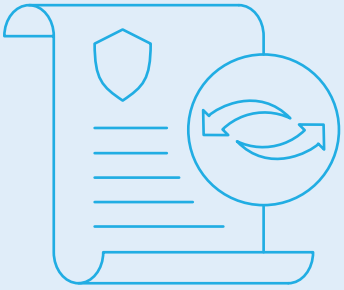
All respondents **(100%)** reported a formal policy defining conditions for data sharing between ministries. This suggests that governments generally recognize cross-government data exchange as a necessary function and have formalized baseline rules on authorization, handling requirements, and permissible exchange channels. However, the presence of a policy should not be equated with effective sharing in practice: implementation depends on interoperable systems, shared standards, workable approval processes, and clear governance and enforcement. In an AI context, gaps between policy and operational capacity can translate into slower access to quality data, inconsistent reuse, and higher delivery risk for cross-ministerial use cases.

Reported principles within data sharing policies are unevenly distributed across technical, legal, and accountability dimensions. **Interoperability and exchange channels** were the most frequently cited principle (45%), reflecting an emphasis on common technical approaches that enable system-to-system exchange across ministries. **Reuse, openness, and public value orientation** were cited by 36%, pointing to expectations that sharing should reduce duplication and support broader reuse and public value. The same share (36%) referenced **security and confidentiality safeguards,** focusing on protecting data during exchange and applying appropriate access controls. A further 36% highlighted **lawful and proportionate sharing,** stressing when sharing is permitted and how privacy and purpose limitations are applied. **Governance and traceability principles** were cited less often (27%), referring to oversight arrangements and the ability to document and audit data sharing activities.



Data Sharing Policy Principles

45%



Interoperability and exchange channels

36%

Reuse, openness and public value orientation

36%

Security and confidentiality safeguards

36%

Lawful and proportionate sharing

27%

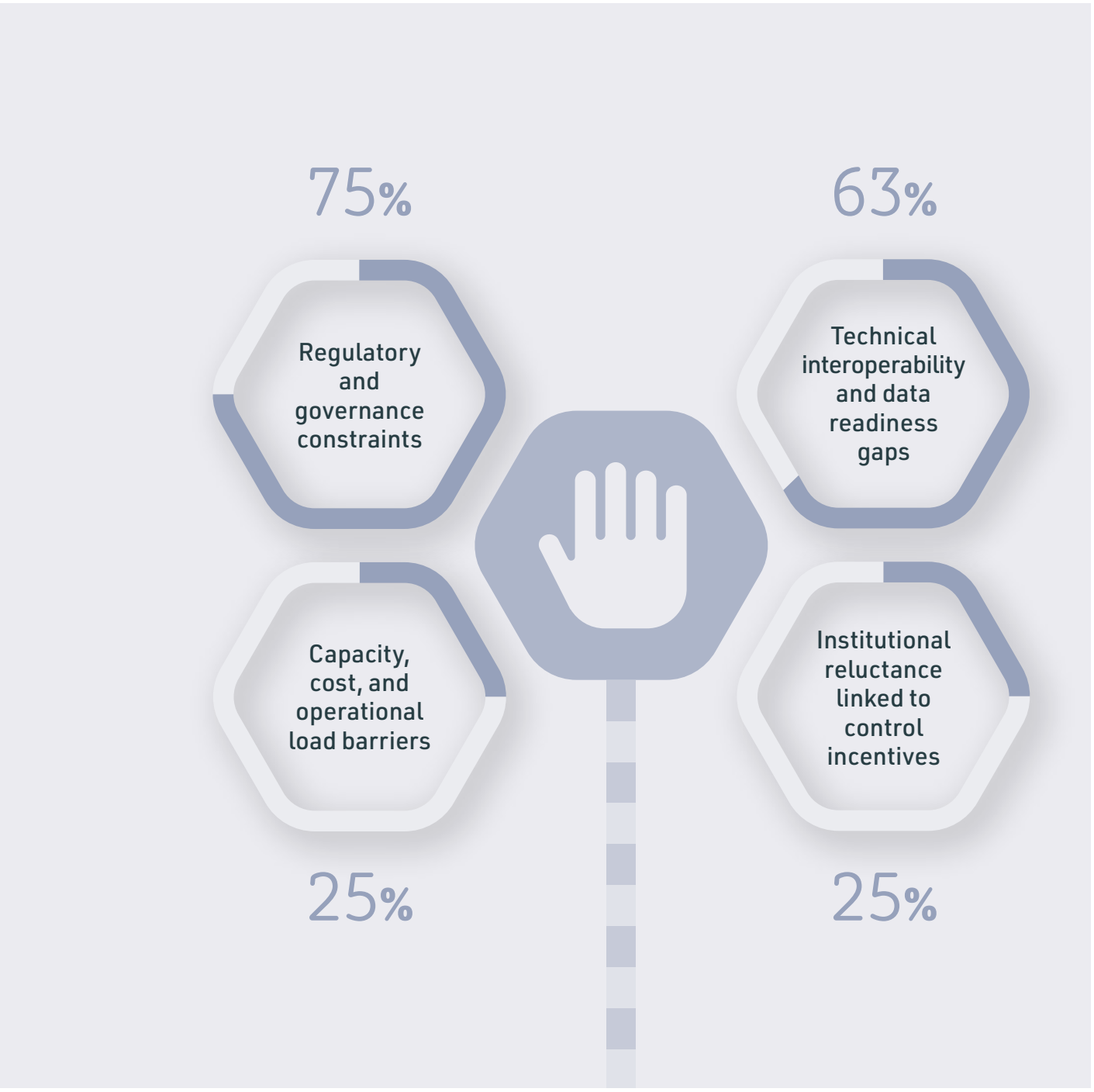
Governance and traceability

This profile suggests that many governments frame data sharing primarily as an operational and compliance challenge - balancing enablement through interoperability with safeguards for legality and security. The comparatively lower emphasis on governance and traceability indicates that accountability mechanisms (e.g., logging, auditability, quality management, and clear oversight roles) may be less consistently embedded as explicit design principles. Weak traceability can limit the ability to demonstrate lawful use, diagnose failures, and enforce responsibilities across ministries and suppliers.

What Prevents Ministries From Sharing Data?

When asked what prevents ministries from sharing data, responses indicate that the most common barriers relate to **regulatory and governance constraints,** reported by 75%. These included privacy-driven limitations, legal misalignment, lengthy approval processes, weak enforcement powers, and unclear oversight responsibilities. **Technical interoperability and data readiness gaps** were also prominent, reported by 63%, including fragmented legacy environments, incompatible technologies, limited integration with central platforms, and weak harmonization. **Capacity, cost, and operational load barriers** were reported by 25%, including limited budgets and personnel, gaps in technical expertise, and operational constraints where sharing creates additional system load or resource consumption that ministries cannot absorb. **Institutional reluctance linked to control incentives** was also reported by 25%.

Image is AI generated



These barriers indicate that improving data sharing typically requires coordinated action across **governance, legal design, and technical standardization,** not only additional funding. Even when cited less frequently, institutional reluctance and operational burden matter because they influence behaviour and can undermine cross-government reuse unless incentives, support, and accountability mechanisms are aligned.

Across the subchapter, a consistent theme is the gap that can emerge between strategic intent and operational execution: where national direction is fragmented, ministries may develop parallel approaches that weaken coherence, slow standardization, and limit reuse at scale, while even strong formal frameworks may remain procedural if accountability, incentives, and technical readiness are uneven.

A second cross-cutting insight is that many approaches emphasize foundational enablers and compliance, but do not always embed **governance** mechanisms that make sharing demonstrable, auditable, and enforceable, particularly through **traceability** and clear responsibilities across institutions and suppliers.

For AI and data-driven services, these gaps can translate into uneven access to high-quality data, higher delivery risk for cross-ministry use cases, and greater exposure to legal, privacy, and security disputes when roles and controls are not fully operationalized.

Image is AI generated

Recommendation

Governments may wish to consider strengthening the alignment between strategic direction and implementation by consolidating fragmented approaches into a shared data strategy or roadmap that links foundational reforms to measurable service outcomes.

Strengthening governance could help by clarifying decision rights, accountability for data quality and reuse, and the enforcement or escalation paths needed when sharing obligations are not met. In parallel, investing in interoperable standards, sustainable data quality practices, and streamlined approval processes may reduce structural friction, while improved traceability and auditability can support lawful sharing, build trust, and reduce risk as AI-enabled services scale across ministries.

2025 OPEN DATA MATURITY ASSESSMENT

Digital maturity can also be assessed through external benchmarks that reflect how consistently governments translate policy intent into usable, trusted data in practice. The **Open Data Maturity (ODM) 2025** assessment[13], published via the EU's official data portal[14], provides a relevant reference point because it evaluates how European countries make public-sector information available and stimulate reuse across four dimensions - **policy, portal, quality,** and **impact** - which align with the institutional and operational capabilities that supports cross-ministry data reuse[15].

In the 2025 ODM clustering, the countries included in this audit group demonstrate a broad spectrum of digital maturity and developmental progress. Some of them - **Estonia, France, Italy, Lithuania, Poland,** and **Slovakia** - exhibit more advanced practices and consistent performance. **Latvia** shows steady and dynamic progress, while **Romania** and **Switzerland** reflect a consolidated pace of development with room for further enhancement. **Albania** and **North Macedonia** are in the process of strengthening and refining their systems, making notable steps toward establishing core capacities and processes.

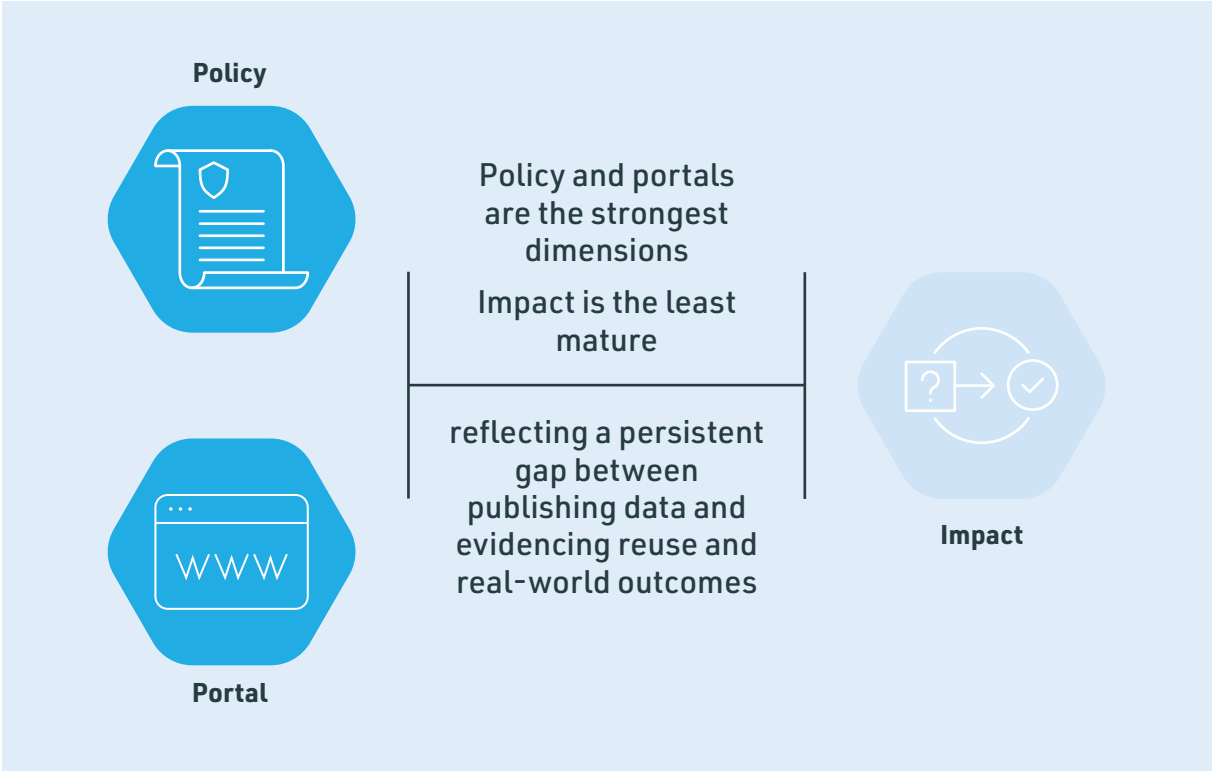
This distribution covers the full range of maturity and creates a practical reservoir of approaches that can support peer learning within the group.

13 The open data maturity (ODM) assessment is an annual exercise conducted to measure the progress of European countries in promoting and facilitating the availability and reuse of public sector information. https://data.europa.eu/en/open-data-maturity/2025#open-data-in-europe-2025

14 The European Data Portal is an initiative of the European Commission and is the official portal for European data. https://data.europa.eu/en

15 Israel is not included in the ODM 2025 assessment scope; therefore, the benchmark comparison reflects only the European participants.

The 2025 results show that, on average, **policy and portals** are the strongest dimensions, while **impact** is the least mature - even among otherwise high-performing countries - reflecting a persistent gap between publishing data and **evidencing reuse and real-world outcomes**. The assessment explicitly describes a "two-speed reality" on impact, highlighting a recurring gap between publishing data and systematically demonstrating reuse and real-world outcomes, pointing to a shared audit opportunity around measurement, accountability, and how governments evidence value, not only how they establish rules and platforms.



Finally, the assessment indicates that maturity can improve quickly when reforms are targeted: **Albania** is highlighted as a major improver, driven largely by portal and quality upgrades. This suggests that, at earlier stages of maturity, even relatively modest and well-focused improvements can translate into noticeable gains when governance, portal functionality, and structured quality processes are strengthened together - but that such gains may represent progress within the "beginner" tier rather than a shift beyond it, which typically requires broader and deeper reforms. This reinforces that digital maturity is not only a long-cycle infrastructure effort, but can shift materially when operating practices are clarified and implementation is managed as a continuous capability rather than a one-time publication exercise.

DATA LAKE

A government-wide data lake is typically intended to consolidate datasets from multiple ministries into a shared environment that supports analytics, secure reuse, and advanced applications, including AI. Unlike point-to-point exchanges, a data lake approach can enable faster discovery and combination of datasets, but it also concentrates responsibilities for access control, stewardship, and lawful processing. As a result, successful implementation depends not only on infrastructure and architecture choices, but also on clear governance, privacy safeguards, and operating models that ministries can adopt consistently. This subchapter examines how governments are approaching these initiatives and what they expect to gain or manage.

Regarding whether there are initiatives to build a governmental **data lake,** 60% reported such initiatives. The remaining participants did not report an active initiative, suggesting that data consolidation is still developing unevenly across governments and may be pursued through alternative approaches, such as distributed interoperability arrangements, sectoral platforms, or incremental modernization of existing data environments rather than a single shared lake. Differences in institutional readiness, capacity, and tolerance for centralization likely shape whether governments pursue a shared lake or maintain more federated approaches.

Image is AI generated

On anticipated benefits and challenges, responses indicate that the most frequently cited benefit, reported by 60%, relates to strengthening **data-driven government,** including better analytics and decision-making from consolidating data, added value from combining datasets, and easier retrieval and reuse across government. Benefits linked to **service delivery** and **citizen outcomes** were reported by 40%, including faster and more automated services, reduced paperwork and improved crisis responsiveness. The same share cited **openness** and **transparency** benefits, including stronger accountability, open data enablement, and reuse by external actors such as businesses. A smaller share, 20%, emphasized **data quality** benefits, including added controls and stewardship to improve reliability of shared data.

Reported challenges clustered around four areas. **Adoption and data maturity barriers** were cited by 40%, including resistance to institutional change, uneven data opening across domains, limited engagement in reuse, and low open data maturity that reduces uptake and value. **Governance and legal-policy readiness** challenges were also cited by 40%, including unclear ownership and processing responsibilities and missing or unclear frameworks for data sharing, privacy, and lawful processing. **Capacity and resource constraints** were reported by 40%, reflecting the technical complexity of delivery, infrastructure costs, staff training needs, and in some cases reduced organizational capacity linked to budget consolidation. **Cybersecurity risk** was cited by 20%, highlighting increased exposure and the need to secure a complex, inter-institutional environment.

According to
5
Responses

Image is AI generated

Data Lake Benefits

60%
strengthening
data-driven government

40%
openness
and transparency

40%
service delivery
and citizen outcomes

20%
data quality benefits

Data Lake Challenges

40%
Adoption
and data maturity barriers

40%
Governance
and legal-policy
readiness

40%
Capacity
and resource
constraints

20%
Cybersecurity risk

Taken together, responses indicate that governments primarily view a data lake as a platform for higher-value data use and AI-enabled analytics, with additional expectations related to service outcomes and transparency. However, they also recognize that the most significant risks stem from readiness and operating conditions, not technology alone. The expected value depends on aligning technical consolidation with sustained institutional adoption and governance that makes sharing routine—supported by clear rules for lawful processing, accountability, and adequate skills and funding. These dependencies mirror the broader barriers identified in cross-ministry sharing: regulatory friction, unclear responsibilities, fragmented legacy systems, and uneven interoperability can prevent ministries from contributing data consistently or reusing shared assets at scale. Where such constraints persist, a data lake may remain underused, be difficult to sustain, or create heightened legal and cybersecurity exposure as consolidation increases systemic risk.

Recommendation

To support effective implementation, governments could define a clear purpose and operating model for a governmental data lake before scaling, including how datasets are onboarded, governed, and accessed across ministries. Strengthening governance and legal-policy readiness could help clarify ownership, processing responsibilities, and privacy conditions, while embedding data quality stewardship may improve trust and reuse.

Governments could also consider a phased approach that links investment to priority cross-government use cases, alongside targeted capacity building and cybersecurity assurance for the shared environment, so that consolidation increases value without creating disproportionate risk or operational burden.

CONCLUSIONS

The chapter indicates that digital maturity is shaped less by the existence of individual instruments and more by how well strategy, sharing rules, and operational capabilities align in practice. Common patterns point to a strong emphasis on foundational enablers, while persistent friction around governance clarity, interoperability, and legal-process complexity can slow reuse and limit cross-government delivery. The external benchmark reinforces that progress on policy and platforms does not automatically translate into measurable impact, highlighting the importance of accountability for outcomes and evidence of reuse. Data lake initiatives reflect similar dependencies, suggesting that consolidation can amplify value only when ministries can contribute data consistently under clear operating rules, supported by sustained capacity and safeguards.

Image is AI generated

GOVERNMENTAL PROJECTS

Governmental AI is increasingly taking shape through concrete projects that translate policy ambitions into real services, operational tools, and measurable results across ministries. The way governments steer AI projects shapes outcomes over time, affecting delivery, accountability, and long-term value. For this broad and fast-evolving technology, a whole-of-government view of applications is also important to support reuse across ministries - enabling shared components, more consistent approaches to governance and controls, and more efficient scaling of solutions that address common administrative needs.

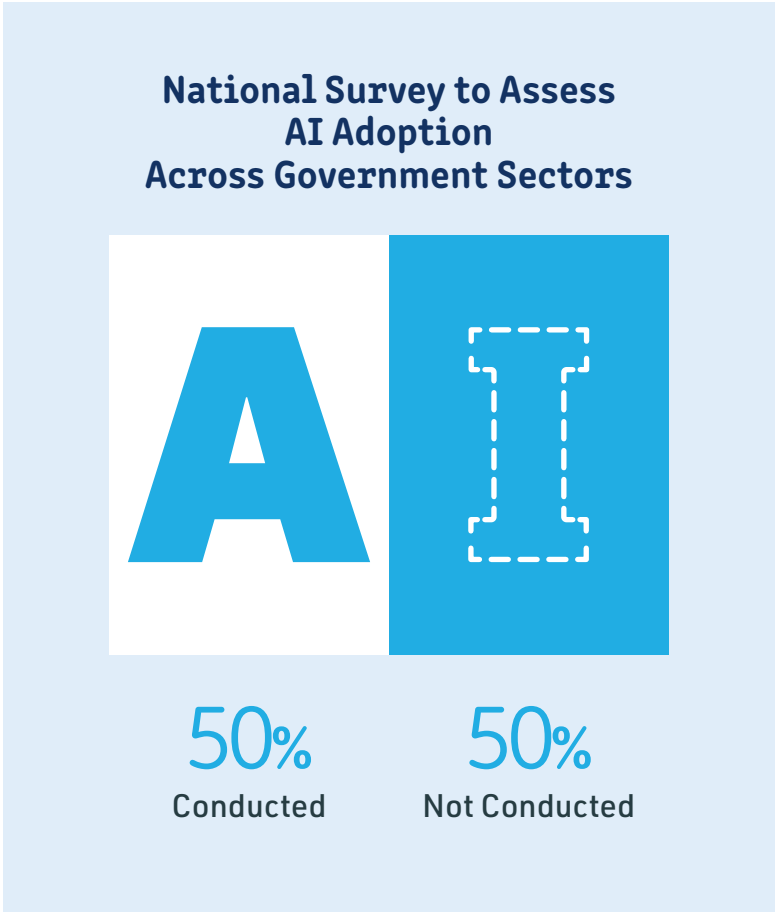
This chapter examines how governments report AI adoption in practice and how they assess its results. It reviews whether governments have a whole-of-government view of AI adoption, how implementation is distributed across government sectors, and which AI use cases are most commonly reported as improving efficiency or service delivery. The chapter also examines how governments evaluate effectiveness in practice by reviewing whether monitoring and evaluation mechanisms exist, which indicators are used to measure performance, and how governments describe observed productivity gains, including the main ways those gains are manifested in operations and service delivery.

Image is AI generated

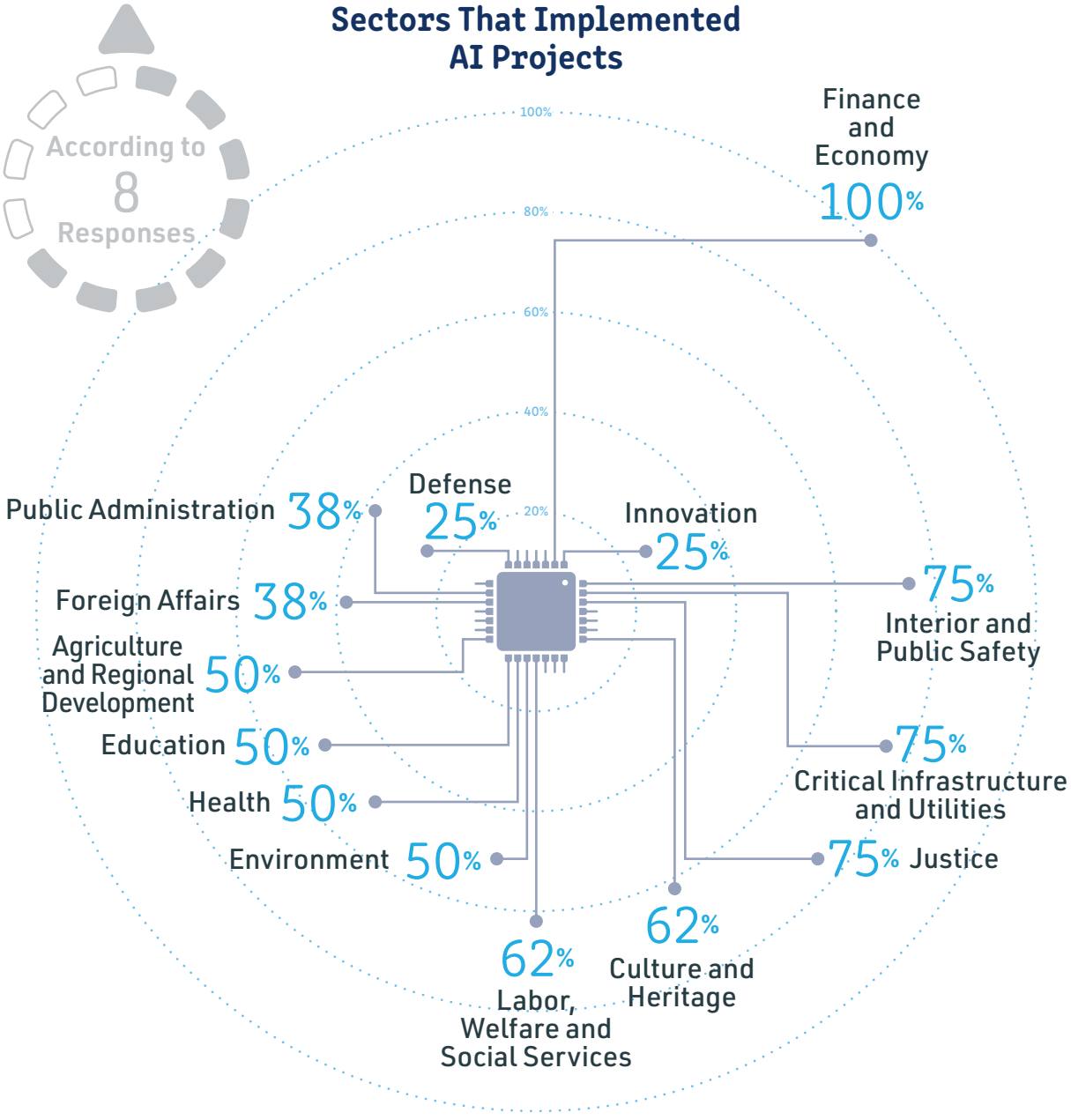
AI IN PRACTICE

AI adoption in government is increasingly distributed across multiple sectors, creating a need for a whole-of-government view of where implementation is occurring and how activity is spreading over time. Sector-level visibility supports strategic prioritization, coordination across ministries, and more credible oversight as AI projects move from pilots to operational services. It also helps identify concentration risks, gaps in coverage, and opportunities to reuse approaches across similar functions. This subchapter frames governmental AI adoption through a sectoral lens, focusing on how governments map adoption across sectors and what the distribution of implementation suggests for portfolio governance and scalability.

50% of governments reported conducting a national survey to assess AI adoption across government sectors, while 50% indicated they have not conducted such a survey. Where surveys were conducted, they represent an explicit attempt to establish an adoption baseline across sectors. This split indicates that portfolio visibility practices are not yet uniform across participating governments, which may affect the ability to track coverage, identify gaps, and align oversight arrangements with the scope of adoption.



When asked which sectors have implemented AI projects or are in the process of implementing them, **finance and economy** were identified by 100% of responders. A second cluster was reported by 75%: **interior and public safety, critical infrastructure and utilities** (e.g. transport, logistics, energy and construction), and **justice.** A further group was cited by 62%: **culture and heritage, labor, welfare, social services and environment. Health, Agriculture and regional development** and **education** were each reported by 50% of responders. Lower coverage was noted for **public administration** and **foreign affairs,** each cited by 38%, while the least frequently reported sectors were **innovation** and **defense,** each identified by 25%.



These responses indicate uneven whole-of-government readiness to manage AI as a coherent portfolio. Governments that established a national survey baseline are better positioned to monitor adoption consistently, support prioritization, and strengthen oversight as projects scale. Where no survey exists, portfolio visibility and comparability across sectors are more limited.
The concentration of AI projects in **finance and economy,** alongside strong coverage in **public safety, critical infrastructure,** and **justice,** indicates that implementation is most consistently present in **operational and risk-sensitive domains** where governments manage high-volume processes and compliance-oriented functions. In contrast, lower coverage in **public administration, foreign affairs, innovation,** and **defense** suggests that adoption is less consistently embedded in **horizontal and strategic domains** that can enable enterprise-wide reuse, standardization, and coordinated scaling. Operationally, this distribution increases the importance of cross-government controls and coordination to reduce fragmentation as AI expands.

Recommendation

Governments should consider establishing a consistent mechanism to map and periodically update AI adoption across sectors, supported by common definitions and minimum reporting expectations that enable comparability over time. Where adoption is concentrated in operational and risk-sensitive sectors, oversight arrangements may need to ensure that performance, accountability, and control requirements are applied consistently across ministries. Where adoption is weaker in horizontal and strategic domains, governments may benefit from clarifying how enabling functions - such as common standards, shared components, and cross-government coordination - will support coherent scaling and reduce fragmentation as sector-level activity expands.

GOVERNMENTAL USE CASES

AI is increasingly showing up in government not as a single program, but as a growing set of concrete use cases embedded in everyday work and service delivery. Mapping these use cases helps clarify what governments are prioritizing, which capabilities are being applied broadly across ministries, and where adoption remains specialized or localized. Use case patterns also matter for governance because different application types imply different requirements for data quality, integration, accountability, and controls, particularly where systems interact directly with citizens or support compliance and formal decision-support processes. This subchapter frames the operational landscape of AI in government by describing the main use cases reported across participating governments.

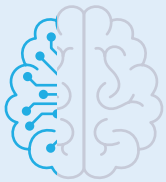
When identifying notable AI applications associated with improved efficiency or service delivery, the most commonly reported examples were cross-cutting capabilities. 67% cited **citizen service and internal support via virtual assistants,** covering front-office question answering and request triage alongside back-office support for HR, knowledge management, and routine staff inquiries. The same share cited **document** and **text processing,** such as translation, format-preserving conversion, classification and tagging, and search or chat over document repositories. In addition, 50% reported **finance, tax, customs,** and **market supervision** use cases, including tax compliance, fraud or anomaly detection, customs and border trade processing, and financial market analysis and manipulation detection. The same share noted **justice** and **courts applications,** including transcription, legal research and summarization, anonymization for publication, and justice-related regulatory oversight.

Notable AI Applications[16]

67%
Virtual Assistants

67%
Document and Text Processing

33%
Cybersecurity and Threat Detection



33%
Data Analysis

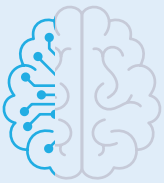
A further set of applications was reported less consistently across governments. 33% mentioned **mapping, imagery,** and **geospatial work,** such as national mapping production, 3D mapping, and interpretation of aerial or remote-sensing imagery. The same share cited **health** and **social security service delivery,** including streamlining administrative benefit or health processes and public health analytics such as tracking or forecasting disease spread patterns. 33% also identified **cybersecurity**

50%

Finance, Tax, Customs, And Market Supervision

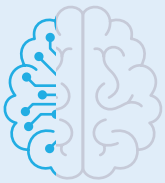
50%

Justice and Courts



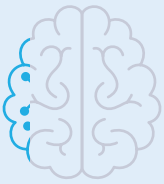
33%

Mapping, Imagery, And Geospatial



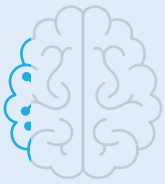
33%

Health and Social Security



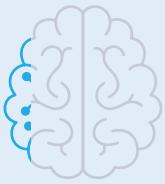
17%

Environment, Climate, And Bio-Monitoring



17%

Transport and Mobility



17%

Communications

and **threat detection,** including triaging alerts or signatures and identifying attack patterns, and 33% referenced **data analysis** as a notable application category. Less frequently, 17% cited **environment, climate,** and **bio-monitoring applications,** including biological sampling analytics (for example pollen); 17% cited **transport** and **mobility applications** for managing traffic, congestion, and transport system operations to improve flow and service performance; and 17% cited **communications regulation** and **radio spectrum applications** for monitoring and managing, including detecting interference and supporting regulatory enforcement.

16 See examples of projects by country in appendix E on page 267.

Overall, the distribution of reported examples indicates that efficiency and service gains are most commonly associated with cross-cutting capabilities that can be deployed broadly across ministries, particularly **virtual assistance** and **document-intensive processing.**
The prominence of **finance** and **justice applications** indicates use in high-impact functions tied to compliance, enforcement, and formal decision-support workflows, where traceability and appropriate controls are material to public trust.
The smaller set of examples in **health, cybersecurity,** and **geospatial work** indicates more uneven diffusion into specialized operational domains that may require more tailored data and integration. Isolated cases in **transport** and **mobility, environment** and **bio-monitoring,** and **communications regulation and radio spectrum** suggest localized adoption rather than consistent portfolio-level coverage.

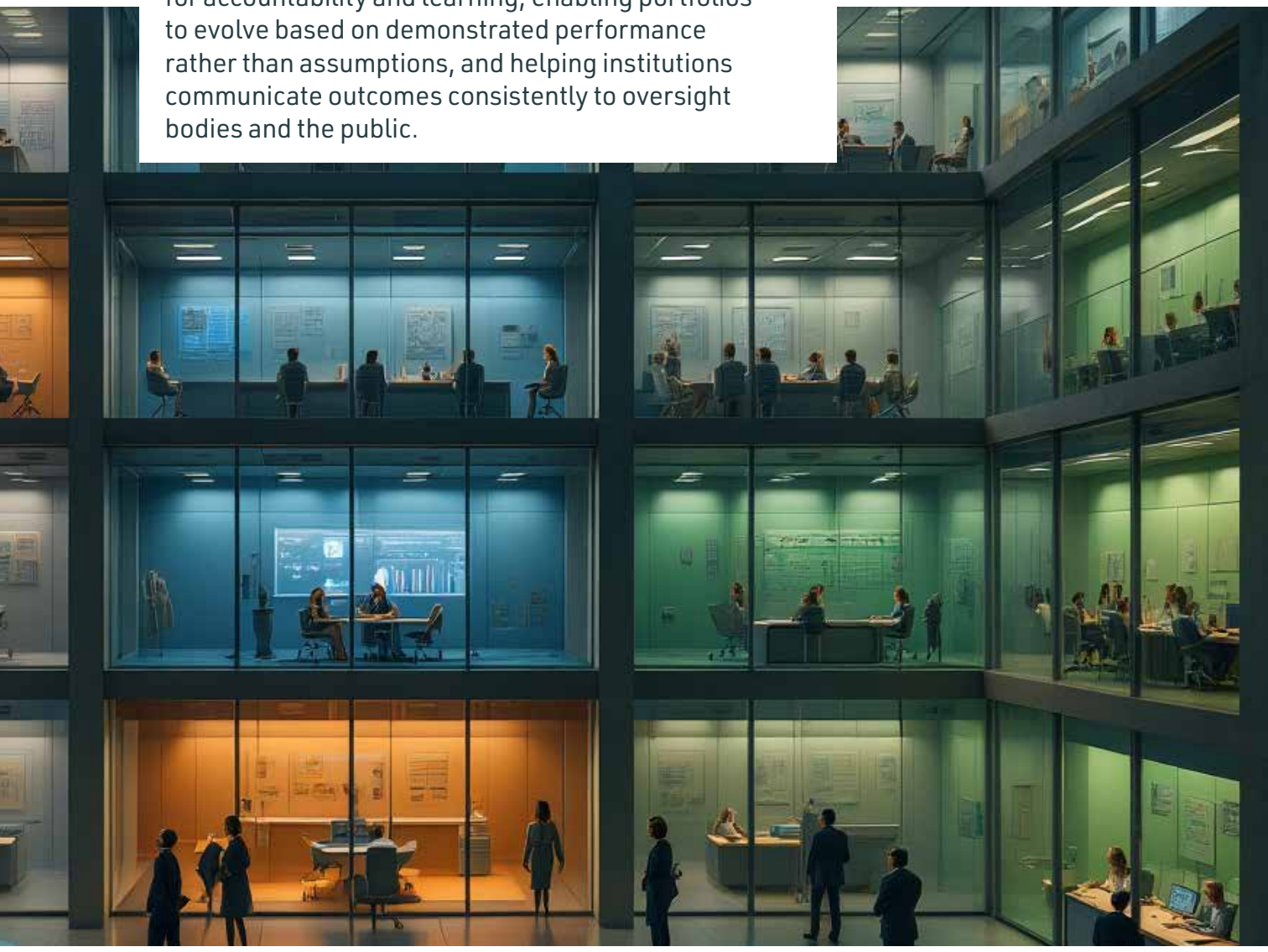
Recommendation

Governments should consider structuring AI portfolios around clearly defined use case categories, with minimum documentation and control expectations tailored to the risk and operational context of each category. Cross-cutting tools that are deployed broadly across ministries may benefit from standardized performance reporting, reusable components, and common assurance practices to support consistent scaling. For specialized and higher-impact domains, governments may benefit from clearer requirements on data readiness, integration, traceability, and oversight to ensure that efficiency gains do not come at the expense of reliability, accountability, or public trust, and that localized deployments can be assessed for reuse where appropriate.


Image is AI generated

EVALUATING IMPACT

Across governments, AI projects increasingly compete for attention, funding, and institutional capacity alongside other modernization priorities, making credible evidence on results a central input to governance. Impact evaluation helps decision-makers distinguish between tools that deliver measurable value and those that remain experimental, while also supporting transparency over trade-offs that may arise in accuracy, service quality, or risk exposure. As AI systems scale from pilots to operational use, evaluation practices become a practical safeguard for accountability and learning, enabling portfolios to evolve based on demonstrated performance rather than assumptions, and helping institutions communicate outcomes consistently to oversight bodies and the public.

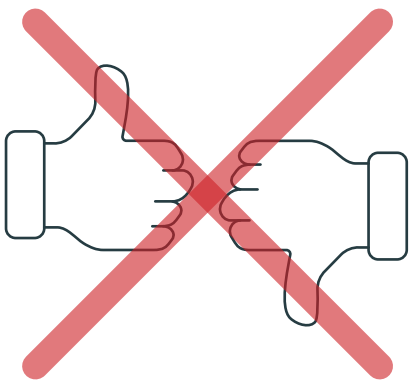


Regarding the monitoring and evaluation of AI project outcomes, **44% reported having mechanisms in place to assess impact and effectiveness,** while 56% indicated they do not.

This suggests that impact evaluation is not yet consistently embedded in project governance, which can reduce visibility over whether AI projects achieve intended results, limit organizational learning across the portfolio, and weaken the evidence base for decisions to scale, modify, or discontinue projects.

When asked which indicators (KPIs) are used to evaluate the effectiveness of AI projects, 83% of governments identified **productivity, workload,** and **resource efficiency measures,** such as productivity gains, time saved, reduced staff effort, and efficient use of budgets, technology, and human resources. 50% cited **usage, adoption,** and **interaction volume,** including uptake rates and activity measures

According to
6
Responses



56%

reported not having mechanisms to assess impact and effectiveness of AI project outcomes

83%

, Workload, and Resource Efficiency

33%

Operational and Technical Readiness

such as interactions, transactions, records processed, or repeat contacts. 33% reported **user experience** and **satisfaction indicators, service quality** and **timeliness measures** (including waiting and response times), **operational or technical readiness** (including integration, approvals, and running costs), and **accuracy or model performance** (including error rates, false positives and negatives, automation rates, and processing performance). Less frequently, 17% referenced **delivery, schedule,** and **sustainability indicators,** including meeting planned goals and timelines, sustained impact after completion, post-delivery iterations, and reuse or scaling across institutions, and 17% cited **security indicators** related to safeguarding systems and data.

KPIs for AI Projects

50%
Adoption

33%
User Experience

33%
Service Quality

33%
Model Performance

17%
Delivery, Schedule, and Sustainability

17%
Security

The reported indicator mix suggests that evaluation practices prioritize **internal efficiency** and **throughput,** while measures linked to **user value, service performance,** and **model quality** are applied less consistently. **Adoption and usage measures** indicate attention to whether solutions are used in practice, but the uneven reporting of **readiness** and **accuracy measures** suggests variable assurance over performance in real operating conditions. Limited emphasis on **sustainability, reuse,** and **security indicators** may constrain governments' ability to assess whether impacts persist, whether practices can be replicated across institutions, and whether projects maintain an appropriate risk posture as they scale.

Regarding whether productivity gains have been observed from implementing AI systems in the public sector or ministry-wide, **78% reported gains, 11% reported no gains, and 11% reported partial gains** (some ministries indicated that productivity increased in certain areas, while others reported no clear change). This distribution suggests that productivity improvement is a commonly reported outcome, but results are not uniform, indicating the need for structured evaluation to distinguish where gains are sustained and scalable from where impacts remain limited or mixed.

78%

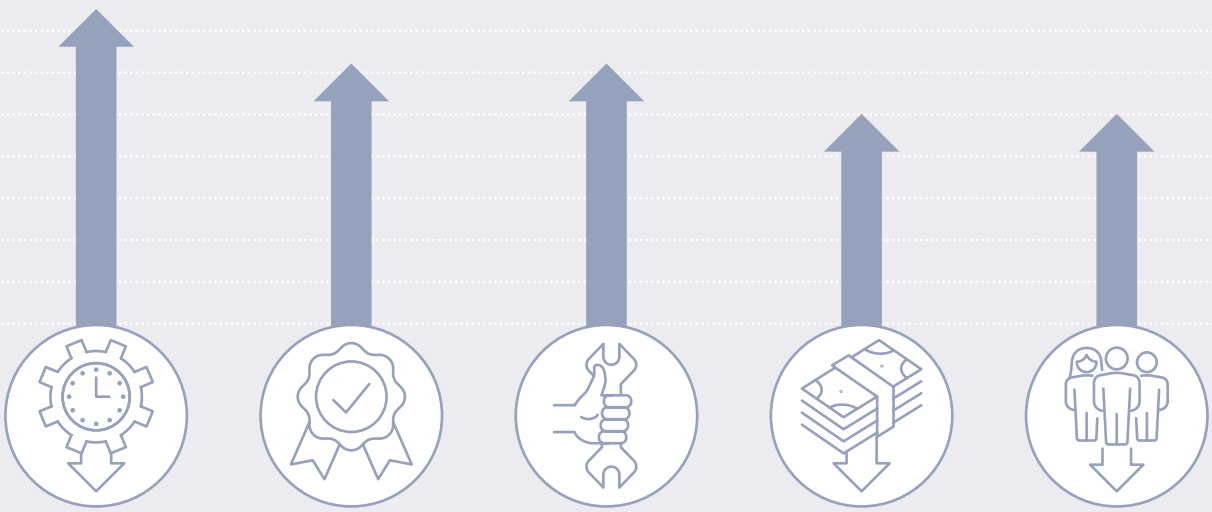
reported productivity gains have been observed from implementing AI systems

Image is AI generated

When asked about the nature of observed productivity gains, 75% reported time and workload reduction, referring to faster completion of tasks, reduced routine work, fewer manual steps, and faster analysis and review cycles. 62% cited quality improvement in outputs and decisions, referring to higher-quality work products, greater analytical precision, fewer errors, and better outcomes.

The same share (62%) reported service delivery improvements, including faster service provision, improved availability (including 24/7 services), and higher customer satisfaction. Together, the most common gains were described in terms of operational throughput, output quality, and service performance.

Nature Of Observed Productivity Gains



50% reported cost savings and efficiency gains, referring to reduced costs and broader efficiency, sometimes quantified as budget savings, including one quantified example of €20.4 million in 2022 with an expectation of €60 million in 2024 in that area. 50% also reported HR-related gains, referring to shifting staff from routine tasks to higher value-added missions, reallocating tasks without necessarily reducing headcount, and delivering higher activity volumes with the same capacity. Less frequently, 37% cited reduced bureaucracy, referring to simplified workflows and fewer physical or paperwork-like actions, while 25% cited gains in fraud prevention and compliance support, better data utilization and availability, and proactive alerting and crisis preparedness.

According to 9 Responses

37% Reduced bureaucracy

25% Fraud prevention

25% Better data utilization and availability

25% Proactive alerting & crisis management

The reported gain profile indicates that governments most frequently associate AI-related productivity with **broadly applicable operational improvements,** which can support scaling when objectives and measurement are defined consistently across projects. The presence of **cost and HR-related gains** highlights the importance of documenting savings and workforce reallocation in a way that supports value-for-money assessment and accountability. Lower-frequency gains linked to **enforcement, data advantage,** and **preparedness** suggest that some projects target higher-impact functions that may carry elevated governance and assurance needs, reinforcing the case for evaluation approaches that address both value and risk across the portfolio.

Recommendation

Governments should consider establishing a consistent evaluation approach for AI projects that links objectives to a balanced set of indicators across efficiency, service performance, quality, adoption, and risk. Where productivity gains are a stated outcome, evaluation practices could more explicitly document how gains are measured, whether they persist over time, and how workforce and budget effects are captured in ways that support value-for-money assessment. At the portfolio level, governments may benefit from standardizing minimum reporting expectations for operational readiness, model performance, sustainability, and security so that scaling decisions are based on comparable evidence and risk remains visible as projects expand across sectors.

CONCLUSIONS

Taken together, the patterns suggest that governments are translating AI ambitions into operational projects, but the conditions for coherent scaling are uneven. Sectoral concentration indicates that AI is being prioritized where governments expect immediate operational impact, such as finance and economy functions and other operationally intensive domains like public safety, critical infrastructure, and justice.

By contrast, weaker presence in horizontal and strategic domains, such as public administration, foreign affairs, innovation, and defense, implies a more limited capacity to standardize approaches and reuse solutions across ministries.

The prominence of cross-cutting use cases, such as virtual assistants and document and text processing, further indicates that value is increasingly tied to capabilities that could be shared, elevating the importance of portfolio-level coordination to reduce duplication and apply controls consistently.

Across governments, implementation appears to be advancing faster than the ability to demonstrate results in a comparable and decision-useful way. Where monitoring and evaluation practices are limited or uneven, decision-makers have less assurance on which projects deliver sustained value, which require redesign, and which should not scale.

The emphasis on efficiency-oriented measures and commonly reported productivity gains indicates that governments are primarily framing success in terms of operational performance, while less consistent attention to sustainability, reuse, and security can leave longer-term value and risk management less visible.

Overall, the findings suggest that stronger, more consistent evaluation approaches are central to scaling AI responsibly while maintaining public trust.

HUMAN CAPITAL

Human capital is where AI ambitions become operational reality. Even well-designed government strategies can stall if institutions cannot attract, develop, and retain the skills needed to build, supervise, and responsibly use AI in everyday work. In this sense, talent is not only a workforce issue - it is a delivery and governance condition that shapes whether AI can be scaled safely and consistently. It also links to the broader audit picture: strategic direction, infrastructural readiness, and implementation arrangements can enable AI adoption, but skilled people ultimately determine what is delivered, controlled, and sustained over time.

This chapter examines how governments are preparing their human capital for AI adoption and oversight. It reviews how skills needs are assessed, how education and workforce development are used to build capability, and how implementation is supported through enablement structures and knowledge-sharing. It also considers approaches to staffing and retention of critical roles, and how these arrangements affect scalability, consistency of practice, and risk management as AI use expands.

Image is AI generated

TALENT GAP

Governments rely on a steady supply of skilled practitioners to design, procure, operate, and oversee AI systems, while research capacity supports evidence-based development and adaptation to national needs. Education systems shape whether AI skills remain confined to a narrow specialist pipeline or become a broad workforce foundation across disciplines and sectors. As AI becomes increasingly embedded in new technologies and services, early and continuous education can help establish practical literacy and responsible-use habits from a young age, supporting long-term readiness for changes in how public services and work are delivered.

In examining industry capacity, **100% reported a shortage of AI experts,** framing it as a broad constraint on access to specialized practitioners across sectors. This uniform finding suggests a shared readiness risk: even where plans and investments exist, scaling AI may remain limited by available expertise, reinforcing the value of shared services and scalable capability-building approaches over isolated hiring.

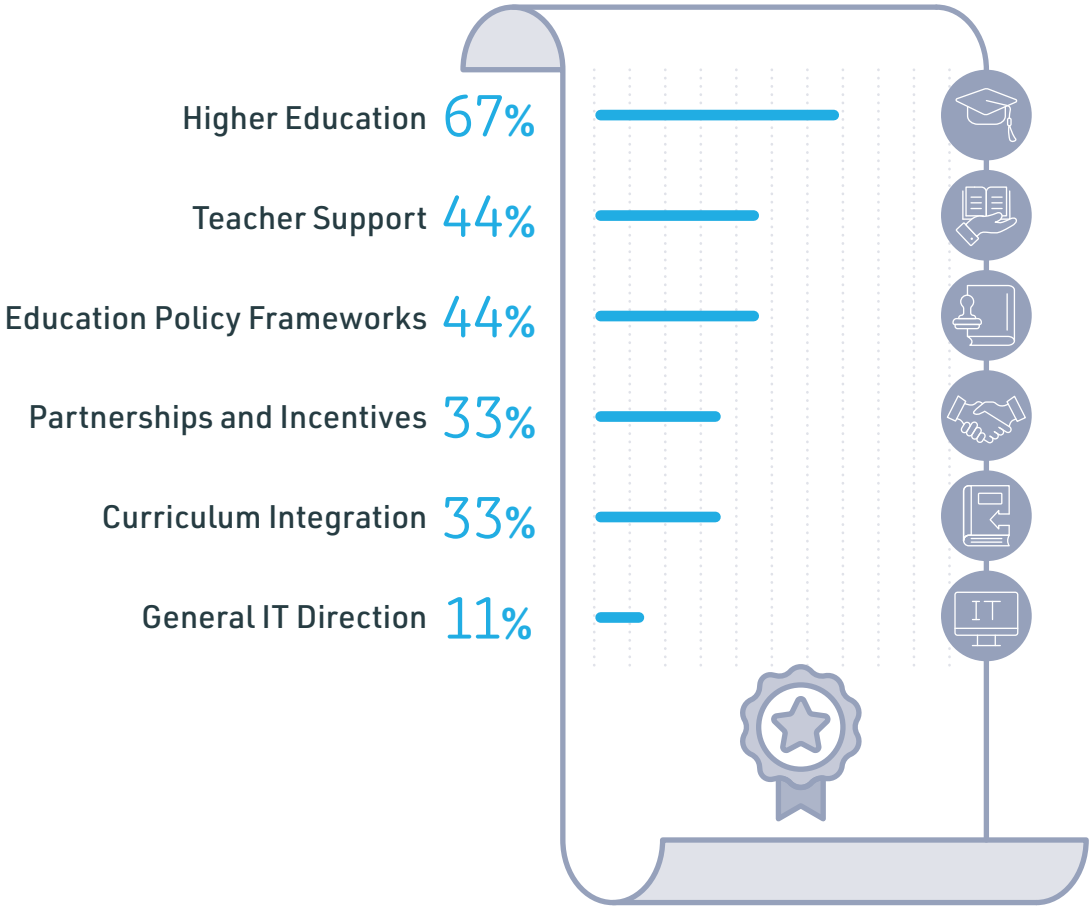
In assessing academic capacity, **78% reported a shortage of AI researchers,** reflecting a less uniform picture than in industry and an uneven research base across participating contexts. This divergence suggests that AI readiness may be influenced by the depth of domestic research ecosystems: where shortages are reported, the ability to generate local evidence, develop context-specific solutions, and sustain innovation may be constrained, while contexts reporting no shortage may have a stronger foundation for longer-term capability building and public-interest research governance.

100%
Reported A Shortage of AI Experts in Industry

78%
Reported A Shortage of AI Experts in Academia

When examining how governments prepare students for AI-shaped labor markets, measures were most often reported in **higher education** (67%), including universities offering AI-related programs, aligning training to labor-market needs, and integrating AI content into non-AI and non-IT study programs. A second cluster emphasized enabling conditions in schools, with **teacher support** (44%) through guidance for classroom AI use and AI-powered "teacher support" platforms, alongside AI **education policy frameworks** (44%) such as national or ministry-level strategies and action plans. Additional measures included **partnerships and incentives** (33%) like scholarships and industry mentors, and **curriculum integration** (33%) through embedded AI modules, vocational ICT tracks, or exam policies permitting AI tools. A smaller outlier relied on **general IT direction** without explicit AI literacy (11%), such as initiatives to increase student interest in IT fields and generic digital-skills programs.

How Governments Prepare Students for AI-Shaped Labor Markets



Overall, the pattern indicates that readiness efforts are more developed in post-secondary settings than in system-wide implementation across earlier education stages. Strengths include attention to widening AI competence beyond a narrow specialist pipeline and the use of governance instruments (education strategies and teacher enablement) that can support consistency and risk control. Gaps remain where measures appear less anchored in standardized curricula and labor-market linkage, which can limit scalability and produce uneven exposure across institutions. The presence of general IT approaches signals a governance risk of implicit AI literacy, weakening clarity on minimum competencies and responsible-use expectations.

Image is AI generated

Recommendation

Governments may wish to consider a more integrated talent approach that links short-term capacity needs with long-term pipeline development across industry, academia, and education.

Strengthening coordination between higher education measures, school-level teacher enablement, and national education policy frameworks could help translate strategy into consistent practice and reduce uneven exposure to AI skills across institutions.

Where labor-market linkage mechanisms are in place, reinforcing partnerships and incentives may enhance practical relevance and support scalability.

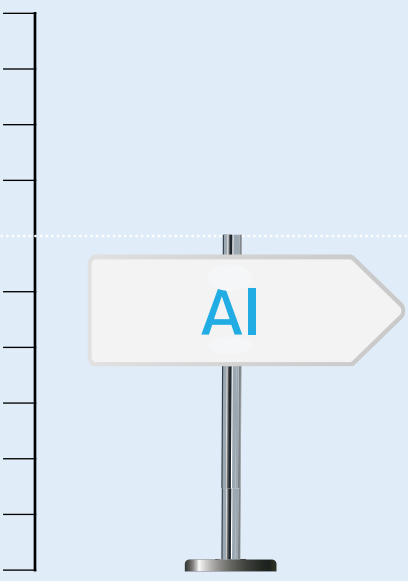
Where approaches rely mainly on general IT direction, aligning AI literacy objectives with existing education and skills frameworks may improve clarity on baseline competencies and responsible-use expectations.

UPSKILLING THE WORKFORCE

AI in government will only scale if the workforce can use it confidently, supervise it responsibly, and embed it into routine operations. Upskilling is therefore not a one-time training activity, but a capability shift that affects delivery capacity, governance quality, and the ability to sustain value beyond pilots. Effective approaches typically combine structured learning with practical enablement - tools, guidance, and expert support that help staff apply skills in real projects and share knowledge across ministries. In parallel, governments must ensure that critical specialist roles are filled and retained to provide oversight, stewardship, and continuity as AI use expands across services and administrative functions.

On workforce upskilling direction, **60% reported that the government is directing staff to further education and training in AI** to meet future needs. This suggests that structured upskilling is present in a majority of contexts, but remains insufficiently universal to serve as a consistent whole-of-government readiness mechanism for scaling AI use under common standards and controls.

According to 9 Responses

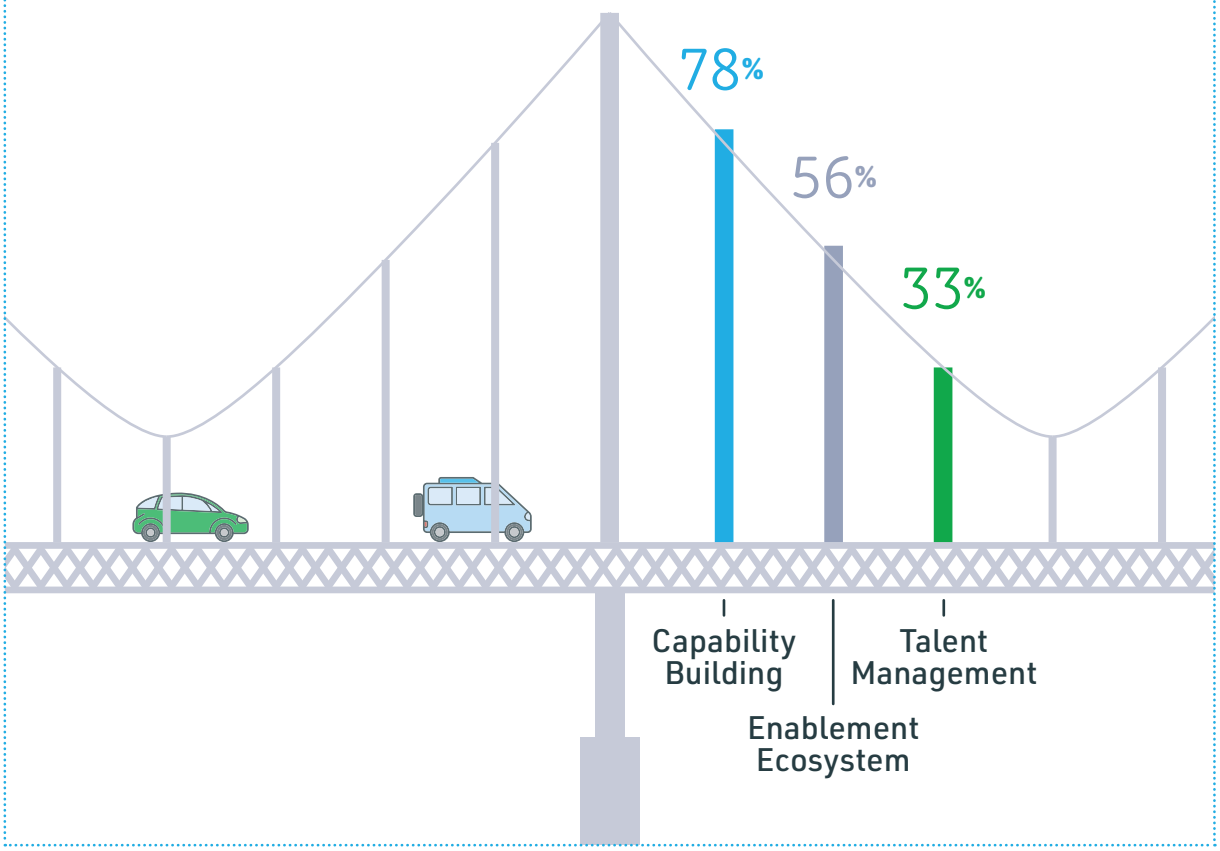


60%

reported that the government is directing staff to further education and training in AI

Across reported approaches to bridging the government workforce skills gap, 78% identified **capability building** as the core strategy, including AI and digital upskilling programs, civil-service training tracks, agency-level courses, continuing education targets, and role mapping to tailor training by focus groups. A second cluster focused on an **enablement ecosystem** (56%), such as AI centers and competence networks, project implementation support, knowledge-sharing arrangements, and collaboration with universities, research bodies, industry, and think tanks to strengthen practical relevance. Less frequently, 33% cited **talent management measures,** including recruiting AI specialists, improving employment conditions, and making public-sector IT roles more attractive, while noting retention gaps.

Approaches to Bridging the Government Workforce Skills Gap



These strategies suggest that many governments prioritize **training** as the main readiness lever, while also recognizing that scalable capability depends on structures that **translate learning into practice** through shared expertise and implementation support. This combination can strengthen governance by enabling reuse and more consistent approaches across ministries, but uneven coverage implies risks of fragmented maturity and variable control quality as AI adoption expands.

The lower emphasis on **talent management** indicates a potential gap in sustaining specialist capacity for stewardship, oversight, and risk management, which can increase continuity risk and reinforce dependence on external providers where internal expertise remains limited.

Image is AI generated

Recommendation

These findings suggest that countries may wish to consider a more balanced workforce strategy that combines role-based upskilling with durable enablement and staffing mechanisms. Strengthening coordination of training pathways across ministries, supported by shared competency models and consistent learning objectives, could help reduce uneven readiness and improve scalability under common controls.

Reinforcing enablement ecosystems - such as competence networks, implementation support, and structured knowledge-sharing - may enhance practical adoption and reuse beyond isolated pilots.

In parallel, aligning talent management practices with the criticality of AI stewardship roles (recruitment, retention, and employment conditions) could strengthen continuity, reduce reliance on vendors, and support sustained governance and value over time.

CONCLUSIONS

Across the chapter, a consistent pattern emerges of talent constraints as a core limiter on scaling AI in government, with skills gaps identified across industry and, in many contexts, academia. Mitigation efforts were most often framed through capability building - education pathways and public-sector upskilling - with less consistent emphasis on early-stage curriculum integration, labor-market linkage, and sustaining specialist capacity through recruitment and retention.

Cross-cutting themes point to governance and scalability challenges: progress depends on coordinated, role-based development and durable enablement structures (competence networks, implementation support, knowledge-sharing) rather than isolated training, while uneven coverage across ministries and education layers risks fragmented maturity, variable control quality, and continued reliance on external providers for critical oversight and stewardship.

Image is AI generated

NATURAL LANGUAGE PROCESSING (NLP)

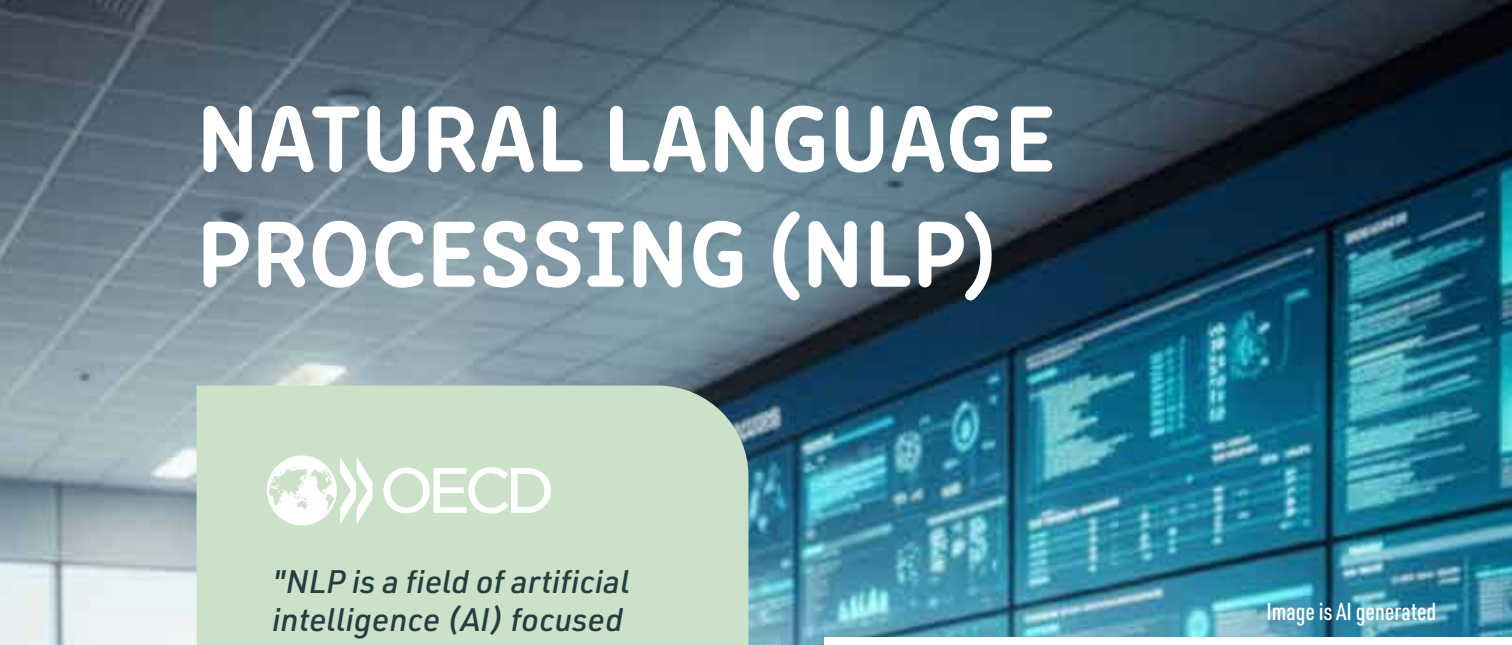


Image is AI generated

OECD

"NLP is a field of artificial intelligence (AI) focused on enabling computers to understand and generate human language. Language models and other NLP approaches involve developing algorithms and models that can process, analyze, and generate natural language text or speech trained on vast amounts of data using techniques ranging from rule-based approaches to statistical models and deep learning.

The application of language models is diverse and includes text completion, text-to-speech conversion, language translation, chatbots, virtual assistants, and speech recognition." [17]

Natural language processing can make government information, records, and services easier to navigate, search, and deliver at scale.

In the European context covered by this audit, most administrations operate primarily in national languages rather than English, and a large share of governmental data, documents, and citizen-facing content is produced and maintained in the local language.

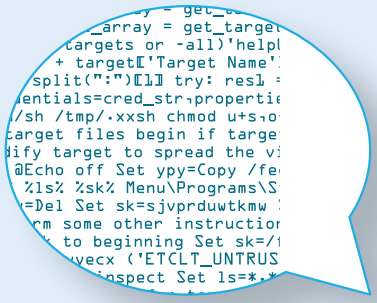
As AI projects move from pilots to operational tools, language capability becomes a practical driver of whether governments can manage internal workflows and engage the public in a consistent and reliable way. These choices also carry distinct risks, since model behavior directly shapes how content is interpreted and presented.

This chapter examines how governments are advancing local-language NLP and how they structure the development of the underlying algorithms.

17 OECD (2023), "AI language models: Technological, socio-economic and policy considerations", OECD Digital Economy Papers, No. 352, OECD Publishing, Paris, https://doi.org/10.1787/13d38f92-en.

Responses reflected uneven progress in developing local-language NLP models. **78% reported active development,** while 22% reported no activity. This can limit rollout of language-dependent services and internal tools, and increase reliance on solutions that do not fully reflect national linguistic needs. The optimal approach may vary by administrative scale and expected return on investment. In larger population countries (for example, France and Italy), broader volumes of language use may support more mature translation and multilingual capabilities, given greater demand and more extensive usage and quality-assurance processes than in smaller administrations (for example, North Macedonia and Estonia).

At the same time, smaller population countries may achieve stronger value for money by leveraging these translation-based capabilities rather than investing in dedicated local-language model development, where the required investment may be harder to justify relative to expected usage and scaling benefits. However, translation-based approaches may still fall short on legal nuance, specialized and cultural terminology, and data control.



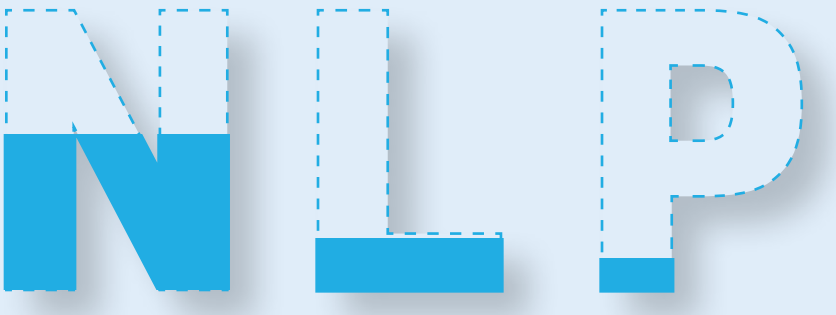
78%

Reported Active Development of Local NLP Models

According to 9 Responses

Most respondents indicated that NLP model development is primarily supported by external capacity. 56% reported development through an **external provider,** 33% reported a mixed model combining **governmental and external contributions,** and 11% reported development **solely within a governmental framework.** Overall, the distribution indicates that in-house development is less common than outsourced or hybrid approaches.

Development of The Models:



56%
through an external provider

33%
combining governmental and external contributions

11%
solely within a governmental framework

Reliance on external or hybrid development models suggests constraints in specialized internal capability, which can limit autonomy over design choices and lifecycle management, including ownership of updates, performance monitoring, and documentation. Hybrid arrangements may support knowledge transfer and shared ownership, but they require clear governance and accountability across parties. With fully governmental development less common, scaling may depend on procurement capacity and vendor oversight, increasing the need for controls that protect continuity, manageability, and adaptability over time while limiting dependency risks.

Image is AI generated

Recommendation

Governments should address two linked readiness priorities: establishing local-language NLP capability where it is still absent, and ensuring it can be sustained operationally over time given the delivery models in use.

Where external providers play a central role, governments should clearly define and enforce lifecycle responsibilities as a condition for scaling, including accountability for maintenance, updates, performance monitoring, documentation, and risk management.

Governments should also promote structured collaboration with academia and industry to strengthen access to expertise, data, and research capacity, and to accelerate high-quality local-language resources.

To support expansion of language-dependent services across ministries, governments should treat local-language NLP as a reusable, shared capability rather than a set of isolated implementations, strengthening consistency of outcomes and coherence of oversight.

APPENDIX A
Audit Questions

National Strategic Plan

1| Is there a national strategic plan for AI approved by the government?

2| If not - are there any ongoing government initiatives or policies that address the development and use of AI?

3| Does the plan have specific goals for increasing public awareness and understanding of AI?

4| If there is a strategic plan, what year was it approved?

5| Does the national AI plan prioritize a comprehensive AI ecosystem or a siloed approach?

6| In your opinion, Which elements of the AI strategic plan are most crucial for its successful execution?

7| What are the key areas included in the strategic plan?

8| Is the strategic plan referring to all AI implementation principles by the OECD?

9| How many of the OECD's AI implementation principles are directly addressed within the national strategic plan?

10| How does the government ensure alignment with best practices outlined by the OECD for AI development and deployment?

11| What is the timeframe outlined in the strategic plan for achieving its key objectives?

12| What are the main goals and indicators listed in the strategic plan?

13| Does the strategic plan determine a governmental entity to lead the implementation?

14| Which governmental entities are involved in the implementation of the plan?

15| What are the main barriers in promoting the field in the governmental aspect?

16| What are the plans to overcome these barriers?

17| What is the position of the country in the international indexes according to the various parameters?

18| Based on the rankings in the international indexes, what were the areas of strongest and weakest performance for this country?

19| Does improving the rankings is one of the governmental stated goals? What steps are outlined to improve them?

Government Budgets

20 | Is there a specific budget allocated to AI purposes?

21 | What is the allocated governmental AI budget?

22 | Does the current budget allocation fit the requirements defined by the strategic program?

23 | What is the breakdown of the budget?

24 | What percentage of the budget outlined in the strategic plan is reflected in the actual budget allocation?

25 | If the budget doesn't fit the strategic plan requirements, what are the reasons for that?

26 | What other alternative funding models or public-private partnerships could supplement government resources for AI development?

Infrastructure

27 | Has the government launched any national initiatives for AI infrastructure development?

28 | How many AI infrastructure development projects have been established in recent years? How many were implemented? How many are finished?

29 | What are the specific types of AI infrastructure being developed or expanded and what are their processing capacities?

30 | Is there a national cloud infrastructure?

31 | What are the current compute resources available in the national cloud?

32 | Is a use in third parties for cloud and computing purposes taking place?

33 | How many AI projects rely on third-party providers for data storage and processing compared to the projects that manage this internally?

Digital Maturity

34 | Is there a governmental data strategy?

35 | How many government ministries have actively implemented the governmental data strategy? How many aren't?

36 | What are the key objectives and priorities outlined in the governmental data strategy?

37 | Has the country developed a digital maturity index to assess readiness and capabilities?

38 | What is the current score of the country in the digital maturity index?

39 | What specific areas of digital maturity are identified as strengths or weaknesses based on the index?

40 | Does the government have a formal policy outlining the conditions for sharing data between different ministries?

41 | What are the data sharing policy principles?

42 | What factors prevent governmental ministries from sharing their data?

43 | Are there initiatives to build a governmental data lake?

44 | How many governmental ministries are integrated into the governmental data lake? How many aren't?

45 | What are the anticipated benefits and challenges associated with implementing a governmental data lake?

Regulatory Guidelines

46 | Have regulatory guidelines been published?

47 | Has the government established a dedicated agency or body responsible for overseeing the development and implementation of AI regulations?

48 | What are the key principles and provisions included in the regulatory framework to ensure responsible and ethical use of AI in governmental operations?

49 | In accordance with the new European law (EU AI Act), are there additional regulatory guidelines initiated by the government?

50 | What are the main challenges and opportunities presented by the EU AI Act for the country's AI development and regulatory landscape?

51 | Does the government require developers of AI systems for public use to conduct bias audits before deployment?

52 | Does the government have guidelines or regulations in place to address ethical concerns related to AI, such as bias, discrimination, and privacy violations?

53 | How many government AI projects have undergone a formal risk assessment for potential ethical concerns (bias, discrimination, etc.)? How many aren't?

54 | What are the ways of dealing with potential ethical risks (bias and discrimination)?

55 | How can the government promote public trust and transparency in the development and deployment of AI technologies?

56 | What measures are in place to ensure that AI systems used by the government comply with ethical standards and guidelines?

57 | Is there a framework or initiative in place to implement the OECD's principles for trustworthy AI within the public sector?

58 | How many of the OECD's trustworthy AI principles have been integrated into the government's AI strategy and policies?

59 | What is the level of maturity of the public sector and/or at the level of a ministry in implementing the principles of trustworthy AI established by the OECD?

60 | Has a maturity index in terms of trustworthy AI been established for the public sector?

61 | When was the maturity index established?

62 | What are the key indicators used to determine the maturity of AI adoption, and what steps are being taken to enhance maturity levels?

63 | Is there litigation regarding the use of AI in each country such as: liabilities, licit uses, limits, protections, etc.?

64 | What are the main legal challenges and implications for AI adoption and deployment within government operations?

Information Security

65 | Does the government have mandatory cybersecurity protocols and training programs for personnel involved in AI projects?

66 | Does the government have policies or regulations specifically addressing data privacy concerns related to AI applications?

67 | How many cybersecurity incidents related to governmental AI projects have been reported in the past year?

68 | How many AI projects involve training/ processing of personal or sensitive data? How many aren't?

69 | What are the main information security risks identified in government projects in the field of artificial intelligence, and what are the ways established to reduce them?

Government Projects

70 | Has the government conducted a national survey to assess the current level of AI adoption across different government sectors?

71 | How many government ministries that have implemented AI technologies in their systems? How many aren't?

72 | Which sectors have implemented AI initiatives? which aren't?

73 | What are some notable examples of AI applications that have improved efficiency or service delivery within government ministries?

74 | Does the government have mechanisms in place to monitor and evaluate the impact and effectiveness of AI initiatives?

75 | How frequently are evaluations conducted to assess AI projects?

76 | What is the average cost of implementing a new AI project within a government ministry?

77 | What have been the key findings or lessons learned from recent evaluations of government AI initiatives?

78 | What are the indicators (KPI) for evaluating the effectiveness of a particular project?

79 | Have productivity gains been seen with the implementation of AI systems in the public sector and/or ministry-wide?

80 | What percentage increase in productivity has been observed due to AI technologies?

81 | What is the nature of the productivity gains observed?

Human Capital

82 | Is there a shortage of artificial intelligence experts in the industry?

83 | Is there a shortage of researchers in the field of artificial intelligence in the academia?

84 | How many educational institutions introduced AI-related courses or programs? How many aren't?

85 | How many individuals have been trained in AI-related skills through government-sponsored programs or initiatives?

86 | What steps are being taken to ensure that students are equipped with AI literacy and skills for future job markets?

87 | Is the government directing staff to further education and training in AI to meet the needs of the future?

88 | How many AI training programs are currently offered to government employees across different skill levels?

89 | What strategies for bridging the skills gap between the existing government workforce and the demands of the AI revolution discussed in the government?

NLP

90 | Has the government developed or is it currently developing NLP models in the local language?

91 | How many NLP projects or initiatives have been funded by the government in the last recent years?

92 | Is the development of the algorithm done in a governmental framework or with the help of an external provider?

APPENDIX B
INDIVIDUAL AUDIT REPORTS

riigikontroll
National Audit Office of Estonia

Overview of the development of AI solutions in public sector organisations

National Audit Office of Estonia Overview on the International Joint Audit of Artificial Intelligence

Overview by the National Audit Office
Estonia to the Riigikogu
Tallinn, 30 May 2025

Summary

Developments in the field of artificial intelligence in recent years have created significant new opportunities. Many Estonian public sector organisations have started to develop, test and use innovative AI-based solutions. The introduction of such solutions should help organisations to better fulfil their tasks, including provide better quality services, make faster decisions, reduce costs.

A joint audit is on course for completion in early 2026 in cooperation with the twelve supreme audit institutions of EUROSAI, the objective of which is to assess the readiness of the government sector to adopt AI solutions. The National Audit Office participated in the joint audit and prepared an overview to provide a picture of how Estonian public sector organisations are developing and using AI solutions and what the main obstacles are in this area.

According to the list of AI based solutions compiled by the Ministry of Justice and Digital Affairs, 130 solutions have been developed in the public sector, but this list does not give an overview of developments in recent years, and experts believe that many of them are not AI solutions. Approximately 30 AI-based solutions have been created in the organisations that responded to the survey of the National Audit Office. Most of these solutions are still being tested and do not offer significant cost savings, better quality public services or faster decision-making.

The main obstacles to the creation and introduction of AI solutions are:

- **The development of AI solutions is hampered by a lack of awareness among employees of the options offered by AI and its areas of application.** On the one hand, the development capacity is limited by the lack of specific technical expertise, for example, the lack of a smart customer from an AI perspective, whose involvement is necessary to develop solutions. Nor do ideas or proposals for new solutions emerge in organisations where the majority of staff have no knowledge of the potential of using AI in their field.
- **The creation of AI solutions is hindered by the poor quality of databases.** The survey carried out in the course of the overview showed that a considerable number of organisations see data quality as an important issue and are working to improve it. At the same time, the survey revealed that as many as one-third of organisations are not actively engaged in improving data quality, which in turn makes it difficult to develop and implement AI solutions.
- **The creation of AI solutions is hindered by the inability to cope with regulatory restrictions.** Difficulties mainly arise from data protection rules that limit the use of personalised data both in the training and implementation of AI solutions.

In order to create a better environment for the development of AI solutions, the Ministry of Justice and Digital Affairs, which is leading the area, should pay more attention to removing the obstacles to the development of solutions. At the national level, it is necessary to support public authorities in

making the right choices in the legal environment, by developing guidance, carrying out training, giving advice, etc. for this.

Organisations themselves must invest significantly more in improving data quality and increasing knowledge to successfully implement AI solutions. In the future, as solutions are developed and data volumes increase, appropriate IT infrastructure solutions (i.e. hardware and software environments supporting computing and software development) must be found to maximise the performance and security of AI solutions.
In addition, organisations must assess whether their planned AI solution is economically reasonable, i.e. whether it will help save costs, improve the quality of public services or enable to make faster decisions.

Contents

What is artificial intelligence (AI) and an artificial intelligence solution?

Artificial intelligence system – a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

Source: European Union Artificial Intelligence Act

1. Artificial intelligence is an area of theory and development of computer systems that aims to create systems capable of performing tasks that traditionally require human intelligence. An AI solution is based on a software algorithm that is autonomous and capable of learning, and performs tasks traditionally performed by humans.

2. The application of AI in public sector organisations allows them to make policies more efficiently, deliver better services, make faster and better decisions and free officials from routine tasks. Given the steady increase in the costs of public sector organisations, it is important to invest in innovative solutions that help make work more efficient and save resources.

3. Systems that process large amounts of information, but are not AI solutions, are often erroneously presented as AI solutions. A key feature of AI solutions is their learning capacity. If a system can analyse the data and improve its performance on the basis of them, it can be considered a self-learning system. However, if a system has fixed inputs and outputs, without the ability to adapt the way it works, it is an automating process, not artificial intelligence.

4. In Estonia, several public sector organisations have started developing AI-based solutions on the initiative of the Ministry leading this area (the Ministry of Economic Affairs and Communications until December 2024 and the Ministry of Justice and Digital Affairs from January 2025). In Estonia, a solution like this is also called *kratt,* a name inspired by folklore.[1]

AI – a practical application based on AI technologies, which is based on a software algorithm that is autonomous, capable of learning and performs tasks traditionally performed by humans.

Source: kratid.ee

Generative AI – AI that can generate original content (e.g. text, images, video, sound or software code) in response to a user's input or query.

Source: www.ibm.com

5. According to the information of the Ministry of Justice and Digital Affairs, the narrow AI is mostly used in AI applications. Narrow AI is able to solve one narrow task and learn from its experience to solve the problem more successfully, but cannot learn in the course of the activity what, for example, the next tasks and problems might be.[2] In addition to narrow AI, generative AI, which can create entirely new content – text, images or sound – is also becoming increasingly common around the world (see Table 1).

[1] Kratid.ee.

[2] https://akit.cyber.ee.

Table 1. Ways to categorise AI

Capacity	Functionality	Technology
Narrow AI	Reactive machines	Machine learning
	Limited Memory	Deep Learning
Generative AI	Theory of Mind	Natural Language Processing
		Robotics
Superintelligent AI	Self-aware AI	Computer Vision
		Expert Systems

Source: National Audit Office, Understanding the different types of artificial intelligence

6. Although the description of an AI solution in the AI strategy meets the main conditions of AI, several specialists interviewed in the audit questioned the AI skills of several of the AI solutions listed in the kratid.ee list, i.e. mainly the absence of the ability of an artificial intelligence solution to learn. From the point of view of the organisation itself, such a solution may also be appropriate and simplify work processes, but it is not an AI solution.

7. The National Audit Office (NAO) wanted to get an overview of the development and use of AI solutions in public sector organisations: how many such solutions are in use and what are the main obstacles to their creation. For this purpose, the National Audit Office conducted a survey among ministries and other major organisations. The National Audit Office sent the questionnaire to 58 organisations and 48 organisations responded (see Table 4 for the characterisation of the overview). The results of the survey are presented in the following chapters and the conclusions drawn from them.

20 responding organisations that have developed AI solutions:

- Ministry of Education and Research
- Ministry of Defence
- Ministry of Economic Affairs and Communications
- Ministry of Finance
- Ministry of the Interior
- Ministry of Foreign Affairs
- Land Board
- Tax and Customs Board
- Agricultural Registers and Information Board
- Rescue Board
- Estonian Information System Authority
- Transport Administration
- Environment Agency
- Information Technology Centre of the Ministry of Environment
- Government Office
- Office of the Riigikogu
- IT and Development Centre of the Ministry of the Interior
- National Archives
- Estonian Unemployment Insurance Fund
- Estonian Public Broadcasting

The public sector organisations that took part in the survey have developed around 30 AI solutions that are actively used

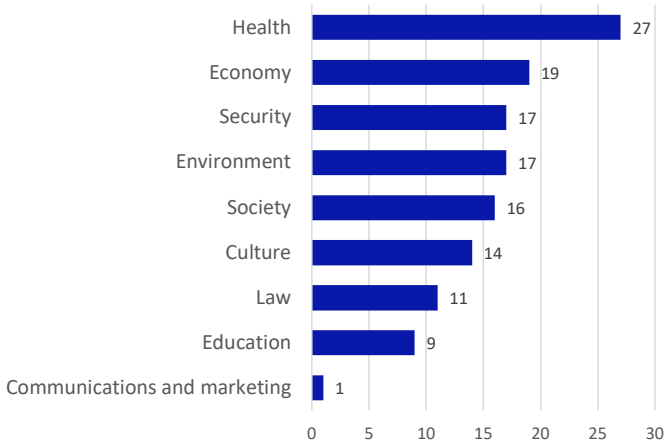
How many AI solutions have been created?

8. There is currently no up-to-date and comprehensive overview of the state of development and use of AI solutions. The overview is necessary to allow organisations to share experiences and avoid developing duplicate solutions.

9. According to the list of AI solutions compiled by the Ministry of Justice and Digital Affairs (kratid.ee), more than 130 solutions have been created in the Estonian public sector or in cooperation with the public sector for different purposes (see Figure 1), ranging from one-off ready-made solutions to solutions that are still in active use or in progress. According to this list, a total of 53 public sector organisations (35 of which are public authorities) have created projects with an AI component to improve their work.[3]

[3] https://www.kratid.ee/kasutuslood-kratid

Figure 1. AI solutions described according to areas on the kratid.ee website



Source: kratid.ee

10. The data of list of AI solutions of the Ministry of Justice and Digital Affairs had not been updated for two to three years at the time of the audit, and therefore there is no overview of developments in recent years. Updating the list of AI solutions regularly is necessary to share information on AI solutions already developed, to exchange know-how on AI development and to avoid the development of duplicate solutions. The list also includes solutions that have now been removed from use. At the time of preparation of the overview, the Ministry of Economic Affairs and Communications, and later the Ministry of Justice and Digital Affairs, were in the process of updating the list of AI solutions.

11. According to the survey of the National Audit Office, 20 out of 48 organisations that responded to the survey have created AI-based solutions. However, the total number of actively used solutions is less than 30. Examples of the most common solutions include machine learning-based prediction models, decision support and speech or image recognition solutions.

AI solutions developed so far

Examples of AI solutions developed by the state

12. The solutions of organisations and the departments vary considerably due to needs. There are more generic solutions (e.g. for transcribing text), more specific solutions (e.g. supporting software development), or forecasting and prediction models (e.g. the Tax and Customs Board has several models supporting the detection of labour tax and VAT refund fraud) in use.

13. The survey of the National Audit Office revealed that the most common solutions are machine learning solutions, including image and facial recognition. Speech recognition, text search and transcription solutions have been added to this in a couple of organisations. AI solutions are also used in software development and text analysis (see Table 2).

Table 2. Examples of the AI solutions of the observed organisations

Text, image or speech recognition	Prediction models	Chatbots
Surface monitoring – detection of field mowing from satellite data (Agricultural Registers and Information Board).	A data mining model for detecting VAT refund fraud (Tax and Customs Board).	Bürokratt (developed by the Estonian Information System Authority, users – Consumer Protection and Technical Surveillance Authority, Tax and Customs Board, Police and Border Guard Board, etc.).
HANS – speech recognition and transcription (Riigikogu). Transcription solutions (Estonian Public Broadcasting), including live subtitles and publicly available transcripts of archived broadcasts.	A model for detecting labour tax fraud, combined with existing rule-based systems (Tax and Customs Board).	Vesta chatbot (previously used by the National Library of Estonia).
Species identification software (Environment Agency (KAUR), Information Technology Centre of the Ministry of Environment (KEMIT)) – the system calculates the abundance of species in a given area using images collected by trail cameras. The images are classified by artificial intelligence and the abundance of species is then determined using a random encounter model based on calculations. Snow cover determination solution (KAUR, KEMIT) – determination of snow cover during weather monitoring.	Decision support OTT (Estonian Unemployment Insurance Fund) – summarises a specific client's situation, predicting the likelihood of finding work in six months, the likelihood of becoming unemployed again and the factors that have the greatest impact.	
Marta – automatic tagging of articles (National Library of Estonia).		
Classification of customs x-ray images to detect contraband (Tax and Customs Board).		

Source: Survey by the National Audit Office

Bürokratt is a chatbot that an organisation can integrate, e.g. in the organisation's website or application, to make its work easier.

Source: bürokratt.ee

The most widely used AI solution is Bürokratt

14. The survey revealed that the most common tool used by organisations is Bürokratt, developed by the Estonian Information System Authority (RIA). Bürokratt is an AI-based communication channel between an organisation and a client. The success of Bürokratt, i.e. the quality of the answers it gives, depends to a large extent on the contribution of the organisations themselves in training it. More than six million euros has been spent on the development of Bürokratt so far and at the moment, it is used in ten public sector organisations.

Reusable AI component – the base component of an AI-based solution, which can be reused free of charge and further developed according to the needs of all public and private stakeholders.

Source: White Paper on Data and Artificial Intelligence 2024–2030

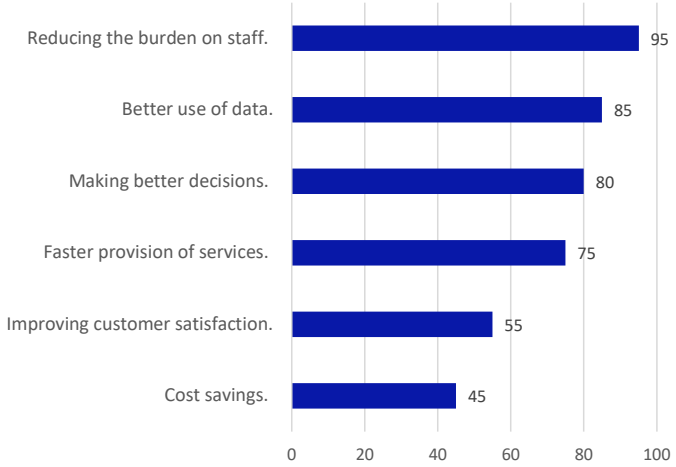
15. Reusable AI components, which can be reused free of charge and further developed according to their needs by all public and private stakeholders have been created in addition to full AI solutions. These components are available in the e-Government Code Repository and on GitHub. Examples of solutions available as reusable AI components include the anonymiser (developed by the RIA), neurotranslation, neurospeech (both developed by the University of Tartu), the Texta Toolkit (Texta) and the quick writer (TalTech).

GitHub – a web hosting service for IT projects with jointly developed version management.

Source: Data Protection and Information Security Portal AKIT (https://akit.cyber.ee/)

16. The organisations that took part in the survey find that the biggest benefits of AI solutions include reducing the staff workload, making better use of data and making better decisions (see Figure 2).

Figure 2. Opinions of the 20 organisations that have developed AI solution of the benefits of creating these solutions (share of organisations, %)



Source: Survey by the National Audit Office

17. In parallel with the AI solutions they have created themselves, public sector organisations also use or have used solutions developed by other Estonian ministries and foreign ready-made AI solutions to make their work easier. Bürokratt is the most widely used solution developed in Estonia and the other solutions mentioned are the Riigikogu shorthand system HANS, the text-to-speech application Texta Toolkit, the public speech recognition service of the TUT Speech Technology Lab Tekstiks, etc. According to the survey of the National Audit Office, the most used foreign ready-made solutions are ChatGPT (is or has been used by 35 organisations), Copilot (17), Grammarly (9) and Gemini (6). Seven organisations noted that they do not use any foreign solutions.

18. Only some AI solutions are in active use, most solutions are still being tested and do not offer significant cost savings, better quality public services or faster decision-making. There is still much to be done to automate work processes more, to extend the scope of use and to reap greater benefits from the solutions. The intentions of organisations to develop AI should be included in their action plan or work plan.

What is the state's AI strategy like?

19. **The state has an overall strategy for the development of AI and the solutions that contain it. The development of these solutions currently depends largely on external funding, with major developments being supported by EU grants. However, most of the expenditure needed to maintain the solutions has to be covered with funds from the state budget.**

20. The creation of the first national AI action strategy of Estonia started in 2018 and was prepared for 2019–2021.[4] The latest AI strategy was created for

[4] Estonia's National Artificial Intelligence Strategy 2019–2021.

2024–2026[5]. While the main objective of the first AI strategy was to create the base capacity for the deployment of AI solutions, the actions of the current action plan are already geared towards making the state more efficient, e-services more accessible and easier to use. So far, the Ministry of Economic Affairs and Communications has not prepared any reports on the implementation of the AI strategies.

21. The focus themes of the strategies have been similar throughout, focusing on topics relevant to the creation of AI solutions, such as public and private sector activities, data, the regulatory environment and R&D. There are also objectives in the strategies for different periods that have remained the same over time, for example in the area of training public sector employees. There are also some objectives that have been postponed, such as the creation of a single infrastructure for AI solutions.

22. In addition to the AI strategy, there are a number of other strategies and agendas that guide the development and implementation of AI solutions, including the White Paper on Data and Artificial Intelligence[6], the Digital Agenda 2030[7] and the Research and Development, Innovation, and Entrepreneurship (RDIE) Strategy 2021–2035[8].

Strategy for development of artificial intelligence of public sector organisations

Most public sector organisations are not planning activities or money for the development of AI

23. An AI strategy, either as a separate document or as part of another planning document of the organisation, is necessary to agree how AI solutions support the overall objectives of the organisation; what the priorities and resource allocation are to avoid developing unnecessary solutions; how the risks of solutions are assessed and their security ensured; how the relevant skills of employees are developed and how innovation in the respective area is supported.

24. The survey indicated that most, i.e. 37 of the organisations currently do not have a strategy or action plan for AI development, nor do they have plans or objectives for implementing and creating AI solutions. In other words – many organisations have not set specific targets, planned longer-term activities or money for the development of AI solutions.

Funding of AI solutions

The state's budget for the development of AI for the period of 2024–2026 is more than €60 million in total

25. According to the AI Strategy for 2024–2026[9], €60 million is planned for the development of AI for the years 2024–2026. In comparison, a total of €243 million has been planned for the development of the e-governance over the same period.[10] 12 million of the money earmarked for the development of AI is allocated directly for the creation of AI solutions, with the rest for activities supporting the area of AI. Supporting activities include, for example, research and development, education and ensuring competencies, language technology development, development of high-performance computing, creation of trusted AI and a regulatory environment.

[5] Artificial Intelligence Strategy for 2024–2026.
[6] White Paper on Data and Artificial Intelligence 2024–2030.
[7] Estonia's Digital Agenda 2030.
[8] Estonian Research and Development, Innovation and Entrepreneurship Strategy 2021–2035.
[9] Artificial Intelligence Strategy for 2024–2026.
[10] Estonia's Digital Agenda 2030.

26. The creation of AI solutions is currently largely funded by EU grants and to a lesser extent by state budget funds, which means that funding for long-term development in the area requires national funding. EU funds enable organisations to implement the first initiative or create an AI-based application. However, in most cases, these funds cannot be used to cover the costs of upgrading and maintaining an application, and therefore it can be difficult for organisations to find the necessary money later on. It would be important to consider the exact purpose, necessity, use and economic viability of an AI solution from the outset, so that the solution developed brings at least as many benefits to the organisation as it costs to create and maintain.

27. The problem of maintaining AI solutions is partly confirmed by the list of 130 AI solutions prepared by the Ministry of Justice and Digital Affairs, as many of the solutions on this list are no longer used or developed further by the organisations. Unless an organisation can find the money to keep an AI solution up and running, it will remain stagnant, lose its relevance and, over time, its usability.

What are the main obstacles to the creation of AI solutions?

The readiness to create and implement AI is low

28. **The main obstacles to the capacity of organisations to create AI solutions are poor data quality, lack of technical expertise, insufficient funding and the inability to cope with regulatory constraints.**

29. Data quality was rated as satisfactory or poor by 80% of the organisations surveyed, and was considered to be the biggest obstacle to the creation of AI solutions. Organisations also cited strict data protection requirements as an obstacle, suggesting that the organisations do not know how to implement the legal requirements in terms of performance (see Figure 3).

30. In addition, the surveyed organisations have highlighted reasons why AI solutions that were already planned did not make it into development: 7 organisations mentioned lack of money and competence, 2 organisations referred to data sensitivity and 2 organisations to the imprecision of the model and failed development attempts, including situations where automation is a cheaper way to achieve the desired objectives.

Examples of quality data characteristics:

- correctness – the data are formally correct (syntactically correct) and substantively correct or authentic (semantically correct);
- completeness – all attributes of a data record have a value and all required records exist;
- timeliness – the data are fresh and their accessibility corresponds to the needs and requirements;
- regularity – the format and structure of the data meets the requirements;
- uniqueness – only one record of a single real-life object has been recorded in the data;
- in the same format throughout.

Source: Estonian Data Management Methodology Project. Data Quality Guideline. European Commission, August 2020

Figure 3. Main obstacles to the creation of AI solutions (share of respondents among 20 organisations, i.e. of the organisations that have created such solutions, %)

Source: Survey by the National Audit Office

Quality of data

Artificial intelligence (AI) model –a mathematical algorithm or representation trained on data that can make predictions, decisions or perform actions that mimic or support human intelligence.

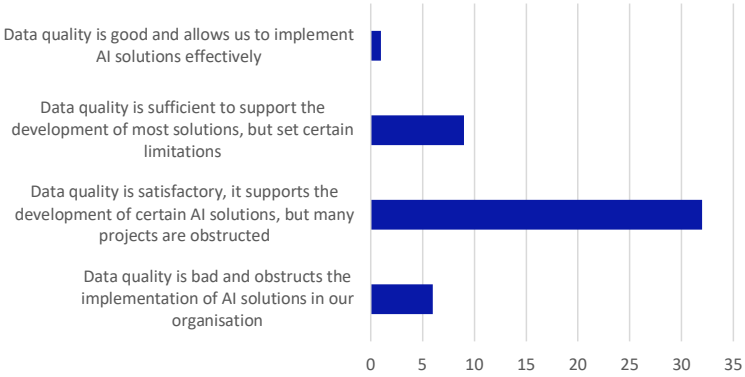
Source: National Audit Office, ISO/IEC22989

31. The accessibility and quality of data are at the core of the creation of AI solutions. The capabilities of AI models will remain limited without reliable and accessible data, which in turn will reduce their practical value. Data quality has a direct impact on the quality of the solutions that can be developed on the basis of them. For example, a machine learning model built on poor quality data is less accurate and reliable. Failure to address data quality immediately could prolong the time needed to develop future data-driven solutions. In addition, the amount of data is not sufficient for training a model in some cases.

80% of public sector organisations that responded find that the quality of their organisation's databases is satisfactory or poor

32. As a result of the survey conducted by the National Audit Office, 80% of the respondents, or 38 organisations, rated the quality of their databases as poor or satisfactory (see Figure 4). This makes it more difficult to create AI solutions in these organisations.

Figure 4. How do organisations rate the quality of their data (the opinions of 48 organisations that responded to the survey, broken down by different responses)?



Source: Survey by the National Audit Office

33. Although the organisations are mostly aware that the quality of the data is not high, no significant progress has been made in this regard. The importance of data and the potential of their use is well recognised both in the organisations and at the level of the state's AI strategy, but the results of the survey of the National Audit Office showed that a third of respondents do nothing to assess or improve data quality. Addressing data quality does not necessarily mean good data quality either. For example, only 36% of organisations have described the basic data of the organisation.[11]

34. Although the Government of the Republic established the regulation "Fundamentals of organisation of services and information management[12]" and Statistics Estonia has prepared guidelines for ensuring the quality of the data in the databases that belong to the information system, many organisations do not deal with their data and data quality preventively, but only after consequences have appeared.

35. An example of the problems caused by poor quality data and why it is important to improve their quality can be found in the area of health. In the health information system, many of the patient health data are entered in free text format, which makes machine-processing and analysis difficult. In order to analyse health data effectively, it is important to ensure that they are machine-readable – this means that there must be agreed standards, data formats and common terminology to describe the data. Entering data into the information system should be done in accordance with these agreements. Machine-readable and standardised health data are important, as they make it possible to provide better and safer care and support effective data-driven decision-making across the health care system.

36. According to the AI strategy, the Ministry of Justice and Digital Affairs has planned a number of activities to improve data quality in databases, but no significant progress has been made in this area. Centrally, guidelines have

[11] White Paper on Data and Artificial Intelligence 2024–2030.

[12] Government of the Republic Regulation No 88 "Fundamentals of organisation of services and information management", adopted on 25.05.2017.

been developed and training on improving data quality has been organised, and several organisations have appointed data managers to coordinate the relevant activities. The main obstacles to improving the quality of databases are the lack of resources and domain-specific knowledge.

Ensuring AI knowledge and skills

37. The survey of the National Audit Office revealed that there are not enough people with sufficient technical knowledge to successfully develop AI solutions and to order or formulate what AI solution needs to be created.

Lack of AI knowledge among employees is an obstacle to the creation of AI solutions

38. Employees, who are engaged in the organisation's main processes on a daily basis, are often the ones who can identify and suggest new ideas for the initiation of AI solutions. They know the details and specific needs of their work the best, and can therefore suggest how to improve work processes and develop AI solutions. For employees to perform their role effectively, it is essential that they have the necessary knowledge of AI capabilities and the skills to identify and formulate needs in a manner that supports the creation of solutions. Interviews with ministries confirmed that there are not many ideas coming from employees and sectoral specialists for the creation of possible AI solutions.

39. The lack of knowledge of AI possibilities and areas of implementation among employees is an obstacle to the development of AI solutions. The survey by the National Audit Office also revealed that one of the obstacles to the development of AI solutions is the lack of AI knowledge of among employees. Twelve of the organisations that responded to the survey claimed that the lack of adequately qualified staff is an obstacle. If the employees lack an understanding of what AI can do and how it can be implemented, projects often remain at level of an idea and solutions are not developed or commissioned.

40. Increasing knowledge in the field of AI requires that employees are consistently provided with meaningful training to develop their skills in using AI. The target set in the AI strategy is to train 500 public sector managers and employees in this area per year.

41. The challenge in the case of training programmes is to train employees in a situation where they lack IT and data background and knowledge and where the area of artificial intelligence seems complicated. There are accessible training programmes and the organisations are also interested in them. The survey revealed that 36 organisations (75% of respondents) have made training their employees to improve data quality a priority, but also they also acknowledged that training is difficult.

Legal constraints and ethical considerations

42. The public sector carries a great responsibility in the development of AI solutions, because they must be developed in a responsible and transparent manner. All applicable legislation must be taken into account and, among other things, the development and use of solutions must comply with the Administrative Procedure Act, the Public Information Act and the Data Protection Act. There is no separate regulation on the development and use of AI in Estonia yet, but there are plans to develop a national regulation on AI in the near future, specifying the organisation of the field (see paragraph 63).

Legal constraints on the development of AI generally relate to the use of personal data

43. Many organisations have difficulties in meeting the regulatory requirements upon the creation of AI solutions and this has delayed or interrupted the development of solutions. Difficulties mainly arise from data protection rules that limit the use of personalised data both in the training of AI solutions as well as in the use of these solutions. Also, organisations do not know data protection rules well enough and are therefore more likely to just abandon their activities.

44. Developing AI models often requires the use of large amounts of data. Large amounts of data allow models to learn and thus provide more accurate information for decision-making. However, a lot of the data used by public sector organisations is personalised and these are exactly the kind of data the use of which for the development and implementation of AI models is restricted due to data protection.

45. There must be a lawful basis for the processing of personal data. This could be, for example, a need arising from a contract or the consent of the individual. This means that without a clear process in place to justify data processing, the use of (personalised) data is not allowed. For example, in the health care sector, patient data can only be used once a treatment process, such as a doctor's appointment, has been initiated. The use of the data of patients in an AI solution without a legal basis is prohibited.

46. While the use of personalised data in AI solutions can bring speed and cost savings to certain decision-making processes, it also raises ethical questions and risks. In the creation of the present solutions, they are mostly related to transparency and assignment of responsibility, and will become more prominent as these solutions are more broadly implemented.

47. In the case of AI solutions, it is necessary to ensure the transparency of its operating processes and it must be clear who is responsible for the data used in the solutions and the decisions provided by the solution. The lack of transparency can generate significant risks, such as wrong or discriminating decisions, as the decision-making process is not repeatable and the way AI made the decision may not be verifiable. In order to mitigate the risks, each organisation must prepare a risk assessment and an impact assessment describing the maximum potential harm resulting from a security breach of an AI system and the impact of decisions made by the system on the fundamental rights of people.

Examples of keywords to ensure transparency:

- traceability – the data sets and processes that are the basis for the decisions of the AI system must be documented;
- explainability – the ability to explain, in a timely and adapted manner, both the technical process of the AI system and the decisions and choices made by humans, e.g. why such a solution was chosen;
- information exchange – an AI system must not present itself as a human, and the user must be offered the possibility to communicate with a human when compliance with fundamental rights must be ensured.

Examples of keywords to ensure responsibility:

- auditability – making it possible to assess algorithms, data and the design process;
- minimisation and notification of negative impacts – the user must be notified of the potential impact of the outcome and the AI developer must carry out an impact assessment;
- legal protection – if the effects of the system are unfairly harmful, mechanisms should be put in place to ensure adequate legal protection.

Source: Commission Expert Group on AI[13]

IT infrastructure

48. The existing IT infrastructure (the computer system and the hardware and software environment that supports software development) have been used for the development and maintenance of AI solutions at present[14]. The AI solutions currently in development and use tend not to set specific IT infrastructure requirements and this has not been a significant obstacle to the development of solutions. However, in the future, as solutions are developed more widely and data volumes increase, we must also be prepared to build IT infrastructure with higher performance and other specific needs.

49. The goal to develop infrastructure on the basis of the government cloud and to prepare a plan for this is separately highlighted in the last two National

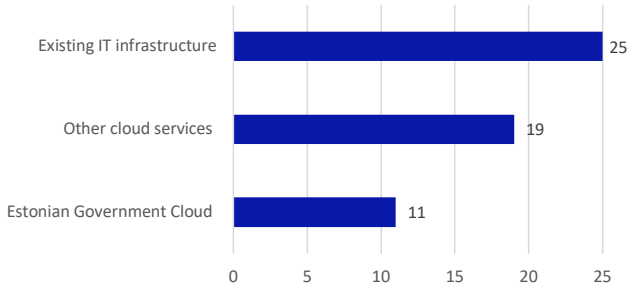
[13] Ethical guidelines for the development of trustworthy artificial intelligence.
[14] ISO/IEC/IEEE 24765.

AI Strategies (Kratt Strategy) (2022–2023 and 2024–2026). As the first step, the National AI Strategy for 2022–2023 outlines the creation of a roadmap or action plan for the development of common infrastructure and services based on the government cloud (deadline September 2023). However, in the AI Strategy for 2024–2026, the goal of creating a roadmap has been postponed by one year and it has not been created yet. According to the Estonian Information and Communication Technology Centre, the creation of the roadmap is at the analysis stage and it is unclear whether this analysis could lead to real solutions in the future.

No separate IT infrastructure is currently needed for the development of AI

50. In the view of AI solutions, the government cloud is currently mainly used to host the Bürokratt solutions of organisations. In general, the same infrastructure used for other IT solutions is also used for the implementation and development of AI solutions (see Figure 5).

Figure 5. What kind of IT infrastructure is implemented for the development and use of AI solutions (opinion of the 48 organisations that responded to the survey, broken down by responses)?



Source: Survey by the National Audit Office

51. In addition to IT infrastructure, performance is also an important aspect in the development of AI solutions. Organisations often do not have the money needed to use the high-performance computing (HPC) solutions needed to run more complex models. This, in turn, reduces the capacity to develop and implement large-scale AI solutions.

Ensuring the security of AI solutions

52. **There have been no reports of major security incidents involving AI solutions. However, more attention should be given to the secure use of both domestic solutions and foreign ready-made solutions in public sector organisations.**

53. The AI assessment section APP.EE.2 "Artificial Intelligence Systems"[15] has been added to the Information Security Standard of the E-ISS created for implementation by public authorities. It includes 22 measures in total. Under the main measures, it is possible to find information on planning the implementation of AI systems, validation of models, inputs and outputs, incident management, as well as confidential data and more.

54. The E-ISS outlines who is responsible for enforcing the security measures for AI systems. The main responsibility lies with the IT department of an organisation. The organisation's management, the chief information security officer, the data protection officer, the compliance manager and the developer are also responsible. The circle of people is big, as the organisation has to know what technology is being used, how and for what purpose.

55. Although the National Audit Office is not aware of any incidents related to the use of artificial intelligence in Estonia so far, the existence of risks in this area must be taken into account. E-ISS requires that an institution must be prepared to detect, report, resolve, escalate and document incidents.

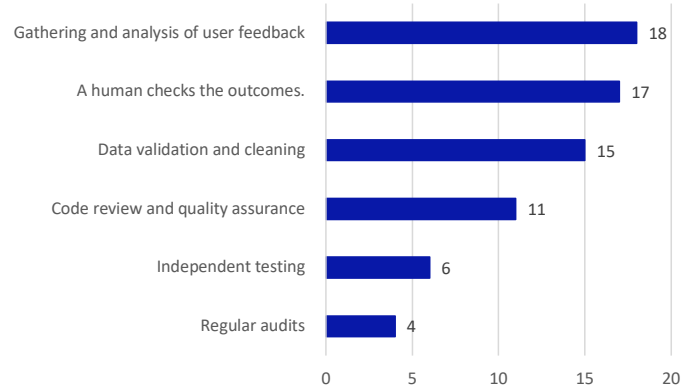
The risks associated with the development and use of artificial intelligence are largely known

56. The risks associated with the development and use of AI solutions or the use of the data they contain are largely known. The survey of the National Audit Office revealed that 29 institutions (60% of the respondents) confirmed that they had assessed such risks. Twenty-two organisations use a separate risk analysis for this.

57. However, the survey revealed that in the organisations where AI solutions had been created, the quality and correctness of the solutions were mostly checked retroactively. The majority of the organisations obtained information for this through user feedback or by checking the outcomes of the solution (see Figure 6).

[15] Draft Estonian Information Security Standard 2024.

Figure 6. How do organisations ensure the correctness and quality of the AI solutions or algorithms it created (number of organisations who chose the answer)?



Source: Survey by the National Audit Office

58. Also, while 41 of the organisations that responded are using ready-made foreign AI solutions, 33 do not yet have internal procedures on how to use these solutions correctly and securely. The lack of a procedure creates the situation where employees do not know which activities are allowed and which are not, which in turn can lead to data leaks or unauthorised access to data.

European Union Artificial Intelligence Act

59. Regulation 2024/1689 of the European Parliament and of the Council on artificial intelligence was formally approved by the European Parliament on 13 March 2024 and entered into force on 1 August 2024.[16] According to the European Union Artificial Intelligence Act, AI solutions must meet high ethical and security standards. The Act sets deadlines by which solutions must comply with the standards of the European Union and national sectoral preparedness must be established.

A human-centred approach to AI seeks to ensure that human values are paramount in the development, implementation, use and monitoring of AI systems.

Source: Ethical guidelines for the development of trustworthy artificial intelligence

60. The Act divides AI solutions into four risk categories: minimal, limited, high and unacceptable risk (see Table 3). The Act sets requirements for solutions based on the level of risk – the higher the risk level, the more restrictions there are. If the risk is the highest, i.e. unacceptable, the Act prohibits the use and development of such a solution.

[16] EU Artificial Intelligence Act or the AI act.

Table 3. Risk levels of the EU AI Act and examples of solutions that could fall into the corresponding risk category

Risk level	Description	Examples of solutions
Unacceptable risk	Divides AI solutions into 8 different categories that are incompatible with EU values and rights. Such solutions are prohibited in the Union.	Detecting human emotions using an artificial intelligence solution.
High risk	High risk includes security components of products already regulated and stand-alone AI systems in certain areas. The solutions may potentially have negative impacts on human health and safety, fundamental rights or the environment. High-risk solutions are regulated the most.	AI solutions integrated into medical devices, lifts, vehicles, other machines and critical infrastructure; automated processes that involve personal data processing; safety devices of products.
Limited risk	Includes solutions exposed to the risk of manipulation or wrong decisions. Such solutions will be subject to the obligation to inform the user that the solution is an AI solution in order to ensure transparency.	Chatbots.
Minimal risk	Includes solutions that do not fall into any of the above risk categories. No additional restrictions are applied to solutions with minimal risk.	Spam filters.

Source: National Audit Office, European Commission (https://digital-strategy.ec.europa.eu/et/policies/regulatory-framework-ai)

61. According to the survey carried out during the preparation of the overview, organisations have mostly rated the risk level of their AI solutions as low, with a few organisations rating the risk as high.

62. The European Union Artificial Intelligence Act prohibits the use of solutions with an unacceptable risk level as of February 2025. New regulations concerning new high-risk solutions will be added as of August 2026. These regulations will apply to all high-risk solutions as of August 2027. These regulations will apply to all solutions that have been created and will be created as of August 2030.

63. A national regulation on artificial intelligence is being prepared under the leadership of the Ministry of Justice and Digital Affairs, which will clarify the organisation of the area (supervision, penalties, etc.). According to the plan, the draft act on the implementation of the on AI Act should be ready and submitted for approval in the second quarter of 2025, and the draft act on the amendment of the Administrative Procedure Act should be submitted to the Government in 2025. Amendments to the Public Information Act are not currently on the agenda and it is not clear what the timeframe for these amendments will be. In Estonia, national legislation will be amended in the near future, and hopefully this will make it clearer for both the organisations and the public what is and is not allowed in the development of artificial intelligence.

/digitally signed/

Ines Metsalu-Nurminen
Director of Audit, Audit Department

Characteristics of the overview

Purpose of the overview

The objective of the overview is to describe how public sector organisations use and develop solutions based on artificial intelligence. Among other things, the focus will be on the prerequisites, obstacles and use cases concerning the creation of AI solutions.

The results of the overview will be covered in the summary report of the joint audit organised by the European Organisation of Supreme Audit Institutions (EUROSAI).

Scope and focus of the overview

The overview covers the period from 2016 to 2024.

Main questions of the overview:

- Is there a strategy and implementation plan for the development of artificial intelligence?
- Are there regulations that set rules for the development and use of artificial intelligence solutions?
- Have activities been planned for the management and improvement data quality in databases, which are necessary for the implementation of artificial intelligence solutions?
- Is there an IT infrastructure for the development and implementation of artificial intelligence solutions and what is it like?
- How are risk management and ensuring security for solutions guaranteed in the development and use of artificial intelligence?
- What kind of AI solutions have been implemented in public sector organisations?

The review included an analysis of documents, an online survey and interviews with various parties.

Analysis of documents

The analysis of documents was based on the following documents:

- the Estonian Artificial Intelligence Strategy (Kratt Strategy) for 2019–2021;
- the Estonian Artificial Intelligence Strategy (Kratt Strategy) for 2022–2023;
- the Artificial Intelligence Strategy for 2024–2026;
- White Paper on Artificial Intelligence and Data for 2024–2030;
- the Data Strategy for 2024–2025;
- Digital Agenda 2030.

Online survey and interviews

An invitation to the online survey was sent to 58 organisations, including ministries, public authorities, constitutional institutions, foundations established by the state and legal persons governed by public law. Forty-eight organisations responded to the survey (see Table 4).

Table 4. Organisations that responded to the survey

Organisations that answered the questions
Ministry of Education and Research
Education and Youth Board
Language Board
National Archives
Data Protection Inspectorate
Estonian Forensic Science Institute
Patent Office
Prosecutor's Office
Ministry of Defence
Defence Resources Agency
Ministry of Climate
Environment Agency
Environmental Board
Information Technology Centre of the Ministry of Environment
Environmental Investment Centre
Transport Administration
Ministry of Culture
Ministry of Economic Affairs and Communications
Estonian Information and Communication Technology Centre
State Infocommunication Foundation
Estonian Information System Authority
Consumer Protection and Technical Regulatory Authority
Labour Inspectorate
Ministry of Finance
Tax and Customs Board
IT Centre of the Ministry of Finance
Financial Intelligence Unit
Shared Service Centre of the State
Ministry of Regional Affairs and Agriculture
Land Board
Rural Development Foundation
Agriculture and Food Board
Agricultural Registers and Information Board
Ministry of the Interior
Emergency Response Centre

Rescue Board
IT and Development Centre of the Ministry of the Interior
Ministry of Social Affairs
State Agency of Medicines
Social Insurance Board
Health Board
Ministry of Foreign Affairs
The Government Office
Supreme Court
Office of the Riigikogu
Office of the Chancellor of Justice
Estonian Public Broadcasting
Estonian Unemployment Insurance Fund

The list of interviewees is given in Table 5.

Table 5. Interviewed parties

Interviewed persons	Organisation	Time of interview
Ott Velsberg – Head of Data	Ministry of Economic Affairs and Communications	10.07.2024
Markko Liutkevičius – Head of the Machine Learning and Language Technology Unit	Estonian Information System Authority	16.07.2024
Jaanika Merilo – eHealth Strategy Manager	Ministry of Social Affairs	09.09.2024
Ott Karulin – Head of State Governance Kaur Karus – Head of Data	Ministry of Finance	14.10.2024
Risto Raaper – Head of ICT	Ministry of Culture	29.10.2024
Gerli Kööse l – Leader of Bürokratt Urmas Sinisalu – Head of the National Library Services Centre	National Library	29.10.2024
Evar Sõmer – Advisor to Secretary General Henrik Trasberg – Advisor of the Legal Policy Department	Ministry of Justice and Digital Affairs	06.09.2024
Sten Kapten – Education Innovation Advisor, General Education Curricula and Courseware Raina Loom – Head of Legal and Personnel Policy Department Margit Grauen – Head of Digital Courseware Riin Saadjärv – Advisor on General Education Curricula and Courseware	Ministry of Education and Research	11.10.2024
Tanel Tera – Head of Business Services Department Martin Õunap – Chief Architect	Health and Welfare Information Systems Centre	09.09.2024
Ivo Tamm – Head of IT Department Mario Liimann – Software Architect Mariell Viinalass – Development Advisor/Business Architect	Agricultural Registers and Information Board	10.10.2024
Alvar Pihlapuu – Head of Development Department	Tax and Customs Board	17.12.2024

Overview completion date

The overview was completed on 17.12.2024.

Overview team

Audit Manager Toomas Viira, auditors Hanna Kätlin Ardel, Jevgeni Lazartšuk, Alo Lääne.

Contact information

Further information on the audit is available from the Communication Unit of the National Audit Office: telephone: +372 640 0777; email: riigikontroll@riigikontroll.ee

An electronic copy of the audit report (PDF) is available online at www.riigikontroll.ee.

A summary of the audit report is also available in English.

The number of the audit report in the record management system of the National Audit Office is 80157.

The postal address of the National Audit Office is:

Kiriku 2/4
15013 TALLINN
Telephone: +372 640 0700
riigikontroll@riigikontroll.ee

Earlier audits by the National Audit Office in the area of data

02.02.2023 – Database access management

29.04.2020 – Availability and use of data for smart state management (memorandum)

All reports are available on the website of the National Audit Office at www.riigikontroll.ee.

Cour des comptes

THE NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH STRATEGY

A strategy in need of more structure and sustainability

Themed public report

April 2023

Executive Summary

Artificial intelligence (AI) is an old concept, first appearing in the 1950s in the work of British computer scientist Alan Turing. Despite considerable debate in the scientific community over the semantic question of what AI is and where it falls, it can be defined by its purpose – to reproduce human intelligence through the use of computers and mathematics. AI developed mainly from the 1980s onwards, with the emergence of machine learning algorithms. In the 2000s, the growth in computing capacity and access to data encouraged the development of deep learning techniques.

AI has many applications today, and has produced innovation and productivity gains in many sectors. The result has been steady growth in economic investment since the 2010s. According to the OECD, AI start-ups attracted almost 12% of global private equity in the first half of 2018, up from 3% in 2011. Research publications have followed a similar trend, with more than 1.2 million publications in 2019, compared with fewer than 40,000 in 2010. In addition to such opportunities, its growth brings with it a number of challenges, not least ethical, particularly in terms of protecting citizens' rights.

As a result, AI has become an issue of growing priority for public authorities. The adoption of national plans by a number of countries since 2017 to encourage its development bears witness to this, and is a response to the strong competition that exists on an international scale to raise technology levels in countries and attract the best talent. In France, a "national strategy for artificial intelligence" (NSAI) was launched in March 2018, with the aim of positioning France as one of the major AI players on the global stage. Initially endowed with €1,527m of public funding for the period 2018-2022, it has focused on five key components: 1) research, 2) higher education, 3) public transformation, 4) dissemination throughout the economy, 5) defence and security. In November 2021, a new "acceleration" phase for the NSAI was announced for the period 2022-2025, with the aim of strengthening France's competitiveness and attractiveness in this field. This new phase builds on the ambitions of the first phase of the strategy, and the public funding allocated to it is expected to be similar to that for the 2018-2022 period. It has also been drawn up in line with priorities at European level.

Breakdown of the state budget initially earmarked for AI strategy for the period 2018-2022

Key areas of national AI strategy	Estimated state funding (€m)
Research	445
Higher education	128
Transforming public action	154
Economy	390
Defence and security	410
Total	1,527

Source: Court of Accounts processing based on data from the national AI strategy coordinator

This report is an initial NSAI assessment. It covers the "research" and "higher education" components, which are the main funding components, amounting to €1,527m and €1,545m respectively in the first and second phases. Over the period 2018-2022, €445m, or almost 30% of the funding allocated to the strategy, was earmarked for research, compared with €134m, or 8.7%, in the second phase. Meanwhile, funding earmarked for training over the period 2022-2025 has risen sharply (50.2% of allocated funding, compared with 8.4% in the previous phase).

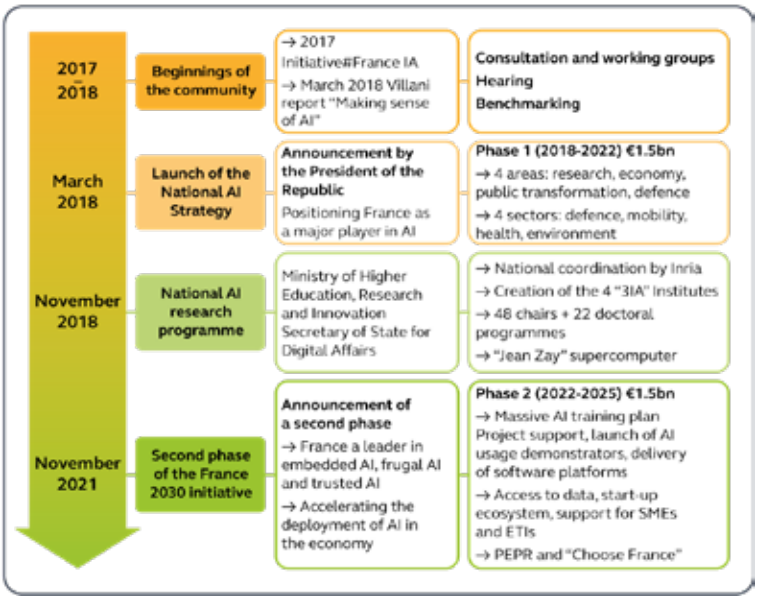
The assessment questions were defined in consultation with the NSAI's stakeholders and the public authorities responsible for its implementation. They were divided into four main questions:

- has the national research strategy strengthened France's position at global and European level? [consistency, effectiveness and efficiency];
- has the national research strategy helped to provide structure for the French AI ecosystem? [relevance and efficiency];
- is the national research strategy for centres of excellence effective and efficient? [effectiveness and efficiency];
- has the national research strategy improved the consideration of ethical issues (frugal and trust-based AI)? [relevance, consistency and effectiveness].

In response, an unprecedented effort to semantically analyse and exploit numerous databases based on statistical and econometric methods was carried out in order to quantify and assess the results of the strategy. This quantitative component was supplemented by numerous semi-structured interviews and focus groups, in addition to a consultation with AI researchers and a participatory workshop with experts in the field.

In 2018, France was one of the first countries worldwide to have a formalised plan for AI. Since then, many countries have drawn up national strategies or specific measures.

Stages in the development of the national AI strategy



Source: Court of Accounts

Initially, the French strategy gave priority to AI research. In addition to the 30% of funding allocated to it for the 2018-2022 period, research has also been the subject of a specific plan, entitled the "national artificial intelligence research strategy" (NAIRS), coordinated by the French national institute for research in computer science and control (Inria). International comparisons based on OECD data, and the more specific study carried out by the Court of Auditors on the AI strategies or public policies of 10 countries [1], show that identifying research as a strategic priority is the most frequent choice made by governments.

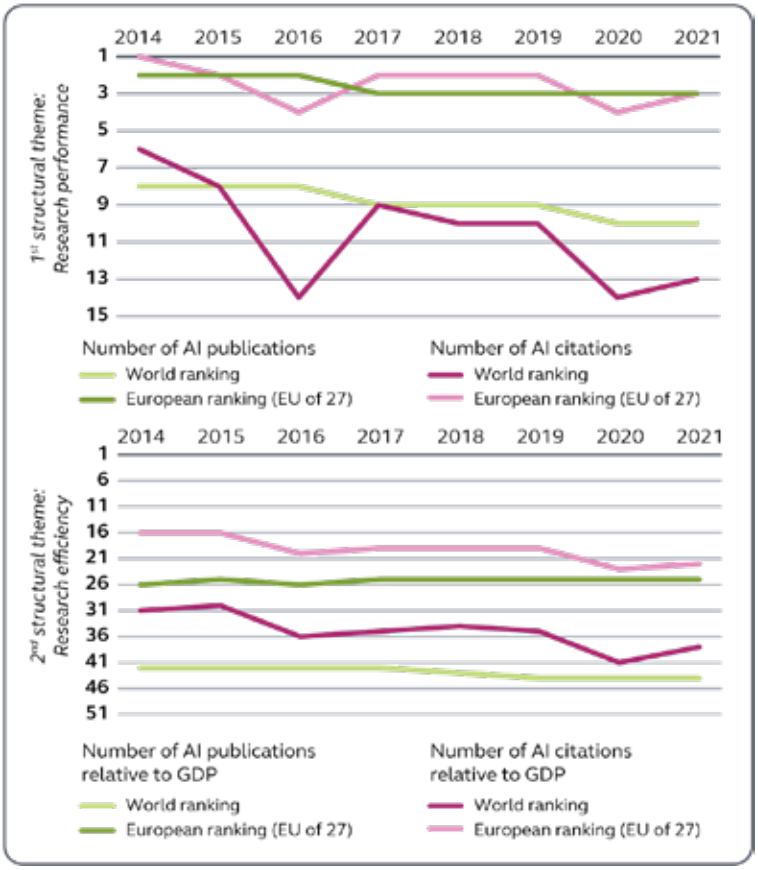
Since its launch, most of the measures planned in the NAIRS have been implemented. In establishing a formal strategy, the public authorities have given a strong political signal about the importance of AI for French research. In fact, over and above the actions set out in the strategy, this is now a key issue in all discussions within a number of research organisations. Evaluations and – more importantly – econometric analyses of global data support the decision to adopt a strategic plan. However, the effectiveness of the strategy to strengthen France's position in AI, in line with the objective initially set for it, has not been proven. Over the period analysed, in terms of the number of AI publications and out of a total of 47 countries compared, France has barely maintained its position in 10th place worldwide, and remains in 2nd place in Europe. However, given the long timeframe involved in research, it is not yet possible to reliably assess the real-world effects of the strategy on scientific output.

In addition, the funding put in place needs to be monitored more closely in order to measure the effects of the financial efforts of this AI strategy on France's scientific standing and organisational structure. The resources allocated to the strategy do not cover all public investment in AI. For the research component, €554.6m was ultimately committed over the 2018-2022 period, although the actual implementation of appropriations is not tracked in a comprehensive and summarised way.

With a view to attracting talent, certain financing tools would benefit from being made permanent. The vast majority (over 80%) of funding was distributed via short-term financial instruments, using calls for projects. However, the lack of clarity over the long-term future of these funding windows is likely to create disruptive effects in training for young researchers (doctoral programmes) or the continuation of research programmes (academic chairs).

[1] United States, Canada, Germany, Finland, Italy, Netherlands, United Kingdom, Switzerland, Israel, Japan.

France's ranking in the world and in the EU of 27 according to complementary and differentiating criteria on the international scene

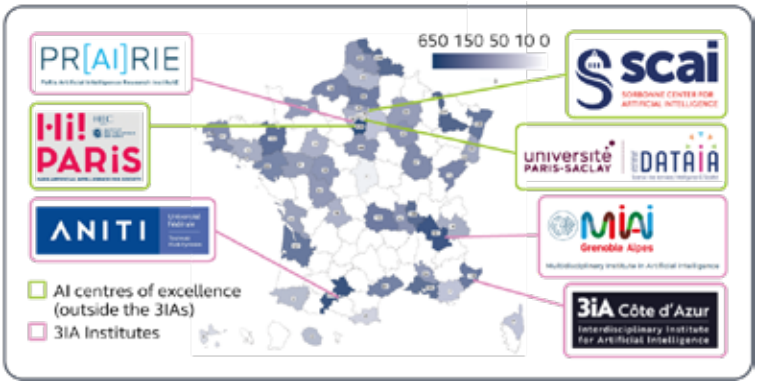


Source: Court of Accounts
Reading note: With regard to indicators relating to the efficiency of research, it should be noted that the Covid-19 crisis may have had an impact on countries' GDPs from 2020 onwards. Tracking country rankings helps to limit the biases associated with standardisation by annual GDP, as shown by the relative stability of the two applicable time series over the period from 2019 to 2021.

The main thrust of the strategy is the creation of centres of excellence in AI [2], through the accreditation of interdisciplinary AI institutes (3IA), the establishment of individual chairs, and the identification of centres of excellence outside the 3IA institutes. The result is a strengthening of geographical areas already active in artificial intelligence, the structuring of an ecosystem and an increase in the scientific output of the sites, although it is not possible to demonstrate the impact of the strategy on the latter development.

[2] The "centres of excellence" bring together three types of entities: the four interdisciplinary AI institutes (3IA institutes) identified during the first phase via a specific ANR call for proposals; the 43 individual chairs held by a researcher identified via another specific ANR call for proposals; the three other centres of excellence, known as "non-3IA", identified by the strategy coordinator in 2021, without being the subject of a call for proposals and whose members may hold an individual chair.

Establishment of themed AI institutes (3IA PR[AI]RIE, MIAI, 3IA Côte d'Azur and ANITI) and centres of excellence (SCAI, DATAIA and Hi! PARIS) compared with areas historically active in this field



Source: Court of Accounts
Reading note: Historical activity in AI is measured through the departmental distribution of AI theses defended between 1989 and 2019 in French higher education establishments, based on open data from theses.fr (ABES). Theses are listed by the year in which they were defended. AI theses are identified using the semantic method developed by the Court. The logos of the 3IAs and AI centres of excellence are taken from their official websites.

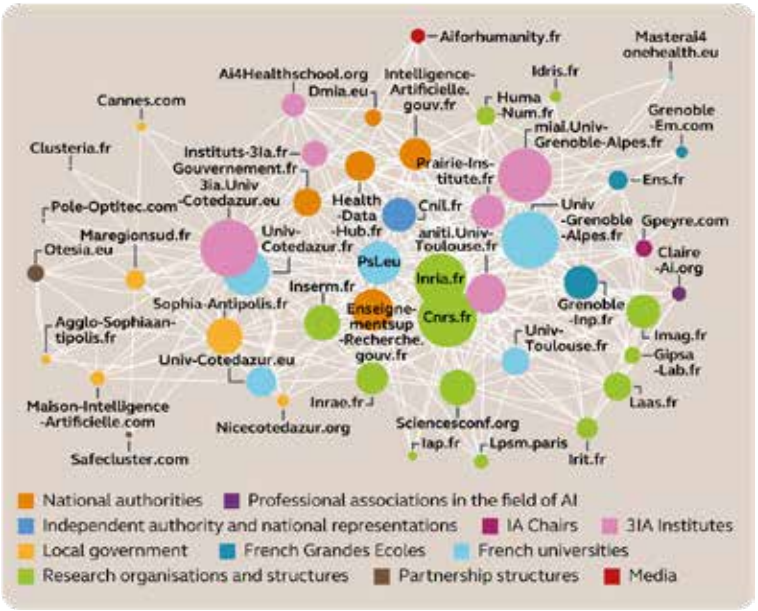
Synergies between centres of excellence need to be strengthened; for example, by adopting a more systematic approach to promoting each other's work. This would help to raise their profile both nationally and internationally, as well as enhancing France's image as a magnet for foreign talent.

At the same time, the work of the 3IA and non-3IA centres of excellence needs to be clarified. The non-3IA centres of excellence were identified after the 3IA institutes had been labelled and – unlike the 3IA institutes – without any competitive call for projects involving an independent jury. The public authorities' expectations of them are therefore less explicit, and their development model less constrained by funding conditions. They are, however, involved in the second phase of the strategy just as the 3IA institutes are. This review process must be accompanied by a review of the timeframe for funding allocated to accredited institutes (currently four years), which is too short-term to allow for leverage effects.

The lack of clarity over time in the associated funding has also been identified for the training of young talent through doctoral programmes and Convention Industrielle de Formation par la Recherche (CIFRE) contracts. Although the strategy has sent out a strong signal in favour of such an approach, it is now important to ensure that the funding needed to sustain this momentum is sustained.

The evaluation shows that the NAIRS provided a means of structuring AI research stakeholders, at a time when AI was not identified as a discipline in its own right. However, this structuring still needs to mature: a comparison of French and German stakeholders based on a network analysis shows that in France, this structuring is still mainly organised around the main research bodies, whereas German university sites and multidisciplinary centres are more effective in structuring their national ecosystem.

Representation of the French sub-network resulting from the 3IA institutes



Source: Court of Accounts, based on the web and the Hyphe tool from Sciences Po Paris

In order to improve coordination between the various players, it is urgently necessary to make changes to the strategy's governance and management. The performance model that was initially developed was ultimately not used. There is no annual report for monitoring the progress of the strategy. Its steering mechanism, provided by national coordination, is not in a position to monitor the various stages of the project, to check funding and expenditure, or to rectify any difficulties that may arise. It has weakened over time, and runs the risk of becoming inoperative. No specific governance arrangements have been put in place for the research component, with Inria being the only operator represented on the strategy's overall steering committee. Making changes to governance could provide an opportunity to create a shared overview of public action in AI, at a time when the measures decided upon in this area remain dispersed across several public policies.

Although the national research strategy has not yet strengthened France's position at global level, the first component of the strategy has prevented the country from falling behind in science terms since 2018. The second component is now crucial to improving France's position in AI in terms of global competition. This "AI acceleration strategy" is refocused on the objective of training AI talent, a priority that has received little attention to date. Total funding for this priority amounts to €776m, including €500m for the "excellence" component and €276m for the "massification" component. The launch of the "Skills and Trades of the Future" call for expressions of interest (AMI CMA) in 2022 is one of the ways in which this effort is being seen operationally.

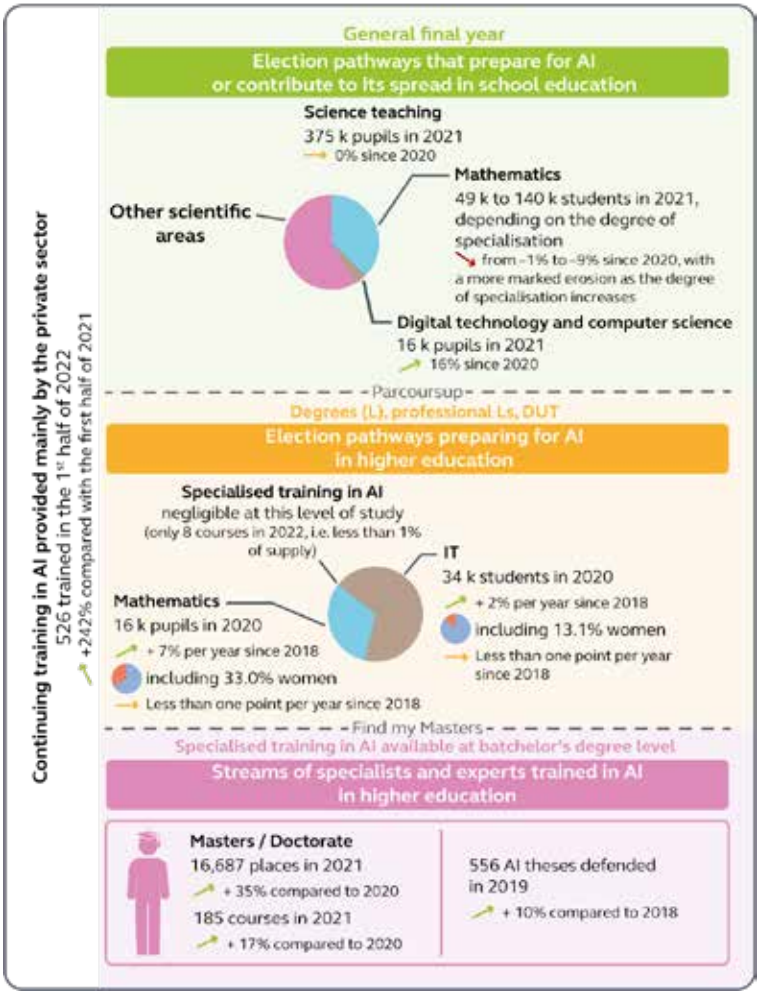
Funding for the second component of the NSAI – acceleration strategy (in €m)

In €m	Research programme	Decentralised and embedded AI	Trusted AI	Dissemination of AI & responsible AI demonstrators	Skills and talents	Total
Public funding	134	265	111	259	776	1,545
PIA 4	73	263.5	97.5	123		557
France 2030					700	700
Other State and local authority loans	61	1.5	13.50	136	76	288
Private financing		310	105	86	5	506
European Union		60	10	16		86
Total	134	635	226	361	781	2,137

Source: Restated by the Court of Accounts based on the press kit of 8 November 2021 and data from the national coordinator

The current limited number of high-calibre public trainers could impede our stated ambitions, especially as there is a tension between investment in teaching and excellence in research. The number of specialist trainers in public higher education is currently insufficient to meet AI training needs, both for initial and continuing training.

Mapping of training courses and growth in the number of learners trained in AI and in its "upstream" election sectors



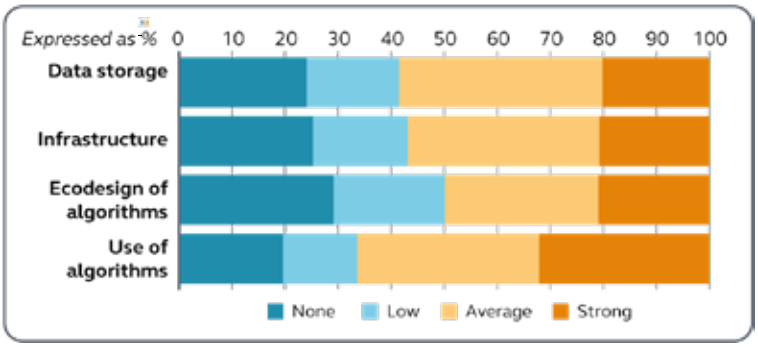
Source: Court of Accounts based on data from the MENJS, the MESR and the Caisse des Dépôts et Consignations, with semantic filtering applied to identify training courses specific to AI. The term "k" represents thousands

For the previous graph, the order of magnitude of the total number of academic AI experts is estimated on the basis of information provided by research operators and universities as part of the consultation carried out by the Court, as well as on the basis of the number of teaching and research staff in university departments where AI is prevalent.

The French approach would benefit from being even more closely integrated into the European approach. Various European research support programmes are designed to encourage the development of AI, including "Horizon Europe" (a total of almost €100 billion over the period 2021-2027) and "Digital Europe" (a total of €7.5 billion over the same period). The priorities of the French strategy were developed in 2018, taking into account the European plan for AI initiated in 2018 and updated in 2021. The acceleration phase now offers the opportunity to further capitalise on the efforts made at European level.

Trust [3] and frugal use of resources [4] are two of the four key themes of the €73m Priority Research and Equipment Programme (PEPR), which is part of the acceleration strategy. However, there is still a need to improve the scientific community's understanding of these issues. Consultations with AI researchers by the Court show that these issues are currently given little consideration in research work.

Perception of how environmental impact is taken into account in research



Source: Court of Accounts – Consultation of the scientific community with respect to AI

This issue is particularly acute with regard to the concept of "frugal AI", with a potential tension between resource efficiency and performance. Frugality should be better integrated into calls for projects; for example, by drawing up a charter or guide to good practice.

For the research component, priorities in this second phase are refocused on attracting talent and addressing social issues, such as trust in AI and frugal use of AI resources. This latest development reflects a reorientation of the research component, which has a greater focus on applied research to take account of the growth of industrial AI.

[3] Trusted artificial intelligence is characterised by its interpretability, explicability, transparency and "responsible" identity.
[4] Frugal artificial intelligence is sustainable and respectful of the environment in its efforts to minimise its consumption of energy and resources.

Audit recommendations

1. Translate public policy on artificial intelligence into a summary budget document that will enable it to be monitored and its effects measured (*MEFSIN*).
2. Specify the respective roles of the 3IA and non-3IA centres of excellence, and then clarify the multi-year funding allocated to them (*MESR, SGPI*).
3. Establish shared objectives and priority indicators for public policy on AI, in line with European strategy (*MEFSIN, SGPI*).
4. Create a scientific and steering committee at Inria, co-chaired by France Universités, to monitor the implementation of the strategy and define future strategic orientations (*MESR, Inria*).
5. Draw up a harmonised, up-to-date map of AI training courses to be promoted via a shared certification label in order to raise their profile and support their expansion (*MESR*).
6. Forecast the need for secondary school teachers, teacher-researchers and researchers trained in the use of AI, and draw up appropriate training plans (*MESR*).
7. Draw up a charter and a catalogue of best practices to define and monitor the environmental impact of AI research, and encourage the development of responsible AI (*SGPI, MESR*).

Cour des comptes

THE NATIONAL STRATEGY FOR ARTICIAL INTELLIGENCE

Public policy on AI : consolidating its successes, broadening its scope

Thematic public report

Summary

November 2025

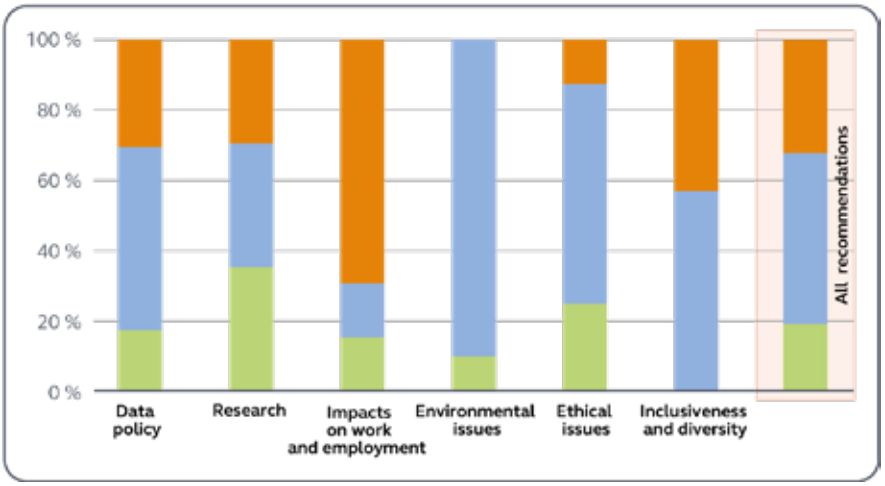
Summary

Following a trend that began in several countries in the mid-2010s, France decided to launch a strategic review of the challenges associated with artificial intelligence (AI) and to develop a specific public policy in this area. The first phase of the National Strategy for Artificial Intelligence (*Stratégie nationale pour l'intelligence artificielle*, SNIA), conducted between 2018 and 2022, focused primarily on strengthening research in this field. A second phase, known as the acceleration phase, was announced at the end of 2021 and has been implemented mainly from 2023 onwards, with the central objective of disseminating AI throughout the economy. In February 2025, on the occasion of the Paris Summit for Action on Artificial Intelligence, the President of the Republic announced a third phase of the national strategy, the details of which were clarified in the months that followed.

The 2018-2022 phase of the strategy: strengthening AI research

The implementation of the first phase of the national strategy for artificial intelligence made it possible to initiate a public policy on AI in France, even if it was only able to cover part of the issues identified in March 2018.

Recommendations from the Villani report of March 2018, ranked according to their level of implementation during the first two phases of the SNIA



Key:
Green: recommendation largely committed to and implemented during the first phase 2018-2022
Blue: recommendation largely committed to and implemented during the second phase 2022-2025
Orange: recommendation still to be implemented (even if initial actions have already been taken)
Source: Court of Auditors, based on the Villani mission report of March 2018 and the national coordinator

The management and implementation of this first phase was based on a complex interplay between numerous actors. The diverse resources allocated by the government ultimately amounted to €1.3 billion, and their monitoring proved to be deficient.

Despite several limitations, the main contribution of this phase was to help initiate the development and structuring of research and innovation in the field of artificial intelligence, with the creation of centers of excellence, the opening of essential computing infrastructures and support for the growth of AI startups in a variety of fields.

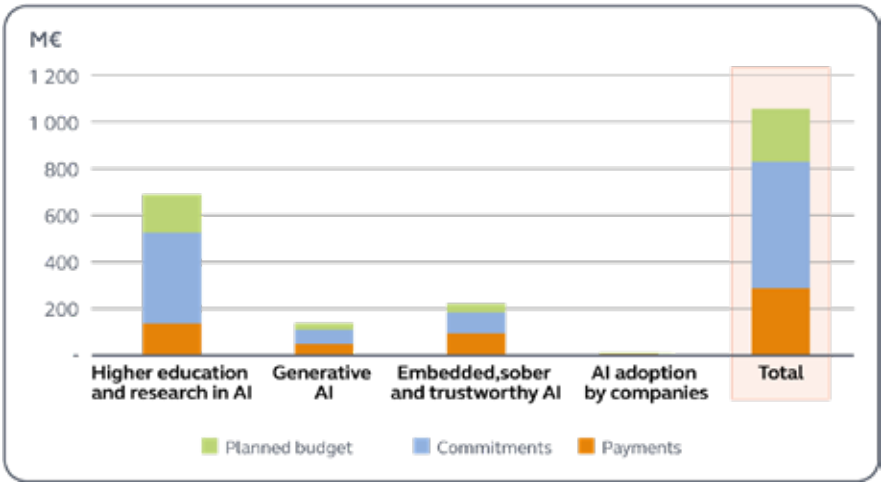
In the other areas covered by the SNIA – defense and security, the transformation of public action and the dissemination of artificial intelligence in the economy – progress has been less clear-cut. Several of the announced priorities, particularly on the key issues of training and supporting change in the economic sectors most affected by AI, have not been implemented or only to a very limited extent, at the risk of causing France to fall behind.

The 2023-2025 phase of the strategy: aiming for the diffusion of AI in the economy

Launched without prior evaluation, the second phase of the SNIA was supposed to take up the challenge of massifying and supporting the diffusion of artificial intelligence in all areas. Announced in November 2021, this phase has seen its priorities, budget and timetable change significantly due to growing constraints on public finances and the need to reallocate resources to support the development of generative AI, an issue that had not been anticipated on the eve of the "ChatGPT revolution".

In total, the government allocated €1.1 billion over the period 2023-2025, which is one-third less than initially announced, and the slow start-up of most of the measures has resulted in a low level of budget consumption (35% as of 30 June 2025).

Budget implementation for the second phase of the SNIA



Commitments and payments as at 30 June 2025
Source: Court of Auditors, based on data from the SGPI and the National Coordinator for AI

The governance of public policy on artificial intelligence has also remained complex, despite some positive developments and several examples of successful coordination with other so-called “acceleration” strategies of the France 2030 programme.

The initial results of this second phase are beginning to emerge in several areas. Although it is still too early to fully assess the effects, the initiatives taken to strengthen the structure and excellence of research and higher education in the field of AI are producing initial results, and France’s position in this area is improving. Our country has risen from thirteenth place in the Global AI Index published in September 2024 to fifth place in September 2025. In terms of research and training in artificial intelligence, France ranks third in the world. More than 4,000 French researchers are currently working on AI.

The mobilization that this second phase has enabled in the field of generative AI has also borne fruit. At the beginning of 2023, France had only one player positioned in this type of system. In just a few months, French industry has made progress in terms of competitiveness and attractiveness, with the emergence of a dozen players operating in a wide variety of fields. The number of French AI startups has doubled since 2021: more than 1,000 of them are active in this field in 2025 and they raised nearly €2 billion in funding in 2024. Sixteen French startups valued at over $1 billion (unicorns) incorporate artificial intelligence into their value proposition, and several major French groups are increasing their offering and investment in AI research. France is the leading European country in terms of the number of foreign investment projects in artificial intelligence, and in terms of hosting research and decision-making centers for Big Tech AI companies.

Efforts to develop computing infrastructure have continued, with the expansion of installed capacity and investment in a new-generation supercomputer. Significant progress has also been made on the issues of frugality and trust. Finally, France is no stranger to the acceleration of European policy on AI and, more broadly, to the fact that international forums are addressing key issues of governance and regulation of the development of artificial intelligence. The success of the AI Action Summit held in Paris in February 2025 confirmed France’s special place on the international stage.

However, alongside these successes, several equally important areas have been neglected. The challenge of massifying and supporting the dissemination of artificial intelligence beyond the circle of specialists – businesses, public administrations, students, citizens – has so far received too little attention, even though it was at the heart of the ambitions set out for this phase of the SNIA and the years 2023-2025 were critical in this regard. As a result, the priority of supporting business demand for artificial intelligence solutions has only benefited from very modest measures, and the expected acceleration and massification of the diffusion of artificial intelligence in the economy has not taken place. The delay in adapting all initial and continuing training programmes to AI has not been made up either, even though this is an area where the stakes are considerable and the risks high. Essential projects concerning schools and universities have yet to be designed and implemented. The transformation of public action through artificial intelligence, which has also not been a priority, has been very disappointing too: despite isolated initiatives, the administration is generally lagging behind. Finally, actions targeting regions and the general public have not been a priority for the SNIA to date, even though they appear all the more necessary as the impacts of this general-purpose technology accelerate, intensify and become more widespread.

The outlook: consolidate the successes of public policy on AI and broaden its scope

A third phase of the SNIA was launched in February 2025, with the aim of accelerating the diffusion of artificial intelligence in businesses.

Artificial intelligence is no longer the same issue it was in 2018, when the SNIA was launched. The revolution brought about by this general-purpose technology is reaching a magnitude that few other technological breakthroughs in history can match. AI is no longer a matter for specialists alone; it affects all fields of knowledge, the economy, and society, and is becoming an essential priority for public policy. Successfully achieving the scale change required by the artificial intelligence revolution requires several prerequisites to be met:

Prerequisites for successfully scaling up AI

Source: Court of Auditors

Given the rapid pace of change in the AI landscape, it would be a mistake to assume that the priorities on which SNIA has achieved initial success no longer require attention. Public policy on artificial intelligence must seek to expand its areas of excellence and aim for even more structural transformations and impacts. Five key areas, which have been under development since 2018, should therefore be further explored:

Areas for further development for more structural transformations

Source: Court of Auditors

Finally, the first two phases of the SNIA have blind spots in several key areas, or at least have failed to achieve results commensurate with the challenges. This is particularly the case in projects that require the involvement of a wide range of stakeholders and links with other

public policies. Five critical challenges, which have not been sufficiently addressed to date, must be placed at the heart of public policy on AI in the coming years:

Critical challenges to be placed at the heart of public policy on AI

Source: Court of Auditors

The national strategy for artificial intelligence has created real momentum since its launch in 2018. France has managed to climb to the top of the European pack, including in the latest and most widely used generative AI technologies. It can compete with its rivals, the United States and China set apart, in most innovations related to artificial intelligence, and its visibility on the international stage, as confirmed by the Paris summit in February 2025, is real.

The Court of Auditors has made ten recommendations, the implementation of which would enable public policy on artificial intelligence to scale up, build on the initial successes of the SNIA, and overcome the limitations and shortcomings identified.

It is on this condition that France, in close cooperation with the European Union and local authorities, drawing on the training-research-innovation ecosystem as well as businesses and investors, even if it means changing its operating methods, will continue on its path to excellence and succeed in embracing all the dimensions that the AI revolution is set to affect, in the service of the common good and with a view to guaranteeing national sovereignty.

Recap of recommendations

The Court makes the following recommendations:

1. By the end of 2025, strengthen interministerial oversight of public policy on AI by establishing an ad hoc general secretariat, and better reconcile the necessary ambition of this policy with the challenges of efficiency and effectiveness by conducting an in-depth assessment of results and seeking greater complementarity with the European level, regions and the private sector (*Prime Minister, Ministry of the Economy, Finance and Industrial and Energy Sovereignty, Ministry of Higher Education and Research, National Institute for Research in Computer Science and Automation*).

Adopt, by the next AI summit in February 2026, a strategy with a view to:

2. Ensure long-term excellence in training, research and innovation in the field of AI by better defining needs, giving stakeholders greater responsibility, reaffirming the purpose of public research and promoting mobility with the private sector (*Prime Minister, Ministry of the Economy, Finance and Industrial and Energy Sovereignty, Ministry of Higher Education and Research, National Institute for Research in Computer Science and Automation*).
3. Increase, in coordination with the European Union, the computing capacities for AI and redefine, through new forms of partnership between the public and private sectors, the conditions for financing, building and operating these infrastructures, which guarantee open access to all users (*Prime Minister, Ministry of the Economy, Finance and Industrial and Energy Sovereignty, Ministry of Higher Education and Research, National Institute for Research in Computer Science and Automation, National Centre for Scientific Research*).
4. Strengthen the transfer of research to industrial development and support the growth of AI companies, including by leveraging public procurement and strengthening the monitoring of industrial acquisitions in the AI sector (*Prime Minister, Ministry of the Economy, Finance and Industrial and Energy Sovereignty, Ministry of Higher Education and Research, National Institute for Research in Computer Science and Automation*).
5. Implement and pursue commitments to trustworthy, frugal and sustainable AI, including at European and international level (*Prime Minister, Ministry of the Economy, Finance and Industrial and Energy Sovereignty, Ministry of Higher Education and Research, Ministry for Europe and Foreign Affairs, National Institute for Research in Computer Science and Automation*).
6. Better anticipate changes in the labor market, adapt teaching methods and tools as well as the content of all higher education courses to AI, disseminate AI in all research sectors, refocus continuing education efforts, and support professional changes related to AI (*Prime Minister, Ministry of the Economy, Finance and Industrial and Energy Sovereignty, Ministry of Higher Education and Research, Ministry of Labor, Health, Solidarity and Families, National Institute for Research in Computer Science and Automation*).
7. Support the acceleration and mass adoption by businesses over the next five years of AI use cases tailored to their needs, including by increasing communication, making available resolved use cases, supporting pioneering businesses on as yet unresolved use cases, and promoting the development of high-performance software associated with sovereign clouds (*Prime Minister, Ministry of the Economy, Finance and Industrial and Energy Sovereignty, Bpifrance, National Institute for Research in Computer Science and Automation*).
8. In coordination with all stakeholders, strengthen access to data for AI systems, guarantee its quality, better protect sensitive data and intellectual property, take into account the latest

scientific advances (federated learning, decentralized AI) and invest in sovereign storage capacities (*Prime Minister, Ministry of the Economy, Finance and Industrial and Energy Sovereignty, National Commission for Information Technology and Civil Liberties*).

9. Build a realistic ambition for electronic components for AI and better coordinate public policy on AI with policies on the infrastructure that underpins its development, particularly with regard to electricity supply and connectivity (*Prime Minister, Ministry of the Economy, Finance and Industrial and Energy Sovereignty, Bpifrance, National Institute for Research in Computer Science and Automation*).

10. Accelerate the transformation of public administrations and policies through AI, in particular through increased use of innovative public procurement and the introduction of incentive mechanisms, support measures and specific training for civil servants (*Prime Minister, Ministry of the Economy, Finance and Industrial and Energy Sovereignty, National Institute for Research in Computer Science and Automation*).

Report of the State Comptroller of Israel – Cyber and Information Systems | November 2024

Special Report

Artificial Intelligence – National Preparedness

Artificial Intelligence – National Preparedness

Background

Artificial intelligence (AI) is an overarching term for technologies developed to enable machines to execute tasks that necessitate human intelligence. The ongoing AI revolution is recognized as a "disruptive innovation" poised to alter various aspects of life and numerous industries significantly. The Ministry of Innovation[1], Science and Technology (the Ministry of Innovation) defines AI as "the capability of a machine to learn to perform human actions and enhance its performance, relying on data, examples, and operational experience, and, in a broader context, all technological operations extracting information and insights from databases."

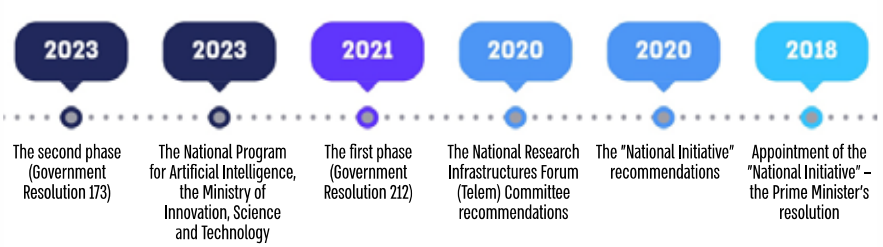
Academic research in artificial intelligence dates back to the 1950s. However, in recent years, particularly following the introduction of various tools and applications (apps) available in the market for diverse fields, there has been a marked advancement in the integration capabilities between man and machines, which some characterize as a genuine revolution. AI is employed in various sectors, including the development of autonomous vehicles, analysis of X-ray images, assessment of credit risks, securities trading, and candidate evaluation for employment. Furthermore, AI systems play integral roles in interactions between consumers and businesses, businesses and other businesses, professionals and clients, labor relations, public sector entities, and the public and general public.

AI was also widely used during the "Iron Swords" War; apart from its operational use, it contributed to the identification and location of hostages and fatalities. In advocacy, AI facilitates the creation of multilingual videos, enhancing accessibility to diverse populations worldwide through voice reproduction, animation, dubbing, subtitles, and translation. Additionally, the war highlighted the use of "deepfake" technology – a form of AI utilized by various parties for propaganda and the dissemination of misinformation.

In May 2018, the Chief of Staff for the National Security Council at the time, following the Prime Minister's directive, appointed project leaders to formulate a national plan to bolster scientific-technological resilience as a critical component of Israel's national security ("the National Initiative"). Thus positioning Israel globally among the top five countries in core technological domains, including artificial intelligence and data science. The Initiative's report was presented to the Prime Minister and published in September 2020.

1 Breakthrough innovation that brings about a fundamental change and often threatens the existing one.

Artificial Intelligence in Israel – Milestones in 2018–2023



In February 2020, the Chairman of the National Research Infrastructures Forum (Telem Forum[2]) appointed a professional review committee led by Dr. Orna Berry to assess the necessity for government intervention to accelerate advancements in artificial intelligence and data science (Telem Committee). The Committee's directive, outlined in the appointment letter, emphasized the importance of focusing on the following aspects: human capital, physical infrastructure, access to databases, and knowledge transfer from academia to industry. The Committee's findings were published in December 2020. In August 2021, following Government Resolution 212, the government approved the Telem Committee's recommendations, initiating the first implementation phase with a budget of about NIS 550 million from 2021 to 2023.

In July 2022, the then-Minister of Innovation launched a "National Program for Artificial Intelligence". This program, crafted by an inter-ministerial team, was officially published by her ministry in January 2023 (the Ministry of Innovation's National Program).

In February 2023, Government Resolution 173 approved an extension to the first phase, approved in August 2021 (the second phase). This resolution included a directive to the Ministry of Finance to allocate a budget not exceeding NIS 500 million, which will be utilized by Telem Forum entities from 2023 to 2026.

This audit report evaluates the national preparedness in artificial intelligence, examines how the Israeli government formulates and enacts a national strategy to position Israel among the leading countries globally, and assesses whether its actions in artificial intelligence will establish a robust foundation for Israel's development and prominence as a scientific and technological power. The preparedness, decision-making, and implementation processes for the government program in artificial intelligence commenced in 2018 and continued throughout the audit period.

2 A voluntary action framework designed to coordinate and pool resources among all national bodies that may benefit from a large research infrastructure (the Directorate of Defense, Research, & Development (DDR&D), the Planning and Budgeting Committee, the Ministry of Finance, the Innovation Authority, and the Ministry of Innovation).

Key Figures

0

Israel has no **long-term national strategy** in artificial intelligence. The government did not approve a **comprehensive and individual master plan for the implementation.** Instead, over the years, it has approved programs in phases implemented slow, lacking, and does not meet the set schedules

only 1 NIS billion

was approved by the government in two phases. most of the amount had not yet been realized. The approved budget is about a fifth of the recommended one by the Telem Committee in December 2020 and about a tenth of the "National Initiative" recommendation from September 2020

drop from 5th place to 9th place

in the Tortoise index out of 83 countries in 2019–2024. This is an international artificial intelligence, index whose ranking is based on – investment, innovation, and application

drop from 20th place to 30th place

in the Oxford index out of 193 countries in 2020–2023. This is an international artificial intelligence index regarding governmental readiness for artificial intelligence. In a sub-index measuring the government's artificial intelligence strategy and its digital capabilities, Israel dropped 33 places (from 35th to 68th) in these years

only 40%

was realized of the first phase budget, the government approved for 2021–2023 (NIS 220 million out of about NIS 550 million). The realization rate refers to agreements that have been signed, of which tens of millions of NIS have not yet been executed or completed

only 11%

the realization rate of the first phase in high-performance computing (supercomputer), which is about NIS 30 million out of the NIS 270 million approved

55%

of the budget allocated in the first phase for human capital was realized (about NIS 34 million out of NIS 62 million), focusing on the needs of academia but not to the industry needs

76%

the budget realization rate in natural language processing in Hebrew and Arabic. However, the realization rate includes an agreement for a language module for which there is a budgetary commitment that has not yet been realized

Audit Actions

From June 2023 to March 2024, the State Comptroller's Office examined the national preparedness in artificial intelligence, assessing Israel's international ranking and the government and relevant ministries' actions to advance a national program for artificial intelligence. The audit was performed in the Ministry of Innovation, the Innovation Authority, the Ministry of Defense, the Planning and Budgeting Committee, the Ministry of Finance, and the National Security Council in the Prime Minister's Office. Supplementary examinations were conducted within the National Digital Agency at the Ministry of Economy and Industry.

Key Findings

The Absence of an Integrating Government Body Supervising Artificial Intelligence National Program – under the government's resolution and the agreement reached between the Minister of Innovation and the head of the National Security Council in July 2022, the Ministry of Innovation, under the then minister's leadership, formulated a national program for artificial intelligence. However, after the change in government in January 2023, the Ministry of Innovation did not comply with the government's resolution to promote and lead in artificial intelligence. The program initiated by the Ministry did not progress to the implementation phase after establishing the 37th Knesset, leading to stagnation on the established milestones. Since the change in government, the Ministry has limited its focus to specific issues within Israel's artificial intelligence sector and has not led to advancement at the national level.

Six years after the Prime Minister decided to promote artificial intelligence and submit it as a program for government approval, an overall national program to advance it has yet to receive government endorsement. Aside from the two phases of the Telem program, the national program introduced by the then-Minister of Innovation in July 2022 remains ineffective when it has not been implemented following the change in government. The necessity for the government's approach to artificial intelligence to be guided by an integrating government body responsible for the execution of the government program is underscored by several factors: the significance of this sector to the national economy and its resilience; The myriad of government ministries and public agencies engaged in the advancement and integration of artificial intelligence technology within the governmental framework; The critical importance of Israel's standing as a global leader in this technological revolution; And the mandate assigned to the Ministry

of Innovation to supervise the government's strategy. As of the audit date, there is no integrating government entity that holds overall responsibility for formulating and leading a national program, pooling budgets, and controlling and supervising the program's implementation and progress.

- **The Drop-in Israel's Ranking in Artificial Intelligence –** Israel aspires to be a leading technological and high-tech player .The audit raised that in 2019–2024, Israel's position in global rankings for activity and investment in artificial intelligence declined. The Tortoise Index dropped from 5th place out of 62 countries to 9th place out of 83 countries. The Oxford Index's ranking dropped from 20th to 30th place out of 193 countries. Additionally, in the Innovation Index, Israel's ranking dropped from 10th place to 15th place out of 133 countries. This decline is attributed, in part, to the findings detailed in this report regarding the government's approval, leadership, and execution of a broad national program in artificial intelligence. Tortoise sub-index data for 2024 indicate that while Israel excels in human capital, research, and development, it lags in government strategy (32nd place), infrastructure (26th place), and operational environment (65th place). The decline in Israel's international rankings in 2019–2024 highlights the urgent need for the government to reassess its policy regarding artificial intelligence.

- **Government Discussion on the "National Initiative" Recommendations –** the "National Initiative" was established at the appointment of the National Security Council per the Prime Minister's directive. Its draft report was presented to the Prime Minister in May 2019, and the final draft was submitted to the head of the National Security Council in December of the same year. Following the changes in government that year, the final report, which included a comprehensive plan for formulating a strategic national response to artificial intelligence and associated projects with a budget of NIS 10 billion, was distributed to all government ministries and made public in September 2020. The report, compiled with input from hundreds of knowledge experts who volunteered their expertise for about two years, identified the promotion of artificial intelligence as critical for Israel's resilience across various sectors, including science, economy, security, and health. The audit found that the Initiative's recommendations were neither presented to the government nor discussed within any authorized government forum, nor were they budgeted or matured for implementation, despite the National Security Council being required to review the "National Initiative" following its completion and implementation for the review of the authorized body which approved the designation. Additionally, according to the agreement with the Legal Counsel to the Prime Minister's Office, the National Security Council was to establish the inter-ministerial team and submit its recommendations to the Prime Minister and government shortly after the "National Initiative" work was concluded, not about a year and a half later.

  Once the Prime Minister, the government, or any other governmental body tasked professional parties to conduct staff work and submit a report based on the recommendations of 14 professional teams and hundreds of knowledge experts, which was to serve as a basis for making an operative decision on a specific issue, the head of

the National Security Council should have completed the process until the government discussed the recommendations following the teams' work and the submission of the report summarizing their findings; However, this did not occur. The failure to forward to the government the conclusions of the "National Initiative" report, which remained unaddressed for two years due to administrative delays unrelated to the Initiative's work, adversely impacted the government's ability to capitalize on the contributions of the exceptional knowledge experts appointed under the Prime Minister's decision.

- **Government Discussion of the Recommendations of the Artificial Intelligence and Data Science Committee (Telem Committee) –** the chairman of the Telem Forum appointed the Telem Committee to assess the necessity for government intervention to expedite the development of artificial intelligence and data science. It was determined that akin to the "National Initiative" recommendations intended to serve as a basis for a government decision, this program, which was completed in December 2020, was not thoroughly discussed within the government but rather in a limited manner under two phases, which were budgeted at around one-fifth of the Committee's recommended budget, at about NIS 1 billion. Consequently, it was not endorsed as a comprehensive master plan nor budgeted with a long-term vision.

- **Regulation –** despite the inherent risks associated with artificial intelligence technology and the imperative to regulate its usage responsibly while upholding fundamental rights, it has been determined that as of the audit end date, the collaborative efforts between the Ministry of Innovation and the Ministry of Justice to advance regulation in artificial intelligence and the principles outlined in the Policy Principles document have not yet received government approval. Israel currently lags behind the European Union, which has already enacted legislation regulating artificial intelligence use based on risk levels. The absence of regulation in Israel presents various risks that generate new legal and regulatory challenges. It is essential to ensure that, irrespective of technological advancements, human beings remain central to decision-making and that the development and application of artificial intelligence are conducted responsibly, safeguarding fundamental rights and public interests, including human dignity, privacy, equality, non-discrimination, and complete transparency.

- **High-Performance Computing (HPC) –** although the necessity for supercomputing infrastructure was identified in 2020 as fundamental for positioning Israel as a leading nation in artificial intelligence, five years later, existing computing infrastructures remain limited and inadequate for advancing research and industry in Israel. This deficiency in computing infrastructure hinders the public sector, academia, and industry's capacity to foster and develop artificial intelligence.

- **Infrastructure for Training Large Models –** it was found that by the end of December 2023, as the first phase concluded, the Directorate of Defense, Research, & Development (DDR&D) did not fulfill its obligations within the partners' agreement to establish an infrastructure for training large models. The Innovation Authority has not

yet regulated a complex calculation infrastructure for scientific use, essential for furthering artificial intelligence technology. Thus, the implementation rate of the first phase for advancing artificial intelligence stood at merely 11%, with about NIS 30 million disbursed out of a total approved budget of NIS 270 million.

- **Natural Language Processing (NLP) –** the Telem Committee highlighted the importance of advancing natural language processing, deeming it essential for employing artificial intelligence capabilities in government ministries and various industries. Therefore, the Program's primary objective is to bridge the significant technological divide between existing capabilities in English and other Latin languages and those in Hebrew and Arabic, the following findings were found:

  - Only on December 31, 2023, the final day designated for the implementation of the initial phase, the DDR&D entered into an agreement of NIS 37 million for developing a Hebrew and Arabic language model project in collaboration with an international company. The first model is anticipated to be implemented by mid-2025, a year and a half after the conclusion of the initial phase. Notably, this financial commitment constitutes about a quarter of the allocated resources for language processing within the first phase. The substantial delay by the DDR&D in advancing the large language model (LLM) for Hebrew and Arabic may severely impede governmental responses to citizens, as the anticipated model is intended to catalyze the digital transformation of the Israeli economy, particularly within the public sector, through artificial intelligence tools.

  - By the end of the first phase, Israel lacked a language model in Hebrew and Arabic for government use and citizen interaction. The total budget realization for developing language processing capabilities for Hebrew and Arabic, necessary to reduce the considerable technological gap compared to English and other Latin languages, reached 76% of the approved budget for this component (NIS 138 million out of NIS 180 million). This realization rate includes the language model agreement, which has only a budgetary commitment of NIS 37 million and has yet to be realized.

- **Human Capital –** it was found that in human capital investment for artificial intelligence advancement, implementing the Telem Committee's program within the first phase approved by the government was partial. As of the end of 2023, only NIS 34 million out of NIS 62 million was realized, about 55% of the allocated budget, mainly addressing academic needs while neglecting industry requirements.

- **Employment of Researchers and Senior Faculty in Academia –** it was found that, although the partner agreement for the first phase allocated about NIS 24 million for faculty admission in academia and around NIS 20 million for dedicated research grants in AI CORE fields, these elements were not executed, by the end of the first phase, by the Planning and Budgeting Committee. Moreover, the Planning and Budgeting Committee and the Innovation Authority lack up-to-date and accurate information on the

existing number of researchers. This deficiency underscores a lack of attention to the necessary training and development of human capital in artificial intelligence, which is critical for realizing the defined objectives.

- **Scope of Scholarships –** it was found that in 2021–2023, the Planning and Budgeting Committee awarded about 50 scholarships, representing 5% of the roughly 1,000 scholarships recommended by the Telem Committee, as part of the implementation of the first phase budget approved by the government. The average annual financial scope was about NIS 10 million, significantly lower than the NIS 100 million per year recommended by the Committee. Thus, the scope of scholarships awarded during the first phase was about 10% of the suggested budget. Furthermore, the Innovation Authority and the Planning and Budgeting Committee lack information regarding the impact of these scholarship distributions on the advancement of human capital in academia in artificial intelligence.

- **Budget Realization of the First Phase –** as of the conclusion of the first phase in December 2023, the budgetary realization was only about 40% of what was approved by the government, which was NIS 220 million out of a projected NIS 550 million. This reflects the implementation of only about 5% of the Telem Committee comprehensive program, which has not been deliberated in full within the government or adequately budgeted. It should be noted that this implementation rate pertains to signed agreements, yet tens of millions of NIS remain unimplemented or incomplete.

- **The Second Phase –** the audit raised that in February 2023, the government endorsed a budget for the second phase in implementing the Telem program, at NIS 500 million, to be executed from 2023 to 2026. However, only in September 2024, over a year and a half after the government's resolution, was the Telem Forum partners agreement signed for implementation from 2024 to 2027. This state of affairs, where the signed partner agreement mandates that the second phase is to commence about one year after the designated implementation date, signifies a substantial gap in adhering to the government's resolution regarding the second phase. This, among other things, given the assessment that in the first and second year out of the four that the government decided upon, only about 10% of the total budget stipulated in the government's resolution will be realized within the framework of the agreement.

  It should be noted that the total budget approved for both the first and second phases was about NIS 1 billion, about one-fifth of the budget recommended by the Telem Committee in December 2020.

- **Data Literacy –** the findings indicate that, although data literacy is a crucial skill anticipated to be necessary across various fields and sectors, neither the first phase approved by the government nor the partners' agreement for the second phase addressed this area. Furthermore, the Ministry of Education was not included in the partner agreements promoting artificial intelligence. This omission of data literacy

education at an early age could hinder the readiness and integration of the next generation into the technological landscape, as artificial intelligence increasingly concerns all aspects of life and is expected to be utilized daily by the general public.

Establishment of a Knowledge Center in the Ministry of Innovation – the State Comptroller's Office commends the Ministry of Innovation for engaging various entities to promote regulatory principles and establishing a knowledge center focused on the regulation and ethics of artificial intelligence.

Key Recommendations

- The Ministry of Innovation should adhere to the government's resolutions and the conclusions reached with the then-Minister regarding collaboration with the National Security Council, thereby leading the government's policy on artificial intelligence. Within this framework, finalizing the national strategic program initiated in 2022 is essential. This program should encompass, among other elements, a vision, milestones, a comprehensive action plan detailing the government bodies responsible for each action direction, timelines for implementation, and a corresponding budget plan. Additionally, it should establish a framework for the periodic evaluation of the state's adherence to the objectives outlined in the plan, as well as mechanisms for individual evaluations of the defined action directions, including updates as necessary. The Ministry of Innovation, Science and Technology is currently tasked with fulfilling its responsibilities, thereby upholding the government's resolution. Strong leadership of a significant national initiative is essential to sustain technological capabilities and relative advantages over other countries. Any deviation from the established implementation path will necessitate a government update to assess the situation and provide a response to advance the government's objective of promoting artificial intelligence. It is recommended that the Prime Minister, who initiated the national program for artificial intelligence in 2018 as a basis for this decision, supervise the government's engagement through the National Security Council to ensure the effective implementation of the national program.
- The Ministry of Innovation should collaborate with the Innovation Authority to facilitate the signing of necessary agreements that advance the computing infrastructure essential for advancing artificial intelligence in Israel.
- Given the importance of developing large language models in Hebrew and Arabic, it is recommended that the Ministry of Innovation work jointly with the Innovation Authority, the Directorate of Defense, Research, & Development, and the National Digital Agency to advance this project and integrate it into government ministries and the public sector.

- Given concerns regarding the insufficiency of the grants program to address the recruitment challenges for new faculty in artificial intelligence, the required number of researchers should be determined, and the Planning and Budgeting Committee should explore alternative solutions for faculty recruitment, implementing them, according to the examination findings, in the future phases.

- The Innovation Authority and the Planning and Budgeting Committee should establish control mechanisms focusing on data collection and analysis to assess the impact and effectiveness of scholarship distribution on enhancing and expanding human capital in artificial intelligence.

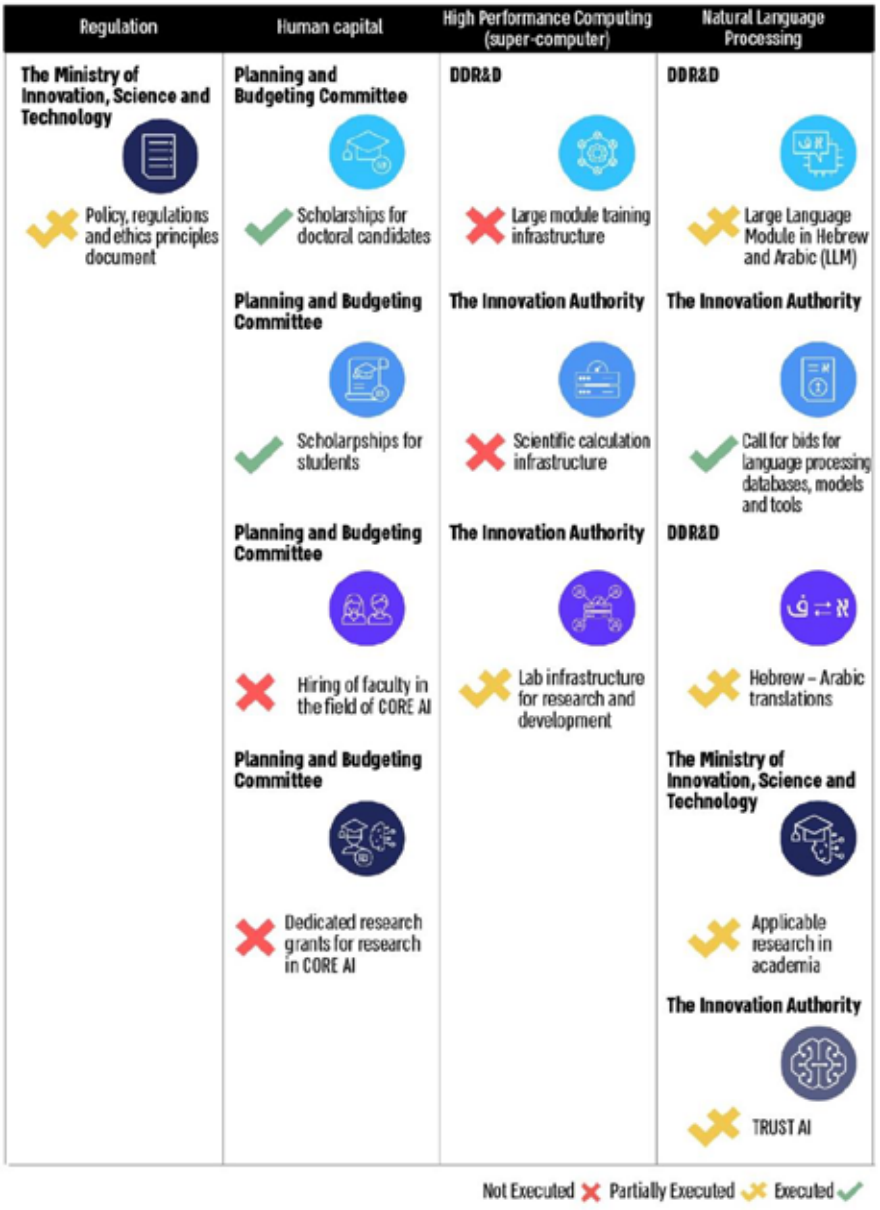
- The Ministry of Innovation should investigate the reasons behind the limited execution of components from the initial phase of the human capital program and ensure comprehensive implementation in subsequent phases. Recognizing that the primary barrier to leveraging capabilities in artificial intelligence is human capital, the Ministry of Innovation, in collaboration with the Planning and Budgeting Committee, should develop a comprehensive strategy for increasing the scope of research and the number of faculty and researchers in artificial intelligence.

- The Ministry of Innovation and the Ministry of Justice should cooperate to update regulatory principles in line with technological advancements and the standards established in the signed international treaty and bring them for government approval. They should also assess the necessity of promoting legislation akin to the practices in the European Union or advancing sector-specific regulation based on concrete risk, as is customary in the United States, United Kingdom, and Australia. In any case, regulatory frameworks are imperative to safeguard state and citizen security against the misuse of artificial intelligence capabilities.

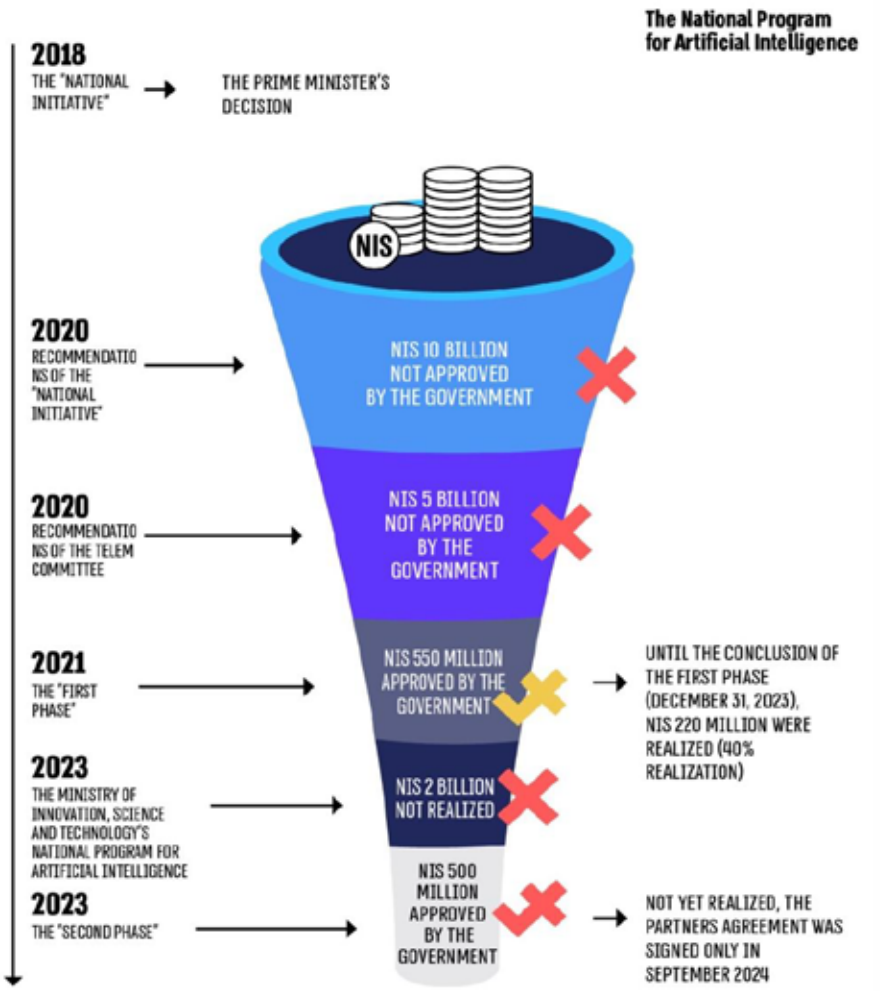
- Having received the mandate from the government to lead and advance the artificial intelligence sector in Israel, the Ministry of Innovation should implement the second phase as outlined in the government resolution, monitor the timelines and content of its execution in collaboration with the Telem Forum and other relevant government ministries and bodies engaged in the promotion and integration of this field in Israel.

- It is recommended that the Ministry of Innovation, with the Ministry of Education, incorporate educational initiatives into the national artificial intelligence program by developing curricula that enhance data literacy. Moreover, following the completion of the subcommittee's work established by the Director General of the Ministry of Education to advance artificial intelligence, the Ministry of Education should formalize its integration into all educational institutions' curricula through a circular from the Director General, formulating a multi-year implementation plan.

The Implementation Status of the First Phase Main Projects



The Budgetary and Substantial Development of the National Program for Artificial Intelligence



Summary

The scientific and technological leadership of the State of Israel is a fundamental pillar of its national security, economic resilience, and the well-being of its citizens. Israel's leadership in these domains strategically compensates for its lack of natural resources and limited human capital compared to other nations. The artificial intelligence revolution has transitioned from a futuristic concept to a core innovative technology impacting numerous facets of contemporary life, serving as a central focal point for international competition across various fields, including science, economics, industry, security, health, education, and employment.

According to the report, while Israel recognized already in 2018 that the technological sector was on the brink of a significant revolution, and the Prime Minister acknowledged the necessity of preparing and implementing a comprehensive national plan on the subject, since that time, the government has failed to lead and implement strategies for approving a broad, long-term national plan and has not initiated its implementation, nor continuously supervised to ensure the necessary progress. Consequently, Israel's standing in the international arena has begun to erode.

Despite the Prime Minister's 2018 decision to establish the "National Initiative" and despite the Telem Committee, a professional review committee appointed to examine the acceleration required for the development of artificial intelligence, having determined in 2020 that a national program in artificial intelligence and data science is critical for the resilience of the State of Israel, there remains no national program approved and budgeted by the government as of 2024. In 2018-2023, two significant plans were developed to advance the field of artificial intelligence at the national level: "National Initiative" and the Telem Committee program; However, these initiatives have either been abandoned or progressed minimally. The audit indicated that the 2021 agreement between the head of the National Security Council and the then-Minister of Innovation that her ministry shall be given overall responsibility and powers for managing the national program and coordinating the government's actions, as supported by the government's resolution, has not been implemented. Furthermore, the National Program formulated by the Ministry of Innovation has not been advanced, and since the change in government in December 2022, the Ministry of Innovation has focused solely on specific areas.

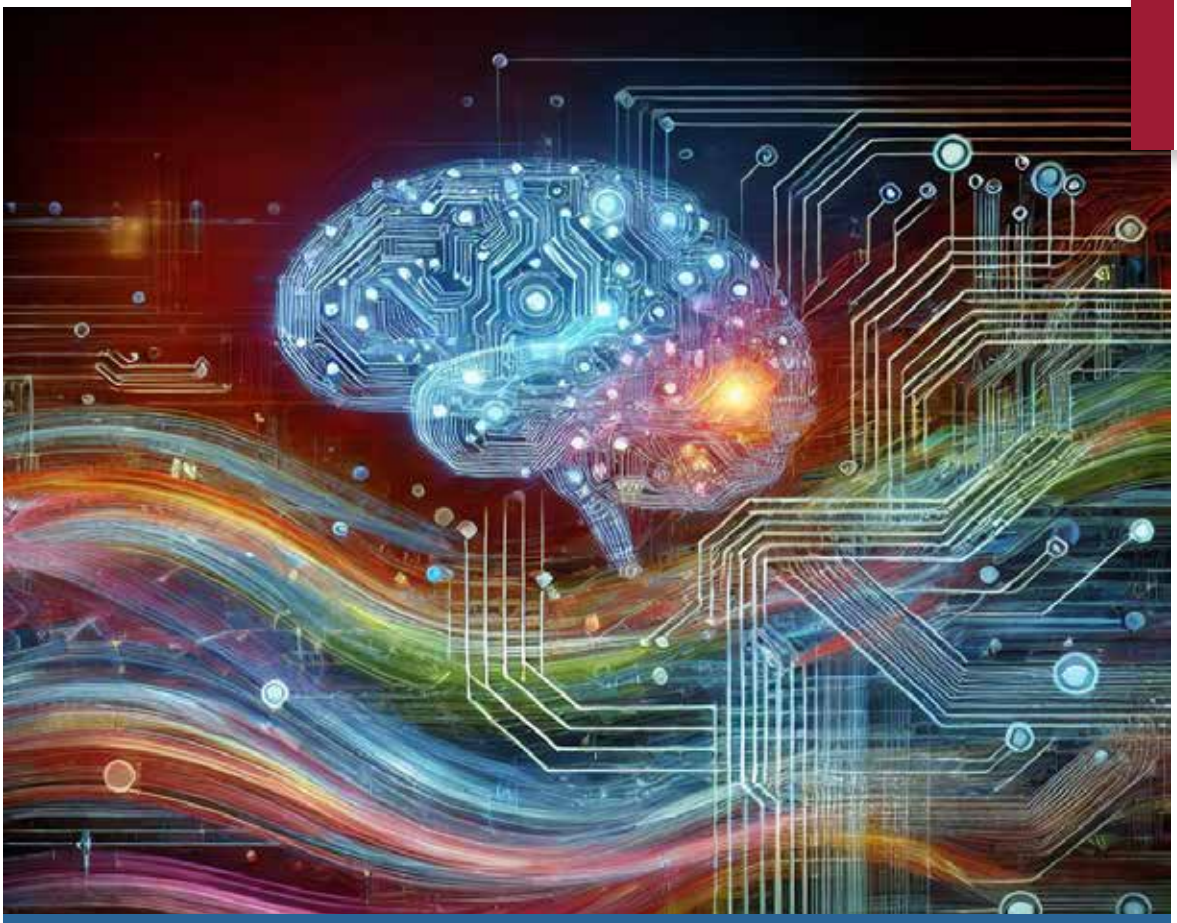
Consequently, about six years after the Prime Minister's decision, and given the accelerated development of artificial intelligence technology globally, Israel lacks a comprehensive long-term national strategy, and the government has not approved a comprehensive and specific master plan for implementation. The government's endorsement of programs has been sporadic, slow implementation, and has not adhered to established timelines. Additionally, the government did not approve the principles of policy, regulation, and ethics regarding artificial intelligence developed by the Ministry of Innovation and the Ministry of Justice, leaving crucial elements unanchored in legislation or sectoral regulation.

It is evident that while the state identified and analyzed the need promptly, it has struggled for several years to make effective decisions corresponding to that need and to implement them accordingly.

To uphold Israel's technological and scientific superiority in artificial intelligence, deemed a national priority, the Ministry of Innovation should lead the government policy, aligning its actions with the government's previous resolutions and the agreement between the then-Minister and the National Security Council. This entails finalizing the national strategic program initiated in 2022, which should encompass a clear vision, milestones, a detailed action plan specifying governmental responsibility for each action direction, implementation timelines, and an aligned budget. Additionally, the Ministry should establish a framework for a periodic assessment of the program's compliance with the outlined objectives and an individual evaluation of the defined actions, including necessary updates. In this context, it must review, among other factors, the current administrative structure responsible for implementing the initiatives approved by government resolutions, which, as of the audit end date, operates voluntarily and without budgetary authority.

The Ministry of Innovation, Science, and Technology should fulfill its responsibility by upholding the government's resolutions. Strong leadership of a significant national program is essential for sustaining Israel's technological capabilities and relative advantage over other nations. Any deviation from the established implementation course necessitates a governmental update to assess the situation and respond accordingly to promote artificial intelligence initiatives further.

It is recommended that the Prime Minister, who initiated the move to advance the national program in artificial intelligence in 2018, monitor the progress of governmental actions in this regard through the National Security Council, guaranteeing the practical implementation of a significant national plan.



Introduction and use of Artificial Intelligence in Latvia

Riga 2025

Latvijas Republikas
Valsts kontrole

Review Report

6 May 2025

Review “Introduction and Use of Artificial Intelligence in Latvia”

The Review Report was drafted based on audit schedule No 2.4.1-72/2024 of the Audit and Methodology Department of the State Audit Office of Latvia of 20 August 2024.

The cover design includes an image generated by AI tool *Microsoft Copilot* on 7 February 2025.

Why has the Review been conducted?

In recent years, there has been a rapid development of artificial intelligence (hereinafter – AI). The topic of AI became relevant in society with wide access to generative AI tools (for example, ChatGPT, Copilot, Gemini, etc.). In 2024, the European Union (hereinafter – EU) adopted the first legal regulation in the field of AI – the AI Act[1], which addresses the risks posed by AI and sets out a set of rules for AI developers and implementers. The AI Act aims to improve the functioning of the internal market, ensure legal certainty, promote the human-centric and trustworthy use of AI, ensure a high level of protection of health, safety and fundamental rights, and support innovation, while protecting democracy, the rule of law and environmental protection.

Even before the adoption of the AI Act, attention was already paid to AI issues in Latvia at the EU level, and the Ministry of Smart Administration and Regional Development (hereinafter – MSARD) prepared informative report "On the Development of AI solutions"[2] and the Cabinet of Ministers took note of it in 2020. When taking note of the latter[3], several important tasks were identified for both the MSARD and other ministries:

- Designate the MSARD as the leading institution in matters of development and implementation of AI solutions in state administration;
- When developing national or sectoral development planning documents or their amendments, ministries shall conduct an assessment of the automation of state administration tasks and the use of AI, and the MSARD shall provide advisory support to ministries;
- In the planning process of the 2020–2029 state budget and EU funds, the ministries shall assess the expenses related to the automation of state administration tasks and the integration of AI systems into services;
- Take note that, in accordance with the European Commission (hereinafter – the EC) Plan, Latvian public sector investments in the development of AI solutions should reach 25 million euros per year by 2029;
- The MSARD shall draft changes to the e-index of Latvia by 30 December 2020 by supplementing it with indicators characterising AI;
- When drafting planning document "Digital Transformation Guidelines for 2021–2028", the MSARD shall identify the introduction of AI solutions as one of the priorities of state administration;
- The MSARD shall develop and submit an informative report on recommendations for the communication of state administration in the field of AI to the Cabinet of Ministers for consideration by 1 June 2020.

AI is also currently a hot topic on the agenda, as the Saeima (Parliament of Latvia) has adopted the Law on the Artificial Intelligence Centre[4] (hereinafter – the AI Centre), and the Cabinet of Ministers has taken note of informative report "On the Implementation of the Requirements of the Artificial Intelligence Act"[5] (See Figure 1).

2020	2021-2023	2024	2025
The Cabinet of Ministers takes note of informative report "On the Development of AI solutions	- National or sectoral planning documents do not always include an assessment of the use of AI - The current legal framework and its application in situations created by AI are not assessed	The EU adopts the AI Act	The Cabinet of Ministers takes note of informative report "On the Implementation of the Requirements of the Artificial Intelligence Act"

Figure 1. Document development progress to date.

The purpose of the Law on the Centre for AI is to create an AI technology ecosystem and establish a legal framework for cooperation among the public sector, the private sector and universities, as well as to establish a Centre for AI to facilitate the transfer of innovations, the development and implementation of AI capabilities in strategic areas that meet national interests and increase the country's competitiveness in health, education, security and defence, as well as in state administration, and other areas. The establishment of a Centre for AI will also contribute to the improvement of public skills in the application of AI capabilities, as well as improve expertise in risk management of AI solutions[6].

Taking into account the relevance of AI in the world, the development of regulation in the EU and progress reached in Latvia, as well as taking into account the expected potential in the use of AI in the world, the State Audit Office of Latvia agreed to carry out joint work to identify the readiness of state administration[7] to implement AI solutions and to create comparative research material on the development of AI in the EU Member States upon receiving an offer from the IT Working Group of the European Organisation of Supreme Audit Institutions (EUROSAI ITWG).

In the joint working group with colleagues from other countries, that is, Israel (coordinator of the joint work), Estonia, France, Italy, Lithuania, North Macedonia, Poland, Romania, Slovakia, Switzerland, nine blocks of questions were determined to identify the situation in the implementation and use of AI (See Figure 2).

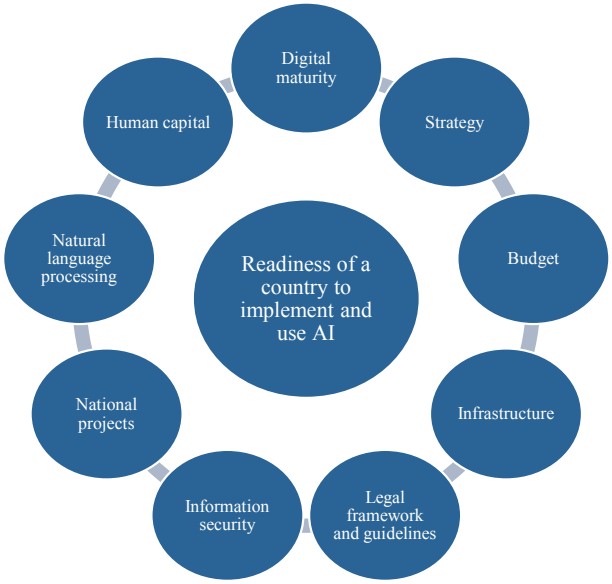


Figure 2. Blocks of questions identified in the IT Working Group.

The results of the joint work are planned to be published in the second half of 2025, but for now we offer to familiarise with the situation in Latvia.

Since the goal of the Review is to summarize facts on current issues in a short time, without drawing conclusions or providing recommendations, we mainly communicated with the MSARD as the leading institution for AI issues in state administration. In this Review Report, we have summarised and provide more detailed information on specific aspects of AI development by outlining both challenges and opportunities. We hope that the issues identified in the Review will be useful for the further development of AI, including when responsible institutions plan and decide on the necessary improvements. The Review Report is mainly addressed to the institutions involved:

- The MSARD as the leading institution[8] in the development and implementation of AI solutions in state administration;
- Foundation "Centre for AI"[9], which will facilitate the implementation of AI in areas with high potential by uniting the public sector, the private sector and science according to national interests, national competitiveness, public skills, ethical, responsible and safe use of AI[10].

Although the regulations of other ministries do not include a precise function in the field of AI, nevertheless, the Ministry of Education and Science, the Ministry of Economics and the Ministry of Defence also play a significant role in the context of AI development when considering the fields of activity of the ministries.

The aim of this Review is also 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.

To identify and understand how AI technologies are used or planned to be used by the state administration in its work, the information system auditors of the State Audit Office of Latvia interviewed the MSARD, compiled publicly available information and surveyed state administration institutions. There were 119 state institutions invited to complete a survey on their experience in the implementation and use of AI, and 83 state institutions responded. We assess the response to participation in the survey and the interest of the public sector as high.

Summary

The Review summarises facts and provides detailed information on key aspects of AI use and its further development in state administration. These aspects include:

- The current situation in the use of AI solutions and plans for their use, initiated and planned projects, spent and available funding;
- The defined strategy for the implementation, use and development of AI;
- Legal framework and requirements, including with regard to information security;
- Readiness for the implementation of AI solutions from the point of view of digital maturity, infrastructure and human capital;
- Progress in natural language processing.

The survey results show that AI solutions are not new to state administration, as 17% of respondents answered that they were already actively using them at work (for example, using both relatively simpler solutions intended for document translation, information search, text and image processing, and relatively more complicated solutions for data analysis, as well as virtual assistants) and 22% of respondents planned to use them. In their turn, 55% of respondents admitted that they did not have a clear plan for using AI.

The survey results also show that state institutions expect specific benefits from the implementation of AI such as reducing the time required for service provision (30%), improving service quality (22%), and transforming (optimizing) the provision of a service or process. At the same time, respondents are less likely to expect that the implementation of AI solutions could reduce service provision costs (10%), ensure service personalisation (7%), and help create new types of services (6%).

The practice and methodological approach in state administration how to achieve these benefits have not yet been established.

The survey has identified both positive aspects and negative issues (See Table 1).

Table 1

Positive aspects and challenges in AI implementation identified in the survey

Positive aspects	Challenges
➢ 28% of respondents said that they planned to include AI goals and priorities in their institution's strategy. 17% or 18% of respondent institutions had already evaluated the use of AI in some document. ➢ State institutions use or plan to use AI solutions to support research, ensure faster decision-making, improve internal processes and provide services or communicate with customers. ➢ 7 institutions or 41% of respondents whose institutions use AI solutions indicated that productivity had increased after the introduction of AI. ➢ 8 institutions or 47% indicated that they are still planning to evaluate whether productivity has increased after the introduction of AI solutions. ➢ Respondents indicated the following productivity benefits: time savings, increased quality, savings in human resources, and faster work completion. ➢ 23 institutions or 62% of respondents whose institutions use or plan to use AI solutions have conducted or are planning to conduct an assessment of the bias/ethical risks of the AI solution (providing incorrect answers, discrimination, etc.). ➢ No incidents related to the use of AI have been identified so far (cybersecurity incidents, attempts to influence the operation of AI, etc.).	➢ There is no common understanding at the national level of what should be considered AI. ➢ 60% of respondents responded that the institution did not have a designated employee or division whose task was to monitor innovations, including the development of AI. ➢ The majority of respondents (54%) indicated that the sectoral policy planning documents did not include information on the implementation of AI solutions and the institution had not adopted a document (strategy, work plan) that would include goals and objectives in the field of AI. ➢ There is no single approach to accounting for investments in the implementation and maintenance of AI and separating them from other investments is impossible. ➢ 40% of respondents responded that the institution had not implemented risk management, which assessed the risks associated with the use of AI. ➢ 69% of respondents indicated that the institution had not developed guidelines for the use of AI.

In the opinion of the State Audit Office of Latvia, three groups of state administration institutions are emerging, each with its own challenges:

- For state institutions that do not have a clear plan for using AI, the challenge is to keep up with the rest of the state administration in certain areas because the possibilities of AI are not being used to make functions more effective;
- For state institutions that are already actively using AI in their work, the challenge is to ensure sufficient control over the results created by AI, including by reducing the risks of information processing quality and confidentiality related to its use;
- In their turn, for state institutions that plan to use AI, the challenge is to ensure implementation with reasonable resources and in a way that achieves the planned benefits.

These challenges mark a significant role in promoting, coordinating, and advising and supporting the implementation of AI. This is the role of the MSARD as the leading institution in the development and implementation of AI solutions and the established the Centre for AI.

On the one hand, AI is a technology but it is characterised by specific risks at the same time. AI is also associated with the need to invest significant financial resources, for example:

- In 2020, when considering Informative Report "On the Development of AI Solutions", the Cabinet of Ministers took note that, in accordance with the European Commission's plan for coordinated AI development, public sector investments of Latvia in the development of AI solutions should reach 25 million euros per year by 2029[11];
- In Informative Report "Strategic Roadmap for the Digital Decade for Latvia until 2030", the budget for measures identified in section 10 "Artificial Intelligence"[12] that can be attributed to AI activities for business and industry is 165.09 million euros. It should be noted that the measures are dedicated to the digitalization of business in general, including the promotion of the use of AI, cloud computing and big data solutions in enterprises, while not separating the activities intended for the aforementioned areas;
- "European Union Cohesion Policy Programme 2021–2027" Specific Support Objective 1.3.1 "To exploit the benefits of digitalisation for citizens, businesses, research organisations and public institutions", Measure 1.3.1.1 "Development of ICT solutions and services and creation of opportunities for the private sector" has allocated 6.5 million euros for AI applications for administrative productivity[13];
- Informative Report "On the Implementation of the Requirements of the AI Act"[14] identifies that the implementation of the requirements of the EU AI Act will cost approximately 1 million euros annually to ensure the implementation of the functions and tasks specified in the AI Act.

One expects that public administration investments in AI could increase in the coming years. It indicates the need to separate AI solutions from general digitalization plans. For its implementation, not only an action plan for the implementation of AI is important, but also a mechanism for accounting and monitoring progress. Moreover, all that effort must be based on a common understanding of what corresponds to AI terminology at the national level.

The Review identifies several areas for the development of AI in public administration to be targeted and balanced at the same time (See Table 2).

Table 2

Challenges identified during the Review

Area	Challenge
Existing situation	➢ Overall, there is no information available on what has already been done in the field of AI implementation, projects implemented, AI solutions implemented, good and bad experiences, resources used and benefits achieved, assessing whether the implementation of AI has improved effectiveness, increased efficiency or promoted other improvements.

	➢ The necessary infrastructure and other resources for the implementation of AI have not been identified.
Strategy	➢ The field of AI in Latvia has been fragmented, with general goals for AI set out in various documents, without a unified and coordinated policy, as there is no strategy for the use and development of AI that would outline the achievable results, deadlines, responsible parties and funding. ➢ A data strategy has also not been developed, but data is one of the most crucial elements for the development of AI. The lack of a data strategy is partly compensated by the fact that general principles for data dissemination and exchange have been set in Latvia for many years. ➢ In the national-level planning document "Digital Transformation Guidelines for 2021–2027" and the implementation plan, it is not possible to identify specific AI development issues and separate them from digital transformation issues. ➢ Similar problems also exist in sectoral planning documents. Only in the welfare and health sectors, there are more specific AI implementation plans and goals outlined in state administration. In other sectors, they are difficult to identify.
Legal framework	➢ The rapid introduction of AI solutions and the willingness of state institutions to recognise the risks associated with the security, ethical and legal aspects of their operation are of concern, making legal frameworks an urgent necessity. Not only is there a lack of legal frameworks and requirements for the operation of AI, but there is also a lack of guidelines to help state institutions implement compliant, ethical and secure AI solutions.
International and national ratings	➢ In international ratings that measure the development of a country, including business environment, research and industry, digital maturity, national innovation capabilities, and AI, Latvia receives lower rankings than Lithuania and Estonia. In addition, there is a trend that the gap with the other Baltic States is increasing. At the same time, Latvia has a good rating in the maturity of open data, which can promote the development of AI solutions. ➢ Since 2022, the e-index assessment of state institutions and municipalities has no longer been carried out in Latvia, therefore, information about the situation in specific sectors cannot be obtained. ➢ Since 2022, the e-index assessment of state institutions and local and regional governments has no longer been carried out in Latvia, therefore obtaining information about the situation in specific sectors is impossible.

We hope that the Review conducted by the State Audit Office of Latvia and the survey results can help those involved in developing AI policy and determining implementation activities to plan the future implementation of AI technologies in state administration, as well as provide the state administration with a broader summary of the problems identified in the field of AI.

References

1 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), https://eur-lex.europa.eu/eli/reg/2024/1689/oj/?locale=LV.

2 Informative Report "On the Development of Artificial Intelligence Solutions" of 4 February 2020 (taken note of at the Cabinet Meeting on 4 February 2020 (Minutes No 5, § 33)), https://tap.mk.gov.lv/lv/mk/tap/?pid=40475479.

3 The Cabinet Meeting on 4 February 2020, Minutes No 5, Paragraph 33, https://tap.mk.gov.lv/mk/mksedes/saraksts/protokols/?protokols=2020-02-04.

4 The Law on the Centre for Artificial Intelligence.

5 Informative Report "On the Implementation of the Requirements of the AI Act" of 25 February 2025 (taken note of at the Cabinet Meeting on 25 February 2025) (Minutes No 8, §49)), https://tapportals.mk.gov.lv/legal_acts/2d28c354-9baa-4aa2-ab31-fb4757687050.

6 Ministry of Smart Administration and Regional Development. "Latvia on the Wave of Innovation: the Saeima Approves the Law on the Centre for Artificial Intelligence" of 6 March 2025, https://www.varam.gov.lv/lv/jaunums/latvija-uz-inovaciju-vilna-saeima-apstiprina-maksliga-intelekta-centra-likumu, accessed on 13 March 2025.

7 In the context of this Review Report, state administration means state administration, excluding local and regional governments. When conducting a survey of state institutions, local and regional governments and their subordinate institutions were not included.

8 Cabinet Regulation No 586 of "Regulations of the Ministry of Smart Administration and Regional Development" of 3 September 2024, Sub-Clause 5.7.1.

9 Paragraph 1 of the Transitional Provisions of the Law on the Centre for Artificial Intelligence.

10 Section 2 of the Law on the Centre for Artificial Intelligence.

11 The Cabinet Meeting on 4 February 2020, Minutes No 5, Paragraph 33, Article 5, https://tap.mk.gov.lv/mk/mksedes/saraksts/protokols/?protokols=2020-02-04.

12 Informative report "Strategic Roadmap for the Digital Decade for Latvia until 2030" of 30 January 2024 (taken note of at the Cabinet Meeting on 30 January 2024 (Minutes No 6, §25)), https://tapportals.mk.gov.lv/legal_acts/82b52f77-febe-4480-ac95-c11eff9c283a.

13 Minutes No 3 of the meeting of the Thematic Committee on Digital Modernisation of 16 July 2024, Paragraph 4.1, https://www.mk.gov.lv/lv/media/19581/download?attachment, accessed on 27 March 2025.

14 Informative Report "On the Implementation of the Requirements of the AI Act" of 25 February 2025, Annex 5 "The Capacity and Resources Required to Implement the AI Act" taken note of at the Cabinet Meeting on 25 February 2025 (Minutes No 8, §49)), https://tapportals.mk.gov.lv/legal_acts/2d28c354-9baa-4aa2-ab31-fb4757687050.

VALSTYBĖS KONTROLĖ
PUBLIC AUDIT

MANAGEMENT OF ARTIFICIAL INTELLIGENCE IN THE PUBLIC SECTOR

9 May 2025

Nr. VAE-6

SUMMARY

Relevance of the Audit

The rapid development of artificial intelligence technologies in the public sector provides the basis for initiatives to automate many repetitive tasks, improve the quality of services and decision-making, and make public sector entities more efficient. Automating processes and optimising activities can reduce time and save public budgets. It is essential to keep pace with global trends in setting development directions, introducing artificial intelligence technologies, and ensuring the right legal environment and infrastructure. According to research, hundreds of millions of working hours can be saved per year worldwide, and as much as 30% of civil servants' working time over a period of 5-7 years.

The audit contributes to an international audit on the use of artificial intelligence in the public sector initiated by the Israeli Supreme Audit Institution. The international audit, which involves 11 countries, assesses artificial intelligence in the following areas: national strategy, funding, infrastructure, digital maturity, regulatory framework, information security, public projects, human resources and natural language processing. The results of the audit are expected to be published in September 2025.

Audit Objective and Scope

The objective of the audit is to assess whether the preconditions are in place for the effective management of artificial intelligence in the public sector.

Main audit questions:

- ✓ whether the conditions are in place for the development of artificial intelligence in the public sector;

- ✓ whether the regulation of the management of artificial intelligence is sufficient to mitigate potential risks;
- ✓ whether the resources needed for the functioning of artificial intelligence are properly managed.

Audited entities:

- ✓ Ministry of Economy and Innovation, as it formulates, organises, monitors and coordinates the implementation of the State policy on technology and innovation, the management of State information resources and digital development[1];
- ✓ Ministry of National Defence, as it formulates policy on cyber security and organises, controls and coordinates its implementation[2];
- ✓ National Cyber Security Centre, as it implements cyber security policy and is responsible for organising cyber security exercises and training[3];
- ✓ Innovation Agency, as it implements national policy on technology and innovation[4].

During the audit, we gathered information and interacted with representatives of the Ministry of Economy and Innovation, the Ministry of National Defence, the National Cyber Security Centre, the Innovation Agency, the State Digital Solutions Agency, the State Data Agency, the Central Project Management Agency, the Lithuanian Association of Artificial Intelligence, and interviewed 163 public-sector entities (the Office of the Government, all Ministries and their subordinate institutions that are managers of the State's information resources, and all municipalities). We collected information from 22 public sector entities that indicated in the survey that they were implementing projects related to the application of artificial intelligence technologies in their activities.

The audit period is 2021-2024. To assess trends and developments, we used data from the previous years (2014-2020) and 2025 in some cases.

The audit was carried out in accordance with international standards of supreme audit institutions. The audit criteria, procedures performed and methods used are described in more detail in Annex 3 'Audit criteria, procedures performed and methods used' (p. 39).

Key Audit Results

Effective management of artificial intelligence in the public sector is not yet possible due to: inadequate conditions for the development of artificial intelligence technologies in the public sector; a lack of procedures and guidelines for the management of artificial intelligence in the public sector; and a lack of proper management of the resources needed for the functioning of artificial intelligence.

[1] Law on Technology and Innovation, Art 9(2); Law on Management of State Information Resources, Art 11(1); Resolution of the Government No 330 of 24 March 2010 "On the Areas of Management Entrusted to the Ministers", paras 2.11, 2.21, 2.24.

[2] Law on Cyber Security, Art 4(2)

[3] Law on Cyber Security, Art 4(3), Art 8(2)

[4] Law on Technology and Innovation, Art 14(1)

1. Adequate conditions are not in place for the development of artificial intelligence in the public sector

- ✓ There are no plans at national level to apply artificial intelligence in the public sector. In 2019, Lithuania became the second EU country to develop an artificial intelligence strategy, but it has not been adopted and has not become a planning document. The provisions of the Strategy have not been translated into planning documents for the 2021-2030 development period. We found that the documents for this period do not define strategic objectives, progress targets and measures for the application of artificial intelligence in the public sector, with funding sources, monitoring and assigned responsibilities. The absence of a national strategic approach on how the public sector can take advantage of the opportunities and benefits of artificial intelligence and the lack of a coherent approach to implementing artificial intelligence solutions could lead to a loss of opportunities for the public sector to solve problems efficiently, optimise business processes, improve quality of services, increase transparency and rationalise the use of available resources (Sub-section 1.1, p. 15).
- ✓ Information on the implementation and use of artificial intelligence solutions in the public sector is not collected at national level, and there is a lack of information on good practices in the use of artificial intelligence in the public sector. The Ministry of Economy and Innovation and the Central Project Management Agency, which manages the projects, do not have comprehensive information on artificial intelligence solutions. All responding ministries (13 out of 14) indicated that they do not collect data on the implementation and/or use of artificial intelligence solutions in the information systems and registers they manage. The examples of good practice provided by the Ministry of Economy and Innovation are limited to publicised prototypes or evaluation against expected changes in performance and cannot therefore be considered as good practice examples. Both ministries and public sector entities implementing projects lack a systematic approach to the application of artificial intelligence in the public sector, and as many as 91% of the entities would like to join successful sharing initiatives on the application of artificial intelligence. Without coordinated implementation and adaptation of artificial intelligence solutions in the public sector, their integration will be inefficient and fragmented, and the public sector may lose the opportunity to solve problems efficiently, optimise business processes, improve service quality, increase transparency and rationalise the use of available resources (Sub-section 1.2, p. 16).
- ✓ The conditions are in place for the development of language resources for artificial intelligence solutions, but the development and availability of resources to the public sector is too slow. The development of language resources for artificial intelligence solutions is being implemented through the activities of the progress measure "Developing technological solutions and tools for the safe use of services". For the development period 2021-2030 EUR 42.35 million are earmarked for the development of language resources, while 69.9% or EUR 29.61 million have been allocated to projects as of 03/01/2025 data, and 5 out of 16 project proposals submitted for the implementation of language resources did not have a signed contract. As the implementation of the projects started in 2024, the development of the language resources and their availability to the public sector has been postponed by one year to 2026 (Sub-section 1.3, p. 18).

2. National legal preconditions for the management of artificial intelligence technologies are not sufficient

- ✓ To implement the provisions of the EU's Artificial Intelligence Act, two draft laws have been submitted to the Seimas for the appointment of two national competent authorities and a single point of contact. The Ministry of Economy and Innovation is responsible for artificial intelligence policy as one of the policy areas of information society development and digital development, but the concept of artificial intelligence is not defined in the relevant legislation. Guidelines on the ethical use of artificial intelligence in science and education have been adopted, but they are limited to the scientific field. For the vast majority (68.2%) of public sector entities assessed during the audit, the national legal framework for artificial intelligence is unclear (lack of definition, institutional responsibilities, regulatory guidelines, governance principles, definition of procedures, etc.), and for as many as 86.4% of the entities, there is a lack of national methodological guidance (aimed at facilitating the practical application of artificial intelligence, ensuring privacy and security, responsible and ethical use, etc.). In order to avoid over-regulation, the Ministry of Economy and Innovation plans to regulate in national legislation only what is required by the Artificial Intelligence Act, and will only propose additional legislation if there is an additional need. Without sufficient national legal preconditions for the management of artificial intelligence technologies, there is uncertainty for public sector actors on how to properly manage and apply artificial intelligence technologies, which limits the growth of innovative initiatives (Sub-section 2.1, p. 20).
- ✓ The mitigation of artificial intelligence risks through a cybersecurity management system is not ensured, as there are no specific requirements and procedures defining how to ensure the security of artificial intelligence throughout its lifecycle. The vast majority (81.8%) of public sector entities do not identify and assess the risks of artificial intelligence when implementing projects related to the application of these technologies in their operations, and none of them carries out an impact assessment or has a plan to mitigate the risks. Entities indicate that risks are relevant but there are no methodologies to manage them. There is a lack of training to develop the entities' competences in artificial intelligence security management and it is not included in the cybersecurity training programme. More than one third (36.4%) of the entities believe that specialised training and exercises would help them to understand new threats, develop their ability to respond to incidents and help them to predict the impact of artificial intelligence (Sub-section 2.2, p. 22).

3. Failure to ensure proper management of the resources needed for the functioning of artificial intelligence

- ✓ The management of artificial intelligence computing capacity is not ensured. The Ministry of Economy and Innovation has not set indicators for these capacities and the periodicity of their monitoring, does not produce monitoring reports, and does not collect information on existing capacities. The State Agency for Digital Solutions assesses the need for artificial intelligence computing resources only after an application has been submitted by public sector entities. Future computing capacity in the public sector is not assessed. The Organisation for Economic Co-operation and Development recommends that a national plan to increase artificial intelligence computing capacity should be developed, periodically reviewed and, where necessary, updated, but the Ministry of Economic Affairs and Innovation does not have such a plan in place. According to the Ministry, capacity building cannot be an area of separate planning as it requires a large amount of public financial resources, therefore artificial intelligence infrastructure is built up when it is decided to meet the expressed need of

state institutions for artificial intelligence solutions. Inadequate monitoring does not assess existing and future artificial intelligence computing capacity, does not ascertain whether the availability of computing capacity meets demand, does not ensure reliable capacity building and the availability of resources for public sector AI projects (Sub-section 3.1, p. 25).

- ✓ None of the public sector entities assessed during the audit have defined data management processes related to the development of artificial intelligence systems, only one out of 22 (4.5%) has a defined process for recording the origin of the data used in artificial intelligence systems and the criteria for preparing the data, 2 entities (9.1%) document the information on the acquisition and selection of data used in artificial intelligence systems, and 5 entities (22.7%) have defined data quality requirements. Entities do not implement the artificial intelligence data controls required by ISO/IEC 42001:2023 Artificial Intelligence Management Standard because they do not see the need, because they are governed by governing legislation, or because they use public data from internal systems. Inadequate information management poses risks to data security (data or data sets may be compromised, including unauthorised access, data loss), privacy (artificial intelligence systems often handle sensitive data, which can expose entities to regulatory or legal issues due to breached confidentiality) and integrity (distorted or biased data can lead to false, inaccurate results or poor decision-making) (Sub-section 3.2, page 26).
- ✓ None (out of 22) of the public sector entities assessed during the audit has a list of artificial intelligence competences or skills that are necessary for building the human resource competences needed to adopt artificial intelligence technologies. Almost half (40.9%) of the entities have not appointed staff responsible for the implementation of artificial intelligence projects, and a small proportion (18.2%) have established project implementation teams. 30.8% of staff involved in project implementation have never received artificial intelligence training and only one in two (50%) rate their skills in this area as at least 8 points. There is no training programme to develop the competences of public sector staff in implementing artificial intelligence solutions, and the Innovation Agency's training focuses on promoting innovation. The training covers artificial intelligence issues, but the majority (75.7%) of the public sector entities surveyed did not participate due to the limited number of participants. 70.1% of respondents do not know where to go for methodological support in applying artificial intelligence technologies in their work. Due to the lack of a systematic approach to the development of artificial intelligence competences, the majority (90.9%) of those implementing artificial intelligence projects point to a lack of coordination of training and competences development. This risks leaving the public sector behind in terms of innovation and the inability to apply it to improve the efficiency of administrative processes (Sub-section 3.3, p. 27).

Recommendations

To the Ministry of the Economy and Innovation

1. To ensure targeted and coordinated development of artificial intelligence solutions in the public sector (key audit result 1):

    1.1. initiate changes to establish a national strategic approach to the application of artificial intelligence in the public sector;

1.2. ensure the availability of information on the integration of artificial intelligence in the public sector and the exchange of good practice.

2. To ensure the timely development and availability of the language resources needed for the development of artificial intelligence solutions for the public sector, to reduce delays and to ensure the achievement of the planned indicators (key audit result 1).

3. To create the conditions for public sector entities to properly apply artificial intelligence technologies, develop methodological guidance on artificial intelligence (key audit result 2).

4. To ensure a targeted increase in artificial intelligence computing capacity, improve the monitoring of existing computing capacity so that it is based on indicators and allows an assessment of the future computing needs of the public sector (key audit result 3).

5. To ensure the security, privacy and integrity of public sector data, there is a need to improve the management of information on the role and impact of data in the development or use of artificial intelligence systems throughout their lifecycle (key audit result 3).

6. To ensure that public sector entities have sufficient competences to adopt artificial intelligence technologies, ensure access to artificial intelligence training and methodological support (key audit result 3).

To the Ministry of National Defence

7. To ensure that public sector entities adequately manage artificial intelligence risks and ensure cybersecurity throughout the artificial intelligence lifecycle, improve the existing cybersecurity regulation so that entities consider artificial intelligence as one of the threats in their cybersecurity risk assessment procedures (key audit result 2).

The measures and deadlines for the implementation of the recommendations, the expected impact of the audit and the indicators for measuring change are set out in the report in the section 'Plan for the implementation of the recommendations' (p. 30). Up-to-date information on the status of implementation of the recommendations, results and developments is published in open data on the National Audit Office website https://www.valstybeskontrole.lt/LT/AtviriDuomenys.

ДРЖАВЕН ЗАВОД ЗА РЕВИЗИЈА
ENTI SHTETËROR I REVIZIONIT
STATE AUDIT OFFICE

FINAL REPORT

PERFORMANCE AUDIT CONDUCTED ON THE TOPIC

OPPORTUNITIES FOR THE USE OF ARTIFICIAL INTELLIGENCE IN THE PUBLIC SECTOR

08 2024 03 13

Skopje, June 2025

ДРЖАВЕН ЗАВОД ЗА РЕВИЗИЈА
ENTI SHTETËROR I REVIZIONIT
STATE AUDIT OFFICE

No.: 34-74/6
Date: 11 June 2025

SUMMARY

The State Audit Office conducted an information systems audit, implemented as a performance audit, entitled "**Opportunities for the Use of Artificial Intelligence in the Public Sector**", with the objective of assessing whether the public sector is prepared to apply artificial intelligence in its operations.

This audit was conducted as a performance audit, in accordance with the Annual Work Programme of the State Audit Office for 2024, and forms part of a parallel audit within the EUROSAI IT Working Group, coordinated by the Supreme Audit Institution of Israel and involving the participation of 11 supreme audit institutions.

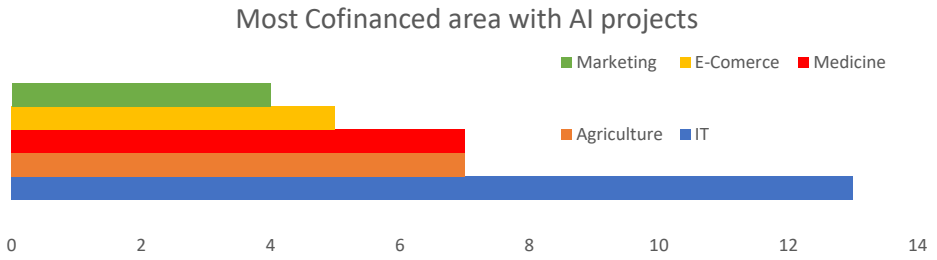
Although artificial intelligence is recognized as a key driver of digital transformation, the audit found that a National Strategy and a comprehensive legal framework governing the implementation of AI projects in the public sector have not been adopted.

Artificial intelligence is referenced in several strategic documents, but predominantly as part of broader policy objectives, without dedicated action plans or a coordinated institutional approach. Investments in ICT infrastructure for advanced research resources—such as supercomputers, specialized servers for big data processing and machine learning, and the development of technological centers — remain limited and contribute to reduced interest in AI-based projects.

Despite the absence of a national strategy and a relevant legal framework for AI applications in the public sector, between 2018 and 2023, 48 projects containing AI elements were financed through the Fund for Innovation and Technological Development, with a total value of EUR 6,110,044.

None of the AI projects supported have been implemented in the public sector. Insufficient promotion and the lack of a public registry of AI projects significantly reduce their visibility,

traceability, and applicability, thereby negatively affecting opportunities for implementation, dissemination, and further public-sector investment.

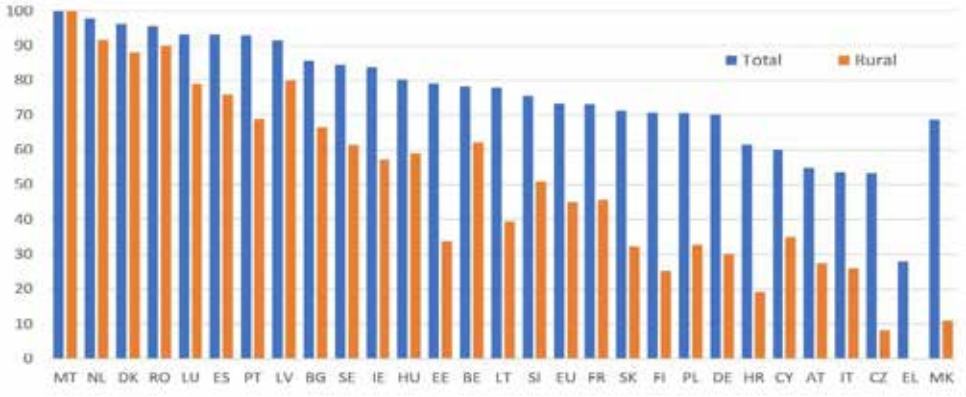


Across 12 sectors (aircraft industry, automotive/ agri-industry, veterinary services, e-business, energy, healthcare, IT/finance, IT/education, public administration, legal sector, manufacturing, and finance), one AI-related project has been co-financed in each sector.

In 2023 the Government of the Republic of North Macedonia launched its first AI-based digital assistant, ADA, aimed at improving transparency and access to information on investment opportunities. The tool is no longer operational despite an investment of EUR 150,000. One of the key reasons is the non-renewal of the contract with the economic operator responsible for the development and maintenance of the application.

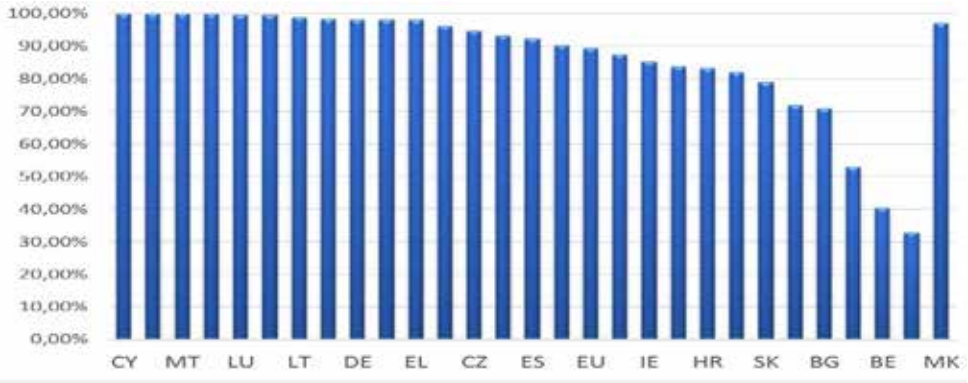
The absence of next-generation supercomputers, reliable data centers, and specialized systems for big data processing limits the country's readiness to deploy AI in the public sector.

Coverage with Very High-Capacity Networks (VHCN) in the EU Member States and the Republic of North Macedonia.



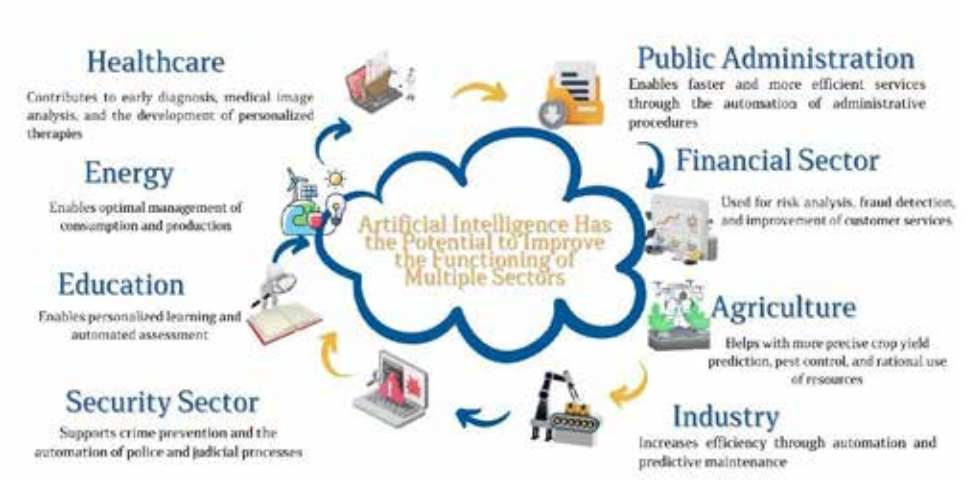
Coverage with fixed Very High-Capacity Networks (VHCN) includes 408,446 households, or 68.23% of the total number of households in the Republic of North Macedonia. Of these, 63,781 households, or 10.65% of the total number of households in the Republic of North Macedonia, are in rural settlements.

Total 5G Coverage in the EU Member States and the Republic of North Macedonia.



Despite official announcements, the technology park in Skopje has not yet been constructed, while existing initiatives remain incomplete. This highlights the need for targeted investment in infrastructure that will enable secure, reliability, and efficient application of modern technologies, in line with European regulations and strategic objectives for digital transformation.

Artificial intelligence has the potential to significantly enhance the performance of multiple sectors:



However, these potentials remain largely untapped due to the absence of a national AI strategy, adequate infrastructure, and limited human resources.

Additionally, limited availability of open data, weak coordination with international bodies, and low institutional readiness are bottlenecks to AI development in the country. Access to open, structured, and machine-readable public-sector data is a key prerequisite for the development of AI-based systems.

Universities play a significant role in developing human capacities for artificial intelligence; however, systemic integration with the public sector and a unified cooperation platform are lacking. Based on responses from six higher education institutions, the largest capacities are identified at the Faculty of Computer Science and Engineering (FINKI) and the Faculty of Electrical Engineering and Information Technologies (FEIT) at Ss. Cyril and Methodius University in Skopje, with more than

1,700 bachelor's theses, 220 master's theses, and 37 doctoral dissertations related to AI. Some universities participate in natural language processing projects such as TTS-MK and ChatMed. Nevertheless, the absence of a public register, formal retraining programs, and a centralized database of AI-trained professionals limits coordinated development in this strategic area.

Natural language processing (NLP) projects represent important steps towards the local development of artificial intelligence, with a focus on preserving and enabling the practical use of the Macedonian language.

The **"Buki" model**, developed by Ss. Cyril and Methodius University in 2024, enables automatic speech-to-text transcription with punctuation and grammatical structuring and is applicable in education, public administration, and for persons with disabilities.

Within the pilot project for the **112-emergency number**, artificial intelligence is used for real-time analysis and decision-support recommendations during emergency calls; however, its full-scale implementation is constrained by additional financial requirements and the absence of a comprehensive legal and technical framework.

These initiatives underscore the need for dedicated investment, language adaptation, and institutional support to fully exploit the potential of artificial intelligence in areas of critical public interest.

Although the legislative framework for personal data protection is aligned with the EU General Data Protection Regulation (GDPR), the audit found that the application of these standards in AI projects is insufficient and poses potential risks. Projects such as the 112 system, which involve real-time AI-based transcription and translation, require specific Data Protection Impact Assessments (DPIAs), a practice that has not yet been systematically established.

The Personal Data Protection Agency lacks sufficient supervisory capacity and is not involved in the drafting of sector-specific legislation. According to the European Commission Report for 2024, "no progress has been achieved in the area of personal data protection", highlighting weak inter-institutional coordination, ineffective monitoring of recommendations, and insufficient accountability of public institutions. "

In the absence of a dedicated national regulatory framework for artificial intelligence aligned with personal data protection legislation, the protection of citizens' personal data cannot be fully ensured. Although the legal basis exists, effective oversight and control mechanisms are required for the application of AI technologies.

The country possesses a foundation for the development of ethical standards in the implementation of artificial intelligence; however, a formalized and comprehensive mechanism regulating ethical aspects has not yet been established. Additional institutional and legal mechanisms are necessary

to ensure ethical, transparent, and non-discriminatory use of artificial intelligence by the public sector, in line with European standards.

The public sector is not prepared to use artificial intelligence in its activities due to the absence of a strategic and legal framework, action plans, a development budget, as well as the current state of ICT infrastructure and human resources.

The recommendations are addressed to the **Ministry of Digital Transformation**, in cooperation with the Government of the Republic of North Macedonia and other key stakeholders, and focus on:

- Establishing a strategic and legal framework for AI implementation
- Improving ICT infrastructure
- Creating a centralized AI project database
- Enhancing international perception of digital maturity and AI readiness
- Strengthening collaboration between public administration, academia and business
- Introducing effective personal data protection mechanisms for AI projects

AUDIT

International parallel audit on artificial intelligence

Federal Chancellery, Federal Statistical Office, Federal Office of Information Technology, Systems and Telecommunication, Federal Office of Communications

KEY FACTS

Artificial intelligence (AI) is increasingly permeating many areas of people's lives and the economy. The debate around AI has gained considerable traction in the media and politics. The Swiss Federal Audit Office (SFAO) is participating in a parallel audit entitled "Examine the government sector's preparedness for implementation of AI technology". The audit was launched in 2024 by the European Organisation of Supreme Audit Institutions (EUROSAI). In further audits, the SFAO assessed the extent to which the groundwork has been laid for the adoption of AI in the Federal Administration. It examined two areas of action: institutional AI frameworks and specific AI projects.

The AI initiatives launched by the Confederation create a framework for institutional AI which provides a firm foundation for the adoption of AI. At the same time, the Confederation has launched numerous AI projects, some of which have already been put into practice. However, pioneering AI projects should be visible to the public and demonstrate the responsible use of AI in the Federal Administration. There also needs to be effective coordination between the two areas of action, to ensure the targeted further development of AI, and to keep pace with the rapid advances in AI technology. Moreover, closer coordination reduces the risk of shadow IT, in other words IT solutions that are developed outside of authorised use and validated infrastructure. It is difficult to regain control of uncoordinated and redundantly structured IT infrastructures at a later date, which impairs both IT security and the administration's economic efficiency.

The institutional framework is being refined and many projects have been launched

The report "Challenges of AI" by the interdepartmental AI working group was the initial spark for the design of the institutional AI framework[4]. Various AI initiatives were subsequently launched, in order to embed the use of AI technology in the Confederation strategically and in terms of regulations. Important milestones have been reached and are now being consolidated. This includes the implementation plan for the Federal Administration's AI strategy, the preparatory work on implementing the Council of Europe's AI Convention and the establishment of a concept to further develop the coordination of federal AI. Together with analyses on infrastructure topics, a sound institutional AI framework will be finalised by the end of 2026.

The "AI projects" area of action demonstrates a great deal of initiative on the part of the Confederation, as over 100 sub-projects have been launched. Specialist offices are using their expertise to develop and run their own AI projects. These bottom-up initiatives include innovative applications such as SwissPollen from MeteoSwiss and the Swiss Energy Dashboard from the Federal Office of Energy, as well as AI-based dialogue systems – chatbots. However, there is a lack of pioneering AI projects which could play a leading role in the Confederation. This would include projects that – irrespective of their size – are practical and show clearly how AI is used in the Confederation, even in sensitive areas of application. They would be essential to demonstrate the responsible use of the new technology and promote acceptance of AI within and outside the Federal Administration.

[4] Report by the interdepartmental working group on artificial intelligence, for the attention of the Federal Council (downloaded on 13.05.2025)

Governance and digitalisation incentives under scrutiny

Federal efforts focused primarily on the design of the institutional AI framework, while AI projects resulted from initiatives by the specialist offices. There is scarcely any overlap between these two areas of action. However, the further development of the AI framework would have to be focused more towards pioneering AI projects, in order to make the precise design more specific. Conversely, the know-how already obtained should flow into pioneer projects which, for example, develop AI-supported, automated systems for decision-making and their preparation. Yet such projects, which can optimise repetitive administrative tasks, are vastly underrepresented.

The efficacy of digital transformation governance should be re-evaluated by the Confederation. The steering model, which provides guidance on digital topics to people in the Federal Administration, has been in place for four years. The aim is to adapt the decision-making powers, so as to strengthen shared progress in the area of digitalisation. This is a desirable approach that is indispensable for a cross-cutting issue such as AI. At the same time, incentives are being sought to make more consistent use of the potential for efficiency gains – notably through the use of AI. If the new governance structure for digital transformation proves useful, it would strengthen the efficiency and competence of the federal government in AI matters.

APPENDIX C
INTERNATIONAL INDEXES[18]

18 The indexes refer to the 2024 editions, as the cross-country benchmarking and comparisons were conducted based on the 2024 rankings. While a newer edition of the Indexes is available, we have opted not to update the comparative analysis at this stage

Full rankings

Country	Total	Government	Technology Sector	Data and Infrastructure
Afghanistan	**16.92**	8.27	22.46	20.05
Albania	**45.47**	47.93	28.36	60.11
Algeria	**39.06**	31.68	33.26	52.24
Andorra	**54.44**	47.34	41.06	74.91
Angola	**26.91**	19.73	15.87	45.13
Antigua and Barbuda	**41.61**	30.68	30.66	63.49
Argentina	**56.40**	64.65	37.09	67.47
Armenia	**44.51**	37.97	32.91	62.66
Australia	**76.45**	86.18	56.26	86.90
Austria	**72.84**	78.37	56.56	83.57
Azerbaijan	**39.92**	35.56	29.43	54.78
Bahamas	**42.03**	31.49	30.40	64.21
Bahrain	**54.33**	45.62	37.61	79.76
Bangladesh	**47.12**	58.52	26.26	56.59
Barbados	**41.11**	32.12	31.69	59.51
Belarus	**39.24**	27.54	34.57	55.61
Belgium	**72.69**	81.26	56.23	80.57
Belize	**37.59**	26.76	30.51	55.49
Benin	**42.97**	59.92	24.30	44.68
Bhutan	**38.78**	34.02	25.58	56.73
Bolivia (Plurinational State of)	**33.08**	22.43	22.92	53.89
Bosnia and Herzegovina	**37.02**	26.74	29.25	55.06

Botswana	**38.16**	35.14	30.23	49.12
Brazil	**65.89**	74.51	44.78	78.38
Brunei Darussalam	**55.45**	45.85	45.87	74.62
Bulgaria	**60.64**	65.19	37.88	78.85
Burkina Faso	**29.28**	25.69	21.22	40.92
Burundi	**21.13**	16.62	18.95	27.84
Cabo Verde	**40.67**	39.58	27.25	55.19
Cambodia	**36.63**	29.18	29.31	51.40
Cameroon	**33.46**	30.10	28.64	41.63
Canada	**78.18**	85.48	61.69	87.35
Central African Republic	**20.26**	12.07	19.95	28.77
Chad	**22.66**	20.94	18.22	28.82
Chile	**63.19**	70.75	44.11	74.71
China	**72.01**	72.90	62.95	80.18
Colombia	**59.33**	71.96	39.00	67.05
Comoros	**26.65**	17.22	23.75	38.97
Congo	**25.12**	22.40	22.71	30.24
Costa Rica	**56.85**	68.46	34.74	67.35
Côte d'Ivoire	**34.69**	31.15	26.10	46.81
Croatia	**51.62**	40.86	39.72	74.28
Cuba	**42.43**	51.55	26.76	49.00
Cyprus	**61.50**	68.53	36.18	79.80
Czechia	**70.23**	76.45	49.50	84.74
Democratic Republic of the Congo	**22.10**	17.96	15.99	32.34
Denmark	**74.71**	84.07	57.17	82.89
Djibouti	**35.19**	23.13	32.84	49.61
Dominican Republic	**52.69**	69.04	24.77	64.27

Ecuador	**41.46**	34.27	29.31	60.79
Egypt	**55.63**	68.98	42.13	55.77
El Salvador	**34.09**	25.50	26.81	49.95
Equatorial Guinea	**27.09**	19.28	25.68	36.31
Eritrea	**22.20**	8.30	23.07	35.22
Estonia	**72.62**	86.71	48.97	82.19
Eswatini	**36.23**	29.11	26.20	53.36
Ethiopia	**38.34**	51.46	21.57	41.98
Fiji	**44.22**	37.02	32.32	63.31
Finland	**76.48**	84.86	60.86	83.73
France	**79.36**	85.29	63.53	89.25
Gabon	**34.15**	25.45	27.77	49.22
Gambia (Republic of The)	**26.95**	23.25	19.67	37.92
Georgia	**46.92**	43.41	34.53	62.81
Germany	**76.90**	79.24	64.91	86.55
Ghana	**43.30**	59.53	25.35	45.03
Greece	**57.70**	50.66	46.55	75.88
Grenada	**37.96**	31.88	28.39	53.62
Guatemala	**36.41**	28.95	23.70	56.59
Guinea	**30.21**	25.63	22.24	42.77
Guinea Bissau	**25.71**	14.65	20.46	42.01
Guyana	**37.23**	26.53	27.56	57.61
Haiti	**20.06**	7.52	18.61	34.04
Honduras	**29.83**	24.72	21.77	43.01
Hungary	**63.63**	74.09	41.81	75.00
Iceland	**69.82**	82.20	47.16	80.10
India	**62.81**	73.32	50.34	64.76

Indonesia	**65.85**	79.86	48.06	69.64
Iran (Islamic Republic of)	**43.88**	26.54	38.82	66.29
Iraq	**40.91**	32.60	35.87	54.25
Ireland	**73.18**	75.47	58.13	85.95
Israel	**74.52**	79.30	61.53	82.74
Italy	**71.22**	78.64	53.12	81.88
Jamaica	**37.79**	34.43	28.82	50.11
Japan	**75.75**	80.31	57.96	88.98
Jordan	**61.57**	74.92	42.64	67.14
Kazakhstan	**51.41**	54.75	33.54	65.93
Kenya	**43.56**	56.20	30.98	43.49
Kiribati	**34.45**	30.85	26.96	45.55
Kuwait	**51.26**	46.49	36.93	70.36
Kyrgyzstan	**36.55**	34.68	24.49	50.49
Lao People's Democratic Republic	**36.08**	28.10	28.79	51.36
Latvia	**61.87**	74.46	35.72	75.43
Lebanon	**46.67**	51.04	40.48	48.48
Lesotho	**28.21**	24.66	21.08	38.90
Liberia	**23.12**	16.58	20.89	31.90
Libya	**33.25**	16.41	34.53	48.80
Liechtenstein	**55.91**	43.70	49.19	74.83
Lithuania	**67.80**	77.63	43.02	82.75
Luxembourg	**70.63**	84.67	43.81	83.40
Madagascar	**28.80**	25.30	21.19	39.92
Malawi	**29.32**	27.85	23.79	36.32
Malaysia	**71.40**	82.47	54.17	77.56
Maldives	**31.43**	33.71	17.22	43.36

Mali	**32.27**	26.00	22.44	48.36
Malta	**63.64**	75.86	39.89	75.18
Marshall Islands	**37.62**	29.94	31.65	51.29
Mauritania	**41.40**	50.12	29.10	44.98
Mauritius	**53.94**	65.31	32.71	63.81
Mexico	**53.29**	43.52	42.27	74.07
Mongolia	**42.36**	36.94	26.78	63.36
Montenegro	**47.43**	39.41	33.40	69.48
Morocco	**41.78**	34.82	36.70	53.82
Mozambique	**24.22**	20.86	18.23	33.57
Myanmar	**34.26**	24.24	33.85	44.69
Namibia	**33.28**	28.56	25.36	45.92
Nepal	**33.14**	30.61	25.44	43.37
Netherlands	**77.23**	84.58	60.12	87.00
New Zealand	**63.98**	55.95	49.56	86.43
Nicaragua	**28.53**	20.07	21.88	43.64
Niger	**25.74**	24.22	17.15	35.87
Nigeria	**43.33**	59.88	27.11	42.99
North Macedonia	**45.12**	36.51	32.36	66.50
Norway	**76.12**	86.38	56.28	85.70
Oman	**62.91**	69.61	41.29	77.84
Pakistan	**40.47**	40.61	36.94	43.87
Panama	**44.39**	35.79	26.97	70.41
Papua New Guinea	**36.85**	32.64	29.50	48.40
Paraguay	**39.54**	36.90	23.15	58.56
Peru	**57.11**	68.60	34.03	68.70
Philippines	**58.51**	74.49	38.58	62.45
Poland	**67.51**	76.53	45.41	80.59

Portugal	**70.93**	79.47	52.49	80.83
Qatar	**68.22**	76.07	46.90	81.69
Republic of Korea	**79.98**	84.59	62.60	92.74
Republic of Moldova	**56.03**	69.38	29.94	68.79
Romania	**58.08**	69.25	40.41	64.58
Russian Federation	**64.72**	72.15	45.38	76.62
Rwanda	**51.25**	71.44	30.30	52.02
Saint Kitts and Nevis	**41.62**	30.26	32.65	61.94
Saint Lucia	**39.11**	31.10	28.63	57.60
Saint Vincent and the Grenadines	**36.65**	29.30	28.11	52.55
Samoa	**37.16**	31.82	27.41	52.26
San Marino	**51.59**	38.65	42.14	73.99
Sao Tome and Principe	**29.63**	24.82	23.69	40.39
Saudi Arabia	**72.36**	80.72	52.92	83.43
Senegal	**46.11**	62.37	28.77	47.18
Serbia	**58.49**	69.88	38.22	67.35
Seychelles	**44.77**	41.41	36.81	56.09
Sierra Leone	**25.34**	21.96	17.72	36.33
Singapore	**84.25**	90.96	68.65	93.14
Slovakia	**63.69**	68.76	41.40	80.91
Slovenia	**65.85**	77.48	43.32	76.76
Solomon Islands	**32.71**	27.69	27.98	42.45
Somalia	**25.32**	19.05	20.36	36.54
South Africa	**52.91**	54.30	39.15	65.28
South Sudan	**18.58**	11.04	19.74	24.96
Spain	**69.25**	74.58	50.75	82.43

Sri Lanka	**45.29**	55.04	32.19	48.65
State of Palestine	**37.53**	24.64	32.75	55.21
Sudan	**24.63**	13.32	24.29	36.28
Suriname	**36.87**	25.79	27.84	56.99
Sweden	**75.40**	80.60	63.45	82.16
Switzerland	**69.42**	59.06	61.32	87.88
Syrian Arab Republic	**16.95**	16.42	18.93	15.49
Taiwan	**74.58**	82.98	56.37	84.38
Tajikistan	**36.72**	51.05	19.79	39.31
Thailand	**66.17**	75.78	44.83	77.90
Timor-Leste	**33.68**	27.03	26.70	47.30
Togo	**31.32**	31.21	20.82	41.92
Tonga	**38.63**	31.75	34.89	49.25
Trinidad and Tobago	**40.14**	32.33	31.53	56.56
Tunisia	**43.68**	28.62	41.07	61.35
Türkiye	**60.63**	70.73	45.13	66.02
Turkmenistan	**32.64**	17.03	32.92	47.96
Uganda	**34.63**	35.57	22.23	46.10
Ukraine	**60.57**	73.42	41.93	66.37
United Arab Emirates	**75.66**	83.89	59.20	83.89
United Kingdom of Great Britain and Northern Ireland	**78.88**	84.47	66.57	85.62
United Republic of Tanzania	**35.08**	36.64	20.98	47.62
United States of America	**87.03**	89.26	80.94	90.90
Uruguay	**62.21**	76.39	33.31	76.93

Uzbekistan	**53.45**	64.71	33.50	62.14
Vanuatu	**39.04**	34.44	30.85	51.82
Venezuela, Bolivarian Republic of	**29.21**	15.50	26.00	46.12
Viet Nam	**61.42**	75.02	43.36	65.86
Yemen	**14.62**	12.90	20.41	10.56
Zambia	**41.87**	60.78	23.22	41.63
Zimbabwe	**32.59**	23.69	27.82	46.27

Global Innovation Index 2025 rankings

GII rank	Economy	Score	Income group rank	Region rank
1	Switzerland	66.0	1	1
2	Sweden	62.6	2	2
3	United States	61.7	3	1
4	Republic of Korea	60.0	4	1
5	Singapore	59.9	5	2
6	United Kingdom	59.1	6	3
7	Finland	57.7	7	4
8	Netherlands (Kingdom of the)	57.0	8	5
9	Denmark	56.9	9	6
10	China	56.6	1	3
11	Germany	55.5	10	7
12	Japan	53.6	11	4
13	France	53.4	12	8
14	Israel	52.3	13	1
15	Hong Kong, China	51.5	14	5
16	Estonia	51.1	15	9
17	Canada	51.1	16	2
18	Ireland	50.4	17	10
19	Austria	50.1	18	11
20	Norway	49.2	19	12
21	Belgium	48.5	20	13
22	Australia	48.0	21	6
23	Luxembourg	47.3	22	14
24	Iceland	47.0	23	15
25	Cyprus	45.5	24	2
26	New Zealand	45.5	25	7
27	Malta	45.4	26	16
28	Italy	44.9	27	17
29	Spain	44.6	28	18
30	United Arab Emirates	44.2	29	3
31	Portugal	43.9	30	19
32	Czech Republic	42.0	31	20
33	Lithuania	40.8	32	21
34	Malaysia	40.6	2	8
35	Slovenia	40.1	33	22
36	Hungary	40.0	34	23
37	Bulgaria	39.1	35	24
38	India	38.2	1	1
39	Poland	37.7	36	25
40	Croatia	37.7	37	26
41	Latvia	37.5	38	27
42	Greece	37.4	39	28
43	Türkiye	37.2	3	4
44	Viet Nam	37.1	2	9
45	Thailand	36.7	4	10
46	Saudi Arabia	36.0	40	5
47	Slovakia	35.5	41	29
48	Qatar	34.6	42	6
49	Romania	34.3	43	30
50	Philippines	33.6	3	11
51	Chile	33.1	44	1
52	Brazil	32.9	5	2
53	Mauritius	32.5	6	1
54	Serbia	31.7	7	31
55	Indonesia	31.3	8	12
56	Georgia	31.2	9	7
57	Morocco	31.1	4	8
58	Mexico	30.5	10	3
59	Armenia	30.5	11	9
60	Russian Federation	30.3	45	32
61	South Africa	30.1	12	2
62	Bahrain	30.0	46	10
63	North Macedonia	29.8	13	33
64	Montenegro	29.8	14	34
65	Jordan	29.7	5	11
66	Ukraine	29.7	15	35
67	Albania	29.6	16	36
68	Uruguay	28.8	47	4
69	Oman	28.7	48	12
70	Iran (Islamic Republic of)	28.5	17	2
71	Colombia	28.5	18	5
72	Costa Rica	28.4	19	6
73	Kuwait	28.2	49	13
74	Republic of Moldova	27.4	20	37
75	Seychelles	27.2	50	3
76	Tunisia	27.0	6	14
77	Argentina	26.8	21	7
78	Mongolia	26.7	22	13
79	Uzbekistan	26.5	7	3
80	Peru	26.5	23	8
81	Kazakhstan	26.3	24	4
82	Panama	25.9	51	9
83	Jamaica	25.2	25	10
84	Barbados	25.1	52	11
85	Belarus	25.1	26	38
86	Egypt	24.7	8	15
87	Botswana	24.6	27	4
88	Brunei Darussalam	24.5	53	14
89	Senegal	23.8	9	5
90	Lebanon	23.6	10	16
91	Namibia	23.5	28	6
92	Bosnia and Herzegovina	23.4	29	39
93	Sri Lanka	22.9	11	5
94	Azerbaijan	22.9	30	17
95	Cabo Verde	22.6	12	7
96	Kyrgyzstan	22.6	13	6
97	Dominican Republic	22.6	31	12
98	El Salvador	22.2	32	13
99	Pakistan	22.1	14	7
100	Cambodia	22.0	15	15
101	Ghana	21.9	16	8
102	Kenya	21.4	17	9
103	Paraguay	21.4	33	14
104	Rwanda	21.1	1	10
105	Nigeria	21.1	18	11
106	Bangladesh	21.0	19	8
107	Nepal	20.2	20	9
108	Tajikistan	20.2	21	10
109	Lao People's Democratic Republic	20.1	22	16
110	Côte d'Ivoire	19.7	23	12
111	Bolivia (Plurinational State of)	19.6	24	15
112	Zambia	19.6	25	13
113	Ecuador	19.5	34	16
114	Trinidad and Tobago	19.3	54	17
115	Algeria	18.9	35	18
116	Cameroon	18.2	26	14
117	Togo	18.1	2	15
118	Benin	17.8	27	16
119	Honduras	17.7	28	18
120	Madagascar	17.6	3	17
121	United Republic of Tanzania	17.5	29	18
122	Myanmar	17.3	30	17
123	Guatemala	17.1	36	19
124	Uganda	17.1	4	19
125	Malawi	16.0	5	20
126	Burkina Faso	15.9	6	21
127	Burundi	15.8	7	22
128	Mozambique	15.4	8	23
129	Zimbabwe	15.4	31	24
130	Nicaragua	15.4	32	20
131	Mauritania	15.4	33	25
132	Lesotho	14.9	34	26
133	Guinea	14.9	35	27
134	Ethiopia	14.4	9	28
135	Mali	14.0	10	29
136	Venezuela (Bolivarian Republic of)	13.7		21
137	Congo	13.6	36	30
138	Angola	13.0	37	31
139	Niger	11.9	11	32

Low-income
Lower middle-income
Upper middle-income
High-Income

Sub-Saharan Africa
Central and Southern Asia
South East Asia, East Asia, and Oceania
Nothern Africa and Western Asia

Latin America and the Caribbean
Northern America
Europe

Note: The World Bank classified Venezuela (Bolivarian Republic of) as an upper-middle income economy until 2021 and has been unclassified since then due to the unavailability of data.

Source: Global Innovation Index Database, WIPO, 2025.

Ranking Table

Countries are ranked by their AI capacity at the international level. This is the fifth iteration of the Global AI Index, published on 19 September 2024.

	Overall	Talent	Infrastructure	Operating Environment	Research	Development	Government Strategy	Commercial	Scale	Intensity
United States	1	1	1	2	1	1	2	1	1	3
China	2	9	2	21	2	2	5	2	2	21
Singapore	3	6	3	48	3	5	10	4	11	1
United Kingdom	4	4	17	4	4	16	7	5	3	9
France	5	10	14	19	6	4	9	8	6	10
South Korea	6	13	6	35	13	3	4	12	7	11
Germany	7	3	13	8	8	11	8	9	5	15
Canada	8	8	18	16	9	10	3	6	8	8
Israel	9	7	26	65	7	6	32	3	14	2
India	10	2	68	3	14	13	11	13	4	36
Japan	11	23	5	53	20	14	12	14	9	31
Switzerland	12	5	11	58	5	19	64	20	29	4
The Netherlands	13	11	7	29	15	17	19	23	13	12
Saudi Arabia	14	60	29	41	42	26	1	7	10	24
Finland	15	14	12	9	18	12	25	15	18	6
Hong Kong	16	21	8	40	10	18	59	11	20	7
Australia	17	17	39	13	11	7	42	21	15	18
Spain	18	18	19	17	26	21	6	32	12	25
Luxembourg	19	12	10	23	16	24	33	26	32	5
United Arab Emirates	20	48	16	47	12	9	23	17	21	13
Taiwan	21	28	4	71	27	15	15	39	17	28
Denmark	22	16	25	15	22	28	18	25	23	19
Ireland	23	25	20	22	29	8	38	19	24	14
Italy	24	19	27	1	21	45	13	43	16	32
Sweden	25	15	21	5	19	30	57	18	27	16
Norway	26	24	22	7	23	42	22	22	25	20
Belgium	27	20	43	31	25	27	48	24	28	26
Austria	28	22	38	39	17	37	36	38	34	22
Portugal	29	29	37	6	32	23	53	30	30	29
Brazil	30	26	36	28	44	29	27	33	19	44
Russia	31	58	44	30	37	20	21	40	22	46
Estonia	32	33	49	42	34	52	44	16	54	17
Malta	33	47	41	26	43	22	30	34	41	27

	Overall	Talent	Infrastructure	Operating Environment	Research	Development	Government Strategy	Commercial	Scale	Intensity
Turkey	34	38	62	11	39	31	14	55	26	45
Czech Republic	35	30	46	64	35	36	17	44	35	33
Poland	36	27	28	36	41	32	39	46	31	37
Slovenia	37	34	35	14	28	54	45	41	46	30
Chile	38	50	24	34	62	46	20	37	33	41
Malaysia	39	59	15	25	38	43	52	47	36	43
Iceland	40	37	9	54	33	53	79	27	66	23
Hungary	41	41	31	46	47	38	50	42	42	40
Greece	42	31	42	83	30	34	66	31	52	34
Thailand	43	66	23	63	63	63	16	54	39	55
Croatia	44	45	61	56	46	62	79	10	47	38
Mexico	45	42	57	20	61	40	47	52	38	57
Lithuania	46	44	47	44	52	51	34	53	49	39
Argentina	47	40	54	12	71	39	46	63	40	54
New Zealand	48	32	30	50	31	33	71	48	57	35
Indonesia	49	36	72	49	24	71	62	45	37	63
Romania	50	56	34	32	56	25	65	69	44	53
Colombia	51	53	51	52	74	49	24	64	43	59
Egypt	52	54	64	18	55	68	37	56	45	61
Bulgaria	53	46	53	56	50	56	31	65	50	47
Qatar	54	63	32	78	36	60	26	77	59	42
Ukraine	55	51	59	38	65	48	40	60	48	58
Uruguay	56	52	40	33	73	67	49	61	51	50
Serbia	57	43	58	78	49	65	35	70	58	48
Vietnam	58	49	33	70	67	58	56	57	53	64
Mauritius	59	80	69	74	69	74	54	28	62	52
Iran	60	65	70	82	40	44	41	83	56	67
Peru	61	61	52	37	81	75	60	73	55	68
Bahrain	62	71	48	60	48	77	72	29	61	56
Jordan	63	72	45	78	45	35	61	72	63	62
Oman	64	75	55	78	66	66	29	80	60	66
Armenia	65	35	66	60	72	47	82	36	73	49
Slovakia	66	39	56	44	51	55	83	49	67	51

	Overall	Talent	Infrastructure	Operating Environment	Research	Development	Government Strategy	Commercial	Scale	Intensity
Philippines	67	78	60	10	77	57	69	67	64	72
Rwanda	68	74	82	26	80	83	43	62	65	69
South Africa	69	69	74	62	64	41	79	35	70	70
Latvia	70	55	50	55	54	59	74	71	78	60
Tunisia	71	62	71	78	53	70	68	59	75	65
Ghana	72	81	77	78	76	82	55	50	74	71
Nigeria	73	77	79	45	70	73	51	68	68	76
Benin	74	83	81	66	79	81	28	66	69	73
Bangladesh	75	73	75	70	68	61	58	78	72	77
Pakistan	76	57	78	68	58	64	63	75	71	81
Iraq	77	82	67	73	59	78	67	74	76	80
Azerbaijan	78	68	65	51	78	80	72	81	77	79
Morocco	79	67	63	60	57	50	76	79	79	75
Algeria	80	70	73	72	60	79	70	82	80	82
Kenya	81	79	80	24	82	69	79	51	81	78
Sri Lanka	82	64	76	66	75	72	75	58	82	74
Ethiopia	83	76	83	78	83	76	79	76	83	83

APPENDIX D
METHODOLOGY USED FOR THE CROSS-INDEX CORRELATION ANALYSIS

Methodology used for the cross-index correlation analysis

To test whether different international indexes tell a consistent story about national AI and innovation capacity, we compared **Oxford AI Readiness, Tortoise Global AI Index,** and the **Global Innovation Index (GII)** using a common country sample and a consistent statistical approach.

Making the indexes comparable

The three indexes use different structures and scales, so we constructed comparable variables before calculating correlations:

- **Oxford AI Readiness (scores, higher = better):** we created composite pillar scores using **simple averages** of the published subcomponents:
  - Oxford Technology Sector = (Maturity + Innovation Capacity + Human Capital) / 3
  - Oxford Data and Infrastructure = (Infrastructure + Data Availability + Data Representativeness) / 3
- (The same averaging logic was applied consistently whenever a composite was needed.)
- **Tortoise Global AI Index (ranks, lower = better):** we created pillar values using **simple averages** of the published ranks:
  - Tortoise Implementation = (Talent + Infrastructure + Operating Environment) / 3
  - Tortoise Innovation = (Research + Development) / 2
  - Tortoise Investment = (Government Strategy + Commercial) / 2
- **GII (ranks, lower = better):** we used the **published pillar ranks directly** (no transformation).

Correlation method. We then calculated Pearson correlation coefficients (r) between the selected Oxford, Tortoise, and GII variables across the 10 countries. Pearson's r measures the strength and direction of association between two variables (from -1 to +1).

Interpreting signs and direction. Because Oxford uses scores (higher = better) while Tortoise and GII use ranks (lower = better):

- A negative correlation between Oxford and GII/Tortoise typically reflects alignment (better Oxford scores correspond to better -lower- ranks).
- A positive correlation between GII and Tortoise also typically reflects alignment (countries that perform well tend to have lower ranks in both).

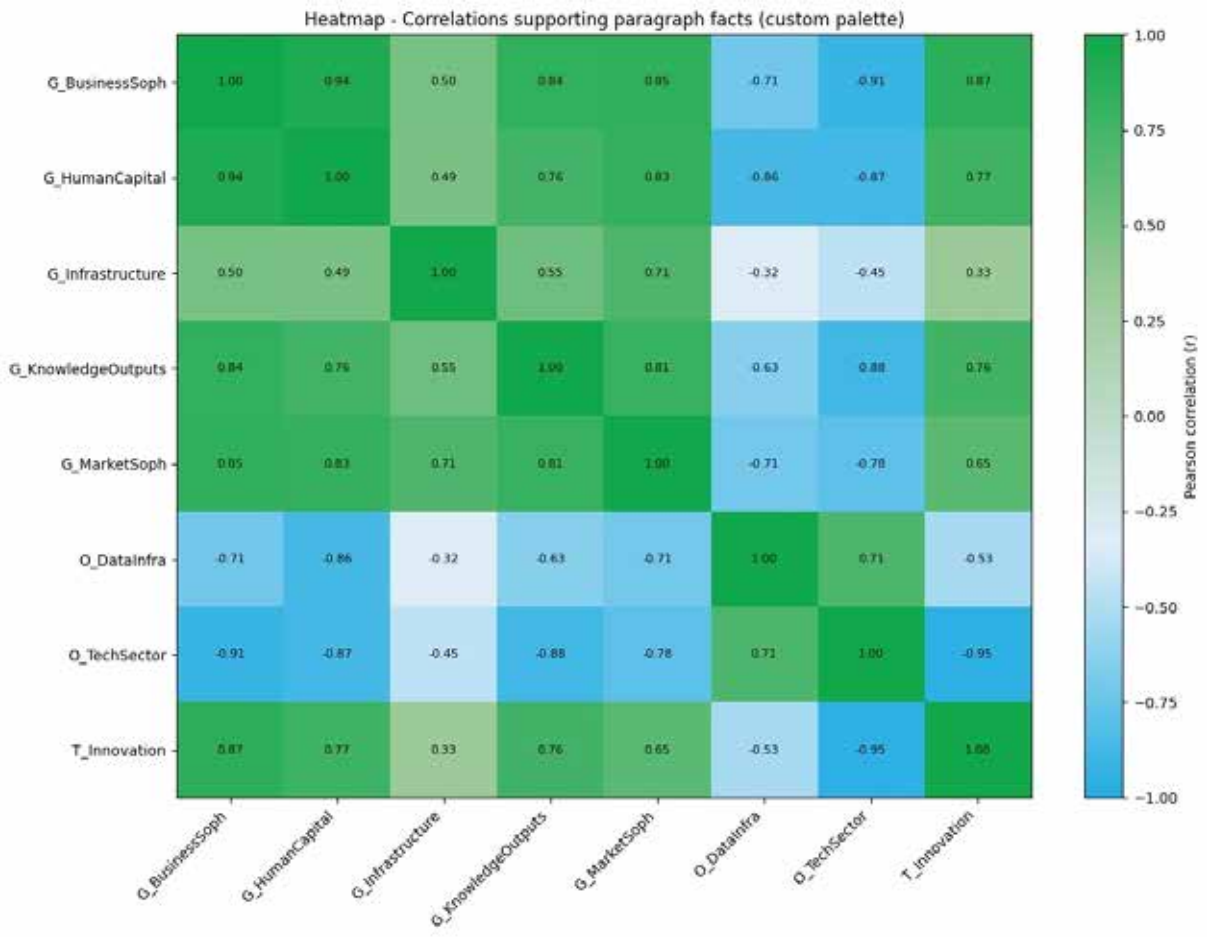
How the appendix evidence supports the paragraph's facts. The conclusions in the paragraph were based on correlations observed in the common sample, including:

- Alignment between AI readiness/tech capacity and human capital (e.g., O_TechSector vs G_HumanCapital).
- The "bridging role" of business sophistication (e.g., G_HumanCapital vs G_BusinessSoph, and G_BusinessSoph vs G_KnowledgeOutputs).
- The idea that AI maturity mirrors broader innovation output (e.g., O_TechSector vs G_KnowledgeOutputs, and T_Innovation vs O_TechSector).
- The limitation of infrastructure as a standalone predictor (e.g., O_DataInfra vs G_Infrastructure being weak compared with its stronger relationship to business sophistication and outputs).

This approach provides a compact cross-validation check: where correlations are consistently strong in expected directions, it suggests the indexes capture overlapping national strengths; where correlations are weaker, it suggests that a dimension (such as infrastructure) may not translate into measurable AI or innovation outcomes without complementary capabilities.

Paragraph fact supported	Variable A	Variable B	Pearson r	Scale note
Human capital aligns with AI readiness	O_TechSector	G_HumanCapital	-0.87	Opposite scaling*
AI maturity mirrors broader innovation outputs	O_TechSector	G_KnowledgeOutputs	-0.88	Opposite scaling*
Cross-index alignment of AI innovation constructs	T_Innovation	O_TechSector	-0.95	Opposite scaling*
Business sophistication bridges education/research and commercialization	G_HumanCapital	G_BusinessSoph	0.94	Same scaling direction
Business sophistication links to innovation outputs	G_BusinessSoph	G_KnowledgeOutputs	0.84	Same scaling direction
Market dynamics align with business sophistication	G_MarketSoph	G_BusinessSoph	0.85	Same scaling direction
Infrastructure alone is not a strong predictor across indexes	O_DataInfra	G_Infrastructure	-0.32	Opposite scaling*
Data/infrastructure is stronger when business capability is stronger	O_DataInfra	G_BusinessSoph	-0.71	Opposite scaling*
Data/infrastructure only moderately tracks innovation outputs	O_DataInfra	G_KnowledgeOutputs	-0.63	Opposite scaling*
Data/infrastructure only moderately tracks AI innovation	O_DataInfra	T_Innovation	-0.53	Opposite scaling*

*Oxford higher=better; GII/Tortoise lower=better



APPENDIX E
NOTABLE EXAMPLES OF AI APPLICATIONS

Notable examples of AI applications that have improved efficiency or service delivery within government ministries

Albania

AI application	Sector / Service
Real-time detection of suspicious transactions. The project was expanded with a focus on the analysis of the wage system and personal income taxes. • Identify anomalies in wage declarations, such as wages inconsistent with the level of economic activity or the relevant sector. • Detecting tax evasion, through the comparison of data reported by employers and other available data (banking, insurance, etc.). • Preventing fictitious declarations and building a fairer and more sustainable tax system.	Finance, tax, customs, and market supervision
Dedicated tool for intelligent translations, created specifically for the needs of public administration. This online tool offers a simple and efficient solution for civil servants, enabling them to upload legal documents in Word format (.doci.docx) and receive high-quality and accurate translations in the target language, while perfectly preserving the structure and original formatting of the document. The main features of the tool include: • Accurate and contextual translation of legal and administrative texts into foreign languages, with an initial focus on English. • Automatic preservation of titles, subsections, numbering, tables and the form of the original document. • Simple and intuitive interface, usable by any administrative employee without the need for specialized training. This tool is a considerable relief for employees, speeding up processes, especially in the context of harmonization with European legislation.	Document and text processing

France

AI application	Sector / Service
At the Ministry of Justice, AI tools help automate the transcription of interviews and assist magistrates in legal research and case summarization, speeding up judicial processes.	Justice and courts
In the Ministry of Education, AI-driven virtual assistants support human resources tasks, allowing staff to focus more on human-centered issues while administrative queries are handled efficiently.	Citizen service and internal support via virtual assistants
An interministerial effort led by the Digital Interministerial Directorate (DINUM) has promoted the adoption of ready-to-use AI solutions across public administrations, simplifying and improving citizen services.	Citizen service and internal support via virtual assistants
The Ministry of Home Affairs (Intérieur) deploys various AI projects to enhance coordination of law enforcement and data management, saving time on daily administrative duties.	Citizen service and internal support via virtual assistants

Israel

AI application	Sector / Service
Ministry of Transport – AI to optimize traffic flow and reduce congestion.	Transport and mobility
Israel Tax Authority – AI for automatic customs classification and faster import processing.	Finance, tax, customs, and market supervision
Israel Securities Authority – Machine learning and NLP for automated market analysis.	Finance, tax, customs, and market supervision
Mapping of Israel – AI and Big Data for automated 3D national mapping.	Mapping, imagery, and geospatial
Ministry of Justice – AI to assess NGO risk and support regulatory oversight.	Justice and courts
National Insurance Institute – AI and OCR to streamline medical committee processes.	Health and social security service delivery
Central Bureau of Statistics – AI search and chat tools to improve data access and accuracy.	Document and text processing
Ministry of Labor – AI platform for personalized labor rights guidance.	Citizen service and internal support via virtual assistants
Civil Service Commission – Gen-AI system for HR knowledge management and decision support.	Citizen service and internal support via virtual assistants

Latvia

AI application	Sector / Service
Virtual assistant	Citizen service and internal support via virtual assistants
Document & image processing	Document and text processing
Data analysis	Data analysis
Transportation sector – AI tools for traffic monitoring and safety.	Transport and mobility
Chatbot ecosystem – a government AI chatbot operating on state and municipal websites, automatically answering frequently asked questions and helping users quickly find information about services.	Citizen service and internal support via virtual assistants
State Revenue Service – AI and data analytics tools to improve tax administration and more effectively identify potential violations.	Finance, tax, customs, and market supervision
Health care: • The first AI powered conversational chatbot developed for a healthcare institution in the Baltics, designed to assist patients with real time information and inquiries; • An AI-powered computer vision solution used for stroke diagnosis and cancer screening.	Health and social security service delivery
Justice sector – an AI tool for the anonymisation of court decisions and judgments to ensure higher anonymisation quality as well as more efficient, secure, and user friendly processes.	Justice and courts

AI application	Sector / Service
Language digitalization – an open source AI language model supporting multiple European languages and facilitating the development of digital solutions for smaller and underrepresented languages.	Document and text processing
Telecommunication networks – AI used for monitoring radio communication networks and ensuring continuous connectivity through precise real-time measurements.	Communications regulation and radio spectrum
Environment – machine learning tools to monitor protected bog boundaries and create precise geospatial layers.	Environment, climate, and bio-monitoring

Slovakia

AI application	Sector / Service
The Office for the Regulation of Electronic Communications and Postal Services has established a "virtual assistant," whose task is to reduce the number of responses by employees and let AI answer basic questions in a controlled manner.	Citizen service and internal support via virtual assistants
The Ministry of Justice of the Slovak Republic uses AI to anonymize court decisions that are published on websites.	Justice and courts
The National Security Office uses AI in the field of cybersecurity (explanation of SIEM signatures).	Cybersecurity and threat detection

Switzerland

AI application	Sector / Service
Creating statistical reports	Data analysis
Classifying documents with keywords	Document and text processing
Identifying potential threats from cyber attacks	Cybersecurity and threat detection
Evaluating climate data	Environment, climate, and bio-monitoring
Analyzing pollen samples	Environment, climate, and bio-monitoring
Identifying the spread patterns of pandemics	Health and social security service delivery
Examine aerial images	Mapping, imagery, and geospatial
Image analysis in customs and goods traffic	Finance, tax, customs, and market supervision
Revealing possible financial market manipulation	Finance, tax, customs, and market supervision
Detecting sources of interference in radio communications	Communications regulation and radio spectrum

Read the full report @
www.mevaker.gov.il

Carrot Design Studio