

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 development¹;
- ✓ Ministry of National Defence, as it formulates policy on cyber security and organises, controls and coordinates its implementation²;
- ✓ National Cyber Security Centre, as it implements cyber security policy and is responsible for organising cyber security exercises and training³;
- ✓ Innovation Agency, as it implements national policy on technology and innovation⁴.

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>.