Digital Transformation of Public Sector: Cases and Best Practices

Table of Contents

Introduction

Digital transformation remains one of the key priorities of the global economy. The process includes not only the integration of new technologies and solutions into the operations and processes of companies and organizations, but also the adoption of new practices and types of management, re-distribution of responsibilities and powers, as well as interaction with external counterparties. According to various estimates, the amount of private investment in digital transformation alone will reach 2.4 to 2.8 trillion US dollars by 2023. Total expenditures on information infrastructure and information technology (IT) will reach 4.6 trillion US dollars by 2023. In addition, it is expected that by 2023, more than half of the world's GDP would be produced by companies and organizations that have undergone digital transformation.

For the public sector, digital transformation is a key priority for a number of reasons:

1. The complexity of economic, social, political, demographic and other processes requires both new approaches to public administration, as well as new methods and technologies for analyzing and processing the information, creating a strategic vision and defining the priorities;
2. Digitalization improves the quality of public administration and the accessibility of public services to the population. In addition, the digitalization of public authorities opens up opportunities for new types of services for the population;
3. Digitalization increases the transparency of the decision-making process of public policy, which in turn enhances accountability and integrity of public administration;
4. In the context of crises, in particular, the COVID-19 pandemic, environmental, social and geopolitical risks, digitalization enhances the ability of the public sector to make timely and informed decisions.

According to some estimates, the global economic effect of the digital transformation of public administration can reach $1 trillion per year.

Evolution of the Digital Government Concept

Public sector organizations are increasingly relying on IT to improve the quality, flexibility and transparency of public services delivery. The process of digital transformation of the public sector began long before the COVID-19 pandemic, but it was the need for massive remote work of employees during the lockdowns that demonstrated the effectiveness of digital formats.

Despite the widespread enthusiasm, digitalization of public sector faces some critic. The data obtained by Deloitte experts in 2015 in surveys of representatives of public authorities in 70 countries of the world, shows that up to 75% of respondents were wary of the processes of transformation, believing that they largely undermine the habitual order of work. At the same time, digital transformation is perceived as an inevitable process.

Digital Transformation in the Public and Private Sectors

The processes of digital transformation in the private and public sectors are largely similar and consist in the gradual transition of digital technologies from the tool to the main driver of strategic development. However, unlike private companies, the digitalization of public sector must meet a number of key conditions:

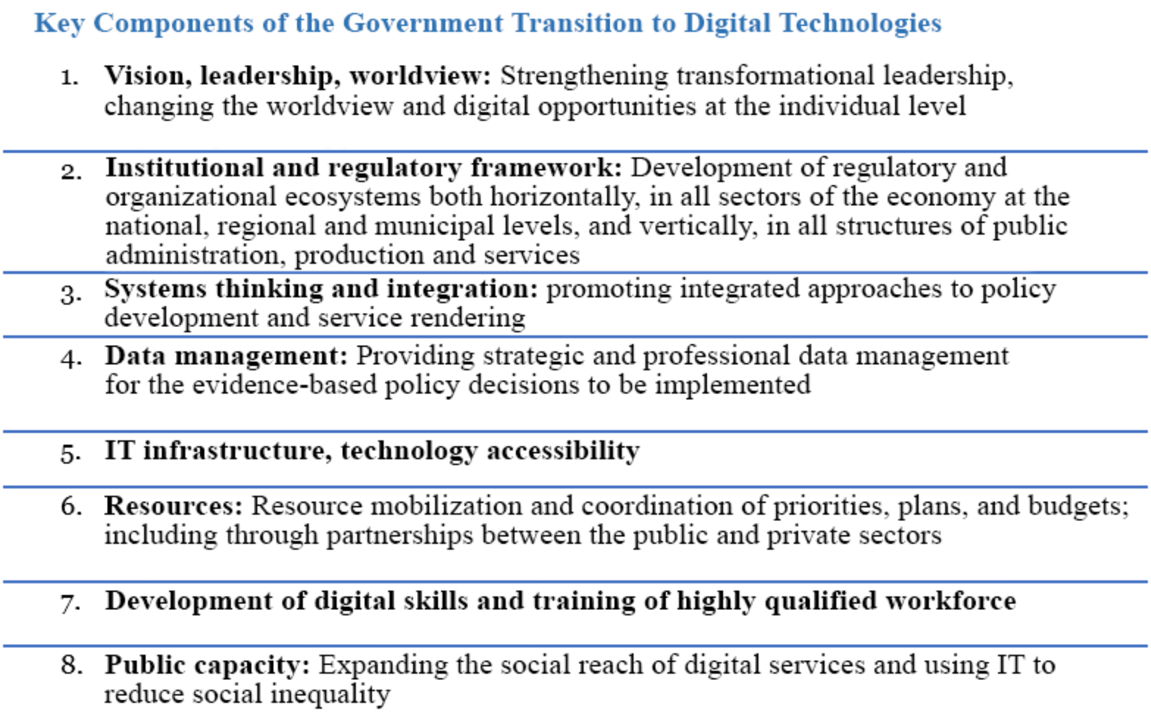
- **Universal nature of public services**. The private sector markets and tailors its products and services to the specific needs of different customer groups. In turn, public services are intended for use by all citizens without exception and must meet the needs of the entire population, as well as be user-friendly.
- **Wider range of applications.** Unlike the private sector, the state provides services in almost all areas, sometimes acting as a competitor to the private sector, and at the same time providing services in spheres that are not available or attractive to private companies.
- **More criteria for assessing the success of digitalization.** Unlike private companies, whose success is measured by cost-benefit categories, the set of efficiency criteria for public services includes not only citizens' satisfaction with the services provided, the availability of these services, etc., but also compliance with strategic goals of national development, which may vary depending on the political situation as citizens' preferences.
- **Higher requirements for reliability and safety.** In addition to the initially high requirements for reliability, quality, accessibility and efficiency, public services are subject to closer attention by representative legislative bodies and supreme audit institutions (SAI).

Moreover, the process of digital transformation of public authorities almost always faces a number of the most characteristic challenges:

- **Limited budgets** for digital transformation, especially for critical technologies and solutions;
- **Strict** rules and procedures for regulating the use of data prevent the rapid introduction of the latest technologies;
- The top priority in the development of products and technologies is **cybersecurity**, rather than user-friendliness and increased efficiency;

- **Impossibility of successful digitalization** of individual public administration bodies – successful interaction and coordinated work requires digitalization of the entire public sector on the basis of common or similar solutions and platforms;
- In the context of centralized decision-making process, the significant "**generation gap**" between the leadership and employees of public institutions largely hinders the rapid digitalization of public administration. The digital transformation of state institutions requires basic educational and technological work to develop a receptive culture and reduce digital divides.

Thus, the implementation of key components of the digital transformation of state structures strongly depends on the political will of the leadership, expressed in national strategic and program documents.



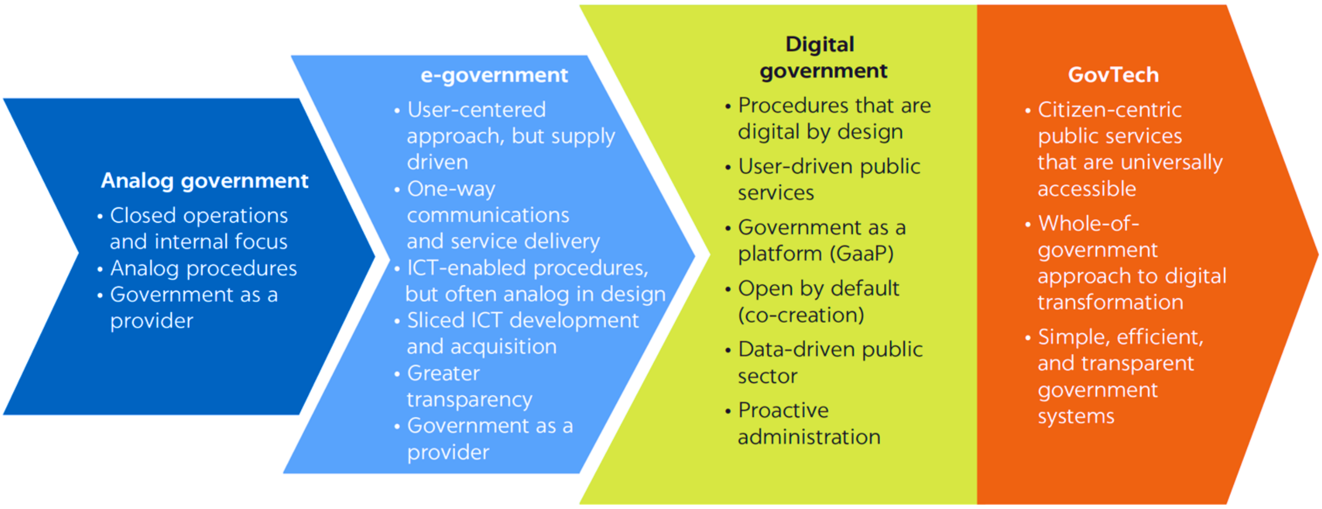
Key Components of the Government Transition to Digital Technologies

1. **Vision, leadership, worldview:** Strengthening transformational leadership, changing the worldview and digital opportunities at the individual level
2. **Institutional and regulatory framework:** Development of regulatory and organizational ecosystems both horizontally, in all sectors of the economy at the national, regional and municipal levels, and vertically, in all structures of public administration, production and services
3. **Systems thinking and integration:** promoting integrated approaches to policy development and service rendering
4. **Data management:** Providing strategic and professional data management for the evidence-based policy decisions to be implemented
5. **IT infrastructure, technology accessibility**
6. **Resources:** Resource mobilization and coordination of priorities, plans, and budgets; including through partnerships between the public and private sectors
7. **Development of digital skills and training of highly qualified workforce**
8. **Public capacity:** Expanding the social reach of digital services and using IT to reduce social inequality

The government is able to compensate the lack of competition as a driver of innovation, by the ability to independently set standards for reforms. For example, the World Bank estimates that in large emerging economies, the digital transformation of the public sector far outpaces that of the private sector.

Digitalization Process of Public Administration

The formation of a digital government is an evolutionary process involving several stages of development.



Analog government

- Closed operations and internal focus
- Analog procedures
- Government as a provider

e-government

- User-centered approach, but supply driven
- One-way communications and service delivery
- ICT-enabled procedures, but often analog in design
- Sliced ICT development and acquisition
- Greater transparency
- Government as a provider

Digital government

- Procedures that are digital by design
- User-driven public services
- Government as a platform (GaaP)
- Open by default (co-creation)
- Data-driven public sector
- Proactive administration

GovTech

- Citizen-centric public services that are universally accessible
- Whole-of-government approach to digital transformation
- Simple, efficient, and transparent government systems

Source: World Bank (GovTech Maturity Index: The State of Public Sector Digital Transformation, 2021)

The **E-government** implies the use of information technologies to automate work processes, improve the efficiency of data management and quality of public services, and develop communication channels. Within the e-government, there are three types of interactions: government-to-government (G2G); government-to-business (G2B); and government-to-citizen (G2C).

UN e-Government Development Model

Stage 1	Online publication of state information
Stage 2	Provision of expanded information on the activities of government bodies, interaction between the government and citizens through the use of electronic forms uploaded to the portal
Stage 3	Two-way interactive cooperation between the government and citizens, gradual involvement of citizens in the process of public administration using information technologies (electronic voting, filling in tax returns, as well as applications for licenses, financial transactions)
Stage 4	Coordination of processes within and between state institutions based on digital solutions, full digital participation of citizens in the process of public administration

Digital Government develops the concept of e-government, uses digital data to proactively provide socially oriented public services.

There are six main components of a digital government:

- Digital **infrastructure**;
- Digital **literacy**;
- Digital **communications**;
- Active use of information **technologies**;
- Legal regulation of the digital **environment**;
- Information **security** and digital **rights**.

The key elements of the digital architecture of the government include a single government information portal, a system of joint management of data from the registers of different state structures; the provision of public services in the format of "one window"; an open database of digital solutions, innovative systems for collecting and analyzing data, ensuring cybersecurity and reliable protection of personal information.

According to the World Bank methodology, the criteria for assessing the effectiveness of digital transformation are:

- **Time** of service provision;
- The **popularity** of digital channels of interaction with the state;
- **Quality** of digitalization of public services;
- **Number** of requests automatically processed;
- Digital literacy **rate** of the population;
- **Reducing** financial costs;
- **Reducing** fraud and corruption.

Priority areas for increasing the digital maturity of government and public bodies are also:

- **Aggregation** and **systematization** of scattered data to improve the delivery of public services;
- **Establishing** safe and flexible technological infrastructure;
- **Building** professional capacity, implementation of personnel policy with emphasis on digital competencies;
- **Interaction** with representatives of the scientific and business communities for the exchange of best practices in the field of digitalization and innovation;
- Periodic **optimization** of work processes, maximum use of labor and technological potential;
- **Development** of the digital ecosystem in accordance with the needs of users of public services.

United Nations (UN)

According to the UN estimates, the global average e-Government Development Index (EGDI) continues to grow, reaching 0.6 in 2020 compared to 0.55 in 2018. According to the results of the study for 2020, 36% (69) states have high EGDI rates, 31% (59) states scored average EGDI rates, 29% (57) countries reached very high EGDI rates, 4% (8) countries have low EGDI rates (the share decreased from 8% to 4% from 2018 to 2020).

The UN e-Government Development Index is published by the United Nations Department of Economic and Social Affairs (UNDESA) every two years, starting in 2001. All of the 193 UN Member States are audited. The composite index includes three indicators:

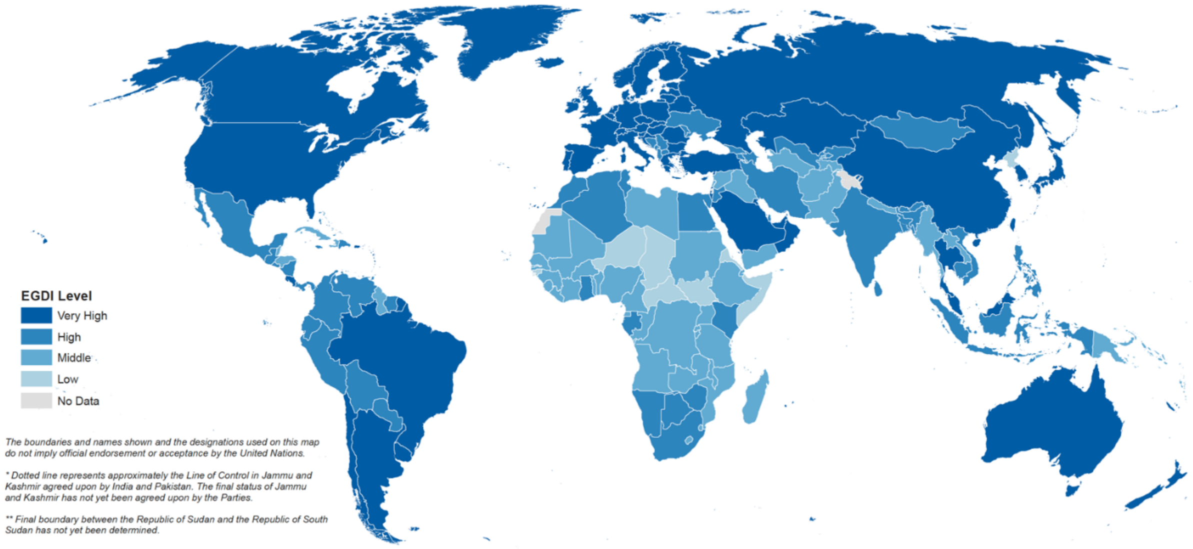
- ***telecommunications Infrastructure*** *Index (TII), based on data from the International Telecommunication Union (ITU);*
- ***human Capital*** Index (HCI) based on UNESCO data;
- ***online Services*** Index (OSI) based on the DESA sociological survey.

Based on the results of the assessment, countries are divided into 4 categories: countries with a very high EGDI rate (0.75 – 1), a high EGDI rate (0.5 – 0.75), an average EGDI rate (0.25 – 0.5), a low EGDI rate (0 – 0.25).

More than 80% of UN Member States digitize public services for citizens. The most common digital services are: registration of a new business, obtaining a birth and death certificate, registration of a building permit, payment for utilities. 95% of countries have a government online portal with basic search and feedback functions.

Guided by the principles of SDG 16 on improving the transparency and accountability of public institutions, governments are actively using digital platforms to organize public procurement and employment. Since 2018, the number of

Geographical division of the four EGDI groups, 2020



The boundaries and names shown and the designations used on this map do not imply official endorsement or acceptance by the United Nations.

** Dotted line represents approximately the Line of Control in Jammu and Kashmir agreed upon by India and Pakistan. The final status of Jammu and Kashmir has not yet been agreed upon by the Parties.*

*** Final boundary between the Republic of Sudan and the Republic of South Sudan has not yet been determined.*

Source: “UN Study: E-Government 2020”

countries posting open vacancies on the Internet has increased by 30%. More than 70% (138 countries) publish procurement/bidding results online, 65% (125) have specialized e-procurement platforms.

The leading countries in digital government development are Australia, Denmark, Estonia, Finland, Iceland, Japan, the Republic of Korea, the Netherlands, New Zealand, Norway, Singapore, Sweden, the United Kingdom and the United States of America. Russia ranks 39th (0.8176) and belongs to the group of countries with a very high rate of electronic participation.

Despite the progress made, the UN experts admit the existing digital divide both within and between regions. Limited financial resources, lack of infrastructure and strategy for digital transformation of public administration, as well as low professional level of responsible persons and stakeholders are the key factors constraining digital development in developing countries.

The digital transformation of public administration requires new approaches, different from the initiatives related to e-government. The priorities of digital transformation in modern conditions are: the introduction of platform solutions, the use of artificial intelligence (AI) and blockchain technologies, increasing the digital maturity of the population, the provision of digital services based on data analysis tools.

Digital government is open and accessible to all stakeholders. Digital platforms are used not only to inform, but also to involve citizens in the decision-making process and to overcome administrative barriers in inter-agency cooperation.

The UN e-Participation Index (EPART) includes an assessment of three components:

- ***e-information**: ensuring participation by providing citizens with public information and access to information on demand or without it;*
- ***e-hearings**: involvement of citizens in discussions and decision-making on public policies and services;*
- ***e-decision-making**: enabling citizens to participate directly in decision-making.*

Since 2016, the evaluated countries are classified into one of four groups based on their respective EPI values: low EPI countries (0 – 0.25), medium EPI countries (0.25 – 0.5), high EPI countries (0.5 – 0.75), very high EPI countries (0.75 – 1). The countries with the highest index of e-participation in 2020 are Austria, the United Kingdom, the Republic of Korea, Estonia, New Zealand, Singapore, the United States, Japan.

Source: OECD, OECD Recommendation of the Council on Digital Government Strategies

The results of the 2020 study show an increase in the number of government portals with feedback, voting and commenting functions. However, many countries still lack the digital resources to provide inclusive services and civil engagement.

Organization for Economic Cooperation and Development (OECD)

Improving the efficiency and transparency of the public sector has been made possible by the introduction of information technology and the conversion of public services to electronic format. The next step is to use digital technologies to create more open, inclusive, and web-based governance models, as well as a culture of data-driven decision-making.

OECD Recommendations for the Development of a National Digital Transformation Strategy

Transparency and Engagement	Management and Coordination	Implementation Support
1. Ensure transparency, openness and inclusiveness of government processes and operations	5. Leadership and political commitment to the strategy	9. Clear business cases for implementation of digital projects
2. Engagement and participation of public, private and civil society stakeholders in decision-making processes	6. Coherent use of digital technologies across policy areas and levels of government	10. Institutional capacities to manage and monitor projects' implementation
3. Creating a data-driven management culture	7. Effective organisational and governance frameworks	11. Procurement of digital technologies based on assessment of existing assets
4. Risk management approach to addressing digital security and privacy issues	8. International cooperation with other countries	12. Ensure that general and sector-specific legal and regulatory frameworks allow digital opportunities to be seized

OECD experts identify six key characteristics of digital government:

- **Digitalization** of the entire decision-making process;
- **Data analytics** as a basis for policymaking;
- Government as a **platform** (formation of a single digital ecosystem);
- **Open** government;
- Dtate policy in accordance with the **needs** of citizens;
- Proactive **provision** of public services.

The OECD E-Leaders Handbook on the Governance of Digital Government presents recommendations for digital transformation and increasing digital maturity of the public sector, based on the experience of the organization's member states and partner countries.

The Handbook identifies three main factors that need to be taken into account in the development and implementation of digital projects.

- **Contextual Factors**. It is necessary to determine the principles and mechanisms of project management in accordance with the political, socio-economic, technological, geographical characteristics of the country.

- **Institutional Models.** Openness, transparency, orderliness and coherence of organizational and management processes are crucial for the sustainable and effective digitalization of the public sector.
- **Policy Levers** are rigid or soft tools that policymakers use to support the sound and coherent implementation of a digital transformation strategy, including strategic planning, financial management mechanisms, regulatory frameworks, and standardization.

The World Bank (WB) GovTech Maturity Index

GovTech is a digital approach to modernizing the public sector that can improve the quality of public service delivery, simplify interaction with civil society, and improve the efficiency of public administration. The concept of GovTech can be understood as a set of very different areas of activity: from the formation of a "smart" urban environment to the use of digital tools to combat crime.

GovTech relies on four main elements:

- **Implementation** of digital platforms based on big data analytics;
- **Development** of public, customer-centric digital services;
- Direct multichannel **interaction** between the state and citizens;
- **Creation** of legal and organizational conditions for the introduction of innovations in the public sector.

In practical terms, GovTech is a set of activities aimed at improving the efficiency of public administration and processes in four main categories:

- **Digital government.** These include, but are not limited to, decision-making platforms, digital identity, e-voting, G2G and G2B services (e-taxes, banking, etc.).
- **Smart city:** urban planning, waste management, transport and monitoring systems, energy saving solutions.
- **CrimeTech:** identity recognition systems, cybersecurity solutions, e-courts, digital anti-money laundering initiatives.
- **Public administration:** educational platforms, healthcare systems, solutions in the field of sports and entertainment, agriculture technologies.

GovTech has enormous potential, but turning digital initiatives into tangible, measurable and consistent results in most countries remains a challenge. The movement towards GovTech requires a unified nationwide approach to digital transformation, the creation of a transparent system of management and decision-making, the use of the potential of public-private partnerships to attract competencies, innovation and private sector investment.

To assess the degree of “maturity” of GovTech, World Bank experts developed the GovTech Maturity Index (GTMI): The State of Public Sector Digital Transformation. The index is based on an assessment of the results of digital transformation in 198 countries around the world. In addition, the report includes an overview of best practices in the use of digital tools in the public sector.

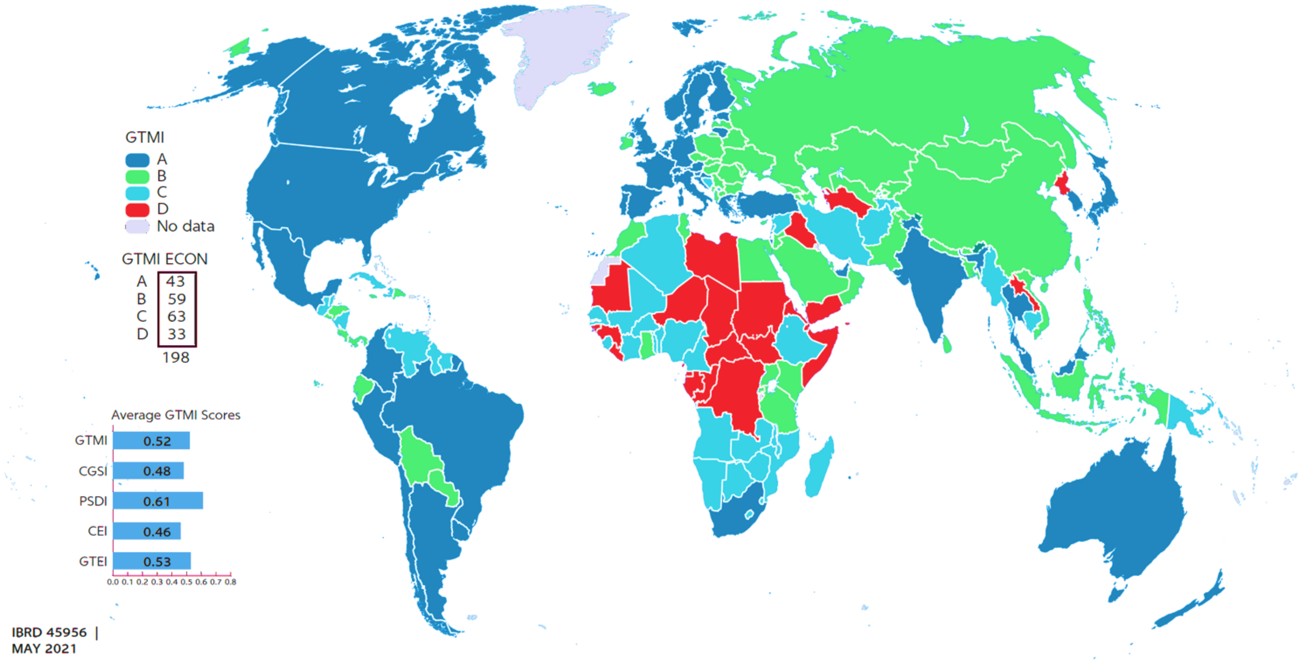
According to the results of the study, in 43 countries, digital transformation occupies the most important place in the strategic agenda of the state, as well as the successful implementation of numerous innovative projects. Among the leaders of digital transformation are Australia, Austria, India, the United Arab Emirates, the Republic of Korea, Singapore, Switzerland, South Africa. At the same time, 33 countries show minimal attention to initiatives in the field of GovTech. The digital divide is most pronounced in sub-Saharan Africa and South Asia.

Despite increased investment in digital infrastructure and the vigorous development of government policies in this area, digital maturity remains insufficient in most countries: 47% of countries lack strategies to develop digital skills among the population.

The main barriers remain:

- **The lack** of political will and regulation on the part of the State;
- **Underdeveloped** digital infrastructure;
- Low **level** of digital literacy of the population as well as civil servants;
- **Ineffective** or insufficient funding.

To increase digital maturity and adapt to the new "normality", WB experts recommend conducting an audit of state approaches to digital transformation: focus on improving the compatibility of existing information systems, creating multifunctional platforms, creating a culture of effective big data management, developing the necessary digital skills among the population.



Source: GovTech Maturity Index (GTMI): The State of Public Sector Digital Transformation

Digital Infrastructure

Digital transformation of public administration is impossible without the development of appropriate information, communication or digital infrastructure. The development of digital infrastructure ensures not only the functioning of public digital services, but also continuous communication with the main users and consumers of services, as well as the prompt collection and analysis of the necessary data. In addition, the continuous improvement and development of digital infrastructure makes it possible to timely adapt the system of public administration and government services to the needs of citizens. Finally, the development of digital services and infrastructure enhances the transparency and accountability of public administration, thereby contributing to the sustainable development of public administration.

The digital infrastructure includes:

- **Hardware**;
- **Software**;
- **Facilities** (e.g. industrial premises and buildings where the relevant infrastructure is located);
- **Networks**;
- **Servers**;
- **Data centers**.

Also, the digital infrastructure can be divided into:

- **traditional** infrastructure (includes all of the above);
- **cloud** infrastructure (allows remote use of infrastructure components).

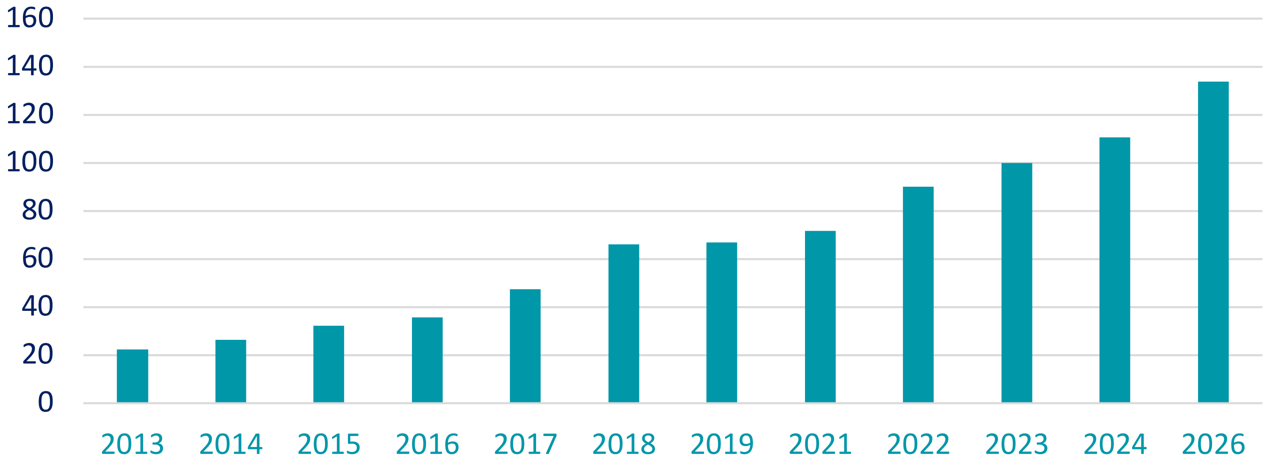
IT infrastructure is one of the main costs components during the digital transformation of the public sector. The total spending of the world's governments for digital infrastructure exceeded $500 billion in 2021. Despite a slight decrease in the annual growth rate of digital infrastructure development costs, it is expected that by the end of 2022, the total costs of governments for digital infrastructure will have increased to $557 billion.

Global Government IT Infrastructure Expenditures by Sector, 2021-2022 (in $ million)

SECTOR	2021	DYNAMICS OF GROWTH COMPARED TO THE PREVIOUS YEAR (%)	2022	DYNAMICS OF GROWTH COMPARED TO THE PREVIOUS YEAR (%)
DIGITAL SERVICES	188.069	10.9	203.922	8.4
SOFTWARE	135.630	14.9	151.885	12.0
COMMUNICATION SERVICES	61.482	1.4	60.996	-0.8
INTERNAL COMMUNICATION	64.245	0.3	65.971	2.7
DEVICES	41.049	17.6	40.390	-1.6
DATA CENTERS	32.735	6.5	34.154	4.3
TOTAL SPENDING	**523.212**	**9.5**	**557.318**	**6.5**

Source: Gartner, 2021, https://www.gartner.com/en/newsroom/press-releases/2021-08-31-gartner-forecasts-global-government-it-to-grow-in-20220

Global IT cloud infrastructure costs in billion USD



Source: Statista, https://www.statista.com/statistics/503686/worldwide-cloud-it-infrastructure-market-spending

In addition to the trend on higher spending on digital infrastructure in general, there has been an increase in government investments in cloud services. Among other things this is due to the general growth in the number and popularity of cloud services, as well as the possibility to optimize costs compared to the traditional approach to developing the digital infrastructure.

At the same time, despite the increase in IT infrastructure costs, it is this area that most often faces a number of serious problems. In particular, the general problems of digital infrastructure development in most countries are often confined to the following aspects:

- **lack of financing** (the rate of development and renewal of technologies and technological solutions exceeds the rate of growth of expenditures on digital infrastructure);
- **lack of qualifications** and skills of employees (up to 40% of public sector organizations face a lack of digital knowledge and skills of employees);
- **low degree** of integration of digital systems and platforms within and between government bodies;
- **availability** of and need to maintain legacy systems;
- **low level** of trust of citizens (citizens are afraid to trust their personal data to government bodies).

Case Studies

SAI	Auditor General Office of Denmark
Title	Report on management of benefits in government IT projects
Date	September 17, 2020
Link	

The SAI of Denmark has conducted an audit of the use by the government and public authorities the benefits from the implementation of IT projects, systems, and infrastructure. According to the auditors, despite significant efforts to digitalize processes and projects, public authorities do not fully use the benefits obtained from the implementation of IT projects.

As for the possible reasons for the inefficient use of digital tools and projects, the auditors note the following:

1. **Ministries do not strictly and systematically monitor and record the implementation of digital projects, as well as the possible benefits of using digital systems;**
2. **Due to the lack of systemic control measures for the benefits obtained, many of them are not fully implemented.**

SAI	National Audit Office of Estonia
Title	Overview of information technology expenditures and investments in Ministries and their authorities
Date	December 19, 2019
Link	

The National Audit Office of Estonia has studied the dynamics of expenditures and investments growth in public information infrastructure. The SAI auditors note that the growth rate of information infrastructure expenditures in public authorities is significantly ahead of budgetary allocations and investments. Personnel costs are a focal area that causes concern of the SAI. However, the increase in salaries did not affect the decrease in the turnover of public authorities IT systems personnel.

The auditors note that the "turnover" of personnel is partly due to the uneven growth of revenues in the public sector and in the economy as a whole. Thus, during the indicated period, the revenues of IT specialists in government bodies increased by 6.7%, while the national average revenue growth was 7.4%.

SAI	**National Audit Office of Estonia**
Title	**Management of software development projects in the public sector**
Date	**September 10, 2021**
Link	

The National Audit Office of Estonia has analyzed the development of nine state information systems, whether the state software development projects may fail, and what sore spots exist in this area. The audit has shown that four of the nine software development projects were unsuccessful. The auditors state the following as the reasons for the failure of the projects:

1. Weak or inadequate planning leads to systems becoming obsolete at the development stage;
2. Lack of consideration of users' needs and qualifications;
3. Continuous and rapid changes in regulations, rules, and legislation in this area;
4. Lack of knowledge and skills of project and program managers;
5. Incompetence of contractors; lack of proper control at all stages of project implementation;
6. Poor coordination between the actions of the customer and the contractors.

According to SAI, the success of information systems implementation depends on a number of factors:

1. The main processes within the government body should be defined and optimized before the information systems are being implemented;

2. Systems should be implemented by competent staff;

3. Civil servants (users) should be involved in the development of the system terms of reference at the design stage;

4. A user feedback form should be created to assess the performance of the system;

5. The development of systems should be taken into account in the legislative process.

SAI	Federal Court of Auditors of Germany
Title	Strategic management of digitalization projects in federal agencies of Germany
Date	July 27, 2022
Link	

Federal Court of Auditors of Germany carried out a number of audits regarding the implementation of national Digitalization Strategy in federal state agencies. In particular, SAI examined the federal government's measures to achieve the goals of the Digitalization Strategy, as well as the relevant actions of the Federal Ministry for Digitalization and Transport (Bundesministerium für Digitales und Verkehr).

SAI revealed that federal agencies have not coordinated their strategies in the field of digitalization with the national program documents of Germany. In some cases, the auditors revealed a complete lack of ministerial strategy, in some agencies digital projects were implemented exclusively within a specific unit, and not the entire agency.

In addition, federal agencies incorrectly assessed the priority of digital development in their activities, inexpediently defining the goals and deadlines for the implementation of projects. As a result, insufficient financial and human resources were allocated for digitalization. SAI added that an interdepartmental committee created specifically for these purposes was not involved in the strategic management of digital projects. It resulted in a significant decrease in the coherence of digital strategies of agencies.

SAI recommended that agencies develop their own digital development strategies consistent with federal program documents. SAI also positively assessed the plans of the federal government to revise the Digitalization Strategy and recommended that the Federal Ministry for Digitalization and Transport actively interact with agencies on digital projects.

SAI	**The State Audit Office of the Republic of Latvia**
Title	**Has Public Administration Used All Opportunities for Efficient Management of ICT Infrastructure?**
Date	**June 7, 2019**
Link	

The State Audit Office of the Republic of Latvia has audited the optimization of digital infrastructure management in public sector. Improving the performance of public administration as a whole is impossible without the effective use and optimization of this infrastructure. According to the auditors, only one agency, the Ministry of Justice, has made significant progress in centralizing its own digital systems and optimizing their work.

The auditors believe that for the digital transformation of government bodies to be successful, a number of conditions must be met:

1. **A system for collecting and analyzing the maximum amount of data should be available;**
2. **A consistent plan for the digital tools and platforms to be applied to the work of the government body;**
3. **A system of feedback and continuous assessment of whether the implementation of digital solutions is effective.**

SAI	Swedish National Audit Office
Title	Obsolescent IT systems – an obstacle to effective digitalisation
Date	December 4, 2019
Link	

In 2019, the Swedish National Audit Office audited the digital systems used by the 60 largest public authorities. The auditors note that most government bodies continue to use obsolescent systems. In addition to the lack of funding, the main reasons why these systems are still in the focus of the SAI include the following:

1. a significant part of government bodies does not have a clear strategy and principles of work with digital systems;
2. employees and management of government bodies lack specialized skills in working with digital systems;
3. there is no process of continuous assessment of whether the information systems comply with the needs and tasks of the government body;

the government has not taken appropriate measures aimed at correcting the situation (in particular, at establishing a single digital ecosystem for government bodies, forming a centralized request for the digital systems performance assessment, and assisting to government bodies in updating information systems and regular monitoring of this process).

Based on the data obtained, the SAI of Sweden makes a number of recommendations for government bodies to work with obsolescent systems:

1. **it is necessary to identify the responsible body/person in the public administration system that will monitor the operation of obsolescent systems and assist the departments faced with this problem;**
2. **it is necessary to develop special tools for assessing (methodology and metrics) the IT systems use performance, as well as the need for their modernization and/or replacement.**

SAI	Swedish National Audit Office
Title	Automated decision-making in public administration – effective and efficient, but inadequate control and follow-up
Date	December 18, 2020
Link	

The Swedish National Audit Office audited the use of automated decision-making systems in public administration in 2020. The SAI notes that, while the widespread implementation of such systems can significantly improve both the performance and compliance of decisions with existing legislation, these systems often suffer from operator errors, as well as from the initial errors appeared during their creation and configuration. Possible errors in such systems could have serious consequences for citizens and undermine public confidence in State authority.

The SAI of Sweden proposes to pay special attention to the development of "knowledge bases" and algorithms for working with automated decision-making systems. These databases and algorithms should contain answers to the questions most frequently asked by operators, as well as standardized solutions for the most common problems.

SAI	Swiss Federal Audit Office
Title	Potential Synergies in Federal IT-Portals
Date	September 17, 2021
Link	

Interaction between public authorities on the one hand and business and citizens on the other is carried out either through a number of specialized sites, or through portals and digital platforms combining several functions and services. These platforms were developed, operated, and improved independently of each other.

The Swiss Federal Audit Office has explored synergies between several federal information portals. According to the auditors, it will take systematic and long-term work to eliminate duplicative functions, as well as to enhance the platforms' performance.

The SAI believes that the key issue is to coordinate strategies for the development of federal information portals and synchronize the updating of their functions, databases, etc. In addition, it is important to achieve a coherent vision of the long-term architecture of government digital solutions.

SAI	UK National Audit Office
Title	National Law Enforcement Data Programme
Date	September 10, 2021
Link	

The UK National Audit Office has audited the National Law Enforcement Data Programme. The Programme, led by the Home Office, was aimed at creating a single database and information service to replace the two existing independent police services. However, according to the SAI, the program faced serious problems, in particular in terms of the initial formulation of the terms of reference (which led to the restart of creating a new service), as well as increased costs. According to the SAI, the current results should be recognized as unsatisfactory, since in the absence of a new service and due to the problems with the support of old ones, this has led to significant problems for end users.

As part of the further development and implementation of the system, the SAI of the UK recommends that attention be paid to the following issues:

1. **To re-evaluate the project taking into account the main requirements of stakeholders and financial costs throughout the implementation cycle;**
2. **To develop a strategy for a gradual transition to the new information system, taking into account the risks of failure to meet deadlines and the need to eliminate errors and shortcomings;**
3. **To conduct a regular assessment of the technical capabilities of the system, as well as the skills and competencies of employees;**
4. **When purchasing under a public contract from different suppliers with regard to the system development, to ensure coordination from a single center (Interior Ministry) based on a risk analysis and interest of the stakeholders.**

SAI	Government Accountability Office (GAO) of the United States
Title	Internet of Things: Information on Use by Federal Agencies
Date	August 13, 2020
Link	

IoT generally refers to devices – from sensors in vehicles to building thermostats – that collect information, communicate it to a network, and may complete a task based on that information. In the course of its study, GAO analyzed how the technology is used by government agencies in the United States. The study summarized the information on departments using this technology, areas of application of IoT, opportunities and risks of using the technology, as well as on internal regulation of the use of IoT. Despite the opportunities of using the technology, many departments refuse to implement IoT, both because of the lack of funds for long-term investments in modernizing the infrastructure, and because their leadership does not see the long-term positive effects of the implementation of this technology.

SAI	Government Accountability Office (GAO) of the United States
Title	Information Technology: Agencies Need to Develop and Implement Modernization Plans for Critical Legacy Systems
Date	April 27, 2021
Link	

According to estimates of the GAO U.S., as of 2021, the USA spends up to $100 billion annually to support the operation and maintenance of information systems. However, many of the information systems used by the U.S. government bodies are either obsolete or rapidly becoming so. The cost of supporting and maintaining these systems is steadily increasing. In addition, these systems are increasingly vulnerable to cyberattacks and other types of threats to their operation. A number of information systems, ranging in age from 8 to 51 years, have been identified by the SAI of the U.S. Typically, the modernization and/or development and implementation of new systems is challenged by the transfer and adaptation of data and its processing and use, as well as the high degree of integration of legacy systems with each other and with public administration processes. Finally, the problem of the special competence of personnel to work with legacy systems is important.

As part of its recommendations, the SAI of the USA highlights the need to develop comprehensive plans for upgrading and/or replacing these information systems. At the same time, these plans must meet a number of criteria:

1. **taking into account the key needs of the customer in terms of improving the performance of the government body when introducing new systems;**
2. **compliance with budgetary constraints;**
3. **the timing of the new system introduction and the related issues of improving employee competencies.**

SAI	Government Accountability Office (GAO) of the United States
Title	Facial Recognition Technology: Current and Planned Uses by Federal Agencies
Date	August 24, 2021
Link	

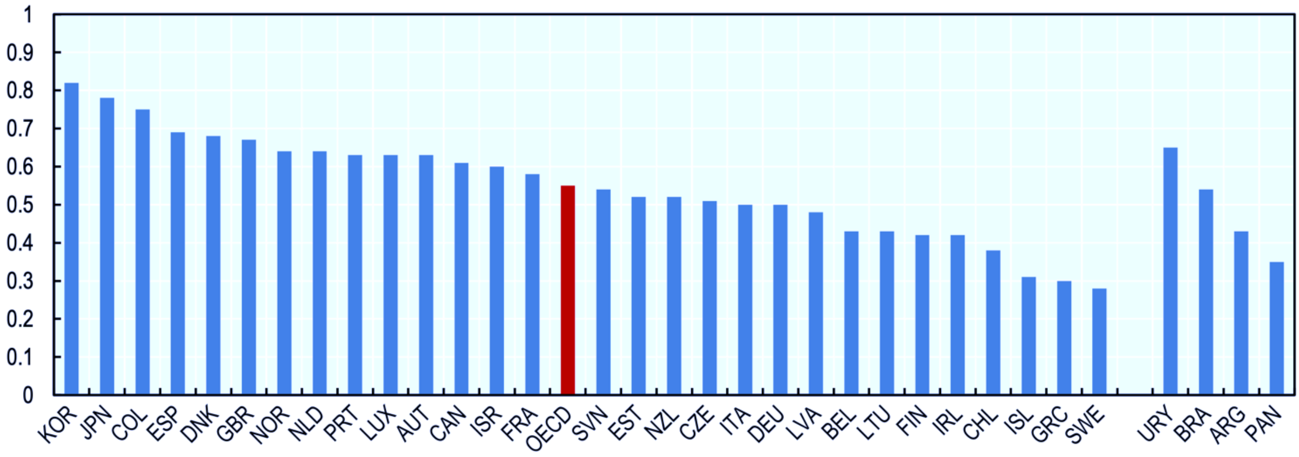
In 2021, as part of a study, the SAI of the USA identified current and potential applications of Facial Recognition Technology (FRT) in government operations. During the audit, the auditors of the SAI interviewed 24 federal public authorities. As expected, this technology is used most actively in public security area, as well as for the public authorities' data and information protection. At the same time, it is noted that given the increasing spread of FRT technology and FRT systems, the government lacks a holistic understanding and a holistic strategy for the development and implementation of this technology.

As In view of the further spread of technology, the SAI of the USA considers it important to develop a holistic strategy for this technology to be applied to the work of government bodies. This strategy should include both an analysis of the opportunities for technology development and the potential risks of their introduction, including the possibility of personal data leakage.

Data Analysis Technologies

With the rapid development of government information systems, the volume of unique data is growing. By strengthening the information and analytical component, data analysis and big data technologies increase the effectiveness of decision-making, especially in terms of health, employment, economic regulation, crime control, and data-driven decision management.

States tend to view in their strategic documents big data as a strategic asset. They try to use it to define strategic goals in public policy, assess the positive and negative consequences of governments' decisions, identify previously hidden dependencies between processes, form risk management systems, and prevent violations. According to the Organization for Economic Cooperation and Development (OECD) Digital Government Development Index, the UK, Denmark, and the Republic of Korea are the leaders in data-driven public sector governance.



Source: OECD, Digital Government Development Index

Given the growing interest of government bodies in the use of big data, the importance of conducting an appropriate audit increases. According to sector studies[1], big data audits include three interrelated levels: technological, managerial, and strategic. Each of them is oriented towards the assessment of the following parameters:

- Effectiveness of the **innovative technologies** introduction to the work of a government body. The key assessment criteria are the quality of data collection, the variety of processing methods, and the development and availability of infrastructure.

[1] Appelbaum D, Kogan A, Vasarhelyi M A. Big Data and Analytics in the Modern Audit Engagement: Research Needs. Auditing A Journal of Practice & Theory, 2017, 36(4):1-27; Al-Sai Z, Abdullah R, Husin H. Critical Success Factors for Big Data: A Systematic Literature Review. IEEE Access, 2020:1-1

- Effectiveness of **organization's structure** in the context of the big data use. Particular attention is paid to assessing the quality of professional training, interaction between departments on the use of big data, and the work of technological centers for processing big data.
- Correspondence between the expected and obtained **results** from the introduction of big data analysis technologies. The assessment criteria are the total number of identified inaccuracies in the operation of data mining algorithms (performance), the social effect of increased transparency of information (legitimacy), and the accuracy of risk management (forecasting).

Despite the undeniable advantages of big data analytics technologies, there are certain risks and limitations to their use. One of the main problems here is ensuring the necessary quality of data, which is usually understood as the sum of the following features:

- **Complete** (there are no gaps in the data preventing their analysis or use);
- **Comprehensive** (all elements describing the target object/event/situation are included in the dataset);
- **Timely** (regular updates);
- **Understandable** (including metadata and machine-readable format);
- **Accurate** (the available data is correct and clearly reflects the current state of the target object, process and/or phenomenon);
- **Consistent** (the available datasets do not contradict each other; the use of different datasets does not affect the accuracy of conclusions);
- **Unique** (items are not repeated within the same dataset);
- **Discoverable** (raw data and data catalogues are obtained from open government information systems and/or within the state department);
- **Machine-readable** (data are presented in formats that can be used by machine algorithms at once and/or with minimal human processing);
- **Inter-operable** (standards, semantics, and common data identifiers are available for processing on the most common technological platforms);
- **Protected** (all requirements for the protection of personal and/or other confidential data are met).

Effective monitoring and control of data quality requires government bodies to develop a clear methodology for data management, as well as to assess its reliability. To achieve the required data quality, in addition to data-cleaning, the OECD experts recommend regular and random data audits. The objectives of such audits are to assess data for compliance with generally accepted standards and set goals, ethical standards (including ensuring privacy), and legislation. Such measures are intended to ensure that actual data are not fabricated to meet any expectations.

Guidance on Conducting Audit Activities with Data Analytics (published by the INTOSAI Working Group on Big Data, WGBD) includes the following methods for data verification during an audit:

- Checking the **completeness** of data by comparing the quantity and volume of partially structured and unstructured data within the arrays provided by the auditee;
- Checking **integrity** constraints of relational models, including primary key constraints, referential constraints, user-defined integrity constraints, etc.;
- Checking the **compliance** of the data with the initial information (financial statements);
- Checking the **total amount** of data, statistical indicators of the main variables, as well as the authenticity of values in data arrays by calculation and aggregation. For example, the range of the main variables is checked to be corresponding to the range presented in the operating report by means of calculating the maximum and minimum values of the main variables and aggregation;
- Checking the **correctness** of reporting (availability of intermittent and repeated values, date range, etc.).

A specific set of big data issues is associated with the provision of open access to governments' data for citizens. The policy to improve the legal regulation of the OECD countries information policy is aimed at reducing administrative barriers and increasing the availability of government data. In 29 of the 32 OECD Member States, central/federal governments require data to be available free of charge, in machine-readable formats, and with appropriate metadata. In 28 of the 32 OECD Member States, data is required to be available with an open license.

In addition, many OECD members have committed themselves to publicly promoting the principle of transparent public administration. Some focal areas include increasing the number of programs to raise awareness of how beneficial the open government data and their reuse are, and increasing the digital literacy of civil servants.

Within the European Union (EU), the EU Directive 2019/1024 dated June 20, 2019, plays a central role in supporting government efforts to improve data transparency by promoting innovation and proper governance. Article 16 explicitly calls on States to "promote the creation of data which are open by design and by default."

Despite the difficulties in ensuring open data and source code in the public sector, these measures contribute to transparency, accountability, and public control over the decisions and results of public policy. In these circumstances, the following seems appropriate:

- **To promote the establishment of quality data ecosystems** by providing people with unrestricted access to data sources and helping to ensure the equitable distribution of information in society;
- **To provide public access to disaggregated data** in accordance with the requirements of confidentiality, security, and respect for property rights; anonymous and granular[2] open data can be used to identify relevant social

[2] Level of detail based on available data. The detail includes data one level below the previous one (in

and economic problems and make fact-based decisions; in turn, such demonstrative results will increase confidence in data analysis tools both within the public sector and in society;

- **To make the source code open** to public control and auditing, especially when personal data or datasets are processed through digital government projects.

particular, hours, minutes, seconds, etc.). The maximum level of detail implies the maximum level of dataset detail.

Case Studies

SAI	Australian National Audit Office
Title	Using data analytics for risk-based performance audit planning
Date	October 25, 2021
Link	

As part of a survey by the Accounts Chamber of the Russian Federation with regard to the development of the INTOSAI Moscow Declaration Provisions, the Australian National Audit Office prepared an overview of the use of data analysis technologies in the audit of government grants. The analysis is based on comparing the databases of conducted tenders and concluded contracts, along with the grounds for concluding state contracts (whether the contract was concluded as a result of a multi-stage standard evaluation procedure or outside of it). This has helped to identify cases where contracts were awarded prior to the formal closing of the tender, which in turn allows for the identification of high-risk contracts.

The Australian National Audit Office believes that the use of data analysis elements in the audit activities makes it possible to:

1. **identify the riskiest projects within all government expenditures;**
2. **identify cases that require closer examination in the course of further audit activities;**
3. **identify conditions that lead to irregularities in tenders;**
4. **adjust the audit program at the SAI level in a timely manner.**

SAI	National Audit Office of China
Title	Audit Data Analysis in the Big Data Era
Date	September 15, 2021
Link	

The National Audit Office of China has systematized the experience of using data analysis technologies and working with big data during audits. Auditors confirm that the use of a variety of data analysis tools to form audit opinions has become a common practice not only within the SAI itself, but also within regional control offices. In addition, it is confirmed that, while developing state programs and projects, public authorities actively involve technologies and specialists oriented towards data analysis and work with big data. Data management, however, often uses the simplest and most basic tools (such as Excel), while the use of programming languages and specialized solutions remains a rare practice. In addition, work with data is complicated by the lack of a unified data register and the possibility of prompt exchange of information, including that of a restricted nature.

SAI	Auditor General Office of Denmark
Title	Report on open data
Date	March 15, 2019
Link	

Access to government data is a key indicator of how transparent the State is. It also helps to ensure economic growth and development. In 2019, the SAI of Denmark investigated the publishing of open government data on the Internet. According to the auditors, the lack of consistency in data sets publication (the data are scattered across 88 sources), as well as the problem with determining the authority responsible for the publication of government data, impede the transparency of the public authorities activities.

The SAI of Denmark highlights a number of follow-up recommendations in terms of open data:

1. responsibilities for the publication of open data should be clearly defined and distinguished between agencies;
2. when selecting data for public access, the principle of “default transparency” must be observed, i.e. all agencies are obliged to make the data publicly available if there is no good reason not to do so;
3. expansion and regular updating of the open data directory is required.

SAI	**Auditor General Office of Denmark**
Title	**The "Moscow Declaration Provisions through SAIs' Perspective" Course**
Date	**September 15, 2021**
Link	

As part of the "Moscow Declaration Provisions through SAIs' Perspective" course[3], the SAI of Denmark prepared in 2021 the "Data analytics in audit" speech. As an example of working with digital sources, a check by the Danish tax office was cited. The SAI used STATA statistical analysis software to work with a large set of data. This approach has led to a better understanding of the size of the Danish Government's debt, the principal debtors, and how to manage the debt effectively.

[3] The course is presented on the digital platform of the University for the INTOSAI Community, www.u-intosai.org

SAI	**UK National Audit Office**
Title	**Using data analytics for risk-based performance audit planning**
Date	**June 21, 2019**
Link	

The UK government is actively using data to improve both policies in various areas, as well as to improve the quality of public administration and provide better services to the citizens of the country. At the same time, there are a number of serious challenges related primarily to the issues of safe use and storage of data (including personal data of citizens), as well as finding a balance of interests of stakeholders related to working with data in order to ensure sustainable and effective investment of public funds in working with data.

The UK NAO believes that further development of the use of data at the government level requires a coherent strategy for collecting, sorting, storage and use of personal data of citizens by government agencies. A special role in this matter is played by the widest possible coverage of departments in order to exclude duplication of functions, powers, and requests.

SAI	UK National Audit Office
Title	Improving government data: A guide for senior leaders
Date	July 21, 2022
Link	

The UK NAO has developed a guidance on data management in the public sector. The SAI noted that data is one of the most important assets of the government and it is vital to foster exchange, improve quality, develop appropriate standards, and form inter-agency data sets. The guide deals with the management of data that is collected for the effective delivery of public services. At the same time, NAO emphasizes that the document can also be useful for managing data for policy making. The document is intended to promote the activities of the management of state bodies: accountants, directors, as well as persons responsible for the provision of public services.

Artificial Intelligence (AI) Technologies

The intensive development and spread of digital technologies in recent decades have significantly changed the landscape of public policy. The focal areas of technological development include artificial intelligence (AI), robotics, blockchain, virtual and augmented reality technologies.

The COVID-19 pandemic facilitated the development of AI technology. Given the extensive pressure in national health systems and severe epidemiological restrictions, AI has been actively used and continues to be used to diagnose diseases, as well as to predict the course of the disease and further spread of the virus. The Stanford Institute for Human-Centered Artificial Intelligence estimates that private investment in AI doubled in 2021 to $93.5 billion. The International Data Corporation (IDC), in turn, forecasts that global spending on the artificial intelligence systems development will rise to $204 billion in the United States by 2025.

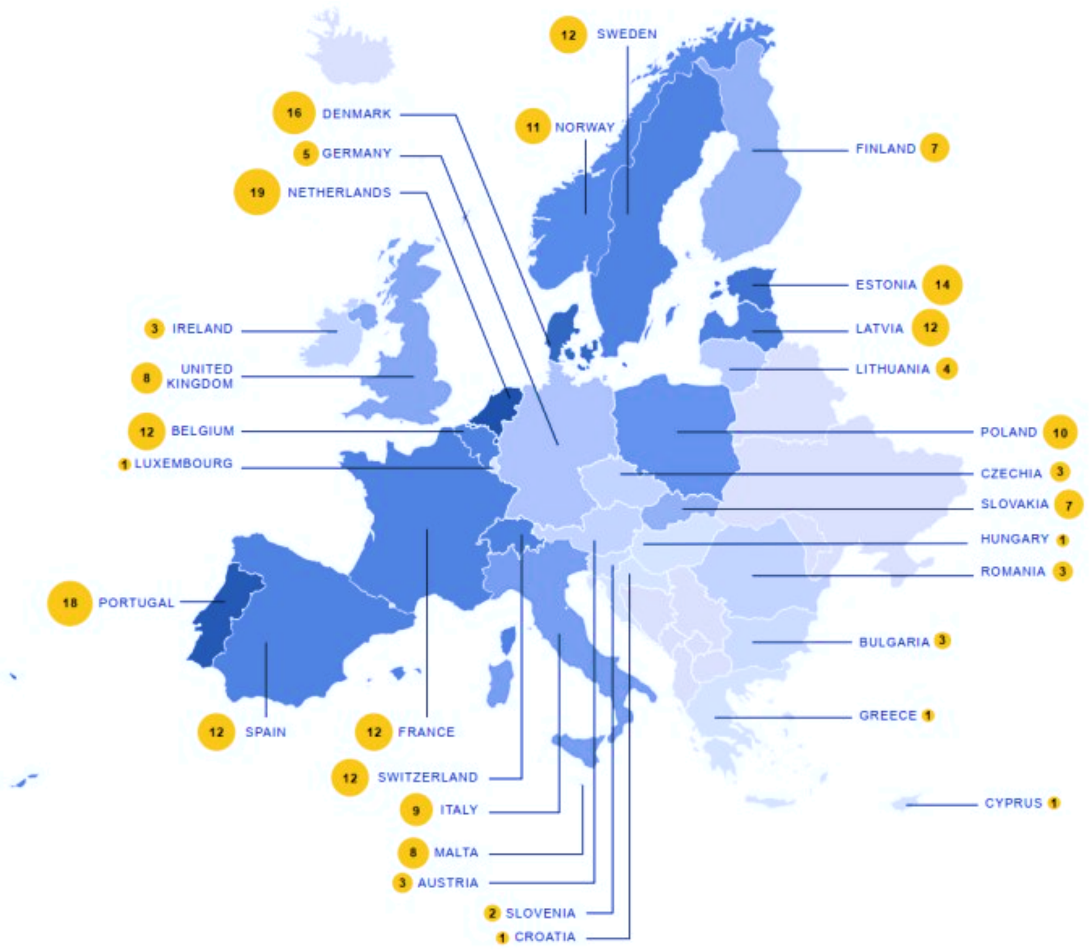
The widespread adoption of AI technologies will lead to a 14% increase in global GDP ($15.7 trillion) in 2030, according to the PricewaterhouseCoopers (PwC) The macroeconomic impact of artificial intelligence report. McKinsey experts expect that by 2030, about 70% of companies will use at least one type of AI technology, which will add $13 trillion to the global economy and ensure the increase in global GDP by 1.2% per year.

With the positive dynamics of public investment in IT, it is artificial intelligence that is increasingly investing. In 2021, federal funding for AI research in the United States increased by 50% compared to 2020 and reached $6 billion.[4] AI technologies provide unique opportunities to improve the performance of public administration, reducing costs and ensuring high accuracy in predicting management decisions. A study by Deloitte shows that automating workflows with AI will save up to 30% of government employees' time.

According[5] to the OECD, more than 60 countries have developed strategies for the artificial intelligence development. National road maps differ in terms of goals, timelines, implementation mechanisms, sectoral focus, budgets, and the nature of government involvement. Among the 230 AI projects initiated by public institutions in the EU Member States, 7 relate to education, 4 relate to culture, 41 relate to health, 14 relate ro housing and communal services, 3 relate to environmental protection, 40 relate to economy, 27 relate to public order, 4 relate to defence, 16 relate to in social services, and 76 relate to public services.

[4] In 2021, the "Artificial Intelligence" Federal Project was launched in Russia. It is planned to invest 24.6 billion rubles in AI within 5 years. For 2021, a budget of 4.7 billion rubles was approved, and 99% of it was executed.

[5] As of April 2020



AI projects in the EU

The nature of government involvement in AI projects varies. OECD experts highlight the following options:

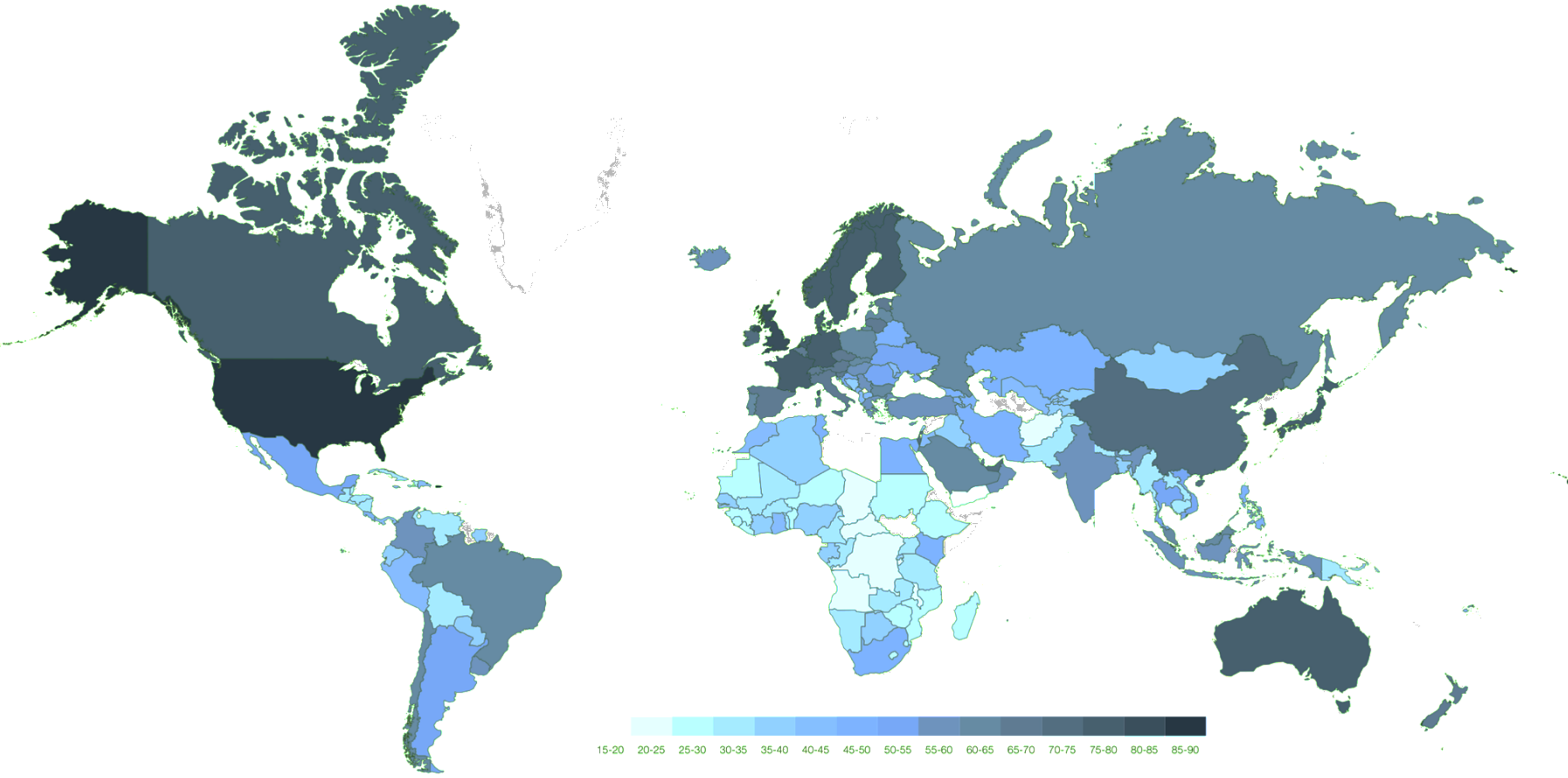
- **Investor**. The state finances the development and promotion of new technologies.
- **Customer**. The state purchases digital products or participates in the development of new software solutions through a public-private partnership (PPP) mechanism.
- **Regulator**. The state, following scientific and technological progress, is updating the relevant legal framework in a timely manner.
- **Standardizer**. The state cause the development of national standards involving all stakeholders and assesses their conformity with the current level of technological development.
- **Data Owner**. Public authorities store and process huge amounts of data, ensuring their security and integrity.
- **Service Provider**. State digital platforms interact with citizens, actively using AI technologies.

The authors of the OECD report "Hello, World: Artificial intelligence and its use in the public sector" highlight the following factors in the development of AI:

- **Development of scientific potential**. Over the past decades, a vast and diverse amount of knowledge in terms of AI has been accumulated; computer algorithms and programming languages have been improved.

- **Technological advancement**. The increase in computing power provides higher computer performance and data processing speed. Data storage costs also dropped sharply, from $1 million per 1 Gb in 1967 to 2 US cents per 1 Gb in 2017.
- **Availability of technologies**. Free collaborative and project management services, online courses and training aids help to increase digital literacy and the use of AI.
- **Increased data volume**. Big data is the main driver of AI. More than 90% of the world's digital data has been produced over the past few years, and the rate of production continues to grow.

Despite the increased attention to AI potential, the results of the assessment[6] of how ready the States are to implement AI solutions in 2021 (Government AI Readiness Index 2021) indicate a significant difference in regional technological development. The average score for tropical Africa and Central Asia is 36.27, while for North America and Western Europe it is 76.75. The industry leaders[7] are the United States, Singapore, and the United Kingdom. The presence of a highly skilled workforce, advanced research, technological infrastructure, and government measures to support innovation also ensured the high position of East Asian countries (5 countries of the region are among the top 20).



Source: Oxford Insights' Government AI Readiness Index 2021

[6] The methodology is based on 42 indicators, grouped into three areas: quality of public administration (whether a targeted strategy for the AI development and relevant legal regulation are present), technological capacities (results of innovation, R&D funding, quality of human capital), and digital infrastructure (whether the data are available and representative).

[7] Russia ranks 38th in this term.

The World Bank (WB) experts outline several promising areas of AI technologies application in the public administration system:

- **Processing** of citizens' applications;
- **Monitoring** of compliance with the legislation and risk assessment;
- Financial **control** of budget expenditures;
- **Optimization** of intra-corporate operational processes;
- Personalized **provision of services** based on the citizen digital profile analysis;
- Efficient **allocation of resources** and assistance in decision-making.

With all the potential benefits of AI, there are significant risks: artificial intelligence bias[8], information security[9], and personal data protection issue. Among the key recommendations for minimizing them are proactive control and monitoring of the AI systems functioning, improving the legal regulation of work with data, providing open access to effective digital models, using several AI systems to perform one task, and expanding international cooperation.

On November 16, 2021, the participants of the UNESCO General Conference approved the Recommendation on the ethics of artificial intelligence. This is the first international document on the ethical regulation of AI use. The basic ethical principles include: respect for and protection of human rights, protection of the environment, ensuring inclusiveness, privacy, human control, and transparency. The document is intended to become a legal basis for regulating the use of AI technologies at the global level.

[8] Bias against one or more groups of people arises from the processing of incomplete, inaccurate, or distorted data, or from developer error/subjectivity. AI systems need to be continuously improved as new data sets and data-processing tools become available.

[9] Many AI systems operate autonomously interacting with each other. In 2010, US stock exchanges fell by 10% due to a malfunction in trading algorithms.

Related Cases

Work with applications of the citizens

- Since October 14, 2020, visitors to the "latvija.lv" **Latvian public services portal** are assisted by a "virtual assistant" Eric. The digital assistant algorithms are based on the log of answers to the questions most frequently asked by citizens.

Public health care

- In 2020, a "**virtual doctor**" was developed in Croatia which can process 50,000 requests per day.
- InferRead™ CT Lung is a software based on AI developed with the support of the **European Union** for analyzing the results of computed tomography and early diagnosis of coronavirus infection.

Anti-Corruption

- With support from **the World Bank**, Brazil has launched a smart public procurement appraisal system in 12 federal states. AI analyzes 27 datasets (250 million data points), including 15 million electronic accounts worth more than $100 billion, information about 750,000 companies, and 30,000 news feeds. During its operation, the system identified 500 firms owned by civil servants; more than 420 firms won tenders from coverup companies.
- **The Academy of Sciences of China** together with the internal audit bodies of the Communist Party have developed a Zero Trust software solution to assess information on income, expenses, and liabilities of civil servants. It is known that Zero Trust revealed violations in the declarations of 8,721 civil servants.

Transport

- In 2017, **the Department of Transport in London** launched an AI-based application that provides up-to-date information on bus routes, nearest bus stops, arrival times, and metro congestion.
- **The Hangzhou transport system** is regulated using AI and big data analysis technology. The traffic management system recognizes traffic accidents, slows down traffic, and sends dispatch commands to the appropriate services.

SAI Case Studies

SAI	Office of the Auditor General of Norway
Title	Auditing machine learning algorithms: A white paper for public auditors
Date	October 14, 2020
Link	

The active introduction of artificial intelligence (AI) and machine learning technologies in public sector requires new approaches to conducting external public audit. The SAIs of Brazil, Finland, the UK, Germany, the Netherlands, Norway and Finland prepared an expert report with an overview of the key risks of using AI and machine learning technologies in public administration and proposals for conducting an audit as part of the activities of SAIs. **The existing risks are grouped into 4 main clusters:**

1. Optimization of AI algorithms and machine learning often does not take into account the requirements of compliance with the law, transparency and accountability of public administration;
2. Problems of interaction between the customer and the contractor, as a result of which a technical solution based on machine learning technologies leads to the complication of public administration processes;
3. Lack of competencies for the use and development of products and solutions based on machine learning technologies within the organization;
4. The problem of regulating the use of personal data when training models and neural networks (there are no relevant guidelines issued by the relevant departments responsible for maintaining the security of personal data).

SAI	Government Accountability Office (GAO) of the United States
Title	Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities
Date	June 30, 2021
Link	

In order to increase accountability and responsibility in the use of artificial intelligence (AI) systems in government programs, as well as the public authorities performance, in 2021, the SAI of the USA developed a guide to the reporting system for the use of AI. The manual is based on 4 complementary principles, including **governance** (use, control and reporting as part of the implementation of AI in public administration systems), **data usage** (use of qualitative data obtained from reliable sources, as well as their correct processing and analysis), **monitoring** (ensuring the reliability and relevance of AI systems), and **performance** (the result of the use of AI systems must correspond to the goals and objectives of government programs and projects).

SAI	Government Accountability Office (GAO) of the United States
Title	Technology Assessment: Artificial Intelligence: Emerging Opportunities, Challenges, and Implications
Date	March 28, 2018
Link	

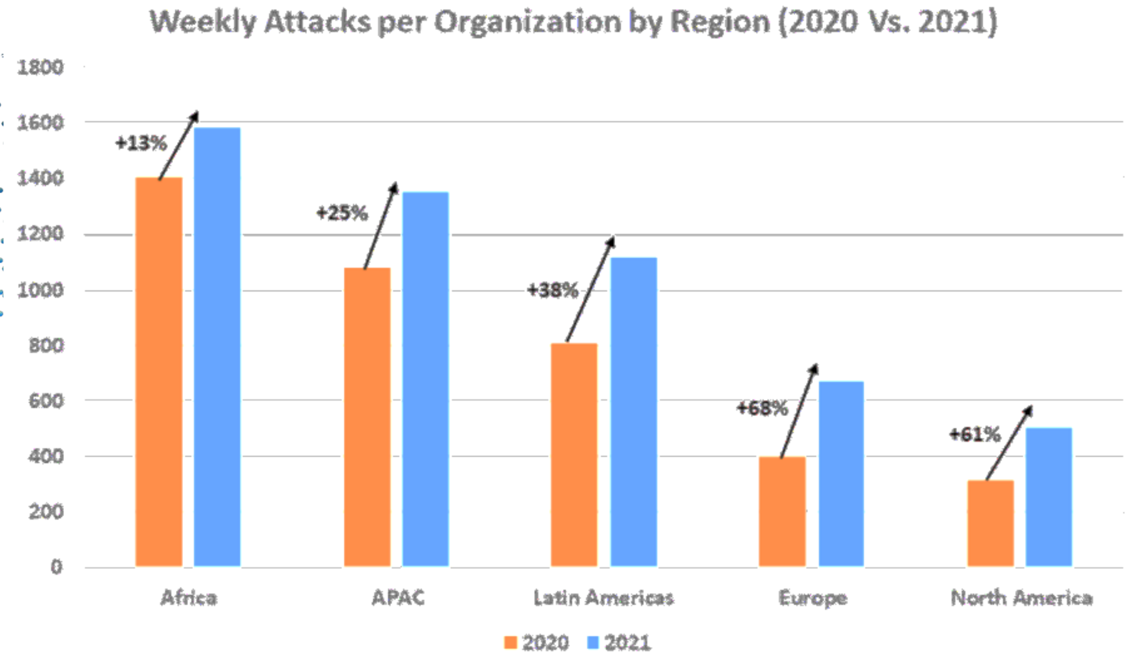
To assess the impact, as well as the challenges that the widespread adoption of artificial intelligence (AI) technologies could lead to, GAO held an expert forum event. Among the key areas that participants drew attention to were cybersecurity, autonomous cars, justice and financial services. Experts note that although the benefits of AI development in most areas are obvious, the active introduction of technology into everyday life faces a number of serious challenges. Among the main challenges are the lack of data for training neural networks, lack of employee competencies, and ethical risks.

Cybersecurity

Digital transformation helps to improve the quality and efficiency of public administration and optimize financial and human resources. In the context of growing digital interdependence accelerated by the COVID-19 pandemic and the complexity of the threat landscape, there is an[10] increasing need to ensure the security of the technological infrastructure of state institutions and the protection of citizens' personal data.

According to the World Economic Forum (WEF) estimates in 2020, the total number of detected malicious programs and ransomware increased by 358% and 435% accordingly. The WEF experts admit that 95% of cybersecurity issues are related to the human factor. At the same time, the global shortage of cybersecurity specialists is 3.5 million people.

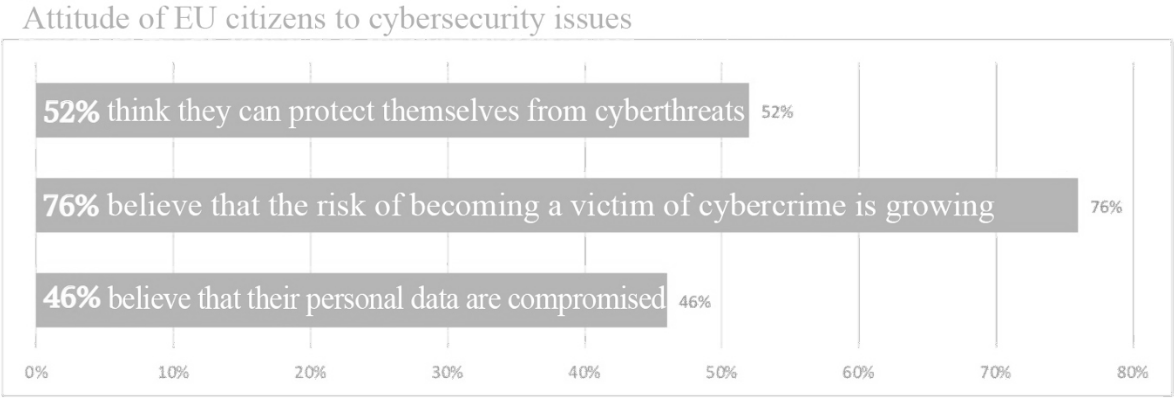
According to the results of the Check Point Research analysis[11], in 2021, the number of cyberattacks on corporate networks per week increased by 50% (compared to 2020). The international average was 925 cyberattacks per week per organization. The most significant increase in the number of cyberattacks was recorded in the European region.



Source: Check Point Research Report

[10] Threat landscape is a set of identified and potential cyber threats for a particular industry, group of users, or a specific period of time.
[11] A division of Check Point Software Technologies Ltd, an international IT security company.

According to the[12] European Union Agency for Cybersecurity (ENISA), the main targets of cyberattacks in 2021 were: state administrative institutions (198 incidents), digital service providers (152 incidents), medical institutions (143 incidents), the financial and banking sector (97 incidents), and the transport sector (54 incidents). The most common types of cyberattacks include ransomware, cryptojacking[13], data breaches, malware, disinformation, non-malicious threats, threats against availability and integrity, and supply-chain attacks.



Source: Special Eurobarometer 499 Survey, January 2020

According to the "Cost of a data breach 2021" IBM report, new digital threats emerge fast, which makes it hard for organizations to prevent them.[14] The transition to remote mode in the context of the COVID-19 pandemic was carried out to the detriment of organizations interests in information security. In 2021, the average financial damage caused by a data breach amounted to $4.2 million. This is a record for the last 17 years.

Currently there is no generally accepted definition of cybersecurity. Different approaches to assessing the efficiency of cybersecurity policies are underway. The UN system uses the definition of the International Telecommunication Union (ITU). The organization's experts view cybersecurity as the collection of tools, technologies, strategies, and guidelines that can be used to protect the organization's information, technical resources, and personnel in a cyber-environment. Other international organizations[15] use the term “information security” as security of information in all its forms and on any media. The focus of the Organization for Economic Cooperation and Development (OECD) is digital security assessment: analysis of the economic and social consequences of cyber threats.

The conceptual approaches of States and international organizations may differ, but the main goal of cybersecurity policy remains to ensure the confidentiality, integrity, and accessibility of information (“information security triad[16]”).

[12] Results: April 2020 to July 2021

[13] Cryptojacking is the unauthorized use of devices to generate cryptocurrency.

[14] The study is based on the analysis of leakage data from more than 500 companies happened from May 2020 to March 2021. In total, the organization analyzed about 100 thousand violations.

[15] The ISO/IEC 27001:2013 international standard

[16] The list of information security guidelines is constantly updated. In 2002, the OECD published an information security model that includes nine guidelines. The ISO/IEC 27001:2013 international standard has 10 guidelines.

The ITU notes an increase in the cybersecurity level of States worldwide. According to the indicators of the Global Cybersecurity Index[17](GCI), by the end of 2020, 127 countries had adopted national information security strategies, and 142 had conducted information campaigns on cybersecurity issues. The leaders are the U.S. (100 points), Estonia (99.48), the UK and Saudi Arabia (99.54 points equally); South Korea, Singapore, and Spain (98.52 points equally); and Russia, the UAE, and Malaysia (98.06 points equally).

Legal Actions	**167 countries have cybersecurity legislation in place**
	133 countries have data protection laws
	97 countries have developed legal mechanisms to protect critical infrastructure
Technical measures	**131 countries have National Information Security Centres**
	101 countries have mechanisms in place to protect children from the dissemination of illegal information on the Internet
Organisational measures	**127 countries have developed national cybersecurity strategies**
	National cybersecurity strategies are updated in 98 countries
	60% of the above 98 countries audit the performance of cybersecurity strategies
Development of professional capacity	**142 countries have conducted cybersecurity awareness campaigns**
	94 countries have launched cybersecurity research programs
International cooperation	**90 countries have bilateral cybersecurity agreements**
	112 countries participate in multilateral cybersecurity initiatives
	In 2020–2021, 140 countries participated in international events, such as conferences on cybersecurity and educational seminars.

Source: ITU Global Cybersecurity Index Report

Despite the progress made, there are still areas that need further improvement: modernization of critical infrastructure protecting measures in accordance with new cyber threats, strengthening the legal regulation of work with personal data, and increasing the overall level of digital literacy.

The ITU guidelines to improve the cybersecurity level of States are the following: regular monitoring of how effectively the cybersecurity strategy is being implemented, improving the resource base of national information security centers, the need to intensify international cooperation, and sharing best practices to counter cyberthreats.

[17] The Global Cybersecurity Index (GCI) was first published by the International Telecommunication Union (ITU) in 2015 and is updated every two years. The objective of the project is to assess the information security system of 193 ITU Member States in 5 focal areas: legal measures, technical measures, organizational measures, professional development, and international cooperation.

Case Studies

SAI	Austrian Court of Audit
Title	Coordination of Cyber-Security
Date	April 22, 2022
Link	

In 2021, the SAI audited the effectiveness of cybersecurity systems in a number of Austrian federal agencies (Federal Chancellery, Ministry of the Interior, Ministry of Defence, and Ministry of Foreign Affairs). The SAI focused on the assessment of the cybersecurity regulatory framework and strategic and operational management. The SAI identified a number of weaknesses, such as the lack of cybersecurity incident operational management plans and an inadequate risk management system. The SAI stressed the need to improve the information security strategy of agencies and recommended they establish a standing cyberspace response team as well as an emergency response center.

SAI	Auditor General Office of Denmark
Title	Five government authorities' compliance with 20 technical minimum information security requirements
Date	January 15, 2022
Link	

As a result of an audit conducted by the Auditor General Office of Denmark in 2021, the auditors concluded that the Ministry of Finance, the Ministry of Justice, the Ministry of Health, the Ministry of Climate, Energy and Housing, and the Ministry of Food, Agriculture and Fisheries had failed to comply with the 20 technical minimum information security requirements that were to be met by 1 January 2020.

SAI	Contact Committee of the Supreme Audit Institutions of the European Union
Title	Audit Compendium: Cybersecurity in the EU and its member states
Date	December 7, 2020
Link	

On December 7, 2020, the Contact Committee of the EU Supreme Audit Institutions published the "Audit Compendium. Cybersecurity in the EU and its Member States." Based on the results of research conducted by the supreme audit institutions of the EU member states, the collection is devoted to the issue of how resilient EU critical information systems and digital infrastructure are to information attacks. It provides background information on the problem of cybersecurity, EU strategic initiatives, and the legal framework; it identifies the main challenges and risks faced by EU citizens and Member States as a result of the digital data misuse. The study was based on the results of 12 audits conducted by the audit institutions of EU member states and the European Court of Auditors on issues related to cybersecurity. The audit results made it possible to identify the vulnerability of digital infrastructure and personal data storage systems (Estonia, France, and Sweden), the lack of resources and the effectiveness of the information security system management (Ireland, Latvia, and Finland), non-compliance with the security standards set by European regulations (Poland and Portugal).

SAI	European Court of Auditors	
Title	Special report: Cybersecurity of EU institutions, bodies and agencies: Level of preparedness overall not commensurate with the threats	
Date	March 29, 2022.	Link
Link		

Due to numerous cases of hacker attacks on the EU information systems, the European Court of Auditors, from January 2018 to October 2021, audited the effectiveness of the EU institutions information security policy. Special attention was paid to the activities of the European Union Agency for Cybersecurity (ENISA) and the EU Computer Emergency Response Team (CERT-EU). According to the European Court of Auditors, the resilience level of EU information systems differs from one institution to another and generally does not correspond to the current scale of cyberthreats. In particular, only 58% of EU institutions have an agreed information security strategy at their management level. The reasons behind the unpreparedness of EU institutions for cyber threats are the following:

- A system for assessing information systems stability or inconsistency is absent;
- Outdated corporate cybersecurity practices;
- Lack of systemic training of employees on information security issues, as well as lack of advanced training programs for specialists of the relevant departments;
- Inadequate information security management system of institutions and selective risk assessment;
- Uneven funding of programs to increase the level of cybersecurity in the EU institutions;

External audit of information security systems is absent in a number of departments.

The European Court of Auditors has called on EU institutions to coordinate information systems more coherently and to take a consistent approach to the development of cybersecurity strategies. It is recommended that the European Commission introduce mandatory cybersecurity rules, increase funding for the CERT-EU, and promote inter-institution cooperation on this issue.

SAI	National Audit Office of Finland
Title	Supplement to the follow-up report: Organizing cyber protection
Date	April 12, 2022
Link	

In 2022, the SAI of Finland assessed how its recommendations for cybersecurity measures improvement were implemented, following an audit of the Ministry of Finance in 2017. The SAI concluded that the recommendations were partially implemented.

The SAI noted that some operational processes to implement cybersecurity measures need to be improved and provided the auditee with recommendations to improve their performance:

- **The Ministry of Finance is recommended to take into account cybersecurity issues at all stages of financing and the "life cycle" of government digitalization projects;**
- **It is also proposed to establish between the Ministry and relevant departments a permanent channel of communication and exchange of data on threats and possible illegal actions in the digital environment.**

SAI	UK National Audit Office
Title	Cyber and information security: Good practice guide
Date	October 28, 2021
Link	

In 2022, the SAI of Finland assessed how its recommendations for cybersecurity measures improvement were implemented, following an audit of the Ministry of Finance in 2017. The UK NAO concluded that the recommendations were partially implemented.

The UK NAO has prepared a guidance for audit committees for reviewing cybersecurity services and assessing the risks of using information systems based on current government requirements. The key issues to be considered when auditing such systems and services are:

1. **The organization's overall approach to cybersecurity and risk management;**
2. **Resources needed to ensure cybersecurity;**
3. **Individual issues, in particular - risk management in the field of information security and data, network security, emergency management, protection against malware, remote work of employees, etc.;**
4. **Related areas, in particular - cloud services, research and development of new technologies.**

SAI	Government Accountability Office (GAO of the United States)
Title	Federal Response to SolarWinds and Microsoft Exchange Incidents
Date	January 01, 2022
Link	

In 2022, GAO analyzed the measures that federal agencies took in response to the hacker attacks on SolarWinds and Microsoft Exchange networks. In January 2019, SolarWinds, a Texas-based software development company whose services are widely used by the U.S. federal government, was hacked. In March 2021, Microsoft reported the use of vulnerabilities to gain illegal access to multiple versions of Microsoft Exchange Server. These hacking attempts were one of the largest hacking attacks ever conducted against the federal government and the U.S. private sector. GAO notes that the U.S. federal agencies reached several conclusions following the hacking attacks:

- coordination with private sector companies has helped to make the incident response measures taken more effective;
- a centralized platform for dialogue between government bodies and private sector companies created has improved coordination among all stakeholders;
- the information sharing between federal agencies has often been slow and time-consuming;
- the evidence-gathering process was limited due to differences in data retention practices across agencies.

Staff Competencies and Capacity Building

Public institutions digitalization is comprehensive process and includes not only the adoption of new technologies, but also building the staff professional capacities. According to WEF experts, a successful digital transformation requires, among other things, strong project management skills. Compact and horizontal organizational structures empower the staff to provide greater flexibility and speed in decision-making. A common practice is to create a separate unit within the public institution responsible for the introduction of innovative approaches, as well as a competence center for training and support in the local use of new technologies.

In addition to creating the project teams and the scaling of digital solutions, it is vital to increase the digital competencies of all employees of government bodies, as well as to train them the "soft skills" necessary to adapt to environment changes. The traditionally conservative nature of the public service can be a major challenge to the adoption of breakthrough technologies in this sector. Compared to the difficulties of mastering new technologies, it is much more difficult for public institutions leadership and staff to change their mindset, which results in the issue of training and advanced training still being acute and necessary for improving the performance of the government. The most common issues faced by public authorities in developing the staff digital skills include:

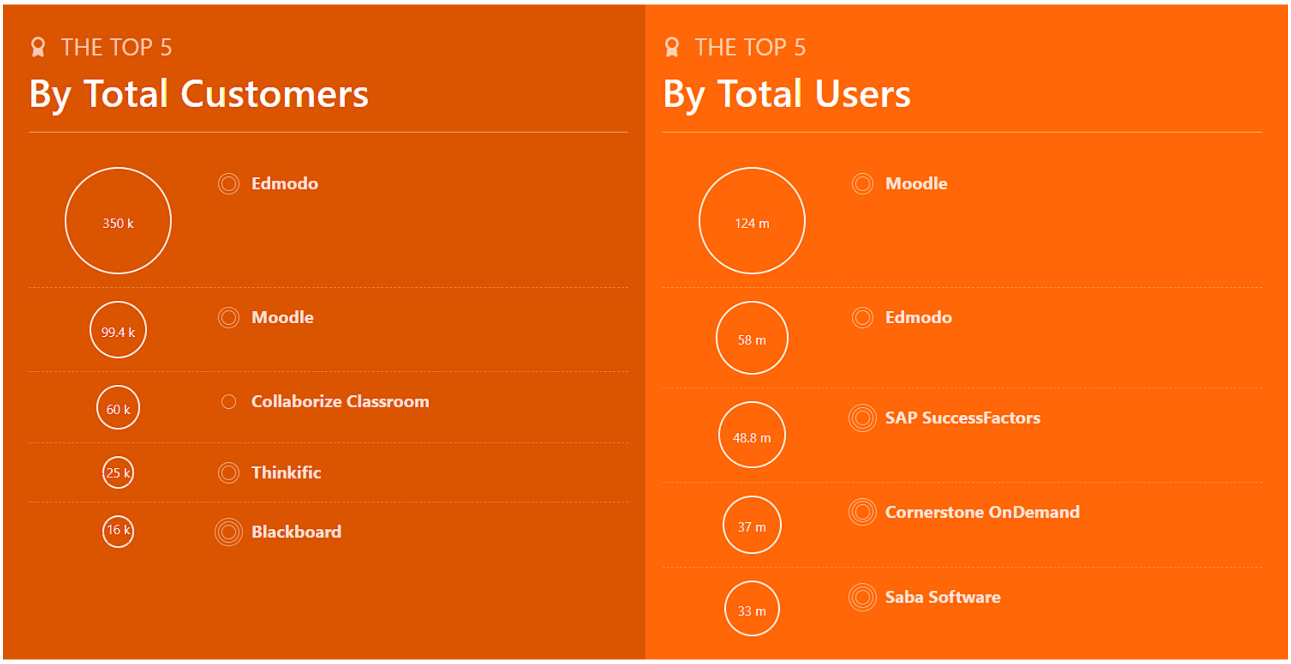
- **Lack of a clear understanding of the tasks**, goals, and risks in the organization of staff training (it is vital to avoid inflated expectations, both in terms of implementation speed and of new skills application);
- **Difficulty in involving private providers** of learning services (the need to create flexible conditions under contracts; a thorough study of the learning services market);
- **Recognition of the need** to work with legacy systems and a continuous process of updating skills;
- **Selection of the right combination** of the necessary skills for specific public administration tasks;
- **Correct choice** of the information presentation method;
- **Providing funding** and material incentives to employees learning new skills.

At the same time, an important problem is the lack of understanding of what set of competencies the employees should have for a successful digital transformation in each specific government body.

Sharing the best practices, experience, and knowledge among government bodies of different countries is as much relevant in the process of training employees as the aforementioned. This is facilitated by the holding of international conferences, working group meetings, webinars, etc., as well as the creation of platforms for the experience sharing. In 2021 alone, the International Organization of Supreme Audit Institutions (INTOSAI) and its members, held more than 70 events on the digitalization of both the supreme audit institutions (SAIs) and the wider public sector. Typically, the public authorities use the services of external experts and/or higher educational institutions to train employees in the form of master classes, seminars, and corporate programs. Thus, as part of increasing the digital literacy of employees, **the SAI of Iran** held a five-day International Training Course on IT Audit (January 17 - 21, 2022). Representatives of the scientific community and IT audit practice were invited as speakers.

The COVID-19 pandemic and the need to organize the remote work of public authorities, including the SAIs, have become important factors in intensifying the process of training employees in digital products, including in a remote mode. Since the beginning of the pandemic, the use of digital **Learning Management Systems** (LMSs) to facilitate improving the employees' skills has become increasingly popular. As early as 2005, the **OECD Centre for Educational Research and Innovation** (CERI) published a study "E-Learning in Tertiary Education," where the authors defined LMS as software designed to provide a range of administrative and pedagogical services (e.g. enrollment data, access to electronic course materials, teacher-student interaction, assessment, etc.). From 2005 to 2022, LMSs evolved from an administrative tool into a full-fledged platform for providing remote learning services.

Today, international organizations and SAIs can not only develop their platforms, but also buy ready-made (so-called "boxed") solutions. The most popular LMSs available are shown in the graph below.



Source: Capterra Survey 2018, The Top 20 Most Popular LMS Solutions https://www.capterra.com/infographics/most-popular/learning-management-system-software/

Many international organizations and SAIs prefer the Moodle platform (e.g., the United Nations Institute for Training and Research (UNITAR), the UN Women, the INTOSAI Development Initiative (INTOSAI IDI), the African Organization of Supreme Audit Institutions of English-speaking Countries (AFROSAI-E), the Pacific Association of Supreme Audit Institutions (PASAI), the E-Academy of the European Court of Auditors).

The LMSs contain large volumes of big data that can help the user evaluate the design of the e-learning course. For example, the completion rate shows how students are progressing and whether they are fully engaged in the learning process, and the satisfaction ratings show how students feel about the content and online instructors. These LMS indicators provide an opportunity to assess every aspect of an online learning strategy and develop measurable goals. Some LMS solutions have customizable reports that allow you to track the problem spots of online courses to achieve the desired results. In particular, course complete results and performance are an important indicator. For example, if half of students are unable to effectively complete a compliance course, it may indicate that the creator needs to better understand the reason behind the problem before changing the content of the course.

However, the key problem of organizing training on LMS platforms is still the lack of adequate testing in terms of knowledge gained and, as a result, the lack of full-fledged certification confirming the level of the employee's necessary skills. An additional difficulty arises with copyright to materials created by several authors.

Case Studies

SAI	National Audit Office of China
Title	National audit under the big data environment
Date	March 20, 2018
Link	

Based on the results of the study, the National Audit Office of China draws attention to the fact that there is auditors' resistance to changes. The SAI is currently promoting a comprehensive digital audit approach that includes general analysis, risk and suspicious activity identification, local inspections, and systemic research. Audit using big data analysis confirms its effectiveness in practice, and also helps to change the attitude of participants in control activities with regard to digital tools.

SAI	Czech Republic Supreme Audit Office
Title	Benchmarking Information Exchange Project (BIEP)
Date	11/2017
Link	

The Czech Republic Supreme Audit Office launched the Benchmarking Information Exchange Project (BIEP) On the platform, it is possible to discuss topical professional issues and conduct a comparative analysis of methodological approaches and audit results in various areas.

BIEP Rubricator

- Real property
- Centralized public procurement
- Municipal housing
- SDGs Implementation

- Roads and road construction
- Digital Education
- Armaments and military equipment
- Crime prevention
- Air pollution

- Ensuring access to drinking water
- Customs systems
- Access to wireless networks in railway transport
- Implementation of control functions
- Welfare
- Excise taxes and duties

The main idea of BIEP is to compare key performance indicators (KPIs) and specific national conditions in different countries. Comparison areas are unlimited. The BIEP aims to save time and audit costs.

SAI	Auditor General Office of Denmark
Title	The In-House Center of Excellence for Data Analytics
Date	January 15, 2020
Link	

The In-House Center of Excellence for Data Analytics has been established in the SAI of Denmark. The staff of the center assists auditors in conducting control activities using new data analysis tools. It is important to note that Denmark twice ranked first in the UN E-Government Surveys.

SAI	European Court of Auditors
Title	Digital Steering Committee
Date	2017
Link	

Within the European Court of Auditors (ECA), a Digital Steering Committee has been established. One of its part is the ECALab – a space where participants share ideas, as well as research, test, and integrate technologies into the audit process. The focal areas of the platform's work are the use of tools for data analysis, visualization, and control of the inspection process.

SAI	UK National Audit Office
Title	Skills passport
Date	June 21, 2019
Link	

One of the main issues in digital transformation of public administration is still how to monitor the knowledge gained and measure the level of digital literacy and competencies of public authorities employees (including SAIs). The UK's National Audit Office has introduced a Skills passport. The auditors fill out a form there on a regular basis indicating how familiar a member is with a particular technology or analytical method of conducting an audit.

SAI	Office of the Auditor General of Nepal
Title	Nepal Audit Management System
Date	January 26, 2022
Link	

The SAI of Nepal has launched the Nepal Audit Management System. The project is aimed at optimizing the process of audit of possible risks. The audit phases supported by the program include:

- Risk-based audit planning;
- Online access to the auditee;
- Online audit quality control and assurance mechanism;
- Online transfer of audit reports generated by the system;
- Archiving of received documents

SAI	Accounts Chamber of the Russian Federation
Title	Digital University for INTOSAI Community (U-INTOSAI)
Date	April 12, 2021
Link	

In 2021, **the Accounts Chamber of the Russian Federation** launched the Digital University for the INTOSAI Community (U-INTOSAI) based on the LMS plugin for WordPress.

Educational materials published on the U-INTOSAI platform reflect the experience of international organizations, academic and business communities, as well as of the SAIs, which contributes to ensuring the capacity and competence of the auditors of the future.

The platform is currently available in seven languages and has more than 1,500 registered users from 196 countries. The platform presents e-courses and podcasts on a wide range of topics relevant for the SAIs: SDGs, public administration, information technology and data analytics, management, soft skills, etc.

While implementing the U-INTOSAI initiative, the team faced a number of difficulties in various areas:

- **Mistrust of potential stakeholders in the new platform and the effectiveness of distance learning in general;**
- **Difficulties in finding educational content suitable to develop skills required by the Community;**
- **The narrow focus of the platform; as a result, it is impossible to conduct classical marketing campaigns to promote the service.**

2022
Accounts Chamber
of the Russian Federation