

AUDIT CHAMBER OF THE REPUBLIC OF ARMENIA



CURRENT REPORT

**ABOUT THE AUDIT RESULTS OF DIGITAL TRANSFORMATION
(DIGITALIZATION) PROCESS OF THE REPUBLIC OF ARMENIA**

2023

TABLE OF CONTENTS

LIST OF ABBREVIATIONS.....	4
SUMMARY	5
PERFORMANCE AUDIT REPORT	6
DESCRIPTION OF PERFORMANCE AUDITING	9
PERFORMANCE AUDIT RESULTS.....	10
Audit question - 1. Are the institutional capacities of the RA public sector sufficient for the implementation of the digital transformation agenda (assessment of readiness for digitization)	10
Audit sub-question - 1.1. Is there an effective cyber security system in RA?	10
Audit sub-question - 1.2. Are there effective human resource management procedures for digitization in the public sector?	20
Audit question - 3. Has the effectiveness been ensured during the implementation of the RA digitalization strategy?	27
Audit question - 4. Is effective budgeting of the digitization process ensured in RA?	34
RECOMMENDATIONS	37

Audit basis	Audit Chamber's decree no. 99-A dates April 22, 2022
Audit entity	High-Tech Industry Ministry
Audit subject	Digital transformation (digitalization) process of the Republic of Armenia
Audit criteria	The Law "On the Structure and Activities of the Government", the RA Government 2021-2026. program, the regulation of the Ministry of High-tech Industry, the digitalization strategy of Armenia, the methodological guidelines approved within the framework of the strategy of the full implementation of the RA program budgeting system, the "National Cyber Security Capabilities" of the EU cyber security operation. Standards defined by the World Bank's "Digital Governance Readiness Assessment Tool" in the format of the country's assessment.
Auditing period	January 1, 2021 to November 30, 2022.
Dates of audit	June 1, 2022 to February 28, 2023.
Audit Methodology	The audit was carried out in accordance with the Audit Chamber's approved audit methodology based on "ISSAI 100 - Basic Principles of Auditing in the Public Sector" and "ISSAI 300 - Principles of Performance Audit" of the higher audit bodies. on jazz standards. A performance audit was carried out, where observation, survey, external confirmation and analytical procedures were conducted. The evaluation was carried out with system-oriented and result-oriented approaches. The audit process was documented, the auditors drew up an audit report, which was presented to the object of the audit in the prescribed manner. The head of the audit facility signed the audit protocol. no objections and explanations were submitted.
Audit Department/ Coordination	The audit was carried out by the Department of Methodology, Analysis and International Relations of the Audit Chamber (Head of Department, Zorayr Karapetyan). Audit was coordinated by the Chairman of the RA Audit Chamber, Atom Janjughazyan.

LIST OF ABBREVIATIONS

NSS – National Security Service

AI – artificial intelligence

CIS – Commonwealth of Independent States

HTIM – High-Tech Industry Ministry

EU – European Union

CEE – Central and Eastern Europe

CB – Central Bank

CII - Critical information infrastructure

CERT - Computer emergency response team

WB – World Bank

RA – Republic of Armenia

AC – Audit Chamber

OECD – Organization for economic cooperation and development

ICT – information and communication technologies

IT – information technologies

SME – small and medium enterprises

SUMMARY

High-tech Industry Ministry as an authorized body in the field of coordination of digitization (digital transformation) processes and promotion of the formation of a unified digital environment and digital economy, as well as the adoption of the RA digitization strategy in 2021, created important prerequisites for pushing the agenda for digitalization in RA.

However, the audit conducted by the Audit Chamber prove that there are significant gaps in the institutional capabilities of the RA public sector, which have a deterrent effect on the implementation of the digital agenda. In particular, a vulnerable cyber security environment carries the risk of limiting the benefits of digitization, which requires institutional frameworks to identify and protect critical information infrastructure.

In terms of limited capacity and problems related to strategic leadership none of the measures envisaged by the digitalization strategy were fully implemented within the set deadlines. Moreover, the strategy itself is not comprehensive, in terms of which separate entities have developed and operate conceptual documents for digitalization of the country, - and as a result, effective program budgeting in the field of digitalization has not been ensured.

In order to address found problems, the Chamber of Audits presented more than two dozen recommendations to the High-tech Industry Ministry, with the aim of contributing to the full realization of the state potential in question.

PERFORMANCE AUDIT REPORT

Turned into fourth industrial revolution era the main distinguishing feature of the Worldwide economy compared to the preceding periods of development is the digital transformation of socio-economic relations and public administration. Digitalization processes bring new opportunities as well as new challenges, the effective management of which is an agenda issue for almost all countries in the world, including the Republic of Armenia. The digital transformation of the RA economy will provide an opportunity to overcome such traditional limitations of economic development and competitiveness such as: lack of access to the sea, partial blockade, domestic market with limited solvent demand, scarcity of natural resources, and will also contribute to the economic development and wide in the sense of the formation of the claimant's attitude towards public services with modern standards among the public and the establishment of institutions providing public services equivalent to it. At the same time, the continuous deepening of digitization activities brings challenges, which, in the conditions of weak infrastructures for ensuring cargo security, lead to risks of neutralizing the benefits of digitization.

In 2022 Audit Chamber started to conduct performance auditing in the purpose to discover the effectiveness of the strategic-institutional frameworks implementing digitization - in ensuring the digital transformation of RA.

Current audit results state that:

- **Regarding the provision of cyber security** - (a) there is no definition of critical information infrastructures in RA, (b) there are no criteria for their disclosure and (c) there is no national register, the condition of which cannot be applied to the Institute for the Protection of CII's national structures, (d) the strategic measure of the creation of the National Center for Cyber Security (deadline: December 2022) was not implemented, which as planned should be the guarantee of the cyber security of the state system while - ensuring the protection of personal data and promote cyber literacy and development, (e) - cyber security industry standards are not in place and not approved (deadline: September 2021), (f) national cyber security plans are not developed, (g) cyber security exercises are - not conducted, (h) there are no requirements for mandatory reporting of cyber-accidents, or in case of real-time registration of cyber-accidents, there are no any technical capabilities to automatically receive and monitor information about them.
- **Regarding the management of human resources** - (a) there are no assessments of the need for human resource capabilities in relation to training with qualified specialists in the field of digitization in RA state bodies, as well as digital knowledge and skills, and educational plans based on them, (b) there are no defined minimum qualification requirements of a digital personnel, (c) there are no unified mechanisms with the involvement of representatives from all bodies, with examples of general discussions of - projects related to digitalization, exposure of risks to ensure interaction and exchange of - experience.

- **Regarding the comprehensiveness of the digitalization strategy** - the digitalization strategy of RA lacks plans, schedule and implementers for the implementation of digital transformations in individual branches of the economy and public administration. Instead, - sectoral strategic measures and initiatives aimed at digitization have been developed and implemented by certain entities.
- **Regarding the implementation of the strategy** – According to the strategy 10 activities planned to be implemented during the period covered by the audit, none of which has been completed within the specified time frame. In particular, (a) within the framework of the 1st measure of the "Institutionalization of Digitization" strategy, it was aimed to form a professional digitization body attached to the HTIM (deadline: May 2021), which was not - implemented, (b) two of the 5 planned digitization standards (cargo security and cloud infrastructure) have not been developed, and the other three (digitalization processes and requirements formation, technical and functional) have been developed, but have not yet been officially achieved, (c) there is no study on which of the existing digitalization platforms technically do not comply with the localization standards, (d) there is no study on what financial consequences the adaptation of the current digital standards to the localization standards will have, including on the state budget, (e) "Data Policy Concept" within the strategic measure it was intended to develop a single unified data policy concept (deadline: December 2021), which was not realized, (f) quality assessment of the current state of the digital platforms listed and operating, definition of target indicators, according to the current indicators the condition assessment measure was not carried out, (g) the planning measure for the creation of the "unified electronic program management platform" was not carried out, etc.
- **Regarding budgeting** - (a) there is no budget program being a logical grouping of the implementation steps of the state policy aimed at achieving the strategic goal of digital transformation. The "1043 – Hi-Tech Industry Ecosystem, Digitization and Digital - Development" program of the RA State Budget mainly consists of measures implemented by the HTIM, which do not include the entire spectrum of state interventions aimed at achieving the goal of digital transformation, (b) budgetary measures related to digital transformation other entities different from the HTIM are also responsible for a number of measures.

Based on the results of the audit, the Audit Chamber concludes that the RA digital transformation (digitization) process did not achieve the target effectiveness during the audit period.

Details are presented in the "Performance Audit Results" section.

Atom Janjughazyan
Chairman of the Audit Chamber

February 28, 2023

19 Baghramyan avenue, Yerevan
Republic of Armenia

DESCRIPTION OF PERFORMANCE AUDITING

Audit purpose

The purpose of the audit was to find out the effectiveness of the strategic institutional - structures implementing digitization in the issue of ensuring the digital transformation of RA, and to present timely, professional and impartial information to the public and the National - Assembly.

Audit questions

To address the above-mentioned goal, the following questions were proposed and audited:

1. Are the institutional capacities of the RA public sector sufficient for the implementation of the digital transformation agenda (assessment for readiness digitalization)?
 - 1.1 Is there a cyber security system effectively operating in RA?
 - I. Is the scope of protection of CII disclosed in RA?
 - II. Have institutional frameworks for the protection of cyber security been effectively implemented in RA?
 - 1.2 Are there effective human resource management structures in the field of digitization in the public sector?
2. Is the digitization process in RA implemented with a comprehensive approach?
3. Has the targeted effectiveness been achieved during the implementation of the RA digitalization strategy?
4. Is effective budgeting of the digitization process ensured in RA?

Audit limitations

No limitations recorded during the audit.

PERFORMANCE AUDIT RESULTS

Audit question - 1. Are the institutional capacities of the RA public sector - sufficient for the implementation of the digital transformation agenda (assessment of readiness for digitization)

Audit sub-question - 1.1. Is there an effective cyber security system in RA?

In particular:

A. Is the scope of protection of CII's disclosed in RA?

B. Have institutional frameworks for cyber security been effectively implemented in RA?

the World Cyber Security Index ¹, Armenia ranks 90th among 193 countries in terms of cyber security, and according to the National Cyber Security Index, ² it ranks 90th among 161 countries. According to the indicated indicators, Armenia's position is one of the lowest in the context of comparable countries (CIS and CEE).

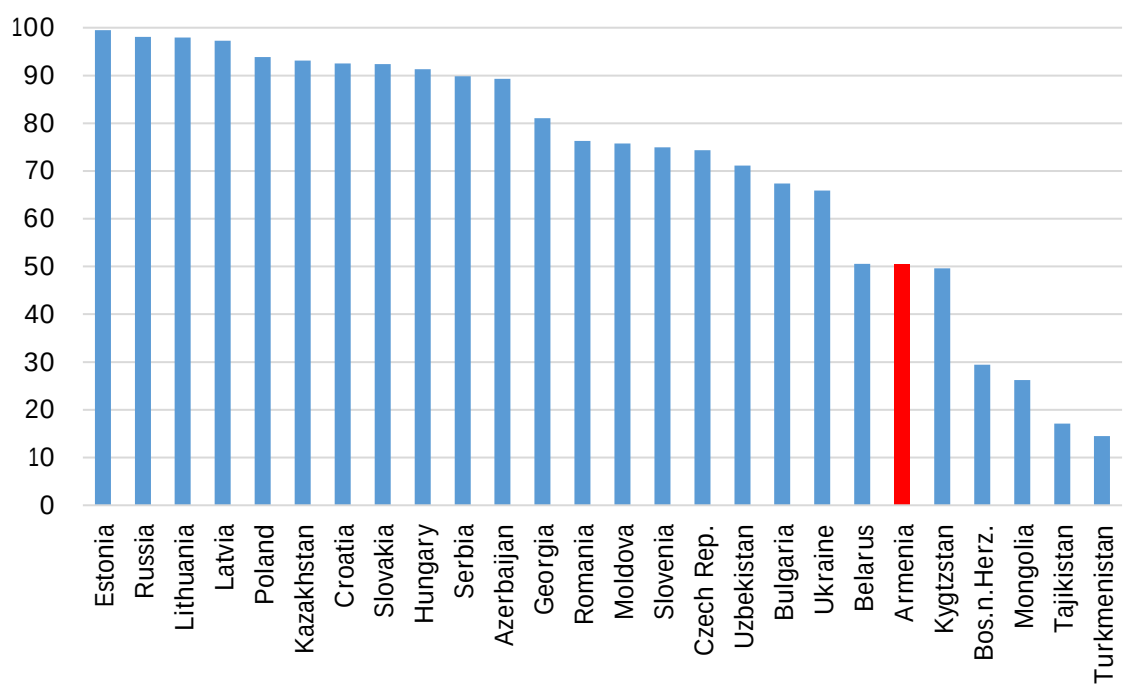


Figure 1: Global Cyber security index

¹<https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>

²<https://ncsi.ega.ee/ncsi-index/>

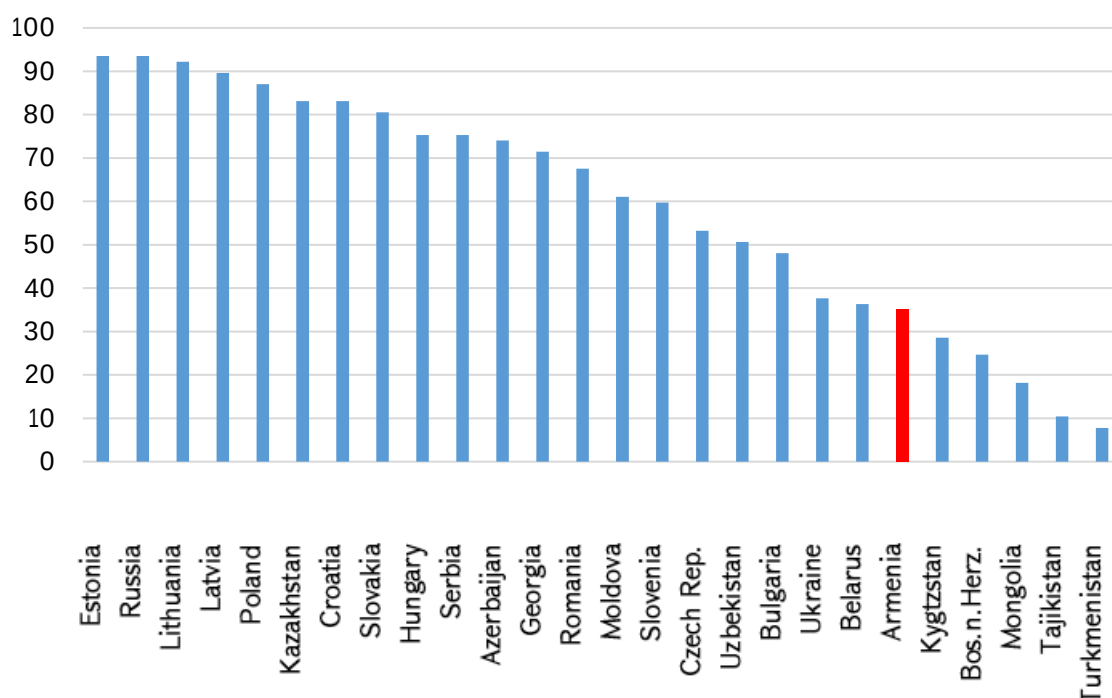


Figure 2: National Cybersecurity Index

A. Was the scope for the CII's protection disclosed in RA ?

Audit criteria

- HTIM develops and implements Cybersecurity Policy of the Government (*Section 16 of the Annex to the Law on the Structure and Activity of the Government*).
- One of the goals of HTIM is to create and strengthen the conditions for ensuring cyber security (*subparagraph 1 of clause 9 of the RA Prime Minister's Decree No. 698-L of 11.06.18 "On Approving the Charter of RA HTIM" (hereafter: the Statute)*).
- Among the functions of HTIM are:
 - approval of legislative acts in regards to the field of cyber security (*paragraph 3 of Article 11 of the Charter*),
 - managing of the IT sector registry in the field related to cyber security (*sub-clause 5 of clause 11 of the Charter*),
 - developing state programs and measures in the field of cyber security, ensuring their implementation and monitoring. (*Subparagraph 17 of Clause 11 of the Charter*),
 - implementation and development of cyber security system (*Subparagraph 24 of Clause 11 of the Code of Conduct*).
- One of the objectives of the RA government is the reform in the information security and cyber security areas. In order to effectively handle the in Cyber threats, challenge monitoring, analysis, informational response and fighting the legislation should be modernize (*Items 1.3 and 2.3 of the 2021-2026 program of the RA government*).

Best Experience:

- One of the strategic goals of ensuring cyber security is the protection of CII, which implies:
 - **Identification of CII** (methodology of identification, national register of CII identified according to critical sectors, availability of the procedure for updating the latter),
 - **Identification and detection of risks related to CII** (the presence of a national body exercising control over the protection of CII, the presence of protection plans specific to each critical sector, the presence of a national risk register, a factor for ensuring the continuity of services provided by CII availability of such information) (*National Cyber Security Capability Assessment Format, EU Cyber Security Agency (ENISA), Strategic Objective 11, Digital Government Readiness - Assessment Tool (DGRA), WB*)³.

Audit results

- There is no legal definition of CII in RA.
- There are no defined criteria for identifying CII, no methodology for their identification has been developed.
- Accordingly, the scope of CII, which should be subject to protection by the state, has not been revealed.

The diagram below presents information about the existence of a legal base in countries comparable to RA (CIS and CEE), which allows identifying CII (in 15 out of 26 countries, it exists in 9, including RA).

Table 1:

Existence of a legal basis for the disclosure of CII								
	Estonia	✓		Latvia	✓		Kazakhstan	✓
	Lithuania	✓		Ukraine	✓		Azerbaijan	✗
	Czech	✓		Bulgaria	✓		Uzbekistan	✗
	Romania	✓		Russia:	✓		Armenia:	✗
	Poland	✓		Hungary	✓		Bosnia and Herzegovina.	✗
	Slovakia	✓		Georgia	✓		Kyrgyzstan	✗

³In this current conclusion, after the standards (best practice citations), their sources are indicated in italics.

	Croatia	✓		Slovenia	✓		Mongolia	✗
	Serbia	✓		Belarus	✓		Tajikistan	✗
				Moldova	✗		Turkmenistan	✗

The main reason for the audit result is:

- the imperfection of the legislative base regulating the field of cyber security in RA.

As a consequence:

- There is no national register of RA CIIs.
- No possibility to implement institutional structures for the protection of CIIs.

Good practice

- *According to the OECD*, ICTs are those interconnected systems and networks which disruption or destruction would have a significant impact on the health, safety, security or economic standard of living of citizens or the effective functioning of the government/economy⁴.
- *According to the Directive 2008/114/EC of the Council of Europe*, a critical infrastructure is an asset, system or part thereof, which is of essential importance for the maintenance of public vital functions, people's health, safety, security, socio-economic quality of life and the disruption of which or the destruction would have a significant impact on the state as a result of failure to maintain said functions⁵. Annex 2 of the Directive provides for critical sectors for the EU (according to the revised Directive, the - critical sectors are: energy, transport, food supply, drinking water, healthcare, financial market infrastructure, digital infrastructure, public infrastructure a vehicle, waste water, banks, space), and the 3rd appendix is the procedure for identifying critical infrastructures.
- *Under US law*, critical infrastructure refers to systems and assets, both physical and digital, that are of such vital importance to the United States that their disruption or destruction would have a debilitating effect on national security, national economic security, national public health, or a combination thereof⁶.
- *Under Singapore law*, ICT is a computer system that is necessary for the delivery of a range of key services on which Singapore depends and the loss or disruption of which

⁴OECD Recommendation of the Council on the Protection of Critical Information Infrastructures C(2008)35, adopted by the OECD Council at its 1172nd Session on 30 April 2008.

⁵Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

⁶42 US Code § 5195c.

would have a debilitating effect on national security, defence, foreign affairs, the economy, public health, public safety or public ⁷order.

- *According to Austrian law*, critical infrastructure is an asset, system or part thereof, which is essential for the maintenance of public vital functions, human health, safety, security, socio-economic living standards and whose disruption or destruction would have a significant impact on the state, as a result of the failure of⁸ some of the mentioned functions.
- *According to the Czech legislation*, critical infrastructure is defined as production and non-production systems and processes, the defective operation of which can have a serious impact on national security, economy, public administration and provision of basic vital needs of the population⁹.
- *According to the legislation of Lithuania*, CII is defined as an electronic communication - network, information system or a group of them, in which the occurrence of an accident will cause or may cause serious damage to national security, national economy or public welfare ¹⁰.
- *According to the legislation of the Russian Federation*, CII is defined as a set of automated management systems of critical infrastructure facilities and information and telecommunication networks providing their interaction, intended for the provision of state administration, defense, security and legal order, the disruption or cessation of which may leave serious consequences. A critical infrastructure object is considered to be such an object, the disruption or destruction of which leads to the loss of controllability, destruction of the infrastructure, irreversible negative changes or destruction of the economy, or significant long-term deterioration¹¹ of the safety of the population's livelihood.
- *A National Center for the Protection of Critical Infrastructures was established in Spain*, which is responsible for the promotion, coordination and control of¹² all activities related to the protection of critical infrastructures in the country.
- *Switzerland adopted the "Critical Infrastructure Protection Act 2018-2022". national strategy*, in which 9 critical sections and 27 sub-sections are specified. A methodology - has been developed that allows determining the priority of sub-sections based on an estimate of the damage expected from a failure in a critical sub-section, which is determined by the impact on other sub-sections, the population and the economy¹³.

Conclusion

⁷Cybersecurity act 2018.

⁸Austria, 2008. APCIP (Austrian Program for Critical Infrastructure Protection).

⁹Kritická infrastruktura – Ministerstvo vnitra České republiky. Ministerstvo Vnitra České republiky. Úvodní strana – Ministerstvo vnitra České republiky (online). ©2015 (cited 2015-09-21).

¹⁰Government of the Republic of Lithuania, Resolution No. 796 of 29 June 2011 on the Approval of the Program for the Development of Electronic Information Security (Cyber-Security).

¹¹Main directions of the government: politics in region: provision security automated system management production and: technological processes critically important objects infrastructures России – ской – : Federation, approved by the RF president: Federation, February 3, 2012, No. 803.

¹² <https://cnpic.interior.gob.es/opencms/en/home/>

¹³ <https://www.babs.admin.ch/en/aufgabenbabs/ski.html>

The lack of criteria for the definition of CII and their identification in RA limits the potential of effective protection of CII, increasing their vulnerability as a threat to national - security.

Recommendations

- Legislatively adjust of cyber security sector including defining CII including their protection provision and legal relations.
- To develop and introduce the legal framework of the cyber security sector in such a way that it forms prerequisites for ensuring at least the conditions listed below and determining the responsible parties for their implementation:
 - Existence of a methodology for identifying CII and keeping their scope up to date.
 - Maintaining an up-to-date (constantly updated) national register of CII.
 - Existence of flexible procedures for defining cyber security requirements specific to each of the CII, equivalent to the needs arising in the given period.
 - Availability of internal and external monitoring institutional structures in order to ensure cyber security requirements for the protection of CII.

B. Are modern institutional frameworks for ensuring cyber security implemented in RA?

Audit criteria

- One of the functions of HTIM is the implementation and development of the cyber security system (*sub-paragraph 24 of paragraph 11 of the Statute*).
- Among the planned measures in the field of digitization is the introduction of the cyber security management and development system, the creation of a cyber security and fact-based center (*paragraphs 1.3 and 2.3 of the 2021-2026 RA government plan*).
- Goals established by the RA digitalization strategy is the provision of a safe digital - environment through the National Cyber Security Center (*point 14, point 2 of the Strategy*).
- Until September, 2021 it is planned to develop cyber security standards, and by December, 2022 to carry out a review of standards, applicability verification and certification of systems (*Points 3 and 5 of Annex 2 of the Strategy*).
- It is planned (until December, 2022) to create a National Center for Cyber Security (*paragraph 5 of the 2nd Annex to the Strategy*).
- One of the fundamental conditions laid down by the strategy is ensuring the digital continuity of Armenia, according to which: (1) the strategic goal of the HTIM is to - guarantee the digital continuity of Armenia, which implies inter-entity cooperation in the direction of strengthening the cyber security complex, (2) it is planned classification

of risks related to cyber security, development of an additional action plan for cyber security and mitigation in the event of a state of emergency and a state of war and - relevant scenarios, as well as implementation of exercises related to individual incidents, definition of measures and principles aimed at systematic management of incidents (*Strategy Clause 6 of Section 4*).

Best experience:

- Among the strategic goals of ensuring cyber security are:
 - **Development of National Cyber Continuity Plans**, which include:
 - Definition of criteria on the basis of which it will be possible to characterize the situation as a crisis in the national economy.
 - Definition of key processes and actions that will allow overcoming the crisis.
 - Clarifying the roles and responsibilities of various stakeholders during a cyber-crisis.
 - Defining the criteria on the basis of which it will be possible to determine the end of the crisis.
 - **The definition of basis security measures**, which implies:
 - Cyber security standards availability
 - National body existence which checks the base security measures' application.
 - **Cyber security exercises** which implies:
 - Availability of cyber security exercise program in national level
 - Involving private sector in exercises
 - All critical sections included in exercises
 - Development of programs aimed at eliminating the problems identified as a result of the exercises.
 - **Development of Incidents notification mechanisms** which implies:
 - Existence of effective mechanisms for mandatory reporting of incidents, including for all sectors of CII.
 - Impact assessment of incidents, development of safety measures based on the latter.
 - **Incident response capacity development** which implies:
 - The mandate of the incident response team is defined by the government, including the powers, role and scope of responsibility depending on the target sector, the type of incident and the impact.
 - Defining the technical and operational requirements that the team must meet. Establishing and promoting standardized incident response and classification practices.

Audit results

- The measures defined by the Strategy aimed at the formation of institutional structures of cyber security have not been implemented, in particular:
 - the National Cyber Security Center was not created (due December 2022), which, as it was planned, should ensure the cyber security system, as well as the protection of personal data and it should promote the development of cyber literacy.
 - not localized and approved cybersecurity industry standards (due September 2021).

Table 2:

Table 2:

Cybersecurity standard for the public sector was set up								
	Estonia	✓		Latvia	✓		Kazakhstan	✗
	Lithuania	✓		Ukraine	✗		Azerbaijan	✗
	Czech	✗		Bulgaria	✓		Uzbekistan	✗
	Romania	✗		Russia:	✓		Armenia:	✗
	Poland	✓		Hungary	✓		Bosnia and Herzegovina.	✗
	Slovakia	✓		Georgia	✗		Kyrgyzstan	✓
	Croatia	✓		Slovenia	✓		Mongolia	✗
	Serbia	✓		Belarus	✗		Tajikistan	✗
				Moldova	✓		Turkmenistan	✗

- No national cyber continuity plans have been developed in RA.

Table 3:

Crisis management plan resulting from large-scale cyber-incidents (legal act)	
---	--

	Estonia	✓		Latvia	✗		Kazakhstan	✓
	Lithuania	✓		Ukraine	✗		Azerbaijan	✗
	Czech	✓		Bulgaria	✓		Uzbekistan	✗
	Romania	✗		Russia:	✗		Armenia:	✗
	Poland	✓		Hungary	✗		Bosnia and Herzegovina.	✗
	Slovakia	✓		Georgia	✗		Kyrgyzstan	✗
	Croatia	✓		Slovenia	✗		Mongolia	✗
	Serbia	✗		Belarus	✗		Tajikistan	✗
				Moldova	✗		Turkmenistan	✗

- Cyber security exercises were not carried out in Armenia.

Table 4:

Implementation of national level cyber crisis management exercise in last 3 years								
	Estonia	✓		Latvia	✗		Kazakhstan	✗
	Lithuania	✓		Ukraine	✓		Azerbaijan	✗
	Czech	✓		Bulgaria	✗		Uzbekistan	✗
	Romania	✓		Russia:	✗		Armenia:	✗
	Poland	✓		Hungary	✗		Bosnia and Herzegovina.	✗
	Slovakia	✓		Georgia	✗		Kyrgyzstan	✓
	Croatia	✓		Slovenia	✗		Mongolia	✗
	Serbia	✓		Belarus	✗		Tajikistan	✗
				Moldova	✗		Turkmenistan	✗

- There are no requirements for mandatory reporting of cyber-incidents, or in case of real-time registration of cyber-incidents, there are no technical capabilities to automatically obtain and monitor information about them. Within the framework of its mandate, the NSS has implemented an incident notification website for the public sector, which partially solves the problem, because in the absence of reporting requirements, the availability of a complete picture of cyber risks and their effective management is not ensured.

Table 5:

Availability of cyber incident reporting requirements

	Estonia	✓		Latvia	✓		Kazakhstan	✗
	Lithuania	✗		Ukraine	✓		Azerbaijan	✗
	Czech	✓		Bulgaria	✓		Uzbekistan	✗
	Romania	✓		Russia:	✗		Armenia:	✗
	Poland	✓		Hungary	✓		Bosnia and Herzegovina.	✗
	Slovakia	✓		Georgia	✗		Kyrgyzstan	✗
	Croatia	✓		Slovenia	✓		Mongolia	✗
	Serbia	✗		Belarus	✗		Tajikistan	✗
				Moldova	✗		Turkmenistan	✗

The main cause of the audit finding is:

- The problems related to strategic leadership.

As a results:

- in RA there is a low level of cyber security, reflected in objective international assessments.

Good practice

- *A national crisis management plan has been developed in Poland, which outlines common roles and responsibilities in a crisis situation. The government is in charge of the political process, which is advised by the Crisis Management Group. The latter is made up of the heads of all entities related to the crisis. In case of crisis regarding CII's, -*

the Ministry of Digitization and Management plays a leading role in overcoming the crisis.

- *Regular cyber security training is conducted in Sweden.* For example, in the field of telecommunications, every two years, the Hera National Communications Coordination Group organizes exercises involving the largest 8 operators. A simulation of an IT attack on financial systems, a cyber security exercise at the national level was also carried out, as well as participation in international exercises organized by the United States.
- *There are several CERT operating in Poland.* In particular, cert.gov.pl is the basic structure for public sector organizations and also provides services to CIIIs on a permanent basis. The tasks of the CERT are to issue security alerts, identify incidents in public/state networks, eliminate and analyze incidents. In addition, there are a number of sectoral CERTs, such as MilCERT in the military sector or CERT Orange in the telecommunications sector.
- *In Croatia, there are mandatory cyber incident reporting requirements for CIIIs.* In the case of other systems, this movement is voluntary. The list of data that must be presented in case of notification is defined.

(A positive action guide for national cyber security strategies, EU Cyber Security Agency (ENISA)).

Conclusion

In the conditions of increasing inclusiveness of society, economy and public administration in the digital environment, the weak institutional frameworks of cyber security or their absence creates significant risks in the issue of ensuring the strategic goals of digital transformation of RA.

Recommendations

- Develop cyber resilience plans aimed at ensuring the digital continuity of RA.
- Localize and establish cybersecurity standards and other basic requirements.
- Plan and execute cyber exercises in response to emergency or incident plans In order to evaluate the capabilities to act responsibly, highlight the shortcomings and plan the measures aimed at their elimination, making the private sector a participant in the planning of the exercises as well.
- Promote the formation and establishment of national, state, and sectoral CERT defining their communication mechanisms with the national body responsible for cyber security.

Audit sub-question - 1.2. Are there effective human resource management procedures for digitization in the public sector?

Audit criteria

Efficient management of human resources related to digitalization in the public sector - implies:

- Defining the digital skills needed to deliver the digital transformation agenda.
- Ensuring the availability of qualified personnel necessary for the implementation of the digital transformation strategy.
- Implementation of targeted digital education at all levels of management.
- collaboration among specialists from different areas of public administration on issues and projects related to digitization.

(WB "Digital Government Readiness Evaluation Tool ", section 4, point "d").

Audit results

- There is no developed and approved comprehensive training and qualification program for staff related to digitization at different levels of management. However, a number of field conferences and courses were organized and conducted, such as:
 - The "CyberGEN2022+Kaspersky" conference was organized as part of the - cooperation between the Central Bank of Armenia and Kaspersky, with the aim of replenishing knowledge and exchanging experience in the field of cyber security.
 - The "CYBERGEN" conference was organized by the CBA, dedicated to the discussion of issues and practical examples related to cyber security management, international standards and best practices, response to incidents, etc.
 - Within the framework of cooperation between the Civil Service Office and HTIM, the training course on "Cyber accident prevention basics" was organized.
- There are no evaluations of the need for human resource capabilities in relation to digital knowledge and skills and there are no educational plans based on them.
- There are no minimum qualifications for digital staff is defined. However, within the framework of the digital services design standards implementation guide, it is planned to define a list of necessary roles in the digital team, which will be part of the team or will always be in a place accessible to the team, and it is also necessary to clarify the scope of their duties¹⁴.
- There are no comprehensive mechanisms with the involvement of representatives from all entities for general discussions of digitization - related projects, risk identification, interaction security, and experience exchange.

The main cause for the findings are:

- Assessment and study of the needs of the digital staff is planned to be carried out after having a map of the services provided by the state.

¹⁴ In particular: Service Responsible / Product: Owner / Service: responsible, users researcher/ business analyst User: Researcher / Business: Analyst, Contents: developer / Content: Designer, UI / UX designer / UI / UX Designer, Programmer / Developer, Quality provision specialist / QA (Quality: Assurance: Engineer), Technical Give it a try / Technical architect /, Lawyer - expert.

- The strategy did not envisage an event for the formation of institutional mechanisms for the interaction of specialists on basic issues and projects related to digitalization.

As a result:

- qualification requirements for staff providing digital services does not provide an opportunity to carry out an assessment of the security of state entities with qualified specialists.
- The lack of qualification requirements hinders the creation of individual learning and training plans.
- institutional mechanisms with the involvement of representatives from all entities does not allow to carry out general discussions and maintain interaction in relation to the projects related to digitalization.

Conclusions

There are no effective structures for human resources management implemented in the field of digitalization.

Recommendations

- Qualification requirements to be included in the job descriptions of employees engaged in the provision of digital services in the public sector.
- Based on the established requirements, carry out a qualified assessment of the supply of rivers and such human resources according to the departments.
- Develop staff training programs based on assessment results.
- Set institutional mechanisms to ensure the interaction of all parties on the issues and projects related to digitization, with the involvement of representatives from all relevant bodies.

Audit question - 2. Is the RA digitization process implemented in comprehensive strategic approach?

The vision of the Republic of Armenia in the field of Audit as well as the directions and measures of strategic reforms in the period under consideration are described in the Government of the Republic of Armenia dated 11.02.21. "Armenia 2021-2025" approved by decision N183-L in the digitization campaign.

Audit criteria

- This strategy is a comprehensive development plan for the country and covers all socio-economic areas. *(Paragraph 16 of Appendix 1 of the Strategy).*
- The digitalization strategy of Armenia aims to ensure the digital transformation of government, economy and society *(paragraph 14 of the 1st appendix of the Republic of Armenia).*

Audit results

- While investigating the strategy, as well as the program of strategy measures and result indicators, it becomes clear that there are no measures, timetables and implementers for the implementation of digital transformations in several areas of the economy and public administration. Instead, sectoral measures and initiatives aimed at digitization are implemented by the respective entities in certain areas. For example, according to the external confirmation process used during the audit, it was recorded that:
 - According to the order N456–L of the RA Minister of Health dated 16.02.21, the program of measures for the development of the electronic health care system was approved, which provides the implementation of the information and the - infrastructure as a whole, and then the entry, processing, storage, archiving and use of health data about each person in the electronic environment. The RA digitization strategy, as well as references to other legal acts adopted by the authorized body of the field, are not present in the legal basis for the adoption of this program. It should be noted that the RA government decision N650-L on “2019-2023 approving the program of activity measures of the Government of the Republic of Armenia ” it was intended to develop the government's decision "Approval of the vision of the development of the electronic healthcare system" and "Approval of the program of activities for the development of the electronic healthcare system" of the Minister of Health the decree, and the RA Ministry of Transport, Communications and Local Technologies (successor: HTIM) was appointed as the overall co-implementor of these measures.
 - In the absence of a comprehensive digitization policy, payments for only 13 out of 47 types of own revenue types of the Yerevan municipality can be made entirely electronically (without the mandatory physical presence of the taxpayer).

The main cause of the audit finding: during the development of the strategic action plan comprehensiveness was not exercised.

As a result:

- Budgeting with a programmatic approach has been limited in the field of digitization.
- Risks of the emergence of significant differences between the levels of digitization in certain fields of the economy, and the effectiveness of the assessment of priorities.
- The effectiveness of the control mechanisms for ensuring the compliance of digitization measures in certain fields with the standards/requirements/policies of the digitization sector has been limited.

Good practice

The Digital Roadmap Austria can serve as an example of positive practice. Prior to the development of the latter, branch digitalization strategies were in operation, which were then integrated into a single strategic document, ensuring the consistency and interoperability of digitization measures implemented in all key sectors, and a comprehensive direction with one common end goal was shown.

In the road map, 12 main sectors are distinguished, in each of which sector-specific measures are planned. For example:

- In the field of *"Health, care and social issues"* there are suggestions for the development of electronic vaccination registers, mother and child electronic medical cards and electronic prescription (e-Prescription), implementation of the telemedicine - platform.
- *"Environment, Energy, Agriculture and Climate Protection"* in the field are intended for improved weather forecasting, optimization of agricultural space and accurate data on - production quantities, sales volumes and inventory levels, use of drones in agriculture, protection of the optimal balance between energy production, distribution, storage and consumption measures for the use of digital technologies in the process, implementation of smart calculators.
- *The "Infrastructure"* field, there are plans to ensure access to broadband internet, develop the 5G standard for mobile communications, expand the economic coverage of high-performance broadband networks, introduce regulations on
- In the field of *"Research and Innovation"*, measures are planned for the implementation of research in the field of cyber security aimed at the use of digital methods in research, research based on quantum physics and quantum technologies.
- *In the "Business"*, there are plans to improve conditions for startups (development of an electronic single window), digitization of the state procurement system, provision of consulting services related to digitalization to SMEs and implementation of training, among regional and local companies at the pan-European level. measures to improve the legal framework in order to ensure equal conditions of competition.

- the *"Employment and Jobs"* field, measures are planned for the development of the "Act of Recognition" regarding the improvement of digital skills of citizens, the acceptability of skills acquired through informal education.
- In the *"Education"* field, virtual educational college expansion activities are designed to provide the opportunity to learn anywhere, to provide science, technology, engineering and mathematics (STEM) specialists and experts, to provide teaching materials, to - strengthen the digital skills of educators, to provide lessons and the use of digital media and e-learning methods for children.
- *"Mobility and Transport"*, there are plans for the use of test environments for automated driving, the launch of laboratories for driverless railway systems, the introduction of legal regulations for the use of data for automated driving, as well as intelligent traffic management systems, real-time traffic information receipt measures.
- In the *"Media and Culture"* field, there are plans to ensure access to art and culture through the use of digital technologies, promote media literacy, expand digital services provided by cultural institutions, and limit hate speech in electronic media.
- *"Integration and Inclusion"*, measures are planned to support the acquisition of ICT and media skills for the elderly and people who do not have ICT knowledge, as a basis for digital participation, measures to improve foreign language access.
- *"Security, protection and trust"* In the field of cyber security, the creation of cyber defense situational centers, cyber security and intelligence, cyber documentation research centers, retraining of cyber detectives at all levels of government, implementation of general data protection regulations at the national level, "privacy by design" and "privacy by default" (data protection through technology and data protection through legal regulations) measures to develop and promote IT systems.
- In the field of *"Politics and Management"* there are activities planned to create citizen-government dialogue, "everything in one place", "non-stop(without application)" processes and platforms, improvement of electronic identification processes, "data-only-once" concept implementation methods.

Conclusion

- A comprehensive approach (whole-of-government approach) was not shown regarding the measures implemented in the field of digitization. Although digitalization strategy - *belongs to the Republic of Armenia*, the composition of the activities planned in the latter's action plan de facto turns it into a Ministry capacity development strategy.
- There are no measures, timetables, performance indicators and performers for the implementation of digital transformations in certain fields of the economy and public administration. Instead, segmental digitization strategies developed by certain entities.

Recommendation

Need for review Armenia's digitization strategy, defining initiatives, timelines, performance indicators, and performers for the implementation of digital transformation in individual segments of the economy and public administration.

Audit question - 3. Has the effectiveness been ensured during the implementation of the RA digitalization strategy?

The vision of the Republic of Armenia in the field of Audit and the directions and measures of strategic reforms in the period under consideration are described in the decision N183-L of the Government of the Republic of Armenia dated 11.02.21 "Armenia 2021-2025 - digitalization strategy management". The goal of the strategy is to ensure the digital transformation of the government, economy and society. The authorized entity for implementation of the strategy is the HTIM.

Audit criteria

, it is planned to implement 10 activities in the period covering the audit.

- Institutionalization of digitization (deadline: May 2021).
- Inventory of current digitization systems and analysis of digital indicators, definition of target indicators (deadline: May 2021).
- Development of digitization standards, formats and procedures (deadline: September 2021).
- Cloud infrastructure requirements/standards (deadline: September 2021).
- Establishing a National Cyber Security Center of Excellence (deadline: December 2022).
- Adoption of data policy concept (deadline: December 2021).
- A plan for access to broadband Internet and digital services (deadline: December 2021).
- Development of a single electronic project management platform (first phase deadline: November 2022).
- Identity authentication, authentication and email signature (deadline: September 2022).
- Update of the strategy according to the results of the first phase (deadline: December 2021).

Audit results

- Within the framework of the 1st strategic activity "Institutionalization of digitization", it was aimed to clarify the full powers, duties and responsibilities of digitization bodies. Until now, the concept of "digitization bodies" has not been defined by RA legislation. Although a document was drawn up by HTIM (not covered by any legal act), which states the powers of HTIM in the field of digitization, defined by legal acts, the powers, duties and responsibilities of other "digital authorities" are not specified. The implementation of this measure is of particular importance in the context of the operation of the " Hayastan Information Systems Agency" fund established by the CBA, taking into account the fact that the latter was not planned for coordination and with the aim of preventing possible institutional dichotomies in the issue of policy development and implementation.

- Within the framework of the 1st strategic activity "Institutionalization of digitalization", it was also aimed to form a digitalization professional body attached to the HTIM (-deadline: May 2021), which was not realized.
- "Inventorization of current digitization systems and analysis of digital indicators, definition of target indicators": In 2021 within the framework of this 2nd strategic activity by HTIM carried out inventorization of existing and developed platforms (services). According to the results of inventory, the number of platforms is 228, of which 12 are under development. At the same time, "EKENG" CJSC has been running the CatIS system since 2018, where information on digital platforms is recorded. It is worth noting that 77 operating digital platforms are registered in the CatIS system, - which is 139 less than what was written by the HTIM. The difference is caused by the lack of a common methodology for the inventory of digital platforms. In addition, the qualitative assessment of the current state of the inventoried and operating digital platforms, the definition of target indicators, and the assessment of the current level according to the established indicators, provided by this measure, were not carried out.
- "Development of digitization standards, formats and procedures" and "Development of appropriate cloud infrastructure requirements/standards" within the framework of the 3rd and 4th strategic measures it is planned to localize the following standards: (1) digitization processes and requirements design, (2) cyber security, (3) technical - requirements, (4) functionality and (5) cloud infrastructure (expiration: September 2021). Cyber security and cloud infrastructure standards have not been developed. Standards for the design of digital services (including the design of digitization processes and requirements, technical and functional requirements) have been developed, but have not yet been officially approved.
- HTIM has not conducted a study of existing digitization platforms that do not technically meet the established standards.
- HTIM did not study what kind of financial consequences the adaptation of currently operating digital platforms to localizing students would have, especially on the state budget's prospective.
- Framework of the 7th strategic measure "Data Policy Concept", it was aimed to develop a unified data policy concept (deadline: December 2021), which was not implemented.
- "Development of a plan for the access to broadband Internet and digital services" within the framework of the 8th strategic activity, it was aimed to develop a plan for the creation of access to broadband Internet and digital services by inventorying and mapping the existing and exploited fiber optic cables in the public and private sectors of the Republic of Armenia. networks, their capacities, analyzing demand according to regional distributions, highlighting technical problems and proposing appropriate solutions. In 2022 HTIM developed and published the draft decision "On approving the strategy and schedule of access to broadband Internet connection in the territory of the Republic of Armenia". It was submitted for consideration by the Government of the Republic of Armenia, which is still in the process of revision. This activity was not implemented within the specified period (December 2021).
- In the framework of the 9th activity "Electronic Program Management Platform", it was aimed to create a unified platform for project management, in the first phase of which,

in 2022. As of November, it was planned to create a prototype or at least a viable product. A tender was held for the procurement of "Technical task preparation consulting services for the creation of a unified electronic project management - platform", according to which the prototype was to be developed. The tender was held, but the procurement contract was terminated due to the lack of necessary financial means.

- "Person identification, authentication and e-signature" strategic activity was planned to be implemented within the framework of the grant program with the support of the EU, but it was not achieved. Currently, this event is being implemented within the framework of the Foundation established by the Central Bank. The following measures have been taken:
 - Ernst & Young was involved in the tender process, whose consulting group would provide the Government with a recommendation regarding the issue of new generation biometric passports and electronic cards.
 - The joint portal of electronic signatures was developed with the joint efforts of Estonian experts, EKENG and VXsoft.
 - Digital electronic identification system was developed.

This activity is not implemented in the specified date (September 2022). Following steps still should be taken:

- Finish the process of e-signature business modeling,
- Implement national e-identification system,
- Start to ensure massive application of the system,
- Complete the development of new generation biometric passports and e-card procurement package development.

Within 8th strategic activity, based on the results of the first stage, it was planned to review the main provisions, indicators, targets of the strategy and develop an updated (amended) version of the strategy (deadline: December 2021), which was not done.

Cause of audit findings:

- Issues related to the Strategic leadership, weak structures of internal control/ constant monitoring of the execution of the strategy.

As a result:

- Risks of institutional dichotomies of development and implementation of public policy in the given field have arisen due to the lack of clarification of the scope of "digitalization bodies" and their powers, duties and responsibilities.
- absence of a unified methodology for the inventorization of digital platforms does not provide an opportunity to find out the actual number of digital platforms (services) operating in the Republic of Armenia. In addition, the lack of criteria for qualitative analysis and evaluation of the current state of existing digital platforms does not

provide an opportunity to get a clue about how existing digital platforms solve the problems they face.

- the absence of officially approved digitization standards, risks have arisen that existing digital platforms will be developed on the basis of substantially different principles, which has a restraining effect on the protection of interoperability of digital platforms.
- In the absence of policies of data management necessary for decision-making based on data in the public sector, it is not possible to perform a unified approach in the - stages of collection, storage, processing, transfer, analysis and archiving of data created as a result of the provision of public services or internal operations.

Best experience

Regarding the data management policy

Digitized public administration relies heavily on digital data. Accordingly, the capabilities of digital data collection, storage, analysis and transmission are of essential importance from the point of view of government's decision - making and the quality of public services provided. Best experience provides the following steps:

- Create national master data registries (population, legal entities, land, vehicles, real estate and others) ¹⁵, which allow state bodies to use and exchange standardized data. For each main register, the scope of institutional responsibility for the processing, updating and updating of register data is defined. There is a legal requirement for all public authorities to use data from key registers instead of collecting and storing their own data.
- Establish a National Spatial Data Infrastructure (SDI) using a Geographical Information System (GIS). Although the RA digitization strategy does not provide for the use of the GIS structure, nevertheless, in accordance with the RA Government's decision N505-L dated 08.04.21, a strategic plan for the creation of an integrated cadastre was approved. The 3rd ten-day period of December should implement the introduction of GIS technologies, the implementation and integration of the cartographic module.
- Use artificial intelligence and big data analytics tools to make better decisions ¹⁶.
- Benefit from state membership of the Open Governance Partnership initiative by proactively publishing open data repositories and encouraging their use. Armenia - joined this initiative in September 2011. Since:
 - the portal of E-draft legal acts was created and publicized,
 - the ability to broadcast council meetings was introduced with the possibility of back-to - back communication and access to community services ;
 - an interactive budget was created in an open data format,
 - the journal system was introduced,

¹⁵ in RA State interoperability on the platform involved is 24 state electronic repository, however now he exists registers separated they are not.

¹⁶ in RA State of websites for applies is Google: Analytics: the tool ; It Edu 2 work on the platform " From Education: work " program of the ingredients one is

- A feedback system with citizens has been implemented regarding public services: <https://gnahatir.am/am/>, through which users can evaluate and express their opinion on the services provided by the bodies of the state administration system.

(The World Bank's "Government Digital Readiness Assessment Tool", Part IV, Section G: Data Infrastructures, Strategies, and Management).

In terms of technological infrastructures

Best experience implies:

- Develop a state digital complex system architecture.
 - The strategy of digitalization of the Republic of Armenia defined an activity for the development and achievement of the architecture of the state digital complex system (deadline: December 2022), which has not yet been implemented. This measure implies considering the state as a unified service provider e-gov platform and considering the state internal management system as a unified architecture, and state departments as subsystems.
- Develop an e-government interoperability or other metadata system with mandatory standards set for each government agency systems.
 - interoperability system (GIP) has been developed and implemented in RA, through which the existing applications of electronic services can be integrated - with various sources of information.
- Develop a service mechanism (Enterprise Service Bus), which will allow the integration of different data sources with different service applications.
 - There is no such mechanism in RA.
- Develop standardized application programming interfaces (APIs) for applications or online services.
 - They are not yet developed in RA.
- In the public sector, design and implement a secure digital network that connects all public entities to exchange services and data through a secure data center hub.
 - There is a tripartite agreement between MTS Armenia - EKENG - HTIM, on the basis of which governmental communication is ensured. The provision of services, as well as the works aimed at ensuring security, are carried out through MTS Armenia and EKENG CJSCs.
- Apply or be ready to apply breakthrough technologies (cloud services, Internet of Things, blockchain, AI, etc.).
 - Strategic measures have not yet been implemented in the direction of the use of breakthrough technologies in RA. There is potential for creating cloud infrastructures, but due to security factors, they are not implemented yet.
- There was widespread availability of electronic document circulation in the public sector.

- In 2007 "Mulberry" system of electronic passport circulation was introduced and is functioning in the RA public sector.
- Having a common digital management platform that acts as the primary interface for all planned digital or email for activities with mobile applications.
 - The e-gov.am platform is active, but there is no mobile application for using the relevant services.
- Availability of a call center / hotline to answer and address inquiries about government services.
 - There is no unified contact center and hotline in RA. However, digital systems have been implemented, such as e-request.am, a unified online request platform that acts as a communication tool between citizens and the government, e-citizen.am portal, through which citizens can digital data about them stored in the state database become available, the level of state interoperability.

(World Bank's "Government Digital Readiness Assessment Tool", Part IV, Section E. Technological Infrastructure).

Conclusion

Of the measures planned by the strategy within the specified period the RA digital transformation process did not achieve the targeted effectiveness.

Recommendations

- Legislatively clarify the concept of "digitization bodies" and confirm the scope of their powers and responsibilities, avoiding the possibility of creating institutional dichotomies related to the development and implementation of public policy in the field of digitization.
- Methodology for inventory of digital platforms, providing for the possibility of dynamic inventorization of platforms.
- Carry out an assessment of the financial consequences of adapting the existing digitization platforms to the expected digitization standards.
- Define quality analysis and evaluation criteria for digital platforms.
- Develop legislation defining data policies.
- In order to modernize the data exchange between public administration bodies and to promote the reliability of data, plan a geographic information system (GIS) implementation event.
- Set a legal requirement for government entities to use data from master registries instead of collecting and storing their own data.

- Develop a program to promote the use of advanced technologies (AI, big data analysis, etc.) in data analysis by state bodies, including the formation and development of human resource capabilities.
- Introduce a mobile application of the existing digital management platform, through which any user will be able to use digital data and electronic services with the possibility of unified identification.
- Strategically define measures for the implementation of innovative digital technologies (AI, big data, Internet of Things, blockchain) with the corresponding risk assessment.
- • Introduce internal accountability/monitoring processes for the strategy execution process.

Audit question - 4. Is effective budgeting of the digitization process ensured in RA?

In the RA state budget, the main budgetary program under the responsibility of the HTIM, aimed at the goal of digitalization, is the program "1043 - high-tech industry ecosystem, digitalization and market development".

Audit criteria

- Budget programs are logical groupings of state policy implementation measures aimed at achieving the same goal (*Order of the Minister of Finance of the Republic of Armenia dated 23.01.17 "On approving methodological guidelines within the framework of the - strategy for the full implementation of the budgeting system of the Republic of - Armenia" N311-A (hereinafter referred to as "Guidelines"), appendix 1, item 4, and item 4.1).*
- RA laws and officially adopted strategies are the main documents that define the government's policy and provide the necessary foundations and direction in the budget process for sectoral issues, goals, final results, strategic directions of state - intervention and for priority setting (*Guidelines, Annex 1, Clause 4, Sub-Clause 4.1).*
- The programs and the measures included in them should be closely related to the specific goals of the state. When defining the purpose of the project, one main goal should be fixed, avoiding multiple objectives and extensive statements (*Guidelines, Annex 1, Clause 4, Sub-Clause 4.1, Clause 11, Sub-Clause 23).*
- One of the statutory functions of HTIM is to ensure the process of design, development and implementation of digitization and electronic management systems implemented in RA state bodies (*Article 11, sub-item 40 of the Code of Civil Procedure).*
- It is one of the statutory functions of HTIM to ensure the effectiveness and safety of electronic management systems and information exchange processes used by RA state administration bodies, as well as support for the formation of priorities and goals (*Article 11 of the Statute, Article 41).*
- It is one of the statutory functions of HTIM is the support to high-tech, digitization, cyber security, innovative technologies, network (internet) international lending organizations' financing programs (*Statute, clause 11, sub-clause 23).*
- HTIM, guided by the priorities set by the Government of the Republic of Armenia, plans to implement the digital transformation (digitization) of the Government of the Republic of Armenia, the economy and society: the introduction of innovative - technologies, cyber security, data policy, electronic implementation and development of applications and electronic management system, coordination of digitization processes, creation of common standards and digitized environment, as well as development of initiatives for the use of digital technologies in the private sector of the economy and programs promoting the use of electronic tools by society and (*Introduction to Strategy Annex 1).*
- The authorized body for the implementation of Armenia's digitization strategy is HTIM (*Paragraph 1 of Section 5 of Strategy Annex 1).*

Audit results

- There is no budget program that is a systematic grouping of government policy implementation measures aimed at achieving the strategic goal of digital transformation. The "1043 - BTA Ecosystem, Digitization and Market Development" program of the RA Government Budget mainly consists of some initiatives implemented by HTIM, which do not include the entire spectrum of state interventions aimed at the realization of the goal of digital transformation.
- A number of budgetary measures related to digital transformation are also responsible for other departments different from the Ministry of Education. For example:
 - Implemented by the RA Prime Minister's Office:
 - Within the framework of the "1018 - Modernization of the State Sector" program "11001 - Third State Sector Modernization Program supported by WB", it is planned to introduce the Electronic Notary System and the electronic system of the service ensuring due execution.
 - 32001 - Acquisition of electronic management systems and equipment within the framework of the third project of the state sector modernization implemented with WB support, it is planned to implement the electronic management systems of the Anti- Corruption Commission and th RA Police.
 - Implemented by the RA Ministry of Justice:
 - planned to implement the Anti-corruption Committee's electronic database within the framework of the "31007 - Ensuring plans for the creation or modernization of electronic resources" program of the "1228 - Development of anti-corruption policy, coordination of programs and implementation of monitoring".
 - of the "1120 - Penitentiary Services" program "31003 - Capacity development and provision of technical training of the Probation Service of the RA Ministry of Justice" measure, it is planned to introduce an electronic surveillance system.
- Functions of ensuring the process of design, development and implementation of digitization and electronic management systems implemented in the RA state bodies, assigned to the HTIM, were not actually implemented.
- Procedures for the selection of high-tech, digitization, cyber security, and innovation technology projects seeking financing from international lending organizations were not carried out.
- The electronic management systems and information exchange processes used by the RA state administration bodies, as well as supporting the formation of priorities and goals has not been implemented.

The main audit findings are:

- The non-comprehensiveness of the digitization strategy, the absence of sectoral - digitization measures.
- The Ministry's lack of initiative in preparing a comprehensive budget plan related to digitalization at the stage of preparing budget requests.
- weak system of internal control regarding the performance of statutory functions.

As a result:

- No effective mechanisms to assess the priorities of digitalization needs of platforms in the public sector.
- The effectiveness of the assessment of financing needs is limited.
- No capabilities to assessing the compliance of the digital platforms envisaged by the authorized body with the unified digitization policy / standards /requirements at the stage of budget planning.

Conclusion

- Budgeting in the field of digitalization has not been shown an approach that corresponds to the structural regulations of program budgeting.

Recommendation

- During the preparation of the 2024 budget application, guided by program budgeting guidelines, take steps to develop a budget program that will be a logical group of measures for the implementation of the state policy aimed at achieving the strategic goal of digital transformation in RA, designating HTIM as the entity responsible for the implementation of the project, and other entities as co-implementers.
- Sign a memorandum of understanding with the Central Bank, reflecting the mid-term/long-term commitment regarding the implementation of financial investments in the field of digitalization, clearly indicating the directions to be financed by the Central Bank, in order to increase the effectiveness of the consideration of budget applications.

RECOMMENDATIONS

to the RA Government

1. Review Armenia's digitization strategy, defining initiatives, timelines, performance indicators, and drivers for the implementation of digital transformations in individual sectors of the economy and public administration.
2. Sign a memorandum of understanding with the Central Bank, reflecting the mid-term/long-term commitment regarding the implementation of financial investments in the digitization process, clearly indicating the directions to be financed by the Central Bank, in order to ensure efficiency at the stage of consideration of the budget applications.

To the Ministry of High-Tech Industry

Cyber security

1. Legislatively regulate the field of cyber security, including defining the CII and legal relations related to ensuring their protection.
2. Develop and implement the legal framework of the cyber security sphere in such a way that it forms prerequisites for ensuring at least the conditions listed below and determining the conditions for their implementation;
 - 2.1. Identifying CII and keeping their scope up-to-date.
 - 2.2. Maintaining an up-to-date (constantly updated) national register of CII.
 - 2.3. Flexible procedures for setting cyber security goals specific to each of the CII, adequate to the needs arising in the given period.
 - 2.4. Existence of institutional structures of internal and external control in order to ensure policy requirements established for the protection of CII.
3. Develop cyber resilience plans aimed at ensuring the digital continuity of RA.
4. Localize and establish cybersecurity standards and other basic requirements.
5. Plan and conduct cyber exercises in response to pre-determined plans in the event of an emergency or incident. for the evaluation of the capacity to act accordingly, the identification of the problems and the planning of measures aimed at their elimination, involving the private sector in the planning of the exercises.
6. the formation and existence of national, state, and sectoral computer emergency response teams (CERT), defining their communication mechanisms with the national agency responsible for cyber threats.

Human resources management

7. Include minimum qualification requirements in the job descriptions of employees engaged in the provision of digital services in the public sector.
8. Based on the established requirements, to carry out an assessment of the provision of qualified staff and the needs of such human resources according to the departments.
9. Develop staff training programs based on assessment results.
10. Setup institutional mechanisms for ensuring the interaction of stakeholders on issues and projects related to digitalization, with the involvement of representatives from all relevant bodies.

Strategic management

11. Legislatively clarify the concept of "digitization bodies" and fix the scope of their powers and responsibilities, avoiding the possibility of institutional conflicts related to the development and implementation of the state policy in the field of digitization.
12. Implement methodology for the inventory of digital platforms, providing for the possibility of dynamic inventorization of platforms.
13. Carry out activities to analyze the inconsistencies of existing digitization platforms with the expected digitization standards.
14. Estimate financial costs of bringing the existing digitization platforms in line with the expected digitization standards.
15. Set criteria for qualitative analysis and evaluation of digital platforms.
16. Develop legislation defining data policies.
17. In order to speed up the exchange of data between public bodies and to promote the reliability of data, plan a geographic information system (GIS) implementation measure.
18. Establish a legal requirement for government bodies to use data from master registers instead of collecting and storing their own data.
19. To develop a program to promote the use of advanced technologies (AI, big data analysis, etc.) in the field of data analysis by state bodies, including the formation and development of human resource skills.
20. Introduce a mobile application of the existing digital management platform, through which any user will be able to use digital data and electronic services with the possibility of unified identification.
21. Strategically define the implementation of digital innovative technologies (AI, cloud, big data, Internet of things, blockchain) with appropriate risk assessment.
22. Introduce internal accountability/monitoring processes for the strategy execution process.

Budgeting

23. During the preparation of the budget application for 2024, following the program budgeting guidelines, take steps to develop a budget program, which will be a state policy aimed at achieving the strategic goal of digital transformation in RA. the logical grouping of the measures for the implementation of the national policy, as the responsible agency for the implementation of the program, with the responsibility of the Ministry, and field entities as co-implementers.

24. On the basis of the above-mentioned recommendations presented in the current conclusion, develop and by order of the Minister approve an activity plan, which will contain the responsible unit(s) for each activity and the schedule.