Republika e Kosovës
Republika Kosova
Republic of Kosovo

Zyra Kombëtare e Auditimit
Nacionalna Kancelarija Revizije
National Audit Office

Audit Report on Information Technology

E-KOSOVA ONLINE SERVICES PLATFORM

Prishtina, August 2025

The Auditor General of the Republic of Kosovo is the highest institution of economic and financial control, to which the Constitution and the Law [1] guarantee functional, financial and operational independence.

The National Audit Office is an independent institution, which assists the Auditor General in carrying out his/her duties. Our mission is to contribute effectively to public sector accountability through quality audits, by promoting public transparency and good governance, and fostering economy, effectiveness and efficiency of government programs to the benefit of all. We are thus building confidence in the spending of public funds and play an active role in securing the taxpayers' and other stakeholders' interest in increasing public accountability. The Auditor General is accountable to the Assembly for the exercise of the duties and powers set out in the Constitution, the Law, the by-laws and international public sector auditing standards.

This audit was conducted in accordance with the International Standards of Supreme Audit Institutions (ISSAI 3000[1]) and the Guidance on Auditing Information Systems (GUID 5100[2]).

Information technology audits undertaken by the National Audit Office are an examination and review of Information Technology systems and related controls to obtain assurance on the principles of legality, efficiency[3], economy[4], and effectiveness[5] of information technology systems and related controls.

The Auditor General has decided on this audit report "e-Kosova Online Services Platform" in consultation with the Assistant Auditor General, Myrvete Gashi Morina, who supervised the audit.

The audit team consisted of:

Samir Zymberi, Director of the Audit Department;
Poliksena Berisha, Team Leader;
Gazmend Lushtaku, Team Member;
Atdhe Gashi, Team Member; and
Gëzim Krasniqi, Team Member.

NATIONAL AUDIT OFFICE – Address: Rr. Ahmet Krasniqi no. 210, Lagjja Arbëria, Pristina 10000, Kosovo
Tel: +383(0) 38 60 60 04/1011
http://zka-rks.org

[1] Law 05_L_055 on the Auditor General and the National Audit Office of the Republic of Kosovo
[1] AISS 3000 – Standards and guidelines for performance auditing based on ONAIS Auditing Standards and practical experience
[2] GUID 5100 – Guide to auditing information systems issued by INTOSAI
[3] Efficiency – The principle of efficiency means getting the most out of available resources. It is about the relationship between the resources employed and the results delivered in terms of quantity, quality and time.
[4] Economy – The principle of economy means minimizing the cost of resources. The resources used must be available on time, in the right quantity and quality, and at the best price.
[5] Effectiveness - The principle of effectiveness implies meeting the predetermined objectives and achieving expected results.

TABLE OF CONTENTS

List of abbreviations

CRA	Civil Registration Agency
AIS	Agency for Information Society
CAAT	(Computer assisted audit techniques)
DDoS	Distributed Denial of Service
KIPA	Kosovo Institute for Public Administration
IRK	Institutions of the Republic of Kosovo
ISO/IEC	(International Organization for Standardization/International Electrotechnical Commission)
RWC	Regional Water Company
MESTI	Ministry of Education, Science, Technology and Innovation
MFLT	Ministry of Finance, Labour and Transfers
MIA	Ministry of Internal Affairs
SDC	State Data Centre
ISDSFP	Information System of the Department for Social and Family Policy
SSL	Secure Socket Layer
IT	Information Technology

Executive summary

The Government of Kosovo has created the "e-Kosovo" platform as one of the developments to improve the provision of public services and increase the efficiency of the administration. This platform aims to facilitate citizens and businesses' access to public services through electronic services, reducing the costs and need for physical presence at counters.

The e-Kosovo platform is one of the systems of state importance, also classified at the national level for its importance, managed by the Information Society Agency. It currently offers 230 public services electronically and serves as a unique gateway for access to services from various institutions, contributing to the transparency and modernization of public administration.

The National Audit Office has conducted an audit of Information Technology with the focus of the audit on the services of this platform: "Child benefits", "Property Tax", "Textbooks subsidy" and the "Electronic Payments" module to assess whether the implementation of the e-Kosovo platform enables citizens to provide efficient electronic services in an accurate, secure and reliable manner.

The e-Kosovo platform has made significant progress in the digitalization of public services, improving access, transparency and efficiency in their provision to citizens and institutions. Steps have been taken to establish technical protection mechanisms and to preserve data and audit trails, which constitute an important basis for the sustainable development of the platform. However, to provide safe and reliable functioning, it is necessary to address existing deficiencies in internal controls, especially in aspects related to Outsourcing, systems development, as well as data control and information security.

The Information Society Agency has not established sufficient standards for contract management, in order to prevent uncertainties in responsibilities for information security. The contracts for the development and maintenance of this platform have not sufficiently addressed the clauses for data protection and response to security incidents. The emergency service ***on the e-Kosova platform have been developed in an unplanned manner and outside standard procedures for documenting software development and technical design***. The service has been developed with accelerated decision-making, without proper documentation, clear technical criteria and an active contract for textbooks subsidies, jeopardizing the quality of the solutions and the fulfilment of their functional objectives.

The AIS does not sufficiently guarantee a secure information environment due to the lack of updated policies and operational guidelines for access and incident management. There are outdated policies and insufficient measures to raise staff awareness, while a complete regulatory infrastructure that addresses information protection in a sustainable manner is missing.

The AIS is not prepared to restore services in cases of emergency or disaster, jeopardizing the continuity of electronic state operations. A documented and tested disaster recovery plan is missing; there are no functional backup centres, while existing backups are insufficient for safe and timely recovery. ***The lack of functional and technical controls in the applications of the e-Kosova platform has created risks to the accuracy of data and the integrity of services***. Deficiencies have been identified in the interconnection of systems for verifying criteria, processing data without technical validations, as well as insufficient controls that have resulted in duplicate applications and repeated payments.

The e-Kosovo platform faces serious shortcomings in application controls, which affect the integrity, accuracy and security of data. For services such as "Child benefits" and "Textbooks

subsidies", the lack of interconnection of systems for verifying criteria such as "residence" has allowed benefits to be received without meeting the necessary conditions. The interconnection of the Child benefit service with the internal system of the MFLT has led to duplicate applications and difficulties in managing the payments. The lack of real-time payment status updates and weak controls in the payment module have allowed the same payments to be executed multiple times, creating financial consequences for citizens.

Although the platform provides a unique and identifiable trace for each transaction, the lack of active and periodic monitoring due to limited human capacity and the lack of standardized procedures limits the ability to identify unauthorized interventions and suspicious activities in a timely manner.

Therefore, the risks identified above indicate that the Information Society Agency, the Ministry of Finance, Labour and Transfers, and the Ministry of Education, Science and Innovation that administer and provide services through the e-Kosova platform need further improvements, in order to ensure data protection and the uninterrupted functioning of digitalized services. In this regard, we have issued a total of 16 recommendations, of which 14 recommendations for the Information Society Agency and 2 recommendations for the Information Society Agency in coordination with the Ministry of Finance, Labour and Transfers and the Ministry of Education, Science, Technology and Innovation. The list of recommendations is presented in Chapter 5 of this report.

Response of the auditees

The Ministry of Internal Affairs and the Agency for Information Society have agreed with the audit findings and conclusions and have committed to address the recommendations given. Meanwhile, we have not received any response from the Ministry of Finance, Labour and Transfers. We encourage the auditees to make every effort in addressing the recommendations given.

1 Introduction

The e-Kosovo Platform is the main state platform where public services found in the offices and physical counters of institutions are provided electronically to citizens, businesses and public administration employees themselves.

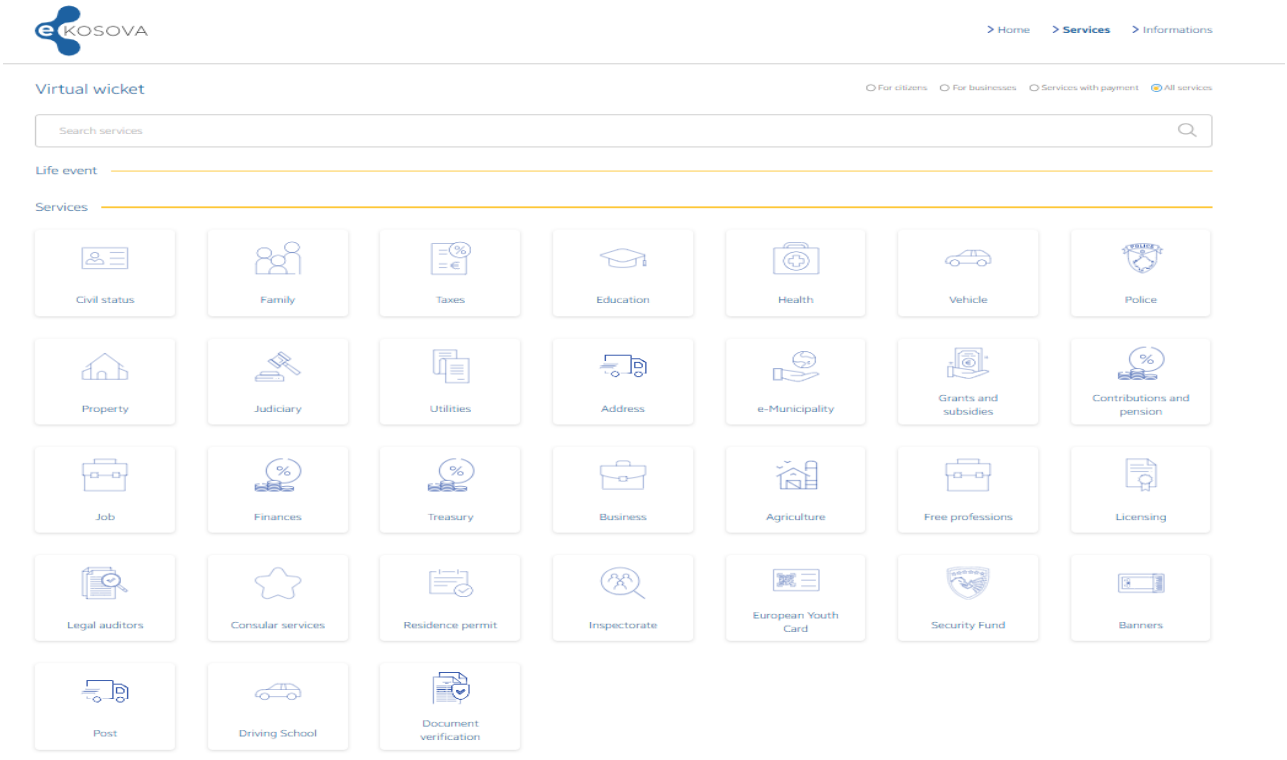
So far, this platform offers around 230 services in electronically, out of 658 central services and 100 local services for each municipality, which are provided physically and electronically.

The e-Kosovo Platform is managed and administered by the Information Society Agency. The AIS was established as an executive government agency within the ministry responsible for public administration, or at the highest state administration authority established by the Government and which is now the Ministry of Internal Affairs.

In 2013, the Assembly of the Republic of Kosovo adopted Law 04/L-145, based on Article 65 (1) of the Constitution of the Republic of Kosovo, on Governmental Bodies of the Information Society, which defines the AIS as the main body for the development and implementation of services in the field of Information and Communication Technology in all institutions of the Republic of Kosovo.

In addition to the services that are developed on this platform, other electronic services are also interconnected through the Interoperability Platform (interaction) and direct connections, which are managed by other institutions, but offer their services through e-Kosova as a single electronic gateway for citizens.

The services offered in e-Kosova are divided into 25 categories, which are presented in the following picture.



Picture 1. Categories of services in e-Kosova

These services facilitate administrative processes and provide faster and easier access for citizens. Among the most used categories of services on this platform are Family and Taxes. In the family category, the most used service is the child benefit service, while in taxes, the property tax service.

The most used services on the e-Kosova platform, which are characterized by a significant monthly financial turnover, are "Child benefits" and "Property Tax". Property Tax is a service integrated by an external back-end system, which, in addition to being widely used by citizens, also contains a payment component, thus increasing sensitivity to possible risks. Also, the Textbooks subsidy service has been included due to issues raised/related to the e-Kosova Platform during the audit process. Therefore, the National Audit Office has focused its audit scope on these service categories, to address key issues in the functioning of the e-Kosovo platform, and has planned that the next audit in the field of information technology will focus on the property tax system.

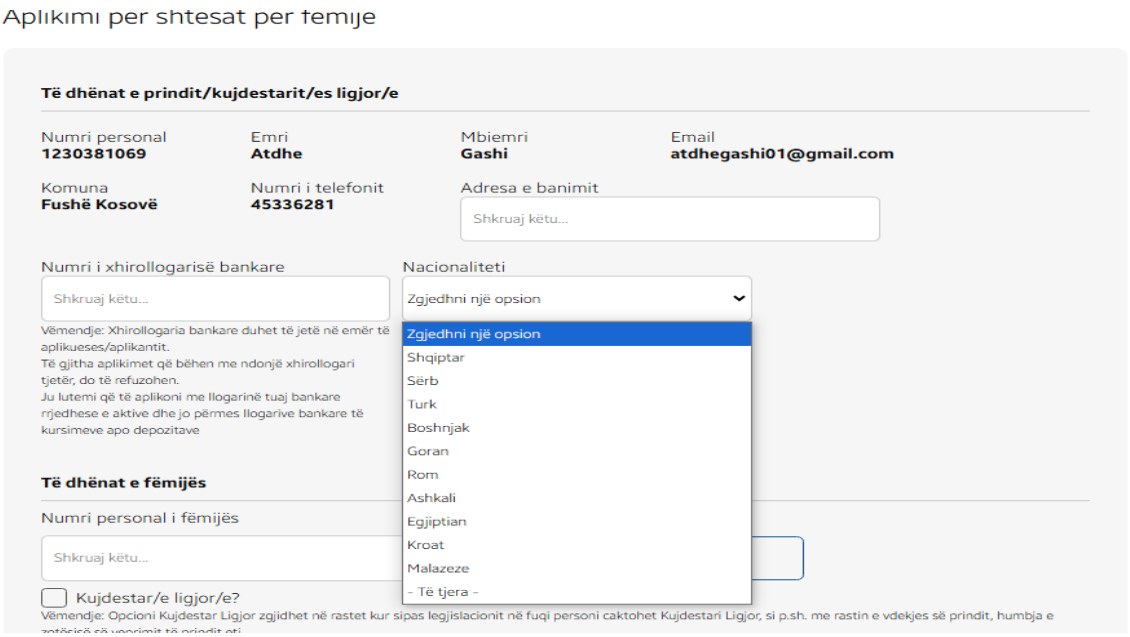
Picture 2. Use of services in e-Kosova

Therefore, we will address these services in more detail below, analysing the processes.

Child benefits

The Child benefit Program is designed to be implemented gradually, covering the age group from 0-16 years.

Parents or legal guardians can apply for child benefits through the electronic platform e-Kosova. The application is made online by following the steps below, as shown in Picture 3:



Picture 3. Application for child benefits

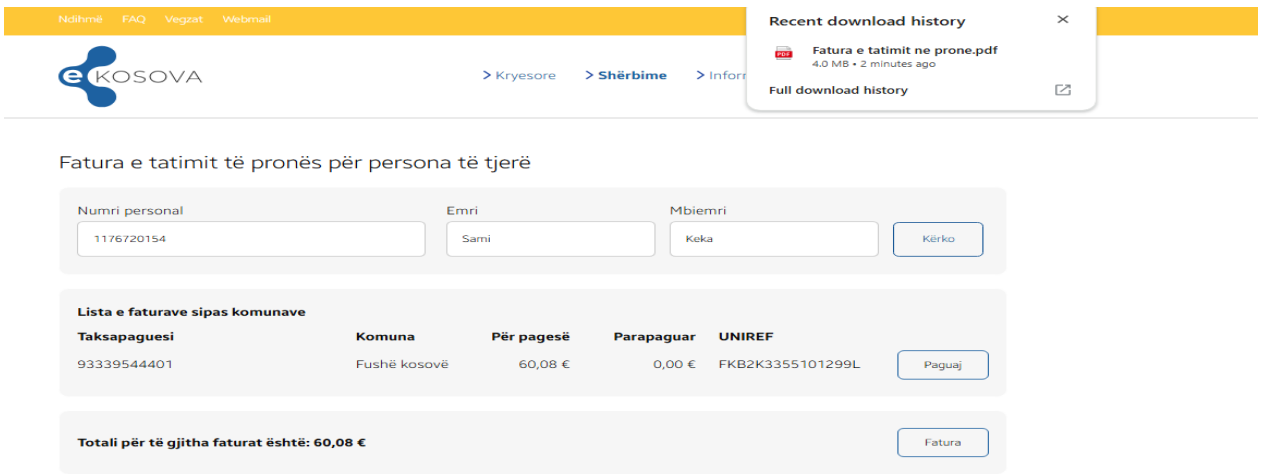
Allowance payments are made every month, usually on the 25th or the following working day, to the bank account of the parent or guardian who has applied. The deadline for applying for child benefits is open from the 01st to the 10th of each month (application is made only once, then the allowance is applied every month until the criteria are met).

Property tax

Property tax in Kosovo is an annual obligation imposed on immovable property, including land and buildings. This tax is an important source of revenue for municipalities and is used to finance local public services.

The tax is imposed on all immovable property, including land and buildings, regardless of their use (residential, business, agricultural, etc.).

The following Picture shows how to download a property tax invoice.

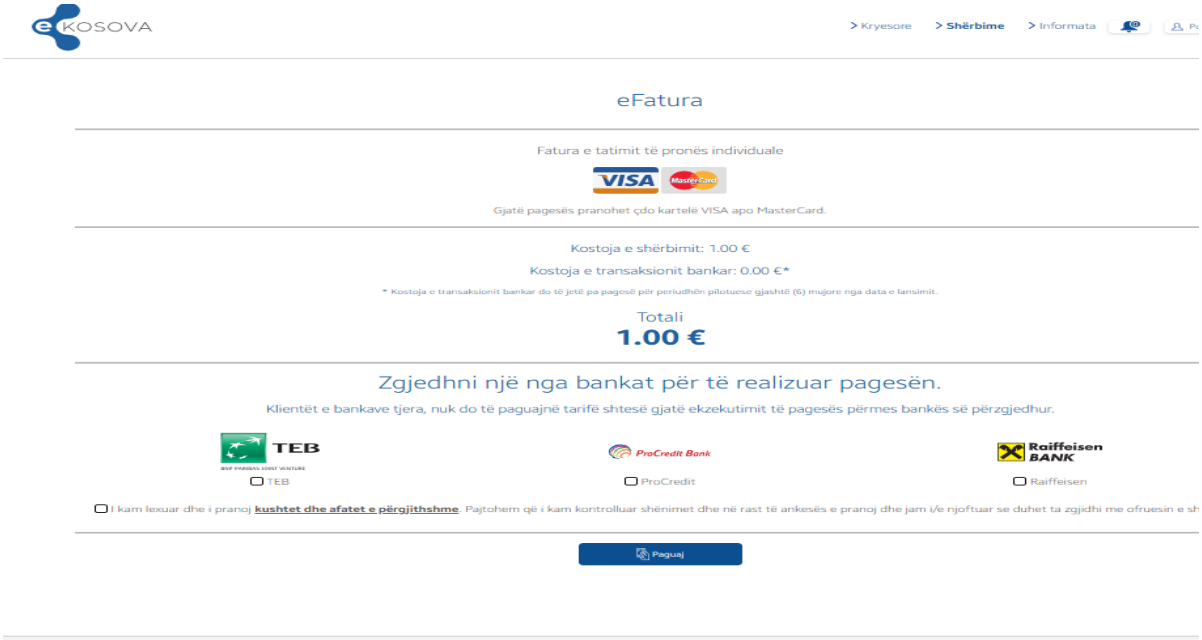


Picture 4. Property tax invoice

Electronic payments through e-Kosova

The eKosova Payment Gateway component represents the web application that is used as an intermediary between e-Kosova and various bank systems for the purpose of initiating and controlling payments, which is one of the most sensitive modules for the citizen and information security.

All services that make payments use this module. After clicking on the "Pay" option in any service that contains a payment, the payment module opens as in the following Picture.



Picture 5. eInvoice for making an electronic payment in eKosova

As shown in picture 4, the Electronic Payments module displays all payment data, including information about "Processing Banks."

Data security in e-Kosova

The mechanisms that have been implemented to provide security in all components of the e-Kosova platform are through firewalls, maintaining audit trails and authentication mechanisms.

2 Audit objective and areas

The objective of this audit is to assess whether the implementation of the e-Kosova platform enables citizens to provide efficient electronic services in an accurate, secure and reliable manner.

With this audit, we aim to provide relevant recommendations to MIA, AIS and the responsible entities in order to improve the information system regarding information security and application development and controls.

To respond to the audit objective, we focused on the area of information security and application controls, as well as issues related to Outsourcing policies and business continuity by selecting the audit areas as follows:

Table 2: Audit areas and issues

Audit areas	Audit issues
1. **Outsourcing**	1. Security
2. Acquisition and development	2. Analysing, prioritizing and managing requests
3. Information Security and Cybersecurity	3. Communications and Operations Management
	4. Intrusion Detection and Protection System
4. Business Continuity Plan – Disaster Recovery Plan [6]	5. Organization's Business Continuity Policy and Plan
5. Application Controls	6. Access controls
	7. Processing controls
	8. Logout data controls
	9. Application security controls

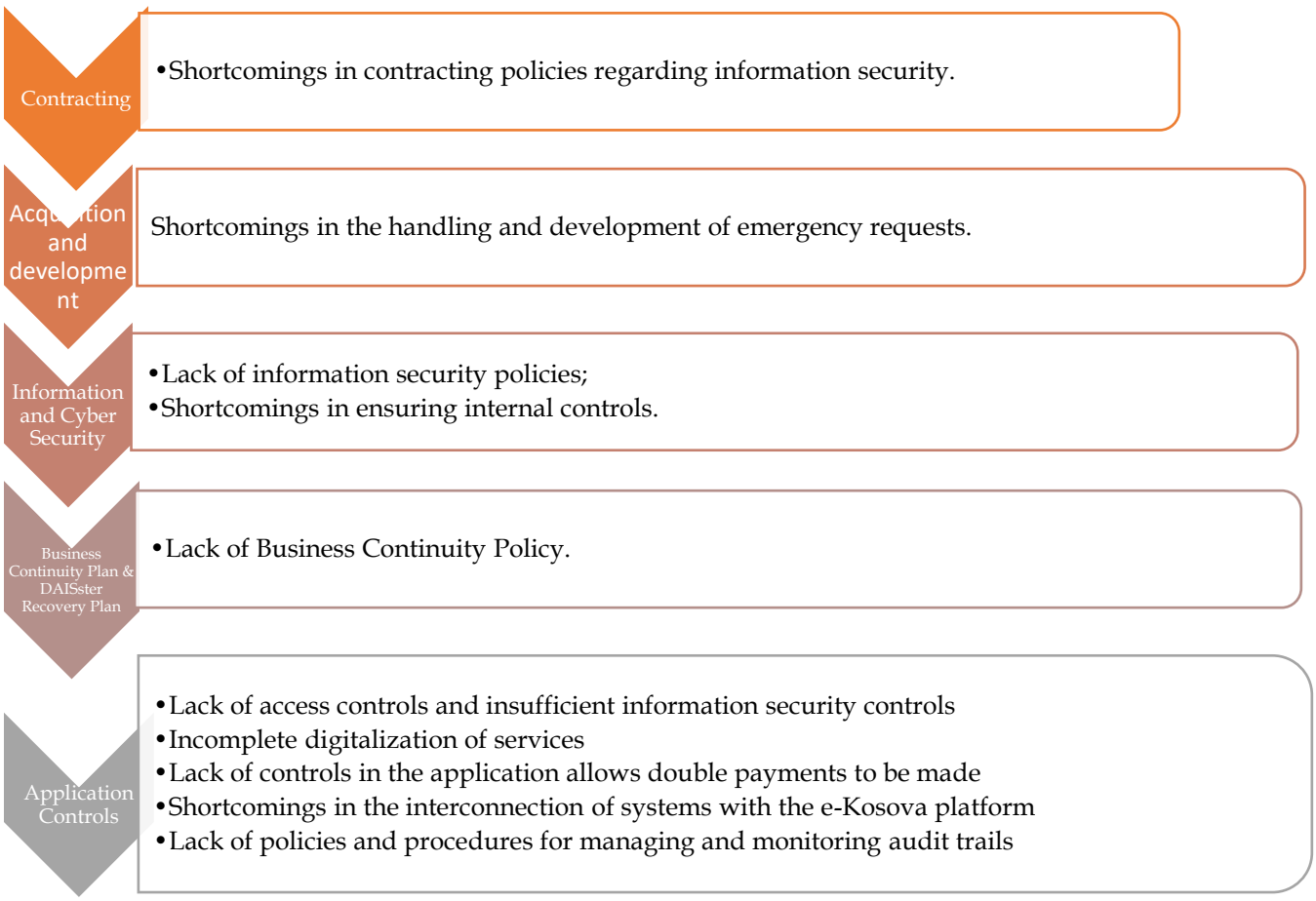
The scope of this audit is the Ministry of Internal Affairs, namely the Agency for Information Society and the departments responsible for the administration, management and security of the e-Kosovo platform. It also includes the relevant units within the Ministry of Finance, Labour and Transfers, namely the Department for Property Tax and Social Schemes Management, which administer the relevant services on the e-Kosovo platform, such as property tax services and child benefits. The audit covered the period from January 2024 until the end of the audit, reviewing the functioning and provision of these services through the e-Kosovo platform. Another separate audit is being conducted for the Property Tax System. In addition, in 2023, the NAO published the information technology audit report "Project Management for Information Technology Systems in the Information Society Agency" where a part of the e-Kosovo platform was included in the audit related to the development and management of the project.

6 BCP & DRP – Business Continuity Plan & Disaster Recovery Plan

3 Audit findings

The e-Kosova platform, by providing around 230 electronic services, has achieved significant progress in the digitalization of public services for citizens. However, alongside the development, several shortcomings have been identified that require improvement, which are presented in this chapter of the report.

The audit findings relate to Outsourcing policies, development requirements, information security controls and management, business continuity plan and application controls of the e-Kosova platform. The findings are structured according to audit areas and issues.



Picture 6. Structure of audit issues of the e-Kosova platform

First part presented in chapter 3.1 covers the issues identified for improvement related to information systems outsourcing (1).

Second part presented in chapter 3.2 covers the issues identified related to development and acquisition (2).

Third part presented in chapter 3.3 covers the issues identified related to information and cybersecurity (3-4).

Third part presented in chapter 3.3 covers the issues identified related to business continuity planning and disaster recovery planning (5).

Fourth part presented in chapter 3.4 covers the issues identified related to application controls (6-10).

3.1 Outsourcing policies

Organizations must have some policies that determine which functions can be contracted and what functions should be developed in the premises of the organization. Outsourcing services in the organization requires close monitoring and is subject to privacy and security requirements[7].

Contractual processes, AIS develops under the legislation in force, but there are deficiencies in incorporating information security during Outsourcing.

Picture 7. Outsourcing Policies (System, Policies and Information Security)

1. The contract does not sufficiently address information security aspects

The organization's security requirements should be appropriately addressed by the contractor. The agreement with external parties that involves access, processing, communication or management of the organization's information or information processing structure, or the introduction of products or services into the information processing system, complies with all appropriate security requirements.[8]

The analysis of the contract and accompanying documentation shows that the content of the contract does not address the information security part. Elements related to information security are mentioned only in the tender dossier, but not in the basic contract.

Furthermore, clauses that determine how data privacy will be maintained and who is responsible in the event of information compromise or any security incident are not included.

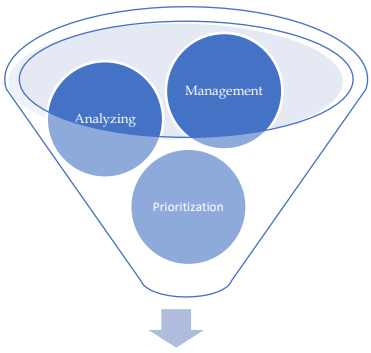
[7] Information Technology Audit Manual, Contracting Policies
[8] Information Technology Audit Manual – Contracting, Security

Based on the existing documentation and current practice, the main focus of the agreement is the technical and functional aspect of the system. Meanwhile, due to the lack of standardized policies, information security is not foreseen in the agreement. For Outsourcing, the AIS refers to the procurement law, which does not foresee a specific policy on information security, but is described only in general form.

The lack of information security treatment and shortcomings in Outsourcing policies jeopardize the security of contracted systems and in the event of an information security incident, there is no possibility of identifying the responsibility of the parties to the contract, as well as monitoring and reporting the incident.

3.2 Acquisition and Development

Development, procurement and outsourcing ensure that requirements management, analysis and prioritization continuously support the optimal fulfilment of user needs for the development of services on the e-Kosova platform.[9]



Picture 8. Development requirements management

2. *Shortcomings in handling emergency requests for the digitalization of the Textbooks subsidy service on the e-Kosova platform and the service is not fully electronic*

The AIS must analyse, prioritize, and manage requirements to ensure that user needs are met in an optimal and cost-effective manner.[10] *Application transactions are executed in accordance with expected behaviour.* [11]

AIS for the development of electronic services on the e-Kosova platform, in addition to planned services, also develops services with emergency or accelerated requests that are handled outside the standard procedures and planning document.

In 2023, the "Service for subsidizing books upon request from MESTI" was developed in an accelerated form. This request was made without technical specifications and outside the usual planning procedures. Moreover, at that time, AIS did not have an active contract for the

[9] Information Technology Audit Manual, Development, Procurement and Outsourcing.
[10] Information Technology Audit Manual – Acquisition and Development
[11] Information Technology Audit Manual – Application Controls, Processing Controls

maintenance and development of the e-Kosova platform, therefore the necessary documents and analyses to ensure the quality of this service were missing.

The technical details and criteria for this service were only discussed in verbal meetings and were not documented. Even in 2024, this service was activated immediately through a request without any change from the previous year.

AIS does not follow standardized procedures for urgent requests, because there is no written process for their handling. Meanwhile, requests for the development of the service have come without relying on technical analysis from the professional staff of the requesting ministry, in this case from MESTI.

Without prior analysis and clear criteria, the digitization service may not meet the needs of citizens. In this case, people who do not belong to or do not qualify for the Textbooks subsidy have benefited.

Furthermore, the Textbooks subsidy service on the e-Kosova platform is not fully electronic. Any other information after the citizen's application is handled outside this platform, manually by the final institution (MESTI).

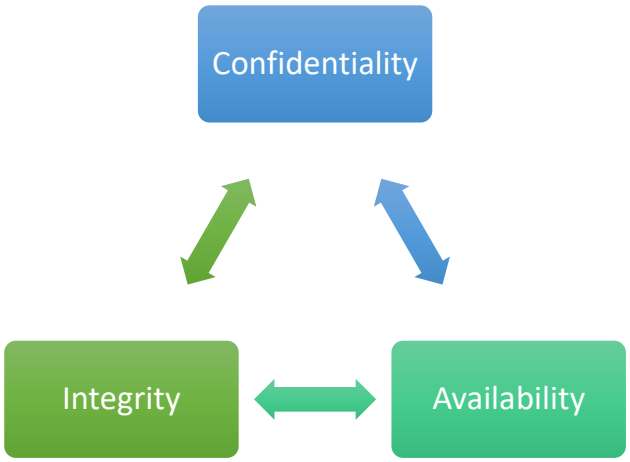
The lack of analysis for the development of a service and the lack of adequate cooperation between AIS as the implementer and MESTI as the requesting and determining unit of criteria has made the development of the electronic service ineffective and its full digitalization has not been achieved by not providing complete and accurate information.

This way of organizing and deploying services negatively affects the effectiveness, security and reliability of the services provided to citizens as well as the advancement and interconnection of this platform with other systems.

Note: The funding/subsidy of textbooks has been audited by the financial audit team and the findings regarding this issue including the financial impact are presented in the Audit Report on the Annual Financial Statements of the Ministry of Education, Science, Technology and Innovation for the year 2024.

3.3 Information Security

Information security is one of the fundamental aspects of IT governance to ensure the availability, confidentiality and integrity of data. For better information security management, the institution must establish mechanisms to enable the management of security-related risks, taking appropriate measures and ensuring that information is available, usable, complete and uncompromised.[12]



Picture 9. Principles of information security

3. AIS operates without an updated and approved information security policy

The AIS should ensure that defined information security policies exist and are approved, communicated and implemented within the organization. Policies should be reviewed regularly or when there are significant changes in the organization, technology or applicable laws[13]. Policies and procedures should form a consistent management environment for internal and external communications. [14]

In 2010, the AIS had drafted information security policies that met the organization's requirements at the time, with which the policy had operated until 2021. These policies were repealed by a decision of the Government. However, they still continue to use the repealed policies as practice, in the absence of their updating. They have not even drafted information security procedures and operate without any regulatory support. Therefore, the developments that have occurred in the AIS and in the field of information security at a global level from 2010 to 2021 have not been reflected in the relevant information security policies. Therefore, AIS does not have an approved and effective information security policy. Although policies and procedures are lacking, the Office of the Prime Minister and the Ministry of Interior, with the support of external institutions and stakeholders, have drafted the 2023–2027 E-Governance Strategy. Its goal is to accelerate e-governance in Kosovo by improving the existing system, adding new functions and using modern practices and technologies. In addition, the AIS has taken protective measures, technical applications and configurations in information systems to protect security from cyber threats.

[12] Information Technology Audit Manual, Information Security.
[13] ISO/IEC 27002:2022 – Information Security Policies
[14] Information Technology Audit Manual - Information and Cybersecurity, Communications and Operations Management

AIS was waiting for the legal basis and, by the end of 2024, the Law for the Creation of the Legal Basis for the Issuance of Sub-Legal Acts by the Government and Ministers[15], which also provides for the issuance of the Regulation on Information Security.

The repealed and outdated security policy, as well as the lack of new guidelines on security practices, leaves employees uninformed and unable to protect the organization effectively and makes the organization more vulnerable to cyber-attacks and the strategy and any other cybersecurity initiatives less effective.

4. AIS has shortcomings in internal controls

The organization must ensure that intrusions are detected and will be detected and combated[16]. The organization must ensure that appropriate measures are in place to prevent, detect and recover from malicious code threats through policies, technical controls and user awareness[17]. The Information Society Agency must take care of the security and protection of electronic infrastructure and data and coordinate activities for the security of IT services.[18]

Technical security applications are implemented by AIS at the level of dedicated protection devices, which are configured to provide advanced protection against intrusions. It also produces written reports on cybersecurity incidents in the ASI's IT infrastructure. However, AIS does not have a written procedure for preventing intrusions.

In addition to the lack of procedures, there are no documents that specify which server or platform ports are allowed or prohibited for access. Although, access to ports is determined according to the technical and software requirements of the institutions.

They also do not produce specific documentation for protection against intrusions, but information on the level of access is stored in the relevant devices that manage security. The same practice is also carried out for the e-Kosova platform.

Furthermore, staff awareness regarding information security is low, the AIS has not conducted awareness campaigns on information security, nor does it have a plan and resources allocated for training human resources in this area. However, the AIS has addressed the awareness activity on information security reactively through notifications and information emails, especially in cases where phishing attempts (electronic fraud used in the category of cyber-attacks to obtain sensitive information) or other security incidents have been identified. In these cases, immediate actions have been taken to inform staff and minimize the risk. Also, the Kosovo Institute for Public Administration (KIPA) is responsible for providing training, including in the field of information security, which is within the framework of its programs for building the capacities of public administration.

[15] Law no.08/L-276 for the Creation of the Legal Basis for the Issuance of Sub-Legal Acts by the Government and Ministers

[16] Information Technology Audit Manual – Information and Cyber Security, Intrusion Detection and Protection System

[17] ISO 27001 – Criteria for protection against malicious code (malware)

[18] Regulation (GRK) No. 02/2016 for Coordination between the Agency for Information Society and Organizational Structures/Information and Communication Technology Officials in the Institutions of the Republic of Kosovo

These deficiencies in internal controls for information security are also due to the lack of resources of the AIS, which is why all security measures have been oriented towards technical security applications.

The lack of procedures for protection against intrusions and control of access to the information system increases the risk of misuse of access and use of unauthorized access, as well as failure to identify intrusions in a timely manner and failure to identify responsibility in cases of information security incidents.

3.4 Business Continuity Plan – Disaster Recovery Plan

The organization should also have a continuity plan to ensure the continuity of the service provider for their activity or take over this from another company.

If the disaster recovery of a critical functional area is compromised, the business continuity will be jeopardized.[19]

Picture 10. Business continuity

5. AIS does not have an effective business continuity policy

The organization should have organizational policies on business continuity, which contain tasks and responsibilities, purpose, resource allocation criteria/principles, training requirements, maintenance schedule, testing schedule, backup plans, and approval levels[20]. The organization should have a plan to maintain and restore business operations, to ensure the availability of information within the required level and at the specified time after an interruption or failure of business processes[21]. Backup copies of applications and

[19] Information technology audit manual, BCP – DRP.
[20] Information Technology Audit Manual – BCP-DRP, Organizational Policy and Plan for Business Continuity
[21] ISO 27001 – Business Continuity Management

databases are made in accordance with standard operating procedures and must be kept confidential according to law. [22]

AIS does not have policies and procedures for business continuity and disaster recovery; they rely on the administrative instruction for information security management of 2010 which is repealed for the implementation of backups. Furthermore, they do not have another centre for business continuity and disaster recovery, or even another similar hardware infrastructure for testing and putting the backup into operation if necessary. AIS has continuously made efforts to create a centre for business continuity by taking actions especially in recent years. Until a permanent solution is found, they create backups on a regular basis for the infrastructure where the e-Kosova platform is located, while they can restore it to the primary infrastructure that is in use, and regular testing of the backup cannot be carried out.

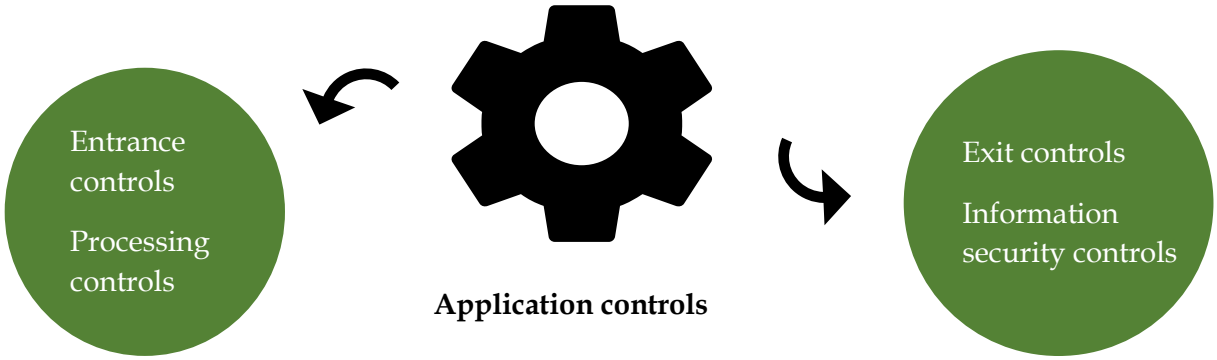
The reason for the lack of policies and procedures for business continuity is the lack of a Business Continuity and Disaster Recovery Centre and the lack of infrastructure. While the lack of this centre is a consequence of the lack of risk-based resource management as a result of poor IT governance in the ASI. However, this year, a contract was signed to provide infrastructure to enable the implementation of a business continuity solution, and a legal basis was created for issuing bylaws.

In the event of a disaster, there is a significant risk that systems will be damaged, data will be lost and, as a result, the operations of these state platforms, including e-Kosovo, will fail to perform/function.

[22] Regulation (GRK) No. 02/2016 for Coordination between the Agency for Information Society and Organizational Structures/Information and Communication Technology Officials in the Institutions of the Republic of Kosovo

3.5 Application controls

Application controls are: controls over input, processing, output, and security functions. They include methods to ensure that: only complete, accurate, valid, and reliable data is entered and updated in an information system, processing accomplishes the correct task, and the result of the processing meets expectations, and data is retained.[23]



6. Failure to apply the restriction criterion in the access controls on the e-Kosova platform for the Child Benefit service

Validation rules should be well-designed, and implemented in the input interaction; different methods for data entry should be documented; invalid data should be rejected appropriately by the application; validation criteria are updated in an appropriate and authorized manner; comprehensive controls should exist as registration rules in case of possibility of essential input controls; there are controls for application inputs.[24] *The Agency supports and coordinates activities between IRKs so that important databases/registries interact with each other.* [25]

The "Child benefits" service has been established on the e-Kosova electronic platform, which is managed by the Ministry of Finance, Labour and Transfers (MFLT), based on the Government's decision in 2024. For the benefit of this allowance, age and number of children criteria have been established, where for families with up to two children aged 0-16, the financial support will be 20 euros per month for each child and for families with three or more children aged 0-16, the support will be 30 euros per month for each child. This decision also stipulates that financial support will benefit all children up to the age of 16 who have Kosovo citizenship and are resident residents in the Republic of Kosovo. However, this criterion is not applied on the e-Kosova platform, in order to prevent benefits from non-resident residents at the same time, therefore, currently the system technically allows the application and benefit of financial support also from children who are not resident residents and who live outside the Republic of Kosovo.

This criterion on the e-Kosova platform is determined by decision no. 55-5/2024. which obliges all citizens born outside Kosovo or who have been delayed for more than three months to apply for an extension to undergo the verification process on the e-Kosova platform. MFLT manages the lack

[23] Information Technology Audit Manual, Application Controls
[24] Information Technology Audit Manual – Application Controls, Access Controls.
[25] Regulation (GRK) No. 02/2016 for Coordination between the Agency for Information Society and Organizational Structures/Information and Communication Technology Officials in the Institutions of the Republic of Kosovo

this criterion applied as a restriction control in the system, manually which is carried out in physical form through the mail.

The e-Kosova platform does not apply the residency criterion as a restrictive control of the system because there is no accurate data on the residence of citizens outside Kosovo and there is no functional connection with systems that can verify this information. The AIS has emphasized that there is no mechanism to verify residence, as there is no access to accurate data from the CRA register.

The electronic service for child benefits on the e-Kosova platform allows the possibility of providing child benefits even to citizens who are not eligible for this service. This is because there are not sufficient entry controls in place in the application due to the lack of criteria on the platform and the mechanism for verifying residency. However, this control is carried out manually by the MFLT.

7. The payment module in e-Kosova allows for double payments without notifying the citizen.

Application transactions execute according to expected behaviour[26]. Application transactions must execute in a controlled and reliable manner, ensuring that they comply with business rules, configuration parameters, and expected processing scenarios. [27]

For electronic services offered on the e-Kosova platform, citizens can make payments through the payment module on this platform. This module is connected to banking platforms and makes payments in real time and safely. Its security level matches that of the banking security mechanisms. However, during the verification of 120,233 transactions/samples for various payments made by citizens through the e-Kosova platform in this module, we encountered 1,112 duplicate payment transactions, for various services such as: police fines, Water for RWC Prishtina, Certificate of rights to individual immovable property, Certificate of rights to business immovable property, Waste in the Municipality of Prishtina, KESCO, HidroDrini, Cadastre, Property Tax. For further analysis, samples of services of the Kosovo Police and the Municipality of Prishtina were selected. From which we have also received additional evidence confirming the existence of double payments, citizen complaints and requests for reimbursement.

The reason for the double payments on the e-Kosova platform is the failure to erase the debt at the time of payment in real time on the e-Kosova platform and allowing the execution of the same payment several times in a row without any prior notification to the citizen and without confirmation of the execution of the first payment. As a result, citizens have paid the same payment for services on the e-Kosova platform more than once.

8. The child benefit application process across the two systems is not fully synchronised or digitalised .

The organization should have procedures in place to ensure that the completeness and accuracy of application results is assessed before the results are used for further processing, including end-user processing, and that completeness and accuracy checks are effective. [28]

[26] Information Technology Audit Manual – Application Controls, Processing Controls
[27] Using COBIT guidelines (especially DSS05 and BAI09) to control processes and ensure the reliability of transaction processing.
[28] Information Technology Audit Manual – Application Controls, Output Controls

In the electronic platform e-Kosova, only the Child Benefits application is made digitally. MFLT accepts these applications in its system on a monthly basis through a manual connection by the IT officer in MFLT, who does it by calling all applications for each month and synchronizing them in the MFLT system, the Information System of the Department for Social and Family Policy (ISDSFP). However, the connection does not have sufficient controls, and during the synchronization of data we have cases of duplication for child benefits. These are prevented and identified through the MFLT system, ISDSFP and those lists are filtered from duplications. So, any information after the citizen's application is handled outside the e-Kosova platform, up to the approval and rejection phase which is carried out by the responsible MFLT official on this platform.

AIS is not informed of any duplications since the communication between the systems is not fully digitalized, resulting in a disconnection between them. The connection is made by importing data through a synchronization file, in the absence of a connection service in the ISDSFP system. At AIS, officials have emphasized that there are no duplicate applications from e-Kosova and we have verified this during the testing of the application, and it has also been confirmed after verifying the samples received from the e-Kosova database, that such a thing is not allowed. But this happens during the process of data synchronization between the two systems.

The e-Kosova platform and the ISDSFP systems are not fully interconnected or operating in real-time, due to communication disruptions. As a result, duplications of applications for child benefits occur.

9. The property tax service does not display the real status of the invoice after payment.

The organization should have procedures in place to ensure that the completeness and accuracy of application results is assessed before the results are used for further processing, including end-user processing, and that completeness and accuracy checks are effective. [29]

The e-Kosova platform is connected to the property tax system (as a back-end system) from which it receives data for the presentation of debt statements and in case of payment, that payment is forwarded to the property tax system. However, the property tax system does not use the payment data to reflect the property tax invoice. So, when the citizen makes a payment for property tax, the property tax system does not use that value received from e-Kosova, but waits for the data sent by the Treasury for the revenues received in the Treasury account.

Therefore, even though the payment has been made and appears on the platform as completed, the payment invoice remains the same and still appears in the system as a debt, enabling the same payment to be made again. This remains until the information is received from the Treasury and this is happening continuously.

Furthermore, in cases where citizens make a payment on the last day of the deadline after working hours, that payment in the property tax system is recorded a few days after its receipt as having been entered into the Treasury account, ignoring the information on the exact date of payment sent by the e-Kosova platform, even though the definition of the article for payment is determined by the property tax law. As a result, the citizen is penalized by the application of interest and penalties. This creates additional expenses and forces the citizen to file complaints in physical form to prove the time of payment within the legal deadline.

[29] Information Technology Audit Manual – Application Controls, Output Controls

The MFLT justifies this with the Treasury revenue regulation and does not take into account the article of the law on property tax regarding payment and payment deadline.

10. The AIS lacks policies and procedures for managing and monitoring audit trails.

Sufficient audit trails must exist that capture modifications, authorized records of critical transactions; audit trails are reviewed periodically to monitor for abnormal activity; audit trails are maintained and stored appropriately; unique and sequential numbers, or identifiers, must be assigned to each transaction.[30]

Audit trails are stored within the system and within the database on the e-Kosova platform. Audit trails are protected from modification and access to their monitoring is separated according to information security standards. From the samples received over 2 million traceability records and analyzed through audit tools (CATs), we assessed that the unique and sequential traceability identification numbers were unmodified and properly protected.

However, although the ASI has created audit trails for the e-Kosova platform and has separated access to audit trails from user access, they fail to regularly monitor audit trails, they do not have a policy or procedure for managing and monitoring audit trails that would determine the time and tasks for officials responsible for monitoring audit trails. But they only monitor in case of suspicious activities and reports of possible incidents.

The lack of resources, especially human resources, made it impossible for the AIS to monitor audit trails on a regular basis, while as for the procedures, they were part of the security policy which has now been repealed.

The lack of a clear policy and procedure for monitoring and periodic review of audit trails, as well as their failure to regularly monitor by AIS for the e-Kosova platform, limits the ability and increases the risk of timely identification of incorrect or unauthorized activities. Although no specific incident was found during the audit period. This compromises the integrity, reliability and security of the information system and may lead to data loss, unauthorized interventions, or institutional liability for inaction.

[30] Information Technology Audit Manual – Application Controls, Application Security Controls

4 Conclusions

The e-Kosovo platform has made important steps towards the digitalization of public services, providing an important tool for facilitating the access of citizens and institutions to various administrative processes, while also improving transparency and efficiency. However, there are still challenges in the integration of systems, information security, data control that affects their reliability, as well as business continuity that affects data security.

Outsourcing

The contract does not sufficiently include information security requirements and measures, such as: data protection clauses and the responsibilities of the project parties in the event of incidents. The contract focuses only on technical aspects, while security is left behind due to the lack of specific policies and legislation, leaving the security of the information system insufficiently addressed.

Acquisition and development

The AIS handles emergency requests for electronic services without proper documentation and planning. The textbooks subsidy service was developed without an active contract and without clear technical criteria, without following standard procedures. This has led to inefficient services and the risk of mismanagement of benefits.

Information security and cybersecurity

The AIS continues to operate with obsolete and outdated information security policies, without written procedures that define how access is managed and intrusions are prevented. This situation leaves employees uninformed and the organization more vulnerable to cyberattacks, negatively affecting the effectiveness of security measures and strategies.

However, the AIS has implemented technical protective measures and advanced mechanisms to prevent intrusions, but the lack of specific documentation and staff awareness of information security increases the risk of misuse, unauthorized access and failure to identify security incidents in a timely manner.

Business Continuity Plan – Disaster Recovery Plan

AIS does not have an effective policy for business continuity and reversal from disasters, as the necessary procedures and infrastructure are missing, including a functional secondary centre. Despite the efforts to create this centre and the realization of reserve copies, they are not enough to ensure a quick and secure restitution of operations in the event of emergency, risking the functioning of critical state systems.

Application controls

Deficiencies have been identified within the e-Kosova platform concerning application controls, including access control, system integration, and information security. The absence of adequate access controls and automated eligibility verification has created opportunities for unentitled benefits, particularly in the 'Child Benefits' and Textbook Subsidies' services, with specific cases documented in the 'School Book Subsidies' service. The platform does not support full digitalisation

and suffers from issues with real-time data synchronization between the systems. As a result, duplicate applications and repeated payments by citizens have been recorded, having a negative impact on both users and the platform's credibility. The lack of policies and procedures for audit trail monitoring and management, combined with insufficient staffing, increases the risk of compromising system integrity, security, and operability. These issues highlight an urgent need to enhance control mechanisms, system integration, digitalisation, and security measures in the platform in order to ensure the reliable and effective delivery of public e-services.

5 Recommendations

We recommend the Ministry of Internal Affairs and the Information Society Agency, the Ministry of Finance, Labour and Transfers, as well as the Ministry of Education, Science, Technology and Innovation that:

1. **Outsourcing policies:** the MIA and AIS, before initiating the development of any information technology project, should address information security requirements with all its elements in all developed information technology contracts, including the preservation of data privacy and the determination of the responsibilities of the parties to the project based on standard information security policies.

2. **Request management**, AIS, for the development of "emergency" requests, should draft a procedure that guides the handling of the request and its documentation, to analyse and develop all necessary elements of development related to the accuracy, completeness and security of information.

   2.1 **Processing controls in the application for the Textbooks subsidy** AIS and MESTI in coordination, for the activation of the Textbooks subsidy service, should draft the requirements with technical specifications and determine the necessary criteria that limit applications only to citizens who are entitled to receive the subsidy and completely digitize the process up to the approval/rejection and receipt of the subsidy through the e-Kosova platform, also defining the roles for approval, rejection and monitoring of the service.

3. **Information security policy**, MIA and AIS should update policies and procedures to protect information security.

4. **Internal controls for information security**, AIS should ensure procedures for preventing interference and managing access to designated ports of platforms and server infrastructure.

   4.1 AIS should document procedures for protection against interference.

   4.2 AIS should provide a plan for raising awareness of Human Resources regarding information security and focus its resources on training and awareness of staff regarding information security.

5. **Business continuity plan**, AIS Management should immediately re-assess risks and orient resources, along with other developments, towards business continuity, starting with the creation of a Business Continuity and Disaster Recovery Centre.

   5.1 AIS should draft, approve and implement policies, procedures and a business continuity plan.

6. **Access controls in the application for the Child Benefit service**, AIS should link the child benefit service with the citizen registers for residency and enable the service to be provided completely electronically. AIS, on the e-Kosova platform, should apply the most appropriate mechanism for identifying residents of Kosovo, using data from all relevant institutions of the country.

7. **Application controls for the payment module**, AIS should update debt statements for citizen services in e-Kosova in real time and establish control mechanisms in the payment module that notify the citizen of the payment being made, preventing double payment.

8. **Logout controls in the application for the child benefit service**, AIS and MFLT should carry out the necessary controls for the connection between the e-Kosova and ISDSFP systems and to implement a secure connection that does not allow duplication of data by realizing the full digitalization of the process through e-Kosova. The data sent by the platform must be processed through the system and not manually.

9. **Logout controls in the application for the property tax service**, MFLT should use the citizen's payment data realized through the e-Kosova platform, which it receives through the connection from AIS to this platform, to accurately implement the law on property tax regarding the payment. In order to communicate with the institutions of the Republic of Kosovo in real time and to present the invoice status also in real time for the payment made by the citizen.

   9.1. AIS should prevent double payment in the "Payments" module of the e-Kosova platform, by notifying the citizen that this payment has already been made once.

10. **Application security controls – audit trail monitoring**, AIS should provide policies and procedures for managing and monitoring audit trails in information systems and shall define tasks for monitoring trails on a regular basis by providing the necessary resources.

ANNEX I. Audit design

Risk areas and audit problem indicators

The e-Kosova platform is one of the most important state systems, classified at the national level, for its importance in providing public services electronically, which aims to make the administration more accessible, transparent and efficient. It is developed and managed by the Information Society Agency (AIS) and aims to reduce dependence on physical counters of state institutions.

The audit of this topic is important, taking into account the recommendations and issues identified in the IT Audit previously conducted by the OPM[31], since e-Kosovo is the main platform for the digitalization of state services, security and integrity are key issues for this platform and for the trust of citizens.

Also, during the pre-study phase, after reviewing documents related to IT systems and citizen services, as well as conducting interviews with officials responsible for the e-Kosovo platform, we identified that despite the progress made in the digitalization of public services, e-Kosovo still faces several important challenges that are:

- Lack of addressing information security issues in the contracts of the e-Kosova platform, as well as the lack of an information security policy, since the information security regulation with which they have operated since 2010 is now not in force. These make the information security and cybersecurity of this system more vulnerable. Since the lack of procedures and their updates in relation to the latest technological developments within the AIS, has left without protective mechanisms for information security and cybersecurity. Such as: Monitoring traces of activities in the information system, monitoring traces for cybersecurity for prevention and detection of intrusions. Lack of separation of roles and responsibilities of access and responsibilities in the system. List of potential risks and a plan for their management. Procedure for responding to information security incidents. As well as the lack of a list of critical infrastructure and a plan for business continuity.

- The lack of mechanisms for protecting information security compromises the data of services in e-Kosova. It becomes more sensitive in the case of processing data related to payments. E-Kosova has many services that contain the payments module; therefore, the lack of these mechanisms makes the payments module more vulnerable to possible cyber-attacks.

- Limited connectivity with other state systems, which leads to manual verifications and delays in updating data for some services. The most used services and with the most frequent circulation of financial means on a regular monthly basis that lead the list of services in e-Kosova have been identified with problems of this nature:

    - **Child benefits**, in the absence of interconnection with the systems for identifying residence, even citizens who do not live in Kosovo can receive child benefits without

[31] Project Management for Information Technology Systems at the Agency for Information Society – IT Audit Report (2023

fulfilling this criterion. This is due to the lack of interaction of the systems and verification of their residence.

- **Property tax**, the data of the property tax service comes with interconnection on the e-Kosova platform, therefore the security of this interconnection needs to be tested, since during the pre-study phase we identified that there is very little documentation for the information security part of the interconnection of services. This service is the most used by citizens and has the payment element that makes it even more vulnerable; therefore, this service has deficiencies in information security mechanisms.

- Lack of digitalisation for some services, especially for vulnerable groups, such as the elderly and people with health problems. An important service identified during the pre-study is the need for physical presence for the continuation of pensions, where pensioners must appear in person at social work offices. This indicates the need for greater analysis during the digitalization of processes and the prioritization and management of the needs for digitalization of services for citizens, by decision-makers for the development of requirements.

The review of the problem indicators identified from various sources, meetings held with the persons responsible for identifying issues in the e-Kosova platform, as well as our assessments based on the Active IT Audit Manual [32] for identifying the riskiest areas from the received documentation orients us to the main problem: the e-Kosova platform has deficiencies in the development and outsourcing of the information system, in the organization of information security and application control.

[32] Active Audit Manual - is a platform developed by ITWG/EUROSAI and WGITA/INTOSAI, used to identify the riskiest areas, define questions, criteria and work methodology during the IT audit process.

System description

3.1. Ministry of Internal Affairs

The mission of the Ministry of Internal Affairs is to ensure the rule of law and public security throughout the territory of the Republic of Kosovo.

The Ministry, in addition to being responsible for building, maintaining and improving security for all citizens of the country, also prepares and implements policies for the administration and communication of systems, being one of the key institutions that manages electronic data in terms of quantity, quality and relevance. The Ministry operates through 8 agencies and its bodies, including the Information Society Agency (AIS) and also 13 departments and divisions.

The IS was established as an executive government agency within the ministry responsible for public administration, or at the highest authority of state administration established by the Government and which is now the Ministry of Internal Affairs.

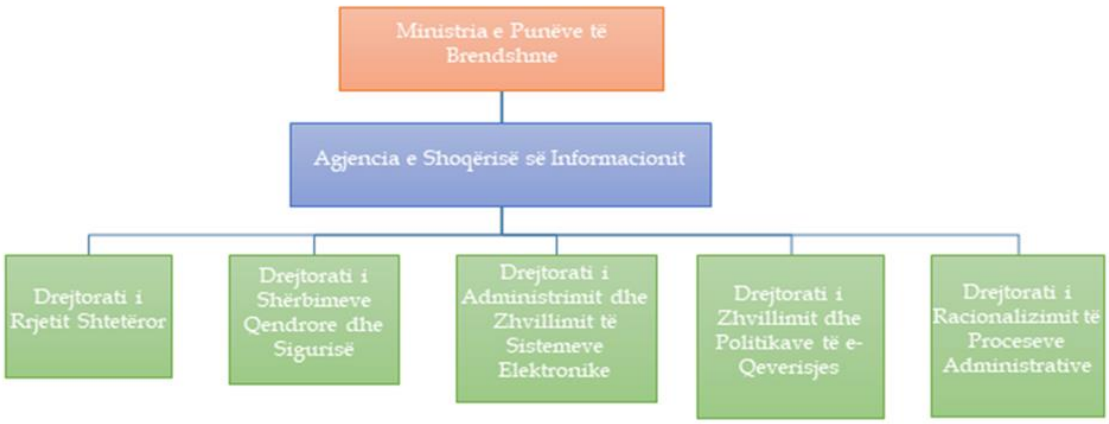
In 2013, the Assembly of the Republic of Kosovo adopted Law 04/L-145, pursuant to Article 65 (1) of the Constitution of the Republic of Kosovo, on Governmental Bodies of the Information Society, which defines the Information Society Agency as the main body for the development and implementation of services in the field of Information and Communication Technology in all institutions of the Republic of Kosovo. The structures responsible for the information society in the institutions of the Republic of Kosovo according to this law are the AIS and the relevant organizational structure or the ICT Management Officer in the IRKs. The bodies responsible for the development of information society services in the institutions of the Republic of Kosovo, their competencies, responsibilities, organization and functioning have also been determined.

Duties and Responsibilities of the AIS:

- Proposes and coordinates all policies related to ICT developments in the institutions of the Republic of Kosovo;
- Prepares the e-Government Strategy and its Action Plan for approval by the Government and monitors its implementation;
- Manages and supervises the implementation of ICT projects in the institutions of the Republic of Kosovo;
- • Supports the development of information technology, promotes investments in the field of information society, the development of training systems in information technology and coordinates, leads and supervises the processes and mechanisms of e-Government in the fields of IT infrastructure, expansion of Internet services. Accumulates, administers, disseminates and stores data in the State Electronic Data Centre;
- Supports the development of security and protection of electronic communication infrastructure and data, as well as combating electronic crime (cybercrime). It also manages and preserves intellectual property and rights related to databases and software, which are state property, and protects personal data in electronic form, in accordance with applicable legislation and facilitates access to public information in electronic form;
- In cooperation with KIPA, identifies needs for electronic training of the Information Society for employees of institutions of the Republic of Kosovo;
- Reviews requests for planned projects and monitors their implementation in accordance with policies and the E-Government Strategy;

- Coordinates activities for the security of electronic services.

The responsibilities for the development of these functions of the AIS have been organized into five directorates, which are presented in the following picture:



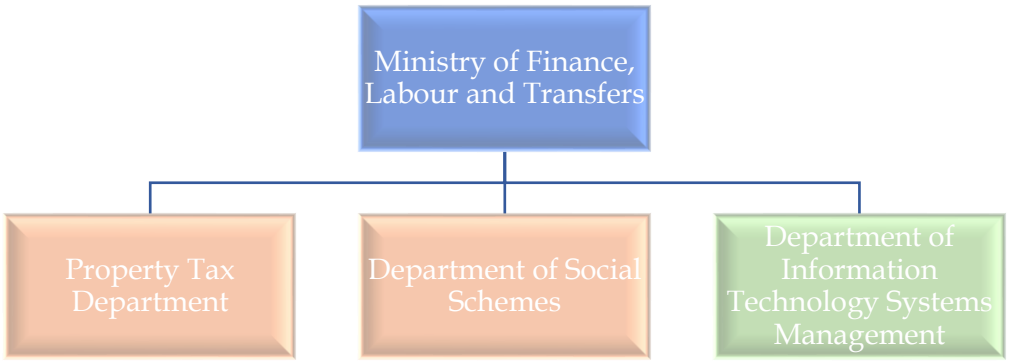
Picture 7. Organization of the AIS

The **Ministry of Finance, Labour and Transfers (MFLT)**, based on the Regulation[33] on the areas of administrative responsibilities of the Office of the Prime Minister and Ministries, has responsibilities for: Preparing, drafting, approving, implementing, evaluating and supervising public policies, drafting legal acts, drafting and approving sub-legal acts, setting mandatory standards in the field of public finance management and taxes. In the field of property tax, the ministry ensures the implementation of tax legislation and supervises the rules for spending public money, contributing to sustainable fiscal and economic management.

For child benefits, the MFLT ensures the calculation and execution of social schemes, including benefits related to family benefits and child benefits, in accordance with the legislation in force. This means that the ministry has a central function in guaranteeing financial support for citizens, including families with children, and in the e-Kosova platform it manages and administers data for services for which it has a role and responsibility, therefore it is also responsible for larger services, such as the property tax service and the child benefit service. MFLT has 8 Agencies and 18 Departments, where within the departments are also the Property Tax Department, the Department of Social Schemes and the Department for Information Technology Systems Management.

The responsibilities of these departments will focus only on services provided through the e-Kosova platform and not on basic systems such as property tax but only on services within e-Kosova and not on the basic property tax system.

[33] Regulation (GRK) - No. 06/2020 on the Areas of Administrative Responsibility of the Office of the Prime Minister and Ministries



Picture 8. Organization of MFLT departments involved in the field of action

Audit scope and questions

The scope of this audit will be the Agency for Information Society and the departments responsible for the administration, management and security of the e-Kosovo platform. The Ministry of Finance, Labour and Transfers with the relevant departments for Property Tax and Social Schemes Management that also administer the relevant services in e-Kosovo for property tax and child benefits.

In AIS: Directorate of Rationalization of Administrative Processes; Directorate of e-Government Development and Policies; Directorate of Administration and Development of Electronic Systems; Directorate of Central Services and Security; and Directorate of State Network.

In MFLT: Department of Property Tax; Department of Social Schemes; and Department for Management of Information Technology Systems.

The focus of the audit will be information security and application controls for the information technology system, the e-Kosovo platform. The audit will cover the period from January 2024 until the completion of the audit.

Audit questions

To answer the audit objective, we have posed the following questions:

1. *Are information security requirements addressed in the contractual documents for e-Kosova and are they consistent with the security policies of the AIS?*
2. *How does the AIS identify, prioritize and manage its requirements for the e-Kosova platform?*
3. *Is the internal and external communication of the information system in e-Kosova secure?*
4. *Is unauthorized access and copying or viewing of sensitive information in e-Kosova prevented?*
5. *Is there an effective business continuity policy in AIS?*

6. *Is it assessed whether the data entered during the application login is valid in the database and by authorized personnel in the e-Kosova platform?*
7. *Does the e-Kosova application ensure the integrity, validity and reliability of transactions during the data processing cycle?*
8. *Is it ensured that the information output to e-Kosova is complete and accurate before further use and is it stored appropriately?*
9. *Is the information secure in the e-Kosova application against misuse?*

Audit criteria [34]

The criteria used in this audit are derived from the Active IT Audit Manual[35]; International Standards for Information Security[36], as well as the ASH Regulation on Coordination between ASH and IRKs.[37].

To assess the identification of needs and addressing information security requirements in the contract for the development of the e-Kosova system, the following criteria have been established:

- The organization's security requirements must be highlighted by the contractor in an appropriate manner.[38]

  The agreement with external parties that involves access, processing, communication or management of the organization's information or information processing structure, or the introduction of products or services into the information processing system, complies with all appropriate security requirements.[39]

To assess the identification of needs and address the requirements for the purchase and development of the contract for the development of the e-Kosova system, the following criteria have been established:

- The AIS should analyze, prioritize, and manage requirements to ensure that user needs are met in an optimal and cost-effective manner.[40]

To assess whether AIS has mechanisms for information security and business continuity, the following criteria have been established:

[34] For more information, consult ISSAI 300, Criteria, p.7.
[35] The Information Technology Audit Manual is a product of the EUROSAI Working Group on Information Technology (WGITA) and the INTOSAI Development Initiative (IDI) for the definition of rules and standards for Information Technology Auditing. - hereinafter the Information Technology Audit Manual.
[36] Information security management system ISO/IEC 27000/01.
[37] Regulation (GRK) No. 02/2016 for Coordination between the Agency for Information Society and Organizational Structures/Information and Communication Technology Officials in the Institutions of the Republic of Kosovo.
[38] Information Technology Audit Manual – Contracting, Security
[39] ISO 27001 – Information Security Policies.
[40] Information Technology Audit Manual – Acquisition and Development

- The AIS must ensure that defined information security policies exist and are approved, communicated and implemented within the organization.
Policies should be reviewed regularly or when there are significant changes in the organization, technology or applicable laws.[41]
Policies and procedures should form a consistent managerial environment for internal and external communications.[42]

- The organization must ensure that intrusions are detected and will be detected and combated[43].
The organization must ensure that appropriate measures are in place to prevent, detect and recover from malicious code threats through policies, technical controls and user awareness.[44]
The Agency for Information Society must take care of the security and protection of electronic infrastructure and data and coordinate activities for the security of IT services[45].

- The organization should have organizational policies on business continuity, which contain tasks and responsibilities, scope, resource allocation criteria/principles, training requirements, maintenance schedule, testing schedule, backup plans, and approval levels[46].

The organization should have a plan to maintain and restore business operations, to ensure the availability of information within the required level and at the specified time after an interruption or failure of business processes. This plan should identify the risks faced by the organization, identify critical business assets, identify the impacts of incidents, consider the implementation of additional preventive controls, and document business continuity plans addressing security requirements. It should ensure that the plan includes the identification and approval of responsibilities, the determination of acceptable loss, the implementation of recovery and restoration procedures, documentation of procedures, and regular testing[47].

State registries and electronic services of the IRKs must be hosted in the SDC or in their Data Centres, but on condition that a backup copy is kept in the SDC. Backup copies of applications and databases are made in accordance with standard operating procedures and must be kept confidential according to the law.[48]

In order to assess whether the e-Kosova platform has application control mechanisms that enable secure logical (software-based) and reliable access to the information system, the following criteria have been established:

- Validation rules should be well-designed, documented and enforced in the input interaction; different methods for data entry should be documented; invalid data should be rejected

[41] ISO/IEC 27002:2022 – Information Security Policies
[42] Information Technology Audit Manual - Information and Cybersecurity, Communications and Operations Management
[43] Information Technology Audit Manual – Information and Cyber Security, Intrusion Detection and Protection System
[44] ISO 27001 – Criteria for protection against malicious code (malware).
[45] Regulation (GRK) No. 02/2016 for Coordination between the Agency for Information Society and Organizational Structures/Information and Communication Technology Officials in the Institutions of the Republic of Kosovo.
[46] Information Technology Audit Manual – PVB-PRF, Organizational Policy and Plan for Business Continuity
[47] ISO 27001 – Business Continuity Management
[48] Regulation (GRK) No. 02/2016 for Coordination between the Agency for Information Society and Organizational Structures/Information and Communication Technology Officials in the Institutions of the Republic of Kosovo.

appropriately by the application; validation criteria are updated appropriately and authorized; comprehensive controls such as registration and authorization rules should exist in case of the possibility of essential input controls; there are appropriate controls and documentation for application logins.[49]

- For data entry in the application, there should be a clear and concise error handling system indicating the type of problem so that corrective action can be taken for any type of error. Errors should be corrected appropriately before processing transactions. Records should be reviewed periodically and necessary corrective action taken.[50]

The Agency supports and coordinates activities between IRKs so that important databases/registries can interact with each other.[51]

- The application should have transaction authorization levels established and enforced through various controls; there should be a clear segregation of duties for data entry; there should be compensating controls for cases in which segregation of duties is not possible[52].

- Application transactions should be executed in accordance with expected behaviour[53].

Application transactions should be executed in a controlled and reliable manner, ensuring that they comply with business rules, configuration parameters, and anticipated processing scenarios[54].

- The organization should have procedures in place to ensure that the completeness and accuracy of application outputs is assessed before the output is used by further processing, including end-user processing; the application output should be traceable; the output should be reviewed for reasonableness and accuracy; completeness and accuracy controls should be effective[55].

- There should be sufficient audit trails that capture modifications, authorized records of critical transactions; audit trails are periodically reviewed to monitor for abnormal activities; audit trails are maintained and stored appropriately; unique and sequential numbers, or identifiers, should be assigned to each transaction[56].

- Application data should be protected in accordance with security standards and the IT audit manual. Effective logical and physical access controls, as defined in the Information Security domain, should be implemented to ensure authentication, authorization, and monitoring of access. The application should also have a documented disaster recovery plan, including secure

[49] Information Technology Audit Manual – Application Controls, Access Controls.
[50] Information Technology Audit Manual – Application Controls, Access Controls.
[51] Regulation (GRK) No. 02/2016 for Coordination between the Agency for Information Society and Organizational Structures/Information and Communication Technology Officials in the Institutions of the Republic of Kosovo
[52] Information Technology Audit Manual – Application Controls, Access Controls.
[53] Information Technology Audit Manual – Application Controls, Processing Controls
[54] Using COBIT guidelines (especially DSS05 and BAI09) to control processes and ensure the reliability of transaction processing
[55] Information Technology Audit Manual – Application Controls, Output Controls
[56] Information Technology Audit Manual – Application Controls, Application Security Controls

backup and recovery mechanisms, as defined in the BCP/DRP domain. Security and recovery plans should be tested regularly to ensure business continuity and information protection.[57]

Audit methodology

To answer the audit questions and to support the audit conclusions, we will apply the following methodology:

To assess the identification of needs and address information security requirements in e-Kosova platform contracts:

- Review of contractual documents. Review of the initial contract for the development of the e-Kosova platform, the current contract for the maintenance and advancement of the e-Kosova platform, as well as the tender dossier with specific terms. Also review of the policies and procedures of the AIS for information security.

To assess the identification of needs and the addressing and prioritization of citizens' requests in the e-Kosova platform contracts:

- Review requests to determine if they include author, date, priority, cost, risk, and other elements. Review and analyze requests or comments on requests from business owners – Government, decision makers, or stakeholders to determine if all views have been collected and summarized for appropriate analysis (acceptance, deferral, rejection, etc.). Review the traceability matrix to determine if approved requests are assigned to development projects and are followed through to completion when implemented. Review the criteria for determining the priority of requests to assess whether they include elements such as cost, basic citizen needs, emergency issues, and new requests.

To assess whether the e-Kosova platform has mechanisms for information security and business continuity, the following are being implemented:

- Analysing the organization's policies and procedures to see if they are adapted to the needs of citizens by comparing them. Verifying how the organization documents its procedures and how it makes them available to all users. Interviewing staff at different levels to examine whether all data handling procedures are known to employees. Checking how often data handling and communications procedures are reviewed and updated. Reviewing the cybersecurity strategy if any and ensuring that it covers the protection of critical assets.
- Verifying regulations for handling physical intrusions in the spaces where the equipment is located. Analysing incident reports. As well as identifying that the organization has a clear policy for preventing unauthorized access.
- Reviewing documents to assess whether the policies comply with general IT policies and address business continuity requirements. Conducting interviews with staff to see how often the policies are updated. Verifying policies to see how they have been approved and whether they are up to date, as well as assessing whether these policies are understandable to staff.

[57] Information Technology Audit Manual – Application Controls, Application Security Controls

To assess whether the e-Kosova platform has application control mechanisms that enable secure, logical and reliable access to the information system, the following tests are carried out:

- Analyse application rules, requirements, documentation and interview business process owners to determine which validation rules should be provided in the business process being assessed. Review whether validation rules are well designed and documented. Verify whether validation checks for input data are in place, run the application in a test environment and test various interactions for input data.
- Handle application errors with its developer or administrator. Verify and confirm whether policies and procedures exist for handling transactions that fail modification and validation checks. Verify whether the system provides messages for any type of error (at the field or transaction level), messages that may not match validation or modification. Verify how the application works if data is rejected by input checks. Verify whether data elements are recorded or if they are automatically filled in.
- Inspect and confirm whether the system design provides an authorized list for use. Verify through inspection of the authorization list that authorization levels are well defined for each set of transactions. Assess whether authorization rules for data entry, modification, acceptance, rejection and abuse are well designed and defined. If there is a table for the division of duties, the way in which the main tasks and work functions are distributed, as well as the transactions allowed, and then analyse the list of users and the list of user access privileges.
- Identify the services provided on the platform and group them according to the importance of the service it provides. Review the platform documentation to verify that it is appropriate, ensures integrity and reliability during the transaction processing cycle.
- Create a checklist of input data if there is any prior review of the services provided. Identifying whether, for certain services, the e-Kosova system is linked to the underlying systems and validates data from the back-end system. Assessing whether the output information after processing in the e-Kosova system is accurate and complete and that errors that appear are identified.
- Analysing and reviewing policies and procedures for maintaining audit trails and the method of their verification. Verifying audit trails and other documents to verify that the audit trail has been effectively created. Identifying who are the authorized persons to revoke or delete audit trails. Ensuring that access to audit trails is limited and only authorized persons can access them. Assessing whether the trails are protected from modification and whether there are unique identifiers for each transaction. Assessing whether the e-Kosova platform has the necessary integrity and reliability.
- Reviewing and analysing platform documentation to see if platform information is secure against misuse. Interviewing IT staff to see how they understand the security mechanisms implemented in the application.

Relevant documents

Laws

Law No. 04/L-145 on Information Society Government Bodies

This law determines the competent institutions, their functions and responsibilities in the development and implementation of information technology in the institutions of the Republic of Kosovo, the establishment of the Information Society Agency, as well as the consolidation of functions and responsibilities in the field of implementation of information and communication technology (ICT).

Law No. 06/L-005 - on Immovable Property Tax

This Law establishes the tax on immovable property and determines the basic rules and procedures for the administration of the tax on immovable property by the municipalities and the Ministry of Finance. The provisions of this Law are mandatory for all institutions and their respective units, responsible for the implementation of this Law, for persons who are obliged to pay the property tax, as well as for other persons who are obliged to implement legal obligations, according to the provisions set forth in this Law.

Regulations

Regulation (GRK) No. 02/2016 for Coordination between the Agency for Information Society and Organizational Structures/Information and Communication Technology Officials in the Institutions of the Republic of Kosovo

This Regulation establishes the standards, the manner of functioning and coordination of activities between the Information Society Agency and the ICT structures or officials of the IRK.

AIS monitors the implementation of this Regulation.

Regulation (MPA) No. 02/2015 on Software and Hardware Standards

The purpose of this regulation is to determine the standards for the use of software and hardware by officials of the institutions of the Republic of Kosovo.

This regulation also determines the purchase, installation and use of licenses used by the IRKs.

Regulation (GRK) No. 06/2018 on Project Management in the Field of Information and Communication Technology

The purpose of this regulation is to determine unique standards and rules for the initiation, planning, execution, monitoring and control, as well as the completion of the project management process in the field of Information and Communication Technology (hereinafter: ICT) in the institutions of the Republic of Kosovo.

Regulation (GRK) - No. 06/2020 on the Areas of Administrative Responsibility of the Office of the Prime Minister and Ministries

This regulation defines the areas of administrative responsibility of the Office of the Prime Minister and the ministries in the Government of the Republic of Kosovo.

Regulation (OPM) No. 02/2023 on Internal Organization and Systematization of Jobs in the Ministry of Finance, Labour and Transfers

This Regulation aims to determine the internal organization and systematization of jobs in the Ministry of Finance, Labour and Transfers.

ANNEX II. Letter of confirmation

REPUBLIKA E KOSOVËS/REPUBLIKA KOSOVA/REPUBLIC OF KOSOVO
ZYRA KOMBËTARE E AUDITIMIT
NACIONALNA KANCELARIJA REVIZIJE / NATIONAL AUDIT OFFICE
11 08 2025

Njësia Org. Org. Jedin. Org. Unit	Shif.klasif. Klasif. Kod Class. Code	Nr. Prot. Br. Prot. Prot. No.	Nr.i faqeve Br. Stranica No. Pages
06	47	1397	1

QEVERIA E KOSOVËS/VLADA KOSOVA/GOVERNMENT OF KOSOVO
MINISTRIA E PUNËVE TË BRENDSHME/MINISTARSTVO UNUTRAŠNJIH POSLOVA/MINISTRY OF INTERNAL AFFAIRS
Kabineti i Ministrit / Kabinet Ministra / Cabinet of the Minister
Nr./Br./No. 0435 Nr. i fq./Broj str./No. pg. 1
Data/Datum/Date 31.07.2025
PRISHTINË - PRIŠTINA - PRISTINA

Republika e Kosovës

Republika Kosova-Republic of Kosovo

Qeveria –Vlada-Government

Ministria e Punëve të Brendshme-Ministarstvo Unutrašnjih Poslova-Ministry of Internal Affairs

LETËR E KONFIRMIMIT

Për pajtueshmërinë me të gjeturat e Auditorit të Përgjithshëm për raportin e auditimit të teknologjisë së informacionit **Platforma e shërbimeve online e-Kosova,** dhe për zbatimin e rekomandimeve.

Për: Zyrën Kombëtare të Auditimit

Vendi dhe data: 31.07.2025

I nderuar,

Përmes kësaj shkrese, konfirmoj se:

- kam pranuar draft raportin e Zyrës Kombëtare të Auditimit **Platforma e shërbimeve online e-Kosova** (në tekstin e mëtejmë "Raporti");
- pajtohem me të gjeturat dhe rekomandimet dhe nuk kam ndonjë koment për përmbajtjen e Raportit; si dhe
- brenda 30 ditëve nga pranimi i Raportit final, do t'ju dorëzoj një plan të veprimit për implementimin e rekomandimeve, i cili do të përfshijë afatet kohore dhe stafin përgjegjës për implementimin e tyre.

Ministri//Kryetari//Kryeshefi Ekzekutiv/Drejtori i Përgjithshëm

z. Xhelal Sveçla
Ministër në detyrë i Punëve të Brendshme

REPUBLIKA E KOSOVËS/REPUBLIKA KOSOVA/REPUBLIC OF KOSOVO
QEVERIA/VLADA/GOVERNMENT OF KOSOVO
PRISHTINË/PRIŠTINA/PRISTINA

National Audit Office of Kosovo
Arbëria District,
St. Ahmet Krasniqi, 210
10000 Pristina
Republic of Kosovo