Republika e Kosovës
Republika Kosova
Republic of Kosovo

Zyra Kombëtare e Auditimit
Nacionalna Kancelarija Revizije
National Audit Office

REPORT ON INFORMATION TECHNOLOGY AUDIT

Civil Status Information System in the Civil Registry Agency

Prishtina, June 2022

The National Audit Office of the Republic of Kosovo is the highest institution of economic and financial control and is accountable for its work to the Assembly of the Republic of Kosovo.

Our mission is to strengthen accountability in the public administration for the effective, efficient and economical use of national resources through quality audits. The reports of the National Audit Office directly promote the accountability of public institutions by providing a solid basis for holding managers of any audited organization to account. In this way, we increase confidence in spending public funds and play an active role in ensuring the interest of taxpayers and other stakeholders in increasing public accountability.

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

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

The Auditor General has decided regarding the content of this IT audit report "Civil Status Information System in the Civil Registry Agency" in consultation with Acting Assistant Auditor General Myrvete Gashi, who supervised the audit.

This audit report was carried out by the team:

Samir Zymberi, Acting Director of the Audit Department;

Shqipe Mujku Hajrizi, Team Leader; and;

Poliksena Berisha, Team Member.

1. ISSAI 3000 – Standards and guidelines for performance auditing based on ONISA Auditing Standards and practical experience.

2. GUID 5100 – Guidance on Audit of Information Systems issued by INTOSAI.

3. Efficiency – The principle of efficiency means achieving the maximum from available resources. It has to do with the connection between the resources engaged and the results given 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 most suitable price.

5. Effectiveness – The principle of effectiveness means achieving predetermined objectives and achieving expected results.

TABLE OF CONTENTS

Executive summary 1

1 Introduction 3

2 Audit Objective and Areas 5

3 Audit Findings 6

3.1 Information Technology Governance 7

3.2 Information security 12

3.3 Application controls 20

4 Conclusions 23

5 Recommendations 25

Annex I. Audit design

Areas of risk and indicators of audit problems 29

System description 30

Role and responsibilities of the parties 31

Audit scope and questions 36

Audit criteria 38

Audit methodology 41

Relevant documents 42

Annex II. Confirmation Letters 43

List of Acronyms

CRA	Civil Registry Agency
AIS	Agency for Information Society
CAAT	Computer – Aided Audit Tools
CISA	Certified Information Systems Auditor
GG	Government Gateway (Centralized platform that serves to connect the systems of institutions, public and private sector)
CS	Civil Status
IP	Internet Protocol
ISACA	Systems Audit and Control Association
ISSAI	International Standards of Supreme Audit Institutions
MIA	Ministry of Internal Affairs
MFAD	Ministry of Foreign Affairs and Diaspora
EO	Economic Operator
DRP	Disaster Recovery Plan
SPO	Standard Operation Procedure
BCP	Business Continuity Plan
CRCS	Central Registry of Civil Status
CSS	Civil Status System
IT	Information Technology
AI	Administrative Instruction
VPN	Virtual Private Network

Executive summary

The Civil Registry Agency (ARC) as an agency within the Ministry of Internal Affairs is the main source of personal data of Kosovo citizens, which are registered and kept in the civil status register, providing proof of data relating to birth, family status, death, their relationships, and any changes that occur in these relationships. Civil status data is administered through the information system.

The National Audit Office has conducted the IT audit for the Civil Status Information System in the Civil Registry Agency, including Civil Status Offices and diplomatic or consular missions of the Republic of Kosovo as users of this system.

The Civil Registry Agency has continuously made developments in the Civil Status System (CSS) to verify and ensure data accuracy, to improve the quality of data recorded in the system and the security of the system itself.

ARC has not established appropriate and functional Information Technology Governance mechanisms. The structure and controls in IT operations are not well defined, exposing the organization to the risk of achieving objectives, ensuring the continuity of operation of information systems and the use of electronic devices.[6]

The information protection and security system implemented in the ARC does not sufficiently guarantee system continuity and data integrity at all times. Also, the consulates within the Ministry of Foreign Affairs and Diaspora and the Municipality of Pristina as users of the system do not guarantee that they have properly preserved data integrity and confidentiality in the information system.[7]

Application controls implemented in CSS do not ensure that only correct and valid data is entered and updated in the system. As a result, there are citizens who are registered twice and are have two personal numbers, as well as different citizens registered with the same book number. Also, there is a lack of connection between CSS and the database of the Cadastral Agency for address registration.[8]

Therefore, the risks identified in IT governance, information security and application controls indicate that the ARC that administers the CSS and the user institutions of this system need improvements so that citizen data is protected and the provision of electronic services to citizens should not be interrupted. In this regard, we have put forward 27 recommendations for the Ministry of Internal Affairs and the Civil Registry Agency, including 1 for the Information Society

6. 3.1 Governance of Information Technology
7. 3.2 Information Security
8. 3.3 Application Controls

Agency, 3 for the Ministry of Foreign Affairs and Diaspora and 3 for municipalities. The list of recommendations is set out in Chapter 5 of this report.

Response of audited entities

The Ministry of Internal Affairs/Civil Registry Agency, the Ministry of Foreign Affairs and Diaspora and the Municipality of Prizren have agreed with the findings and conclusions of the audit and have pledged to address the recommendations given, while the Municipality of Pristina has not given answer.

1 Introduction

Civil registration is the process by which a government records the vital events (births, marriages and deaths) of its citizens. The main purpose of civil registration is the generation of legal documents required by law that supports an individual's right to be recognized as a person before the law and recognizes their formal relationship with the state.

The Civil Registry Agency (CRA) is responsible for managing the processes related to the application of personalization and the issuance of documents for citizens of the Republic of Kosovo, for foreign citizens and for stateless persons, when they have temporary or permanent residence in the territory of the Republic of Kosovo, as well as for foreign citizens who have granted asylum in the Republic of Kosovo.

Therefore, CRA is the main source of personal data of Kosovo citizens, which are registered and kept in the registry of civil status, proving birth, family status, death, their relationships and any changes that occur in these relationships.

The civil status service in Kosovo is organized in:

- Central level of civil status service, respectively the Agency;
- Local level of civil status service, respectively Civil Status Offices; and
- Civil status service in the diplomatic and consular missions of Kosovo.

The types of civil status documents issued by civil status offices are the following:[9]

- Birth certificate;
- Extract from the central register of civil status;
- Citizenship certificate;
- Marriage certificate;
- Death certificate;
- Residence certificate;
- Certificate of marital status;
- Certificate of family relationship.

9. Administrative Instruction (MIA) No.25/2013 on Civil Status Documents

CRA has developed the centralized information system "Civil Status System" (CSS), to enable the Civil Status Offices and diplomatic and consular missions of Kosovo to issue these documents as well as to register and update citizen data, in order for the services to be available at all times. The system was operationalized on February 19, 2013, and has been used to print various civil status documents.

The system also allows to produce statistics on the number and type of each component of the civil status that is registered or updated in the Central Register of Civil Status (CRCS).[10]

Table 1 provides statistical data on the number of births, marriages and deaths in 2018, 2019, 2020 until September 2021.[11]

Year/Fact	Births	Marriages	Deaths
2018	40,916	21,744	13,987
2019	39,063	22,276	14,235
2020	33,127	16,151	15,740
2021	43,994	22,528	18,772

Table 1. Statistical data on the number of births, marriages, and deaths in 2018, 2019, 2020 and 2021

As CRA provides vital, reliable and timely information, it has entered into agreements with many public and private institutions to provide them with the necessary requested information. Through this system, it is possible to exchange data with the systems of other institutions. Figure 2 shows the data flow process in CSS.

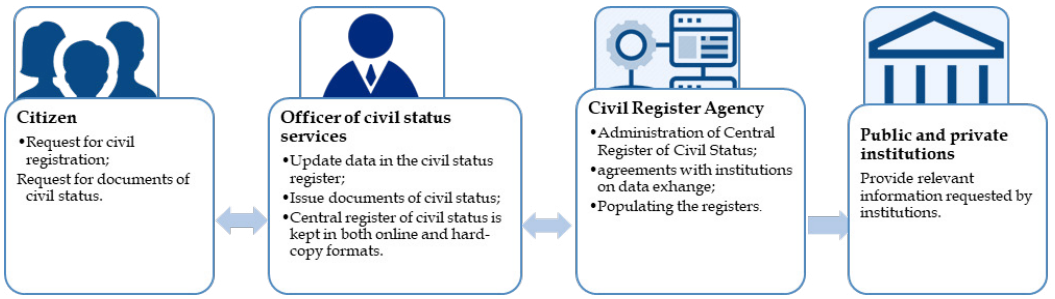

Figure 2. Data flow in the Civil Status System

CSS also provides vital information on an ongoing basis, it helps the government in planning, policy development and appropriate services and resource allocation. Further, this information is used for electoral services, personal identification services, population registers, etc.

10. Administrative Instruction (MIA) No.11/2017 on Central Register of Civil Status

11. Data ensured by the Department of Civil Status – Central Register of Civil Status.

2 Audit Objective and Areas

The objective of the audit is to assess the administration and information security of the civil status information system of the Republic of Kosovo, whether it is maintaining data security and privacy, data integrity and availability.

This audit is aimed at providing relevant recommendations for the relevant parties in order to improve IT services.

Audit Areas

In order to achieve the audit objective, we have focused on the area of IT governance, information security and application controls and have selected the following audit areas:

Audit areas	Audit issues
IT governance:	1. *Organizational structure, Standards, Policies and Procedures* 2. *Management of changes in information systems* 3. *Business Continuity Policy, Plan and Organization*
Information security:	4. *Information security policies* 5. *Access control* 6. *Application Security Controls*
Application controls:	7. *Input controls* 8. *Output controls*

3 Audit Findings

This chapter presents the audit findings related to the activities of the parties responsible for the administration and information security of the Civil Status System in the Civil Registry Agency and the Ministry of Justice, the Municipality of Pristina and the Municipality of Prizren as system users. The findings are structured in three parts, interconnected according to the audit areas shown in figure 3.

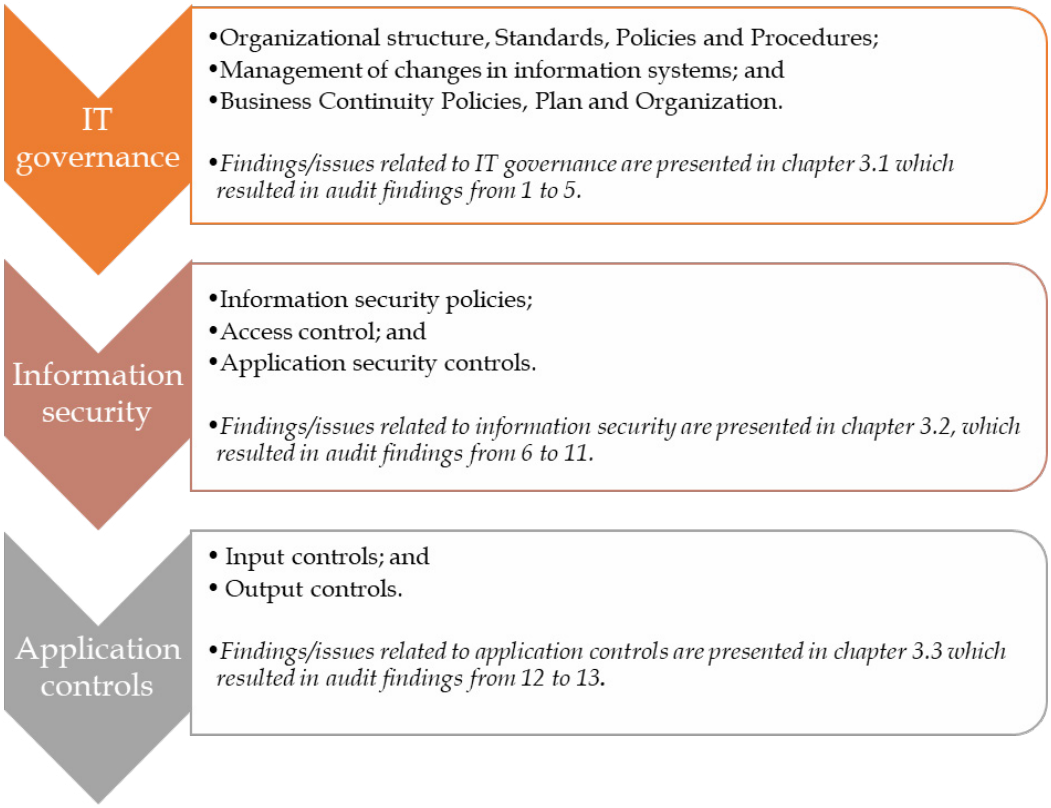

Figure 3. Structure of audit issues for CSS

The issues/findings are presented with an ordinal number and correspond to the same number of recommendations in chapter 5.

3.1 Information Technology Governance

IT governance is defined as the overall structure that guides an institution's IT operations and ensures that IT systems support and enable the achievement of the institution's objectives, and plays a key role in defining a controlling and reporting environment. The key elements of IT governance are: IT strategy and planning; structures, standards, policies and procedures, development and procurement, human resources, etc.[12]

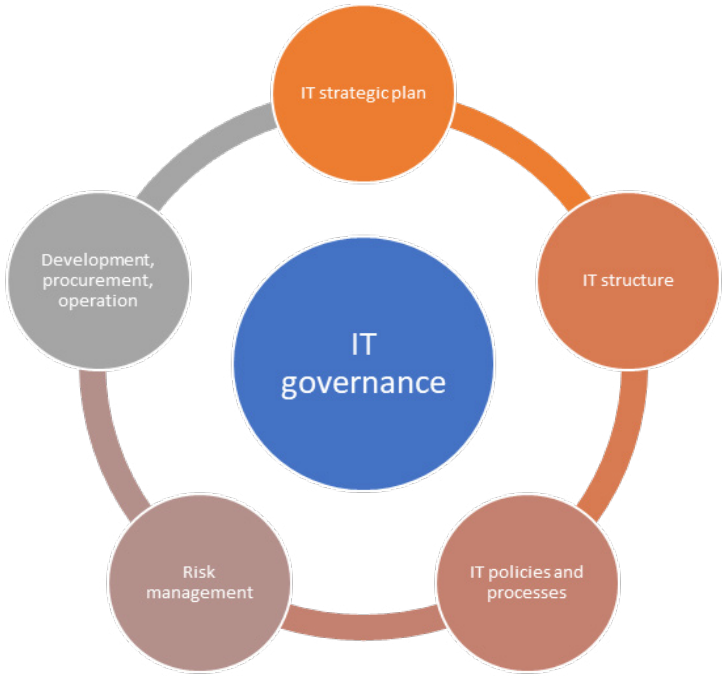

Figure 4. General IT governance structure

1. *ARC does not have a clearly defined IT structure and the roles and responsibilities related to CSS*

The IT structure within the organization as well as its roles and responsibilities must be clearly defined in order to properly maintain IT services.[13]

CRA does not have a clearly defined structure with separate IT department responsibilities. According to the regulation for internal organization in the Ministry of Internal Affairs and CRA, the IT structure in CRA is distributed in several departments and sectors, as a result of which we have duplication of responsibilities within those departments and sectors. Also, there are several users in CSS for the administration of the system, because, according to the same

12. Information Technology Auditing Handbook, IT Governance.
13. Information Technology Auditing Handbook, IT Governance Audit Matrix.

regulation, the administration of the system is defined in more than one sector. However, in addition to the duplication of the same responsibilities that have been made possible through the internal organization regulation, there is also a conflict of responsibilities since the database administrator is also the systems administrator.

According to 2015 CRA organogram, the database administration division/sector has 5 administrators: vehicle registry, CS registry, databases, system and network administrator, as well as the sector leader.

Whereas the 2013 Regulation for the internal organization and systematization of jobs of the Ministry of Internal Affairs provides that the Database Administration Sector has other tasks similar to the IT Department within the Ministry of Internal Affairs. The regulation also defines other sectors that have responsibilities similar to those of the Database Administration sector.

Further, the Regulations for the internal organization and systematization of workplaces for CRA have not been updated since 2013. According to CRA officials, this is due to legal issues that are expected to be regulated within CRA.

As a result of the failure to update the regulation, IT management is not done in a hierarchical way, rather IT responsibilities are distributed in different departments. The lack of proper separation of tasks, responsibilities and the failure to create a clear IT structure can cause delays in the provision of appropriate and efficient services for CSS and CRA, create difficulties in the management and administration of CSS, as well as make it impossible to maintain the integrity of the information and processing infrastructure.

2. *CRA lacks IT policies and procedures*

The organization must document, adopt and communicate appropriate policies and procedures to guide business and IT operations in order to achieve its mandate.[14]

CRA has the administrative guidance for the central civil registry as a process, but there is a lack of IT policies and procedures. Although it uses AIS IT regulations and administrative guidelines, these documents are not sufficient to define, design and ensure the availability of information systems, the implementation of security standards in the field of IT for the protection of information assets and implementation of standards and best practices to ensure continuous IT advancement and IT infrastructure maintenance.

14. Information Technology Auditing Handbook, IT Governance Audit Matrix.

CRA has not drawn up internal IT procedures, on the grounds that duties and responsibilities have not yet been clearly defined in the absence of a regulation for the systematization of jobs.

In the absence of IT procedures and policies, there is a risk that employees and third parties will not protect IT assets and the institutional objectives will not be achieved. Also, there is a risk that the information systems will be compromised, considering that the institution holds important and confidential data.

3. ***CRA does not have policies and procedures for managing changes in information systems and does not perform software documentation for the changes made in CSS***

The organization must have policies and procedures for managing changes in information systems, including procedures and responsibilities for recovery of affected areas due to the unintended impact of the change, procedure for emergency changes and updated documentation to reflect the nature of the change. Change controls should be defined in the change management procedure: Change request - validation - acceptance - prioritization - design change - change testing - implementation - documentation.[15]

In absence of policies and procedures for change management, CRA has followed this practice: for the changes it makes in CSS, the CRA, namely the sector of the Central Registry of Civil Status (CRCS) prepares the change request, which is submitted to the project manager, who verifies, prioritizes and approves the request, which is then carried out by the economic operator.

For the changes implemented until February 2022, only the economic operator has performed the testing for the change implemented in absence of testing infrastructure. However, during the audit, after we raised the issue of the lack of a testing system, CRA took action by preparing a testing environment, so that testing can also be performed by the requesting unit. Despite the improvement of the process for carrying out the tests, there are still no records that the testing was carried out, there is no procedure on how a test should be carried out, and no report has been drafted on the carried out tests. As a result of this form of testing, the audit found errors after putting the new version of the system into operation.

The economic operator, after implementing the modified version of the software in the actual system, creates a process manual as a guide for system users, a document which is not satisfactory as an adequate documentation of the software.

After the implementation of changes in the information systems, CRA has no procedure in place for withdrawal from the unwanted changes in CSS. However,

15. Information Technology Auditing Handbook, IT Operation Audit Matrix.

when unwanted changes emerge, CRA asks the economic operator to improve the unwanted changes in CSS.

Also, CRA does not control emergency changes16 in CSS, and uses the same practice for emergency changes as the one used for ordinary changes.

ARC, since it follows an unwritten practice for change management, has not considered it necessary to design IT procedures for changing and testing the application. As a continuation of this, it has not considered it necessary to develop the withdrawal procedure for the unwanted impact during the changes made in the information systems, as well as there is no procedure and it does not control the emergency changes in CSS, since it considers that none of the changes that performed at CSS do not need to be treated as emergency.

In absence of procedures and policies for the management of changes in information systems, there is a risk that undesirable changes will be made in the CSS, which directly affects the provision of services to citizens and jeopardizes the continuity of the system/business.

4. *CRA does not have a plan on the continuity of the information system operation*

The organization must have a plan on the continuity of the work of the information system, which enables the continuation of activities. The AIS policies also oblige the Institutions of the Republic of Kosovo to draw up such a plan. In order to implement this plan, the main work processes of the organization must be identified, the reaction time, the recovery time and the loss period must be determined.[17]

CRA has not developed a plan for the continuity of information systems or business, this is also a consequence of the lack of a defined IT structure with its roles and responsibilities. Despite the lack of a business continuity plan, ARC saves the CSS backup on a daily and weekly basis, but in the absence of hardware space, they are also stored on external drives. Moreover, the new backup overwrites the old one every time, which loses track of previous changes, thus increasing the risk of not identifying certain events.

The lack of a plan for the continuity of information systems and business continuity management increases the risk of failure of ARC processes in the event of a natural disaster or primary systems failure.

16. In emergency changes, change management procedures for defining, authorizing, testing and documenting changes cannot be followed. However, after the implementation of the change, the organization must perform controls to determine whether there are any unforeseen effects of the change on the application and existing security controls and complete the necessary documentation as performed for the management of changes in the system.

17. Information Technology Auditing Handbook, PVB/PRB Audit Matrix.

5. *CRA has not developed a logical and physical infrastructure solution for data recovery for business continuity*

In order to have an effective plan for the recovery of information systems, the organization must define an organizational structure in case there is a need to activate this plan, and must perform testing in certain periods to verify if it can restore the work processes in case of natural disasters or system failure.

CRA has not provided a solution for the information systems disaster recovery centre, but has directed this request to AIS to provide the necessary infrastructure. AIS has treated this request with priority by presenting it as a request in procurement planning. However, the procurement office of the Ministry of Internal Affairs removed this project from its priorities on the grounds that there were several contracts of a similar nature that had to be reviewed in terms of what was included in those contracts. The lack of sufficient justification/ description for the realization of the project for raising the hardware capacities by AIS also contributed to the removal of this project. However, after the necessary clarifications from the requesting unit, this activity/project is expected to proceed in 2022.

The identified deficiencies present a risk of failure and loss of data and work processes of the CRA, which would make it impossible to achieve the continuity of the organization and the provision of services from the civil status.

3.2 Information security

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

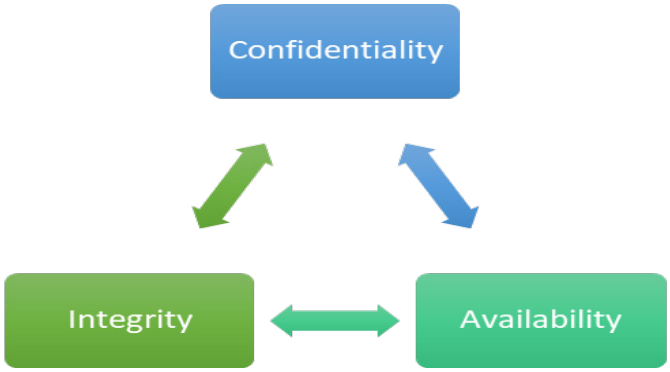

Figure 5. Principles of information security

6. *CRA does not have a policy and operating procedure for information security*

Information security policies cover all operational risks and are capable of reasonably protecting all critical information assets against loss, damage, and abuse. Personnel must understand and maintain information security.[18]

Although there is an AIS administrative instruction[19] in place for the implementation and maintenance of information security, the CRA has not implemented the activities according to this instruction. Additionally, the CRA has not developed an information security operating policy and procedure to provide overall guidance for protecting the organization's confidentiality, integrity, and availability. Likewise, it failed to perform an analysis of the risks related to the exposure of information and incidents, and the CRA staff did not receive any training on information security awareness.

18. Information Technology Auditing Handbook, Information Security Audit Matrix.
19. Administrative Instruction No. 02/2010 on Information Security Management

This happened because the Agency had not assigned specific responsibilities for information security management, therefore the official responsible for the implementation and monitoring of information security policies and procedures in the existing organizational structure had not been assigned.

In the absence of an information security policy and procedure, risk analysis, and defined information security roles, the agency reduces management's ability to assess the organization's exposure to security threats and related risks. It also increases the risk that information security vulnerabilities remain undetected and reduces the ability to protect the information contained in its IT systems and IT assets. As a consequence, unwanted interventions in systems can be caused, and remain unidentified in time.

7. *The CRA does not implement the signing of the confidentiality statement with internal and external parties*

Information security policies must protect all confidential information related to internal and external parties. Employees, contractors, and third-party users should be required to sign a confidentiality or non-disclosure agreement as part of the terms and conditions of their initial employment relationship.[20]

The agency gives civil status officials, consular officials, and economic operator staff access to the civil status system, which contains personal data of citizens, without signing a confidentiality statement.

The CRA is dependent on a third contracting party for the maintenance of the CSS. In the CSS maintenance contract, the confidentiality requirement is part of the general terms of the contract. For breach of confidentiality, there are no specific requirements as regards specific legal procedures. Granting or requesting access, processing, communication, or management of information assets are not defined, and nor are security limits and its obligations, which control how the EO will utilize the organization's assets, the access to information systems and services. As a result, the CRA has considered it sufficient to sign the contract with the EO and the employees so that they agree to the conditions and maintain confidentiality during the contract period.

Likewise, CSS users of the civil status sector in municipalities and consular missions do not sign a statement of confidentiality before opening an account in the system. As a result, in consular missions in the absence of authorized staff, to provide services to citizens of the Republic of Kosovo, officials give credentials to local staff who are not authorized to have access to the CSS.

20. Information Technology Auditing Handbook, Information Security Audit Matrix.

The act of not signing the confidentiality statement was a consequence of the lack of an information security policy, which according to international standards for information security[21] should also contain the control of confidentiality.

Non-signature of the confidentiality statement by officials and third parties who have access to the civil status system puts the Agency at risk in protecting the use, access, and disclosure of information and personal data during the employment relationship and after the end of the employment relationship of the officials as well as the termination of the contract with the EO. In the absence of this statement, system users and third parties are not informed of the responsibility to protect, use, and disclose information in a responsible and authorized manner.

8. *Deficiencies in controls and monitoring of the CSS network security*

The network must be managed and controlled to protect the information in systems and applications. Controls must be implemented to ensure the security of information on the network and the protection of services from unauthorized access.[22] *Remote work must be authorized and controlled.*[23] *Remote access to the state network must be done with an official or professional e-mail account.*[24]

CSS servers are not located in the government domain. Moreover, these servers are not even located in the "Firewall"[25], risking the protection of services from unauthorized interventions and information leakage, as well as making it impossible to monitor and detect intrusions into the information system. The failure to put the CRA servers within the Firewall protection by AIS was a result of the fact that the CRA had requested that the IP addresses of the servers not be changed as it was necessary to reconfigure connections with other institutions that use CRA web services for data exchange.

AIS, due to the existing infrastructure and due to not being able to change IP addresses, has not implemented the placement of servers in the Firewall. At the end of the audit process, we were informed that CRA and AIS have started to take some actions improvement actions for placing the servers in the Firewall[26].

21. ISO/IEC 27001

22. Iso/Iec 27002 on Information Security Controls.

23. Administrative Instruction no. 02/2010 on Information Security Management, Article 38.

24. Standard no. 01/2016 on Internet Access, AIS.

25. "Firewall" -is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.

26. These actions are untested by the audit and remain to be addressed in the future.

Also, deficiencies have been identified during remote access via VPN [27] by CSS administrators and EO officials who provide CSS support. In addition, CRA database administrators and EO employees remotely log into the state network and CSS with one shared account with a generalized name.

In order to realize remote access, the CRA had asked AIS to allow access to a specific account with a general name and which account has access to a specific IP address. This IP address was located on a computer in the offices of the CRA, which serves as the point of communication of the end device with the servers of CSS in the data centre at AIS, which is used to log into the servers of the system in cases where remote work is necessary. According to the manager for database administration, the contractor accesses CSS after being authorized and is under his supervision during the time when the contractor performs actions in the system.

The use of the general account by the administrators of CSS and EO prevents the identification of accesses and interventions in the information system, which intervention can happen more easily in the absence of the placement of servers in the domain and firewall.

9. *Audited institutions have deficiencies in user access controls*

Access policies should provide a basis for controlling access to information. Segregation of duties, and controls should be in place to prevent unauthorized changes to information systems and systems configuration. Access rights to the use of information systems for all employees, contractors, or third parties must be terminated at the moment of termination of the contract, or adapted to changes in responsibilities.[28]

In the CRA, MFAD, the Municipality of Prishtina, and the Municipality of Prizren, there are deficiencies in the management controls of user access to CSS. These deficiencies are the result of the non-implementation of AIS policies and the lack of internal operating procedures for information security that would serve to protect the information within the systems while assisting in their operation and functioning.

27. VPN (Virtual Private Network) - enables an encrypted connection through the Internet from a device to a network.

28. ISACA-CISA Review Manual 27th Edition, 2019, Protection of Information Assets.

Control deficiencies in user access are presented below:

- **In CRA there are no logical access controls even though there are users with full access to CSS.** Database administrators have full access to the CSS database, system server administration, and application administration. This is due to the lack of proper segregation of duties. Also, CSS administrators use general and shared accounts to administer CSS servers, database, and application.

- **It has been identified that in the CSS application there were five (5) officials who were in charge of "Administration".** This role enables opening and closing user accounts, as well as defining and changing roles and responsibilities for user accounts. Furthermore, we have identified that the activities of privileged users are not even monitored in the absence of the information security officer.

- **In CSS, an official has more than one account.** Upon analysing the system, we identified that it provides the option of creating a user account, who can be assigned a role with different privileges depending on the need to perform different work activities. However, the CRA had not used this option. We identified that an official (user) had more than one account with different privileges, and there are cases when a user had up to four (4) active accounts in CSS. According to officials, the opening of more than one account for a user is done because the user performs different work activities that require different privileges (roles). Meanwhile, the roles are not defined by the system administrator, but by the EO. Also, in the CSS application, there were active accounts with non-standardized and non-customized names. Such an account was also used by the EO, but during the audit the CRA took action and deactivated this account.

- **In consular missions, user accounts are used by unauthorized officials.** Only civil status officials and consular officials who are certified by the CRA should have the right to access the CSS. But, upon analysing the traceability related to the activities of the users in the consular missions we identified that some user accounts carried out activities in the system even during the period of annual/medical leave of the officials. This happened due to the lack of officials in some consular missions where consular services are provided. As a result, there is no alternative user who would be a substitute for signing the documents, so the account was used by other officials who were not authorized to access CSS.

- **Access rights for using the CSS of civil status officials or consular officials are not terminated at the moment of termination of the contract**

or change of job position. In the Municipality of Prishtina and the diplomatic or consular missions, we have identified that there are accounts of officials who were not immediately deactivated upon termination of the employment relationship or change of job position. In addition, some user accounts have had activities on CSS even after the termination of the employment relationship. This is due to the fact that the Ministry of Internal Affairs and Diaspora and the municipalities do not immediately notify the CRA about the deactivation of the officials' accounts in the CSS. However, the civil status officials themselves willingly notify the CRA to cut off access to CSS. At the end of the audit process, the MFAD has taken actions regarding the notification for suspending the accounts of officials in the system who finalized the mission at the consular offices. However, MFAD needs to provide controls regarding this process.

- **CRA does not perform a periodic review of access rights of CSS user accounts.** During our analysis, we identified 32 user accounts that are active and have not logged into CSS for more than 6 months. There were accounts that have not been logged into the system since 2015. As a security measure, in August 2021, the CRA implemented a procedure in the system which automatically blocks user accounts in cases where the user does not access the system for 30 days. Also, the CRA does not perform a periodic review to manage whether the user account should be active and whether the role and privileges of CSS officials match the job position.

The non-separation of duties and the lack of monitoring of users with full access to CSS might put a risk that would cause deliberate and unauthorized transactions to be carried out/changed/deleted. Likewise, the transactions carried out in the CSS may not be identified and it may be impossible to preserve the integrity of the data and the information and processing infrastructure. Using full access accounts exposes the entire information system to intentional or accidental risks.

Not terminating access to user accounts in time and not controlling user account access to CSS, may also pose risks since system users would be able to deliberately perform unauthorized activities that would affect the protection of personal data, disclosure of information, and loss of reputation of institutions.

10. *Shortcomings in password management*

The defined criteria for password management must be configured in the information system. The password must be changed at certain periods of time.[29] *The procedure for password management must be read and understanding the procedure must be mandatory for users of the systems.*[30]

In CRA, it was identified that there was no password complexity configured in "Active Directory31 for official accounts. Likewise, both in the CSS application and in the "Active Directory" the requirement to change the password at least every six (6) months is not implemented and requirement for the minimum number of password characters in the systems is not implemented either. In CRA, as a protective measure, the use of authentication cards has also started, as the second factor of computer authentication.

As regards the "Active Directory" subdomain in the Municipality of Prishtina and the Municipality of Prizren, the request for the user to change the password of the official account in certain periods of time was not configured and during the activation of the account, the user is not obliged to change the initial password.

Due to the lack of an internal procedure for the management of passwords in information systems and in the absence of an information security officer who would control the implementation of the procedures, the CRA and the municipalities had neglected the implementation of the criteria for passwords in the systems.

Failure to implement the established criteria for password management in systems risks that the password of the accounts will be discovered by unauthorized persons and these accounts will be misused, as well as the accountability of user activities cannot be implemented.

11. *CRA's shortcomings in the control and monitoring of audit trails*

There are sufficient audit trails that capture modifications, authorized records of critical transactions. Audit trails are reviewed periodically to monitor abnormal activities. Audit trails are properly maintained and stored, unique and sequential numbers or identifiers are assigned to each transaction.[32]

29. Regulation no. 02/2015 on the official e-mail account.

30. ISACA – CISA Review Manual 27th Edition, 2019.

31. Active Directory is a Microsoft service for authorizing and authenticating IT users and devices in the organization's network domain.

32. Information Technology Auditing Handbook, Information Security Audit Matrix.

The CRA in the CSS application has well implemented the traceability of user activities in the application. However, we have identified that database administrators have full access to audit trail tables in the CSS database. So the traceability data is not protected from modification. Furthermore, there is no monitoring of the activities of the database administrators who have full access to the systems and of the economic operator who has access to the application. This is due to the lack of the information security officer and the information system for monitoring the activities of users in the systems. The CRA checks user activity in the CSS application only with a special request for any civil status official account.

Also, the CRA has deficiencies in the control and monitoring of audit trails during data exchange. Regarding the exchange of data with public and private institutions, which is carried out through web services, the CRA does not have complete audit traceability. There is no information on which user of the institution has accessed and which IP address requested to receive such data. This is because the CRA has not developed this function. However, data exchange through the Government Gateway (GG) platform[33], which is administered by AIS, provides the necessary audit trail data. Data exchange via web services is now only done with institutions that are not integrated into the interoperability platform.

Lack of audit trail monitoring makes it impossible to identify unauthorized user activities in time. Moreover, database administrators' full access to audit trails can result with changes/misuse of data in systems by bypassing or deleting audit trails. Also, the lack of audit trails of user activities through data exchange increases the risk of disclosure of information and protection of personal data, and makes it impossible to identify who made the transaction.

33. The centralized platform that interconnects the systems of institutions, the public and private sectors.

3.3 Application controls

Application controls are controls over the input, processing and output functions. This includes methods to ensure that: only complete, accurate and valid data is entered and updated in an information system, processing accomplishes the desired tasks, processing reports meets the expectations, and the data is stored.

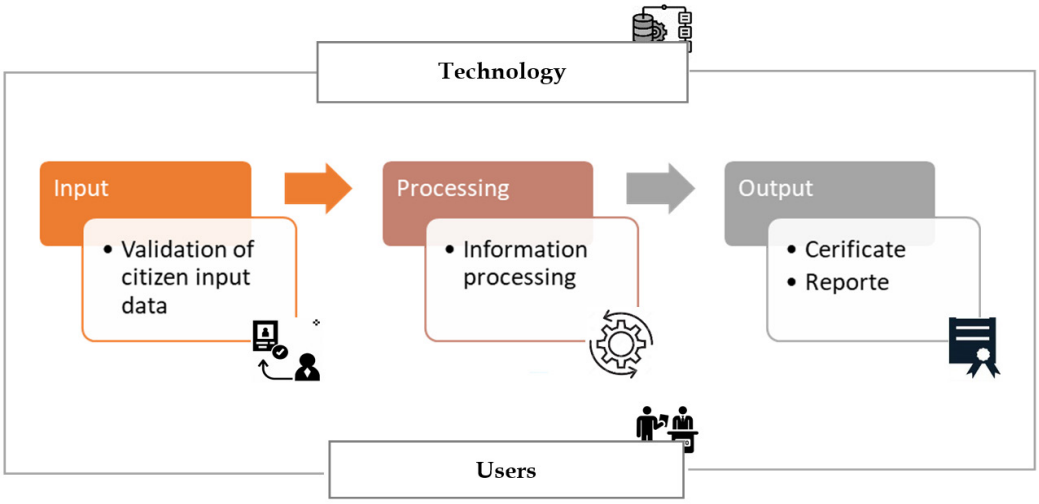

Figure 6. Data input-processing-output model in the information system

12. ***In CSS there are deficiencies in the search for data on the citizen and it allows the registration of a citizen with the same data more than once***

Validation rules must be well designed, documented, and implemented in input interaction. The application properly rejects invalid data. Validity criteria are updated in an appropriate and authorized manner. Controls must exist in the information systems to establish the level of authorization of transactions which should be implemented through various controls, and there must be a correct segregation of duties for the establishment and approval of data.[34]

During the analysis of the data on the registration of citizens in CSS, we identified that the system allows the registration of the same citizen more than once. So, if only one marked letter of the name or surname that has the same meaning, but is marked in different languages, is treated as a different character. Although CSS supports the use of official languages, the system has not developed a function for comparing the content of characters/letters in different languages, e.g. (Sh, š, Ş).

34. Information Technology Auditing Handbook, Application Controls Audit Matrix.

This has happened because when the civil status official searched for the citizen in CSS to verify whether he is registered or not, he searches for the citizen's data with one of the letters of the alphabet in another language, or one other

different character was used compared to the one he/she previously used to register, and thus the system does not identify that citizen is already registered. So the system allows the continuation of the steps for the registration of the same citizen, as a new citizen.

Also, in CSS there are no authorization controls for placing data in the application. The rules for approving input data have not been developed in CSS. The official who registered the data also approves them in the system. So, during the registration of citizens' data in CSS, double verification of data is not done to assess their accuracy.

From the analysis of the citizens' data, it was identified that the civil status official recorded the data incorrectly by permuting the letters in the name or the numbers in the birthday. However, as a measure to verify the accuracy of the notes, the CRA has developed in CSS the pre-printing of the notes that have been placed in the system, for the citizen to confirm and sign that those data are correct. Then the citizen's data is registered. Also, the CRA has created a special role for the first time registration in the CSS, for citizens over the age of 18, and the civil status offices have determined the officials responsible for the possibility of registering these citizens.

However, during the analysis of the citizens' register, 855 citizens registered twice in CSS were identified, who have two different personal numbers, of which 237 have the same name and date of birth, as well as the same name and date of birth of their parents, but the physical ledger data is different in some field in the system. Some of these cases are citizens who have a temporary number as a result of data migration in the system in 2013 and a personal number that was generated by the system.

Also, 7255 records were identified in the citizens' register, where two to seven different citizens were registered in the system with the same data of the physical book of the civil status register. Apart having few cases that resulted from not adequately referencing physical books in different offices of the same Municipality, there is no other explanation for these cases. CRA has developed the function for limiting the registration of citizens with the same book number. However, the registration process in the system has shortcomings as the verification and approval of the data registered in the CSS is not done before the citizen's data is registered. Likewise, the system has not been developed to enable the attachment of documents (birth/death or marriage certificates, municipal

or judicial decisions, book data, etc.) of the citizen to the system to assess the accuracy of the data. As a result, the official can record data other than those in the citizen's file.

This makes the authenticity and accuracy of the data difficult and makes it impossible to verify those inaccuracies in time. Moreover, these shortcomings in the CSS risk that the data of the citizen who is equipped with two personal numbers, will be misused by providing citizenship to the non-resident citizen of Kosovo. Also, this leads to inaccurate statistical data of citizens registered in the Republic of Kosovo.

13. *CRA has not established adequate input validation controls for the address field in CSS*

The application must have validation procedures in place to protect against data entry errors.[35]

According to the law on address system[36], the Cadastre Agency is responsible for the database for all address designations. However, during the registration of the citizen or the change of the address data, the address field of the citizens in CSS does not get the data from the address system in the cadastral register, but the data is only recorded in the address field by the official as plain text. The lack of a connection between the database of the civil status system and the cadastral system is because these agencies have not yet determined the method of connecting the systems.

As a consequence, we do not always have accurate data in the address field and we also have duplication of address data at the state level, given that the CSS also provides data to other systems through the connections it has made. Therefore, the impact of incorrect addresses also causes an effect on those systems that receive data from the CSS and as a result, the correct address of the citizen is not identified, which also affects the preservation of public safety and the improvement of services for citizens.

35. Information Technology Auditing Handbook, Application Controls Audit Matrix.

36. Law No. 04/L-071 on Address System.

4 Conclusions

Information technology governance

The CRA does not have a clear IT structure, and this is also a consequence of the lack of updating and improving the internal organization regulation. As a result, the CRA has failed to define roles and responsibilities for the management and administration of information systems, causing duplication and conflict of responsibilities. Although the CRA uses AIS policies, it has not made an assessment of their use or implementation. Also, CRA has not drafted internal IT policies, jeopardizing the achievement of the Agency's objectives.

In the absence of a procedure for managing all changes in the CSS, the CRA has deficiencies in controlling changes in the system. Also, the testing for change is not performed by the requesting unit but by the EO which implements it directly in the productive environment. As a consequence, there are cases when undesirable changes occur in the application which directly affect the service provided to citizens for civil status and also jeopardize the continuity of the system - business.

The CRA has not provided sufficient mechanisms for the continuity of the CSS work. It has not drawn up a plan for the continuity of the system's work, and it has not made logical and physical infrastructure solutions for business continuity and data recovery. Therefore, there is a risk that in the event of a natural disaster or system failure, the CRA may not be able to restore the necessary critical data in an optimal time, increasing the risk of data loss and service delivery.

Information security

The CRA does not implement effective controls to mitigate vulnerabilities that could result in loss of system integrity, confidentiality and availability. Policies and procedures for information security have not been drafted, and there is no designated information security officer. As a result, the CRA has not ensured that the likelihood and impacts of operational risks have been properly assessed. Likewise, staff training for information security awareness has not been carried out.

The signing of the confidentiality statement for CSS users, contractors and third parties is not applicable, risking the protection of confidentiality and the integrity of citizens' data. Also, there is a lack of information and awareness of users regarding their responsibilities to protect and use information in a responsible and authorized manner.

The CRA does not perform controls and monitoring to protect the security of CSS's information on networks as well as controls on user access to systems,

increasing the risk of unauthorized intrusions into systems, disruption of services, leakage of information, and failure to protect personal data. The use of general administrator and shared accounts have been allowed, database administrators have been given access to the application, and the CSS application has been allowed to be administered by multiple CRA officials, jeopardizing the accountability of the activities of the users who administer the system and the reliability of the data.

The CRA does not carry out controls and monitoring for database administrators who have full access to audit trail logs, and there is no regular monitoring of user activities in CSS. Likewise, there is no full traceability for the data exchanged through web services with other institutions. As a result, unauthorized user activities may not be identified, which increases the risk of personal data protection and information disclosure.

The MFAD and the Municipality of Prishtina no longer notify the CRA on time to deactivate user accounts upon the termination of the employment contracts or the change of official position, and the CRA does not periodically review user accounts of the CSS to ensure that they remain suitable for their role. As a result, the integrity and exposure of personal data has been jeopardized since the credentials of officials who have terminated their employment relationship or do not have authorization have been used.

Also, the regulations and standards for password management in information systems do not apply to CSS user accounts. These shortcomings do not guarantee the security of user accounts from cyber misuse. As a consequence, the integrity, confidentiality, and protection of data in the information system are at risk.

Application controls

The CRA has continuously made developments in the CSS to improve the quality of the data recorded in the system, but not all the data are correct. It has been identified that the system contains citizens who are registered twice as well as there are citizens who have two personal numbers. Also, there are different citizens registered with the same book number. These shortcomings in the system may allow the official to register the citizen without validating and verifying the accuracy of the data, and risks that the citizen's data will be misused.

The CRA has not validated the field for the registration of the citizen's address in the CSS, because the method of connecting the CSS with the information system of the Cadastral Agency has not yet been defined. As a consequence, text may be entered by the official in the address field and lead to errors in the citizen's address registration. This also affects the exchange of information with other systems, the provision of citizen services, and public safety.

5 Recommendations

The following recommendations were provided to the Ministry of Internal Affairs and the Civil Registry Agency:

1. **IT Structure.** Ensure that the IT structure is clearly defined in the internal organization regulation, dividing roles and responsibilities for the management and administration of information systems, databases, infrastructure, and information security;

2. **IT policies and procedures.** Design, approve and implement information technology policies and procedures, communicate them in order to provide leadership and oversight of daily operations for the administration of information systems. Create mechanisms for monitoring their implementation as well as draw up reports on the level of policy implementation;

3. **Management of changes in systems.** Design, approve and implement policies and procedures for change management in CSS. The CRA must make the request to the economic operator to carry out the software documentation for every change that is made in the CSS and ensure that the software documentation is carried out;

    3.1. **Withdrawal procedure.** Design, approve and implement the withdrawal procedure for the unwanted impact during the changes made in the information systems and implement it for any unwanted changes in CSS;

4. **Plan and policies for business continuity.** Design, approve and implement the continuity plan based on IT standards and best practices for business continuity;

5. **Systems recovery plan.** Prioritize the implementation of IT projects in order for AIS to create a physical and logical, infrastructural solution, based on ISO IT Standards for continuity of CSS;

6. **Information security policy and procedure.** Draft, approve and implement the information security policy, which defines the organization's approach to managing its objectives on information security. The policy should be communicated to all employees and relevant external parties, and should create mechanisms for monitoring the implementation of the policies and draw up reports on the level of their implementation;

6.1. Risk analysis. Perform risk analysis and management to protect the organization's information. Risk analysis includes determining the value of each organization's information system as well as the degree to which the organization is exposed to risk;

6.2. Training plan. Provide and implement a training program for the awareness of all staff on information security;

7. **Confidentiality statement.** Implement the signing of confidentiality and non-disclosure statements with employees, contractors and external parties before allowing access to the civil status system;

8. **Network Security**. Place the CSS servers in the state domain and perform the proper configuration of IP addresses for placing the CSS servers in the "Firewall". AIS should install the servers of this system in the "Firewall";

8.1. VPN access. CRA should create personalized accounts for users who have access to the VPN, so that every action can be traced, leading to the responsible person, and all access and activities in the information systems are monitored;

9. **Access management procedures.** User institutions of CSS[37] should implement AIS policies and design, approve and implement the internal procedure for managing access and privileges of users in information systems;

9.1. Privileged accesses. The CRA should make the separation of duties for the administration of the systems and the database. As regards the system and database administration personalized accounts should be opened and used, and user activities should be monitored;

9.2. Application administration. CRA should appoint a permanent official and an alternative official for the administration of the CSS application, and other accounts which administer the application should be deactivated;

9.3. User Accounts. The CRA should ensure that in CSS the usernames are unique and the account is adapted to the job role and responsibilities. User accounts should be standardized and personalized. Duplicate accounts in the CSS application should be deleted and the EO should be prohibited from accessing the real system and the productive (real) system versions except for read-only access, with special approval and supervision by CRA;

37. Ministry of Internal Affairs, Civil Registry Agency, Ministry of Foreign Affairs and Diaspora and Municipalities of the Republic of Kosovo.

9.4. Access rights. The Ministry of Internal Affairs and Communications in consular missions should establish an alternative official for the provision of consular services and the accounts of consular officials should not be used by other officials who are not authorized to access the CSS;

9.5. Termination of access and change of privileges. The MFAD and the municipalities must timely notify the CRA upon terminating the employment relationship of the civil status officer/consular officer or upon changing his job responsibilities, deactivating the user account, or adjusting privileges to the job position at CSS;

9.6. Periodic review of accounts. CRA should review the access rights of CSS users on a 6-monthly basis at least, to ensure that they are valid and appropriate for their job function. It should also deactivate the accounts of officials who have terminated the employment relationship;

10. Password Management. CSS user institutions should design, approve and implement the internal procedure for password management based on administrative instructions on the official email account and international standards for information security;

11. Audit trail control. The CRA must protect audit trails from modification/ deletion. A copy of the audit trails should be stored in real-time and they should not be in the control of the CSS database and systems administrators, to ensure the integrity of the audit trail data. It should also provide mechanisms for monitoring the traceability of user activities in information systems;

11.1. Audit trails on web services. CRA should exchange data with other information systems through the most secure platform-GG. As regards systems that cannot exchange data with this platform, CRA should make the necessary developments in web services, so that there is full traceability of user activities;

12. Citizen's search. The CRA should develop the function in the CSS to search so that when a citizen's data is written with a letter/character in different languages but with the same meaning then the citizen should appear if he/ she is registered;

12.1. Level of records' authorization. The CRA should develop in the CSS the division of transaction authorization levels and apply them through controls for placing the citizen's data in the application and for the approval of the data before the citizen's registration in the system;

12.2. Attaching documents to the system. CRA should develop in CSS the possibility of attaching electronic documents of the citizen based on which the registration or change of his data is done, so that the authenticity of the documents is enabled;

12.3. Data quality. The CRA should verify the citizens registered twice in the CSS and assess which are the correct data of that citizen and it should block the other personal identification number from receiving services; and

13. Address field. The CRA should implement the link of CSS to the Cadastral Agency database and the data for the address field should be validated by this database.

The recommendations are related to the findings presented and the issues within them, resulting in 27 recommendations.

Annex I. Audit design

Areas of risk and indicators of audit problems

The Civil Registration Agency (CRA) uses the information system for better management of civil status registration. The Civil Status Information System contains data for every citizen of Kosovo, foreign citizen, or stateless person with temporary or permanent residence in the Republic of Kosovo, as regards registration, completion, change, correction, cancellation, issuance of certificates, and updating the civil registry data.

This system enables faster information regarding the identity and vital events of the individual and citizens are able to be provided with official documents. Also, this system interacts with other information systems of the public and private sector for the exchange of data in electronic form, providing updated and timely data.

Preservation of confidentiality is one of the main principles of the central registry of civil status, and the CRA must ensure the accuracy and completeness of the data recorded in the information system through which these data are managed. So, attention should be focused on maintaining confidentiality, data privacy and data integrity.

Research and analysis of CSS documents has identified that there are deficiencies in the protection of personal data, namely in maintaining the confidentiality of data from system users and from the contractor and third parties. Likewise, the process of connecting the civil status system with the unique address system has not yet been completed, which is an obligation derived from the implementation of the recommendations from the European Monitoring Mission for the electoral process and electoral reform, a process which is found in the program of European Reform Agenda (ERA2).

During the visits made with CRA officials, it was identified that there are deficiencies in policies and procedures for information security. There is no procedure for managing changes in the CSS and test system, making the changes of functions directly in the real system (production system), and there is no business continuity plan in case of any disaster, risking the availability of information. The remote access of the economic operator is realized with VPN using the generalized account which is used by the head of the IT unit in CRA. In the CSS user list, there are active users identified in the system who have not logged in since 2015.

Review of the problem indicators identified from various sources as well as from our assessments based on the Active IT Audit Manual for the identification of the most risky areas from the received documentation and the meetings held with the persons responsible for the management of the information system for the registration of civil status leads us to the main problem of administration and information security of the Civil Status System.

System description

The establishment, organization, structuring, tasks, responsibilities and financing of the Civil Registration Agency, which was established as an agency within the Ministry of Internal Affairs have been regulated pursuant to Article 65 (1) of the Constitution of the Republic of Kosovo, as well as the Law on the Civil Registration Agency (CRA). The Civil Registration Agency is the highest civil status service body.

The organization and internal structure of the Agency has been arranged as follows: the Office of the General Director and four directorates with a total of 15 sectors, as well as 4 separate sectors within the Office of the General Director.

The CRA is responsible for all processes related to the application, personalization and issuance of documents for citizens of the Republic of Kosovo and foreign citizens and, among other things, administers and maintains the database of the central registry of civil status. As for the administration of civil status registration actions CRA uses the "Civil Status System" information system, which has been developed on the platform. NET[38] and the database is on the SQL platform. This system provides the basis of the population register and unique identification.

The Central Registry of Civil Status (CRCS) is established by collecting and updating data from Principal Registers of Civil Status and Special Registers. The CCSR is established through the procedure of transferring personal data from the physical registers of persons found in the principal registers of civil status, special registers and new facts of birth, marriage and death, to the electronic register by the authorized official of the status civil or consular officer. The actions taken by the Civil Status Sector are shown in figure 1.

38. NET is an open source developer platform for building applications.

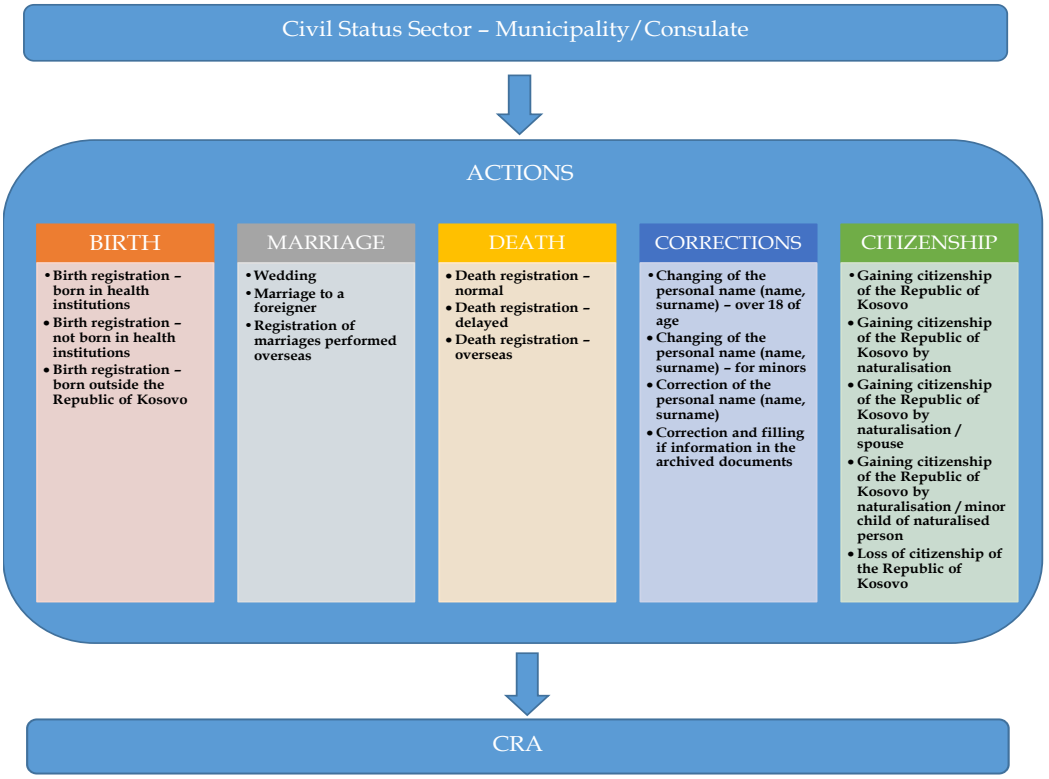

Figure 1. Description of the Civil Status System

Role and responsibilities of the parties

Duties and Responsibilities of the CRA

- Is responsible for all processes related to the application, personalization and issuance of documents for citizens of the Republic of Kosovo and foreign citizens;
- Registers vehicles and issues driver's licenses;
- Administers and maintains the database of the central registry of civil status; Cooperates with the authorities of foreign countries regarding issues related to the field of its activity;
- Proposes and initiates the issuance or completion and amendment of the scope of laws and sub-legal acts;
- Provides professional and efficient services to all citizens;
- Performs work and other tasks within the competence of the agency.

Directorate of Civil Status

Administration of the Central Register of Civil Status (CRCS) is done by the CRA, respectively by the Directorate of Civil Status and the Sector of the Central Registry of Civil Status. The relevant official of the CRCS in CRA has the right to perform actions in the CRCS after having administered the basic documents in accordance with the relevant legislation in force.

The duties and responsibilities of the Directorate of Civil Status are as follows:

- Ensures the implementation of relevant policies and legislation on civil status;
- Supervises, organizes, and coordinates the work related to the registration of civil status facts that are located in Kosovo and abroad;
- Provides support in planning, organizing, and supervising the work of municipal civil status offices;
- Administers the central registry of civil status;
- Prepare periodic and annual reports on the general situation of civil status;
- Drafts and assists in the preparation of normative acts related to the Directorate of Civil Status.

The Civil Status Sector, the Verification Sector, and the Sector of Central Registry of Civil Status are part of this Directorate.

Civil Status Sector in CRA

The duties and responsibilities of the Civil Status Sector are as follows:

- Ensures coordination and implementation of civil status policies in Kosovo;
- Ensures the implementation of rules and procedures for civil status;
- Plans, organizes, and manages the procedures of authentication, verification of civil documents, verification stamp, data collection, data protection, and storage;
- Communicates and cooperates with municipal civil status offices, as well as other bodies related to all civil status issues;

- Organizes and coordinates work related to the registration of civil status facts of persons located outside Kosovo, foreign citizens located in Kosovo, as well as informs the relevant countries;

- Handles requests and offers recommendations for the authorization of persons to sign certificates in the municipalities, for the form and content of the certificates, and for any eventual change in the civil status, in which case he/she notifies the liaison offices and foreign governments;

- Is responsible for developing effective systems and procedures for civil documentation.

Sector of the Central Registry of Civil Status

The Central Registry of the Civil Status Sector (CRCS), which operates within the Directorate of Civil Status in CRA, is responsible for the establishment, expansion, operation and technical maintenance of the CRCS.

The duties and responsibilities of the Central Registry of Civil Status Sector are as follows:

- Creates and administers the central registry of civil status;

- Approves and keeps evidence related to the requests for use of the central registry of civil status by civil status officials;

- Evidences mistakes made by civil status officials and helps to find possible solutions;

- Saves and secures the other electronic copy (Back-Up) of the central registry of civil status;

- Proposes special measures that guarantee the security of data in the central registry of civil status;

- Provides reports and statistics for all components of civil status of citizens who are registered in the central registry.

CRA Database Administration Sector

The duties and responsibilities of the CRA Database Administration Sector are as follows:

- Prepares strategies for the security and maintenance of databases that are within the CRA in coordination with the DASK of the MIA;
- Ensures the operation of all databases which are under the competence of this sector and the CRA;
- Manages and monitors applications and all existing databases under the responsibility of this sector and the CRA;
- Administers all electronic data registers in the CRA, in cooperation with the sectors and directorates of the CRA and with the DASK of the MIA;
- Collaborates closely with other sectors and directorates of the CRA, to implement the change process in applications and databases, respecting the needs for system security, quality and efficiency, support, and training;
- Closely cooperates with the responsible officials of the CRA sectors and departments, during the evaluation of the needs and the preparation of the documentation related to the security of the databases under the competence of the CRA;
- Maintains the IT infrastructure in the CRA directorates;
- Manages network infrastructure and computer maintenance in CRA directorates and local units in municipalities in cooperation with DASK;
- Coordinates all IT activities of the CRA, with the DASK of the Ministry of Internal Affairs.

Civil Status Sector in Municipalities

The Civil Status Sector consists of civil status officials who perform actions of civil status service such as completing, updating, and administering civil status registers, developing administrative procedures, maintaining civil status acts, issuing civil status documents as well as other legal administrative actions in accordance with the legislation in force.

The Civil Status Sector, at the request of the party, issues these types of civil status documents and performs the following actions in Figure 3:

Documents	Actions
•*Birth certificate;* •*Extract from the Central Registry of civil status;* •*Certificate of citizenship;* •*Marriage certificate;* •*Death certificate;* •*Residence certificate;* •*Certificate of marital status;* •*Declaration of the joint household;* •*Evidence from the archive;* •*Act of death;* •*Certificate on family breadwinner;* •*Residence document.*	•*Minutes for the acceptance of paternity/maternity;* •*Actions in case of marriage registration;* •*Actions in case of birth registration;* •*Actions in case of death registration;* •*Actions related to the acquisition of and release from citizenship;* •*Develops procedures for changing and correcting the personal name;* •*Subsequent registration;* •*Re-registrations;* •*Change of residence;* •*Correction of name and surname as well as other personal data.*

Figure 7. Types of documents and actions carried out by the Civil Status Sector

In order to obtain a civil status document, the civil status officer may request additional documentation from the party to verify the factual situation.

Consular service in diplomatic missions - Registration of acts of civil status

In the consular missions previously allowed by the decision of the Minister of Foreign Affairs, the head of the consular mission assumes the functions of civil status officials in maintaining and registering civil status acts. In order to fulfil this duty, he/she keeps the registers of births, deaths, and marriages. The head of the consular mission:

- Officiates/performs acts of marriage, if this is allowed by the laws of the receiving country and if at least one of the spouses is a citizen of the Republic of Kosovo, as well as issues marriage certificates. Marriages by the head of the consular mission are registered in the marriage register and the Ministry of Foreign Affairs is notified, in order to perform further actions;

- Registers in the register of marriages the marriages of citizens of the Republic of Kosovo, concluded by the relevant authorities of the receiving state, according to the laws in force of the Republic of Kosovo and the receiving state, based on official certificates;

- Issues the marriage license for citizens of Kosovo, defined by the relevant law of the Republic of Kosovo, if the marriage is concluded in the civil status offices in the consular district of the receiving state, in case one of the spouses is a foreigner.

- Registers in the birth registry citizens of the Republic of Kosovo born in the consular district, based on official certificates issued by the relevant local authorities. In defined deadlines, the relevant acts of civil status of births, deaths, and marriages are sent to the Ministry of Foreign Affairs in order to be forwarded to the competent authorities of Kosovo.

Audit scope and questions

The scope of this Audit will cover the following:

- The CRA Database Administration Sector which is responsible for the management and maintenance of applications and databases;

- Civil Status Directorate, namely the Civil Status Central Registration Sector which is responsible for the creation, expansion, operation, and technical maintenance of the CRCS and the Civil Status Sector which is responsible for the development of effective systems and procedures for civil documentation;

- The Civil Status Sector in the Municipality of Prishtina, as the municipality with the largest number of citizens, and the Civil Status Sector in the Municipality of Prizren as the municipality inhabited by communities that use more official languages.

During the execution of the audit, a visit to the Consulate of Kosovo in Zurich was planned, as the consulate with the largest number of issued documents and with the largest number of errors during the use of the CSS, but after the director's comments on the lack of financial means and the impossible travel abroad, the scope shall only cover the country of Kosovo.

The focus of the audit will be the Information System for Civil Status, which serves for the administration of the central register of civil status, and which is used by Civil Status Offices and diplomatic or consular missions of the Republic of Kosovo.

The audit will cover the period from 2020 and until the period of the audit phase.

Audit questions

1. Is there an organizational structure, policy, and procedure that enable the organization to achieve the mandate for the institution's goals?

2. Does the organization implement a standardized procedure for controlling all changes to key IT systems and applications?

3. Are emergency changes properly controlled when change management procedures for defining, authorizing, testing, and documenting changes cannot be followed?

4. Does the organization have a sustainable plan and procedures for business continuity?

5. Are there effective business continuity policies in the organization?

6. Does the organization have an appropriate strategic direction and support for information security regarding security policies, its coverage, and awareness at the organizational level?

7. Does the organization have clear and efficient policies on access controls?

8. Has the organization ensured controls so that only authorized users have access to information?

9. Does the application have adequate controls for input validity?

10. Have valid data been entered by the authorized person in the application?

11. Does the application ensure that output information is complete and accurate before further use and that it is stored appropriately?

12. Is the storage of the results of the data properly organized?

13. Are the application's tracking mechanisms sufficient for its purpose?

14. Is the application information secure in case of misuse?

Through these questions, we aim to find out if the CCS maintains the security, privacy, and integrity of the data in accordance with the standards and good practices of the information systems.

Audit criteria[39]

The criteria used in this audit are derived from international standards of information technology/information systems[40], control objectives for information technology, good practices from the field of information technology[41], the Active IT Audit Manual[42] and laws and regulations of civil status.

In order to evaluate IT governance in CSS, through the definition of IT requirements, and policies and procedures for the operation of the information system, the following criteria have been established:

- The IT structure within the organization must be defined, and its roles and responsibilities must be clearly defined to properly maintain IT services.

-The organization must document, adopt and communicate appropriate policies and procedures to guide business and IT operations in order to achieve its mandate.

-The organization must have policies and procedures for managing changes in information systems, including procedures and responsibilities for recovery of affected areas due to the undesired impact of the change, procedure for emergency changes, and updated documentation to reflect the nature of the change. Change controls should be defined in the change management procedure: Change request - validation - acceptance - prioritization - design change - change testing - implementation - documentation.

-The organization must have a plan on the continuity of the work of the information system, which enables the continuation of activities. For the realization of this plan, the main work processes of the organization must be identified, and the reaction time, the recovery time, and the loss period must be determined.

-In order to have an effective plan for the recovery of information systems, the organization must define an organizational structure in case of the need

39. For more information consult ISSAI 300, Criteria, p.7

40. International Standards of Supreme Audit Institutions issued by the International Organization of Supreme Audit Institutions (INTOSAI) & Information Technology Audit and Assurance Standards and Guidelines issued by the Information Systems Audit and Control Association (ISACA).

41. Control Objectives for Information and Related Technologies (COBIT) issued by the IT Governance Institute & Information Technology Audit Manual, a product of the EUROSAI Information Technology Working Groups (WGITA) as well as the INTOSAI Development Initiative (IDI) & CISA revision manual, edition 26, 2016.

42. The Information Technology Audit Manual is a product of the EUROSAI Information Technology Working Groups (WGITA) as well as the INTOSAI Development Initiative (IDI) for the definition of Information Technology Audit standards, further Information Technology Audit Handbook.

for the activation of this plan and must perform tests in certain periods to verify if it can restore the work processes in case of any natural disaster or systems failure.

In order to assess that the CRA has mechanisms for information security, the following criteria have been established:

- Information security policies cover all operational risks and are able to reasonably protect all critical information assets against loss, damage, and abuse. The personnel must understand and maintain information security.

- The head of the civil registration agency authorizes the provision of data requested by various institutions and bodies, in accordance with the guidelines approved by him/her and the Council of the state agency for the protection of personal data. The guide determines the type and amount of information that can be provided to the requesting institutions and bodies, taking into account the laws that regulate their organization and operation, as well as the legislation in force for the protection of personal data.

- Information security policies must protect all confidential information related to internal and external parties. Employees, contractors, and third-party users are required to sign a confidentiality or non-disclosure agreement as part of their initial terms and conditions of employment.

- The network must be managed and controlled to protect the information in systems and applications. Controls must be implemented to ensure the security of information on the network and the protection of services from unauthorized access.[43] Remote work must be authorized and controlled[44]. Remote access to the state network must be done with an official or professional electronic account.

- Access policies should provide a basis for controlling access to information. Segregation of duties, and controls should be in place to prevent unauthorized changes to information systems and systems configuration. Access rights to the use of information systems for all employees, contractors, or third parties must be terminated at the time of termination of the contract, or adapted to changes in responsibilities.

43. Iso/Iec 27002 for Information Security Controls.

44. Administrative Instruction no. 02/2010 on Information Security Management, Article 38.

- Defined criteria for password management must be configured in the information system. The password must be changed at certain periods of time[45]. The procedure for password management must be read and knowledge of the procedure must be mandatory for users of the systems.

- Sufficient audit trails that capture modifications, and authorized records of critical transactions are in place. Audit trails are reviewed periodically to monitor for abnormal activities. Audit trails are properly maintained and stored, and unique and sequential or identifying numbers are assigned to each transaction.

In order to assess that CSS has application control mechanisms that enable safe, logical, and reliable access to the information system, the following criteria have been established:

- Validation rules are well-designed, documented, and implemented in input interaction. Invalid data is properly rejected by the application. Validity criteria are updated in an appropriate and authorized manner. There are controls on the information systems for setting transaction authorization levels and they are implemented through various controls, and there should be accurate segregation of duties for setting and approving data.

- The application must have validation procedures to protect it against errors when entering data.

45. Regulation no. 02/2015 on Official Email Account.

Audit methodology

In order to answer the audit questions and in order to support the audit conclusions, we will apply the following methodology:[46]

- *Analysis of the legal and regulatory frameworks of the CRA, which are determining criteria for the implementation of civil status registration;*
- *Review of the organization structure of the IT sector;*
- *Analysis of policies and procedures designed for IT systems;*
- *Checking if the responsibilities for IT security are well defined;*
- *Checking if there is a process for prioritizing proposed security initiatives, including required levels of policies, standards, and procedures;*
- *Analysis of documents for the protection of privacy and confidentiality;*
- *Analysis of documentation of cases of processes and of the workflow which is applied in the civil status registration system, as well as the user manual of the system;*
- *Analysis of tables obtained from the CSS database with CAAT tools (IDEA, Excel) to assess data sequences and data harmonization;*
- *Assessment of information security and logical access to applications and databases;*
- *Evaluation of input and output controls of the application;*
- *Reviewing documents to assess that policies address business continuity requirements by defining the organization's sustainable objectives, organizational structure, and responsibilities for contingency planning; and*
- *Conducting interviews with responsible officials.*

46. The methodology to be used is detailed in the audit matrix.

Relevant documents

List of laws and regulations relevant to this audit:

- *Law No. 04/L-003 on Civil Status;*
- *Law No. 04/L-160 on Civil Registration Agency;*
- *Regulation (GRK) No. 36/2013 on the Internal Organization and Systematization of Jobs in the Ministry of Internal Affairs;*
- *Administrative Instruction (MIA) No.11/2017 on Central Civil Status Registry;*
- *Administrative Instruction (MIA) No.25/2013 on Civil Status Documents;*
- *Administrative Instruction (MIA) No.17/2015 on the General Registration Procedures of the Fact of Birth, Marriage and Death;*
- *Administrative Instruction (MIA) No.19/2015 on the Conditions and Procedures for Personal Name Change and Correction;*
- *Administrative Instruction (MIA) No.06/2016 on Personal Number;*
- *Administrative Instruction (MIA) No.24/2015 on the late Registrations in the Civil Status Registers;*
- *Administrative Instruction (MIA) No.12/2018 on the Conditions and Procedures of Passing the Professional Examination for Civil Status Officials;*
- *Regulation (MPA) No. 01/2018 on Electronic Databases;*
- *Administrative Instruction (MPA) No. 02/2015 on Official Email Accounts;*
- *Administrative Instruction No. 02/2010 on Information Security Management; and*
- *Law no. 06/L-082 on the Protection of Personal Data.*

Annex II. Confirmation Letters

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 **"Sistemi Informativ i Gjendjes Civile në Agjencinë e Regjistrit Civil"**, dhe për zbatimin e rekomandimeve.

Për: Zyrën Kombëtare të Auditimit — Vendi dhe data: 27.05.2022

I nderuar,

Përmes kësaj shkrese, konfirmoj se:

- kam pranuar draft raportin e Zyrës Kombëtare të Auditimit **"Sistemi Informativ i Gjendjes Civile në Agjencinë e Regjistrit Civil"** (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.

Xhelal Svçlla, Ministër i Punëve të Brendshme

Republika e Kosovës
Republika Kosova
Kosova Cumhuriyeti

Komuna e Prizrenit
Opština Prizren
Prizren Belediyesi

LETËR E KONFIRMIMIT

Për pajtueshmërinë me të gjeturat e Auditorit të Përgjithshëm për raportin e auditimit të teknologjisë së informacionit **"Sistemi Informativ i Gjendjes Civile në Agjencinë e Regjistrit Civil"**, dhe për zbatimin e rekomandimeve.

Për: Zyrën Kombëtare të Auditimit

Vendi dhe data:

I nderuar,

Përmes kësaj shkrese, konfirmoj se:

- kam pranuar draft raportin e Zyrës Kombëtare të Auditimit **"Sistemi Informativ i Gjendjes Civile në Agjencinë e Regjistrit Civil"** (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.

Kryetari i Komunës së Prizrenit
Shaqir Totaj

Republika e Kosovës
Republika Kosova-Republic of Kosovo
Qeveria –Vlada-Government
Ministria e Punëve të Jashtme dhe e Diasporës / Ministarstvo Inostranih Poslova i Dijaspore / Ministry of Foreign Affairs and Diaspora

Prishtinë
Datë: 20.05.2022
Nr. Ref 331/ 2022

LETËR E KONFIRMIMIT

Për pajtueshmërinë me të gjeturat e Auditorit të Përgjithshëm për raportin e auditimit të teknologjisë së informacionit **"Sistemi Informativ i Gjendjes Civile në Agjencinë e Regjistrit Civil"**, dhe për zbatimin e rekomandimeve.

Për: Zyrën Kombëtare të Auditimit

I nderuar,

Përmes kësaj shkrese, konfirmoj se:

- kam pranuar draft raportin e Zyrës Kombëtare të Auditimit **"Sistemi Informativ i Gjendjes Civile në Agjencinë e Regjistrit Civil"** (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.

Donika Gërvalla – Schwarz
Zëvendëskryeministre dhe Ministre e Punëve të Jashtme dhe Diasporës

REPUBLIKA E KOSOVËS – MINISTRIA E PUNËVE TË JASHTME DHE DIASPORËS – REPUBLIKA KOSOVA – REPUBLIC OF KOSOVO – MINISTRY OF FOREIGN AFFAIRS AND DIASPORA – Prishtinë / a

Adress

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

Prishtina, June 2022