Republika e Kosovës
Republika Kosova
Republic of Kosovo

Zyra Kombëtare e Auditimit
Nacionalna Kancelarija Revizije
National Audit Office

AUDIT REPORT ON INFORMATION TECHNOLOGY

Electronic public procurement system e-procurement

Pristina, August 2023

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 audit report "Electronic public procurement system e-procurement" in consultation with Assistant Auditor General Myrvete Gashi Morina, who supervised the audit.

This audit report was carried out by the team:

Samir Zymberi, Director of the Audit Department;

Arbërore Sheremeti, Team Leader;

Saranda Husaj Baraliu, Team Member;

Gazmend Lushtaku, 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 CONTENT

Abbreviations

CA	Contracting Authority
CPA	Central Procurement Agency
KBRA	Business Registration Agency
CRA	Civil Registry Agency
TAK	Tax Administration of Kosovo
HR	Human Resources
GDP	Gross Domestic Product (in the Kosovo Report)
CBK	Central Bank of Kosovo
BRK	Budget of the Republic of Kosovo
PPRC	Public Procurement Regulatory Commission
MFLT	Ministry of Finance, Labor and Transfers
MIA	Ministry of Internal Affairs
BO	Budget Organizations
EO	Economic Operator
PEFA	Public Expenditure and Financial Accountability
PIP	Public Investment Program
RKS	Republic of Kosovo
KFMIS	Kosovo Financial Management Information System
IT	Information Technology
NAO	National Audit Office

Executive summary

The development of the public procurement system is one of the strategic priorities of the Government of the Republic of Kosovo as part of the national structural reforms and within the framework of the Public Administration Reform. The use of information technology for the public sector, particularly the procurement system, is a driving element for increasing efficiency and effectiveness during the implementation of procurement legislation. The Public Procurement Regulatory Commission is responsible for the development, operation and general supervision of the public procurement system in Kosovo, including the electronic information system "E-Procurement".

Considering the importance of this system, the National Audit Office has conducted an information technology audit, in order to assess whether the Public Procurement Regulatory Commission has effectively managed IT operations, to ensure that the "E-Procurement" electronic system continuously supports the public procurement process and maintains its integrity.

The audit results show that the electronic e-procurement system has helped to increase the efficiency, effectiveness and transparency of the development of public procurement activities. However, deficiencies have been observed in the information technology processes that affect the continuous preservation of the stability and integrity of this system.

Governance, operations and outsourcing of e-procurement need to be improved[6]**.** PPRC lacks sufficient IT professional human resources and there is no proper division of duties among the current IT officials. As a result, the performance of key tasks for the system operation is performed by external economic operators, which might increase the risk of creating dependence on third parties. Also, there is no electronic register/system of the problems and incidents that occur, in order to categorize them, identify the most frequent problems, and the possibility to address them.

The deficiencies identified in the governance and IT operations may put a risk to this institution making it unable to implement all the tasks, responsibilities and objectives defined by law, thus endangering the continuity of the operation of this system.

Input controls and e-procurement security need to be further developed[7]**.** In the modules of the e-procurement system, the necessary controls or restrictions, and the connections with the basic systems of the Republic of Kosovo, to prevent the processing of incorrect data, and in particular user data were not established.

Information security policies were not complete in terms of electronic account management. Invalid or fictitious accounts were not identified to be deactivated or closed, while passwords were rarely changed by users. Also, instead of official e-mail, users had used private e-email, and furthermore, the same email was used to open more than one account, exposing the user's credentials to other

[6] The detailed shortcomings are presented in Chapter 3- 3.1 Governance, operations and outsourcing of "e-procurement"; page 11
[7] The detailed shortcomings are presented in Chapter 3- 3.2 Input controls and "e-procurement" security; page 16

people. About 50% of users did not comply with the terms and conditions for using the electronic procurement system as well as the administrative instructions for official electronic accounts.

In addition, the electronic accounts and the activities carried out from these accounts were not monitored either by the contracting authorities that have the obligation to maintain their users or by the PPRC as the owner of this platform.

Unnecessary opening of user accounts, non-closure of passive user accounts as well as lack of monitoring of user accounts, among other things, weaken the work of the e-procurement platform, increase the risk of information security threats, and increase the possibility of misuse of accounts for activities outside the rules of public procurement.

Therefore, we have given 13 recommendations to the Public Procurement Regulatory Commission (in cooperation with the relevant institutions of the Republic of Kosovo), in order to address the issues surrounding the continuous support of the public procurement process as well as maintaining the integrity of this system. The list of recommendations is presented in Chapter 5 of this report.

Entity response

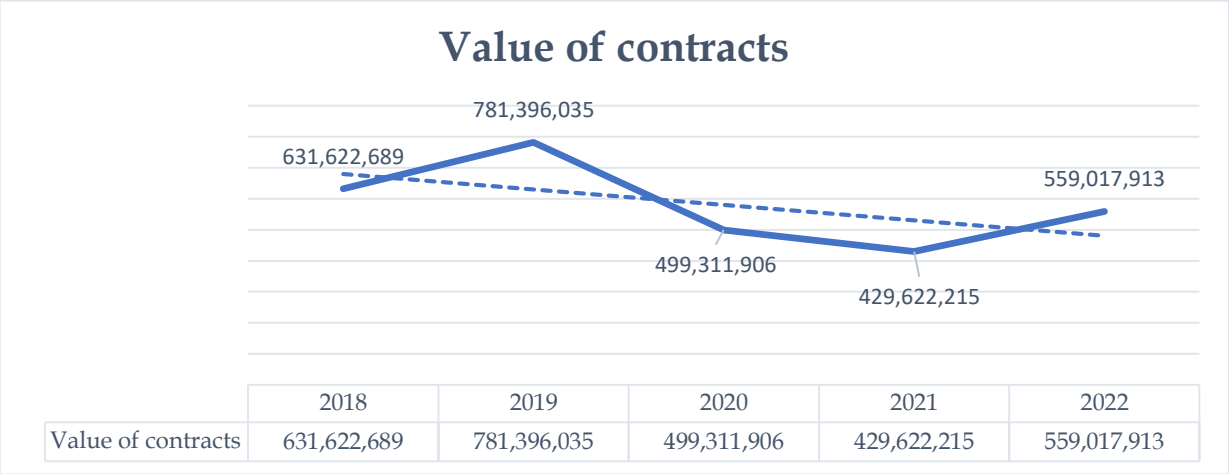
The Regulatory Commission of Public Procurement has agreed with the audit findings and conclusions and committed to address the recommendations given.

1 Introduction

Public procurement [8] is a key aspect in public administration, which is related to the public financial system and has social and economic results. As such it is a key determinant of government effectiveness and the quality of public services and infrastructure. So, public procurement is about how public authorities spend public money, when they buy goods, hire work or services on the market[9].

A significant part of the state budget is spent through public procurement activities. The public procurement market in Kosovo during 2021 was estimated at 5.65% of Gross Domestic Product (GDP)[10], while in 2022 it was estimated at 6.50% of GDP[11]. During 2022, a total of 10,290 public contracts worth 559,017,913 euros were signed[12].

Figure 1 Value of signed public contracts 2018-2022



	2018	2019	2020	2021	2022
Value of contracts	631,622,689	781,396,035	499,311,906	429,622,215	559,017,913

The main source of funding for 2021 for public tenders was from the budget of Kosovo with about 80%, from own revenues with about 19% and 0.4% were financed by donations[13].

The functioning of the public procurement system represents an essential issue of public finance management for the public administration in Kosovo. A genuine system of public procurement enables the most efficient and reasonable use of public funds, enabling substantial savings of the Consolidated Budget of Kosovo, as well as significantly contributing to the fight against corruption, misuses and, at the same time, to the economic development of Kosovo. Therefore, the Government of Kosovo in March 2016 has decided that electronic procurement is applied to centralized procurements, while from January 2017 electronic procurement has become mandatory for all budget organizations[14].

[8] Public procurement is a process that deals with the supply of goods, the provision of services and the execution of works, using public funds, according to the legislation in force on procurement

[9] It is important that taxpayers' money is spent effectively bringing the best benefits to the country.

[10] Country Report for Kosovo 2021, 2020

[11] Annual performance report, PPRC-2022

[12] Annual performance report, PPRC-2021

[13] Annual Audit Report, 2021

[14] National Public Procurement Strategy 2017-2021, Strategjia-per-Prokurimin-Publik.pdf (rks-gov.net)

All publications in electronic procurement are transparent, public and accessible to any interested party, including signed contracts and documents on the evaluation of eliminated and awarded offers (CA decisions on the evaluation of offers and standard letters for successful and eliminated tenderers).

Even in 2022, the e-procurement platform is one of the most used systems at the government level, used by businesses, citizens and stakeholders.

Table 1: Activities from the Electronic Procurement System 2018-2022

Year	Offer submitted	Contracting Authority	Economic operators	Users	Development of procedures	Contracts signed
2022	29,000	208	14,440	36,000	11,140	9,042
2021	24,600	201	12,000	32,000	6,900	6,200
2020	25,500	197	9,450	24,800	6,657	5,389
2019	100% through the platform	190	7,650	20,500	7,627	5,630
2018	97% through the platform	190	6,000	16,000	6,781	5,174

The use of information technology for the public sector, and in particular for the procurement system, is a driving element for increasing efficiency and effectiveness during the implementation of the procurement law.

2 Objective and audit areas

The objective of this audit is to assess whether the PPRC has effectively managed IT operations, to ensure that the "E-Procurement" electronic system continuously supports the public procurement process and maintains its integrity.

With this audit, we aim to provide relevant recommendations to the PPRC and other system users in order to improve their approach in relation to the management of system services.

Audit areas are IT governance, outsourcing, information security, application controls and IT operations. These areas include audit issues, such as:

Audit areas	Audit issues
1. **IT governance, operations and outsourcing**	1. Organizational structure/people and resources
	2. Management of the continuity of operations of the E-Procurement system
	3. Management of problems and incidents
	4. Change management; and service level agreement (SLA)
2. Application Controls and IT Security	5. Input data and connections with other systems
	6. Management of privileges
	7. Confidentiality
	8. Traceability mechanisms

The scope of this audit is the PPRC, with a special focus on the electronic procurement department, which is responsible for ensuring the uninterrupted operation and functioning of the services offered by E-Procurement;

This audit covered the period from January 1, 2017 to June 30, 2023, i.e., from the time when electronic procurement became mandatory for all budget organizations, with a focus on the latest developments of the system and the department, specifically in the last two years.

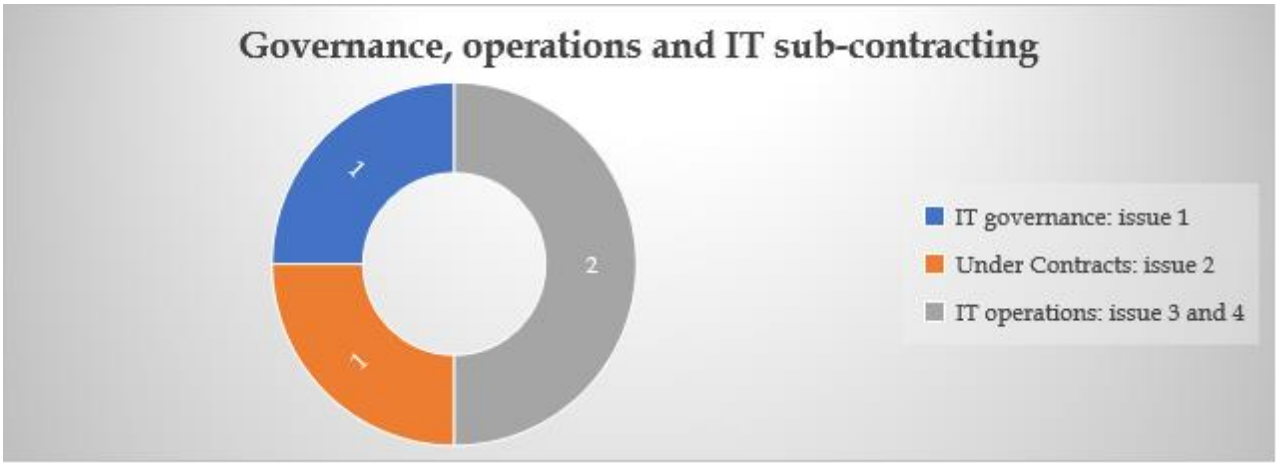
The detailed methodology applied during this audit, the questions and the audit criteria are presented in Annex I.

3 Audit findings

This chapter presents the issues from the audit of the electronic public procurement system that are related to its support and efficiency. The issues are structured in two parts.

The first part presented in chapter 3.1 covers issues related to IT governance, operations and outsourcing, which need improvement in order to ensure that the electronic e-procurement system continuously supports the public procurement process.

Figure 2 presents the number of issues and their ranking according to the areas of governance, operations and outsourcing of "e-procurement"



The second part presented in chapter 3.2, covers the identified issues related to input controls and security in the application, which affect the integrity of this system to ensure that correct data is processed in this system and by authorized persons.

Figure 3 presents the number of issues and their ranking according to the areas of input controls and security in the "e-procurement" system

3.1 Governance, operations and outsourcing of e-procurement

The most key element of IT governance is human resources, which ensure that sufficient resources are allocated to IT to achieve the needs of the organization. IT operations are described as the day-to-day tasks involved in running and supporting an institution's information systems. While during outsourcing, the institution must ensure that it is able to continue IT services in case the subcontractors are no longer able to provide these services.[15] Below we have presented the findings as a result of the lack of effectiveness in these three areas of information technology.

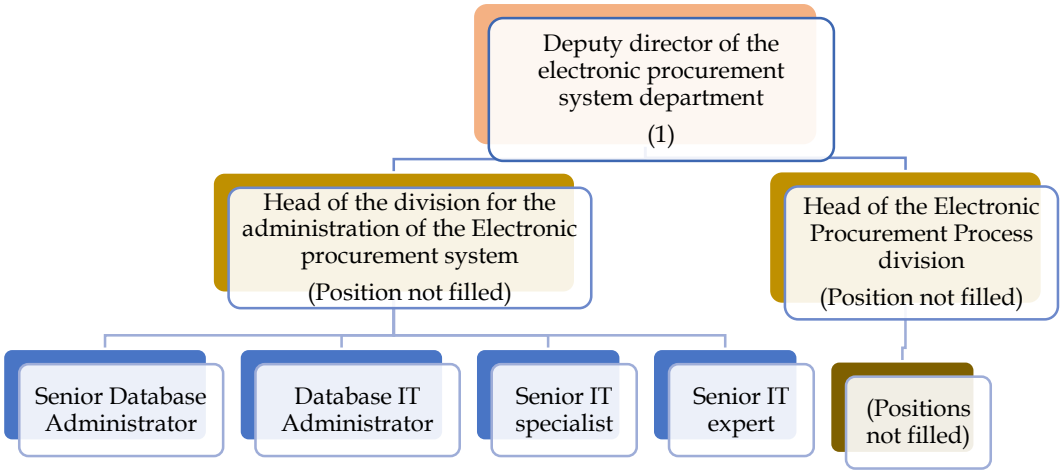
1. *The PPRC does not have a complete organizational structure and clear division of IT roles and responsibilities*

In order to enable the effective operation of the e-procurement system, the department of the electronic procurement system must divide the roles and responsibilities of human resources in order to fulfil its mission. The PPRC must have a plan for achieving current and future requirements to meet its needs for the most effective operation of the E-Procurement system. [16]

In the organizational structure of the PPRC, the e-procurement system department is clearly positioned and managed by the director of the department who reports directly to the Chairman of the Board of the PPRC[17].

According to the regulation, the number of employees in this department should be 8 (eight), while currently the number of employees is five (5), and the positions according to the act-appointments are: deputy director of the department, senior database administrator, IT administrator for the database, senior IT specialist and senior IT expert, while three (3) positions are vacant, two of which are senior leading positions. Below we have presented the current state of filled and vacant positions.

Figure 4: Systematization of personnel in the public procurement department according to labor contracts



[15] Information Technology Audit Handbook, IT Governance, IT Operations and Outsourcing
[16] Information Technology Audit Handbook, Chapter 2, IT Governance
[17] Regulation no. 01/2020 on internal organization and systematization of jobs of the Public Procurement Regulatory Commission, https://PPRCcms.rksgov.net//uploads/RREGULLORE_Nr_012020_81dd85b299.pdf

As can be seen from the figure above, the e-procurement department has not filled all the positions foreseen and approved by the budget law as well as according to the regulation on the internal organization and systematization of jobs, in which case the director of the department position is substituted by an acting director, while the two leading positions are not filled at all. While the IT procedures, the information security officer had a key or essential role, the PPRC has not mentioned this position in the regulations nor within the organizational chart.

According to the employment contracts/act-appointments, there is no employee in the division for electronic procurement processes. However, in practice, we have noticed that the entire staff of the electronic procurement department is engaged in providing the service-assistance (via telephone lines, e-mail or direct contacts) to all users of the electronic procurement platform. The two people employed as database administrators who belong to another division, are continuously engaged in performing this function, making it impossible to perform the primary tasks defined in the contract.

Also, the senior IT expert has almost the same duties and responsibilities as the director of the e-procurement department, and moreover, the responsibilities of the information security officer according to the procedures are delegated to these officials. This situation has also created a conflict of positions and responsibilities or even their duplication. While the IT specialist is tasked with system administration, in practice he performs the task of database administrator. So, according to the act-appointment, they have other positions, while in practice they perform other tasks.

Also, two important expert positions for infrastructure administration and one expert position for database and application were initially covered by donors and continued with special service contracts.

In order to fill the position of information security officer, so far, no efforts have been made to engage such an officer. It is worth noting that this official would be responsible for identifying threats, assessing vulnerability, determining risk, implementing control strategies to reduce the risk of potential cyber-attacks both from inside and outside the budget organization.

The lack of professional positions occurred as a result of staff resignations, while the non-filling of the positions of department director and division heads occurred due to the lack of applications by candidates in these internal competitions for movement within the category. However, they have not announced an external vacancy. The improper division of tasks and responsibilities has come as a result of the lack of personnel, in which case the existing personnel had to cover all IT tasks, and for other tasks, staff from other departments were engaged and they were also covered with contracts for special services.

The lack of sufficient professional resources may risk that the PPRC will not be able to implement all the tasks, responsibilities and objectives defined by law. Also, improper separation of duties can lead to non-identification of potential risks such as misuse of assets, unauthorized disclosure or misuse of information, unauthorized access, reduced accountability, etc.

2. *The PPRC does not have a strategy to ensure the continuity of the e-procurement system*

The institution must have well-defined ownership of the system as well as sufficient documentation of this to be able to continue operations within the critical function if contractors or vendors are unable to provide the service. The institution must have a strategy to ensure the continuity of the E-procurement system either with internal human capacities or other contractors in case of a failure by the service provider. [18]

PPRC has determined system ownership and provided sufficient evidence that system documentation is complete including the system development process as well as system design, such as source code acceptance documentation, system documentation, of changes in the system, infrastructure documentation, diagrams, etc.

However, the PPRC does not have any strategy nor internal capacity to continue operations of the e-procurement system for long periods of time, since it has continuously provided external contractors for both maintenance and individual consultant-contractors for special services to cover the provision of certain services, the lack of which would make the daily operation of the system impossible and is critical for ensuring the continuity of its operation.

According to the officials of the PPRC, efforts or strategies have been continuously made on how not to create dependence on third parties, initially by concluding short-term contracts with the EO with the aim that the PPRC will raise the resources. Also, each new maintenance contract had fewer outsourced services, but most of these works were still covered by individual subcontractors.

While, regarding the development of internal capacities, PPRC's strategy was to train personnel with full-time contracts thus delivering them various training sessions such as in the area of information security, COBIT, ITIL, etc., so that in the future the continuity of services provided by third parties is possible, including the transfer of knowledge from these parties in the contracts; however, it has not been able to meet this objective.

Despite the fact that the PPRC has taken measures related to the ownership and documentation of the system, the lack of internal capacities for the development of contracted services has risked creating dependence on third parties.

3. The PPRC is not efficient enough to manage problems in the system

The organization must establish mechanisms for the detection and documentation of conditions that may lead to the identification of an incident. These mechanisms are intended to prevent the occurrence of similar incidents or problems in the future. The organization must have an incident/problem management system where all incidents that occur are reported.[19]

The PPRC has an incident management policy and procedure in place that clearly describes how to handle IT security incidents. Within this procedure, cases of information security incidents must be reported to the information security officer. However, at the moment in this institution, no official is charged with these duties. Likewise, such a position is not foreseen in the internal organization

[18] Information Technology Audit Handbook, chapter 5, Outsourcing
[19] ISACA – CISA Review Manual 27th Edition, 4.8 Problem and Incident Management.

regulation. Consequently, in the absence of the information security officer, the information security incident management procedure is partially implemented.

The tasks and responsibilities of the division for electronic procurement processes include, among other things, information related to problems in the electronic procurement system which are addressed to the help desk officials, as well as the preparation of reports of the activities in question. The PPRC follows a process around the requests submitted at the help desk officers, and depending on the nature of the requests/problems some are resolved within the help desk while others are transferred for their resolution to the IT officers, to the rules or monitoring officers , but there is no written procedure about this process and help desk management in general.

In addition, there is no electronic register/system of problems and incidents that occur, in order to categorize them, identify the most frequent problems that occur and the possibility of handling them through guidelines, changes in the system in order to increase the efficiency of work or focused trainings based on the most frequent problems for users of the e-procurement system.

Since the introduction of the electronic procurement system, the PPRC has received requests for solving e-procurement problems from users via e-mail, telephone lines and in person, even though a proposal was prepared in 2018 related to the process of handling these requests but it has not been applied.

From the reports of this division, there are an average of 200 requests per week related to possible problems in the e-procurement system that are made by contracting authorities or economic operators, while a significant number[20] of phone calls are not included in this report due to the reason that they were more of an informative nature.

The lack of an electronic registry or system may have several consequences. This may lead to unresolved issues, delays in responding, failure to identify root causes or recurring issues, as well as an increase in workload and decreased efficiency of this division.

4. PPRC does not have a procedure for managing changes in information technology systems

Any changes in information systems must follow a defined change management procedure, including emergency ones, which must be approved before implementation in the operational environment. [21] *Also, the PPRC should have a detailed service level agreement along with all the requirements and should continuously monitor if the contract activities are being implemented.*

The PPRC has drafted but not approved a draft document as of 2018, the purpose of which is to define a policy and process for the software development of the PPRC e-procurement platform and any other platforms and software within the PPRC. This procedure highlights software requirements and activities, but also outlines steps for other e-procurement platform changes

[20] During the observation of the process, within 30 minutes there were six phone calls; if this rate is continuous then it turns out that there are an average of 300 phone calls per week.

[21] ISACA-CISA – Revision Manual, 26th Edition, 2016 – Chapter 4, Operations, maintenance and support of information systems.

during launch and development phase. However, this document does not include the process for emergency changes.

Although this policy has not been approved, the processes followed by the PPRC have been based on this policy regarding the changes it has made to its systems. Also, for changes in applications, the contracts include the key elements of the agreement at the service level, including the practices that will be followed for change management as well as for escalated incidents and other problems. However, we have noticed that these elements are not specified with individual IT service providers.

PPRC has hosted the main (production) hardware and software components of the electronic procurement system in the spaces of the Data Center at the Agency for Information Society (hereinafter AIS). Meanwhile, the premises of the Data Center of the Ministry of Finance, Labor and Transfers (hereafter MFLT), host the hardware and software backup components of the electronic procurement system. So, the operation and functioning of the electronic procurement system is dependent on the operation and functioning of the infrastructure of the data center managed by AIS-Ministry of Internal Affairs (hereafter MIA) and DIT-MFPT.

Due to the importance of the functioning of systems and agreements in the function of providing services and operating the electronic procurement system, PPRC since 2017 with MFLT and 2018 with AIS-MIA, have prepared Memorandums of Understanding and the Service level agreement with the necessary elements, but these agreements have not been signed yet. According to PPRC officials, despite the meetings held with these institutions, they have not yet received a response from these institutions.

The lack of a change management procedure increases the risk of deviating from a defined plan, allowing unauthorized, untested and insufficient changes that may impact system operations or fail to identify errors during the testing phase. Also, the lack of agreements between the organization and the service providers increases the risk that the PPRC will not properly define and monitor the operation, full functionality and availability of the e-procurement system.

3.2 Input controls and "e-procurement" security

The objectives of input controls are to check the validity and authenticity of source data preparation, authorization and input actions so that accurate, reliable and complete data is accepted by the application. Whereas, information security can be defined as the ability of a system to protect information and system resources in accordance with the terms of confidentiality and integrity. Managing user accounts and monitoring their activities are among the most important elements of information security. In these points, our audit has highlighted the following deficiencies:

5. ***Input controls in the application are not sufficient to prevent the processing of incorrect data***

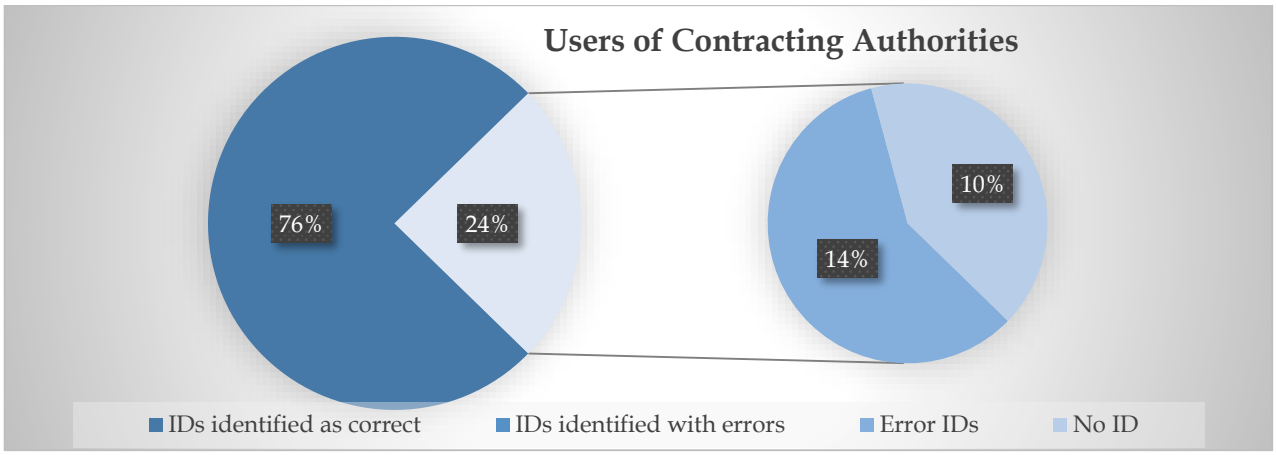
The institution must have well-designed, documented and implemented validation rules in input interaction. Invalid data should be properly rejected by the application. Validity criteria are updated in an appropriate and

authorized manner and there are comprehensive controls such as registration and authorization rules in case of the possibility of essential entry controls. [22]

Taking into account that the electronic public procurement system is one of the most used systems in the institutions of the Republic of Kosovo, the input controls for data registration, in particular of users, should reject invalid data. We have tested the registration module with all its components for economic operators and contracting authorities. Mandatory fields in this module are first name, last name, identification no. (ID or fiscal number), email, etc. However, in these areas, the controls or restrictions necessary to prevent the processing of incorrect data were not established.

Thus, due to the lack of developing the necessary restrictions, only from the active users of the contracting authorities out of 17,600 total, we identified 4,100 error IDs, of which about 1,700 accounts that do not have the ID of users operating within the contracting authorities. In addition, the system has allowed other non-digit characters to be registered in the ID field, which in principle should contain digits. In the figure below, we have presented the percentage of error IDs compared to the total IDs that are registered for the contracting authorities.

Figure 5 represents the percentage of error IDs compared to the total IDs of the active contracting authorities until March 2023



Also, the module for registration of economic operators does not work properly to distinguish between resident and non-resident EOs. This would have avoided improper registration of business numbers at least for resident EO.

There was also a lack of controls in the input data in the email registration field. We have identified at least 50 user accounts registered with emails that do not meet the standards and are therefore unusable accounts. As a result, in order for these users to log in to this platform they have to open other additional accounts, loading the database with invalid information.

Moreover, the fields that contain text such as first name, last name, etc., allow the use of characters such as: " . , ; ! @ <>", which reduce the possibility of eventual cyber-attacks.

[22] Information Technology Audit Handbook (ZKA, 2022) – Chapter 8, Application Controls, Access Controls

The electronic procurement system also receives data from TAK; however, we have noticed that there are shortcomings in the application interfaces because the data received from TAK before their final processing may be changed and processed with those changes in the e-procurement application including the fiscal number.

The PPRC has not paid enough attention to testing the application to validate certain fields in order to prevent incorrect registrations. According to them, the primary focus has been for the system to be functional and the processes to be executed without obstacles. Also, the lack of connections with the basic systems of the Republic of Kosovo has influenced this system to accept incorrect data.

Allowing the recording of incorrect data affects the performance of the system by unnecessarily increasing its capacities, does not maintain the integrity of the database, and affects the incorrect overview during the compilation of statistics. Incorrect data or mixing of characters in the system fields during user registration also increases the risk of access by unauthorized persons from outside.

6. E-procurement is not connected with other government systems

In the E-procurement application, additional controls such as authorized registers should exist to prevent incorrect data from being entered.[23] *Through the registration process, users create their virtual identity (account) in the system that is linked to their physical identity and that of the organization (Contracting Authority or Economic Operator) that they represent in the system.*[24]

The electronic procurement system as of January 1, 2017, is mandatory to be used by all institutions of the Republic of Kosovo for the development of all public procurement activities, therefore the interaction between the electronic procurement system and other relevant IT systems of the government should be realized to increase the efficiency and transparency of this system.

Until now, this system exchanges data only with TAK, which exchange has made it possible to increase efficiency during the registration of economic operators. However, e-procurement has not foreseen the necessary connections in order to receive other information in TAK, for example, such as the certification of tax debts, which is a criterion for the development of procurement activities.

The electronic procurement system collects and stores the personal data necessary for the identification of users. However, this system is no longer connected to the CRA system, and as a result of the lack of this connection, all data for the user must be filled in manually, leaving space to process incorrect data. As a result, at least 11% of users' virtual identity (account) does not match their physical identity.

Also, the electronic public procurement system has no connection with the KFMIS system either, which would have increased the efficiency in particular of the users of the KFMIS system, using the signed contract as well as the contract number from E-procurement, which is unique, and which would have been used for any payments related to the contract. Connection with KFMIS would also

[23]Information Technology Audit Handbook (NAO, 2022) – Chapter 8, Application controls, Input controls
[24] Regulation No. 001_2022 on public procurement

help in other processes such as the Statement on the availability or commitment of funds, considering that a procurement activity cannot commence without this step. The invoiced value and paid value are also useful information if this correlation is made. So, these are points that would enable better efficiency of the work of procurement officers.

Interconnections with these electronic systems were not initially foreseen and this is why there were no initiatives taken for their realization. Although initiatives have been taken with KFMS and there is an agreement for the realization of this connection, there is still no exchange of information.

According to PPRC officials, with the entry into operation of the interoperability framework implemented by AIS, it is foreseen that the necessary exchanges will be made. Also, it states that in case of unavailability of other systems, it may lead to the failure of any procurement process in general.

However, the interconnection between the basic systems of IRK avoids possible inaccuracies and misuse of the procurement processes. In the meantime, the registration of users by inserting their data manually without a connection between the systems has created room for users to register more incorrect data and has reduced the work efficiency for the users of this system.

7. *There are deficiencies in the management of accounts in the electronic public procurement system*

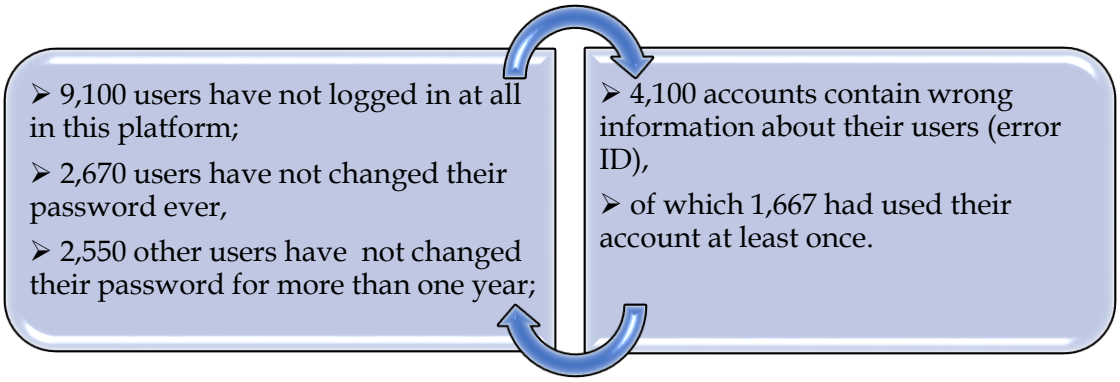
All users of information systems must have unique and personalized accounts (user IDs), which are used only for individual use. The password of the administrator account should be known only by one individual, stored in secure premises and they should be able to use the system when the administrator is not available. Accounts with full access should be monitored on an ongoing basis.[25]

PPRC, within the framework of information security policies, has also approved the policy of terms of use and eligibility for users of the electronic public procurement system. The instructions provided to users of this system include various instructions, however they do not include instructions on the appropriate circumstances for closing or deactivating an account. Additionally, the instructions do not specify how to review accounts in order to identify potential cases of invalid or fictitious accounts.

From the data on all active users of contracting authorities until March 2023, 16,700 users were registered on the e-procurement platform. In the figure below, we have presented the deficiencies that emerged from the user analysis.

[25] The ISO/IEC 27000 family of standards from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC); Administrative instruction (MAP) no. 02/2015 on official electronic accounts;

Figure 6: Analysis of active user accounts of contracting authorities.



The situation is similar with the active users of economic operators, where out of 15,153 users who were registered on this platform, at least 1,421 users had the wrong IDs, at least 1,519 users had used the same ID more than once and for different companies.

In addition, user accounts did not have a set standard for naming them. This can cause difficulties in their identification and monitoring.

Based on these data, we conclude that user accounts have never been reviewed by the contracting authorities who have the obligation to maintain their users, as well as by the PPRC as the owner of this platform. Also, the system has not configured the possibility of changing credentials after a certain period as preferred by information security standards. Another reason for not using the accounts is the opening of the accounts by mistake by the contracting authorities and not closing them after identifying the error, and also not closing the accounts when officials change jobs or are transferred to other institutions. Consequently, at least 50% of users have not complied with the terms and conditions for using the electronic procurement system as well as the administrative instructions on official email account.

Unnecessary opening of user accounts, non-closure of passive user accounts as well as lack of monitoring of user accounts, among other things, weakens the work of the e-procurement platform, increases the risk of information security threats, and increases the possibility of misuse of accounts for activities outside the rules of public procurement.

8. The process of opening user accounts in e-procurement is not efficient

The e-Procurement System implements appropriate technical measures to protect users and their personal data. These technical measures consist of email activation, Secret Questions, password principles, robot protection ("captcha"). Each user must provide an official e-mail which is used for communication with the system. [26]

For opening accounts in the electronic procurement system, the key element for maintaining credentials and confidentiality is email. According to the administrative instruction (former Ministry of Public Administration now MIA) no. 02/2015 on official email account, official accounts

[26] Regulation no. 001/2022 on public procurement; Article 3 Requirements for users of the electronic procurement system

– is the official account used by the users of IT state system to access electronic services. And according to this instruction, in order to use electronic services, one must use the official account.

However, from the list of users, for contracting authorities from public institutions, we have identified at least 4,600 users who used private/unofficial accounts to open accounts in this system.

Moreover, taking into account that official email accounts cannot be borrowed or used by other persons, in 64 cases we found that the credentials of more than one user were sent in the same email (in total there were 408 such user accounts). There were cases where the credentials of 96 users for the same organization were sent to an official electronic account.

This has happened as a result of not complying with the rules of using the system as well as the lack of awareness of the importance of information security about the use and storage of credentials by the main procurement officials in the relevant institutions. Also, the lack of establishing mechanisms in the system that only one email must be used for an active account has enabled officials in institutions to open more than one account with the same email.

Exposing user credentials to other persons violates the principle of confidentiality, increasing the risk of exposure and misuse of information. Also, this enables non-authorized officials to perform actions in the system on behalf of other persons, not respecting the laws and principles of public procurement.

9. There is no monitoring of user activities

The application and database must have audit trails that capture changes, negligence and authorized logs for critical transactions; Audit trails should be reviewed periodically to monitor unusual activities and should be properly maintained and protected; Unique and sequential numbers or identifiers must be assigned to each transaction. [27]

By verifying tables as well as tests in the application, audit trails have recorded every change that occurred including which data or fields were changed, when they were changed, what was changed, and who made the change. Also, from the controlled tables, each event registered in the application has been associated with a unique sequential number which has preserved its consistency. This has influenced the system to maintain its integrity and the audit trail to be complete.

However, in PPRC the preventive mechanisms for detecting any unusual activity are not sufficient. The PPRC does not monitor the activities of economic operators contracted to maintain the application, as well as users who have full access to both the application and the database.

The review of trails of activities in the system is not done on a regular basis. Trails are monitored only with special requests, in case of any complaints from contracting authorities or economic operators. Moreover, the personnel assigned to monitor the trails according to the procedure for logging and monitoring, have full access to these trails and monitor themselves, so it is a conflict of

[27] Information Technology Audit Handbook (NAO, 2022) – Chapter 8, Application Controls, Application Security Controls; The ISO/IEC 27000 family of standards from the International Standardization Organization (ISO) and the International Electrotechnical Commission (IEC);

monitoring and supervision of their activities. Also, they have not drawn up reports related to the activities registered in the files of the electronic procurement system.

The lack of an adequate tool for monitoring user activities was among the causes of the non-monitoring of users, especially those with full access to the system, as well as economic operators contracted for system maintenance.

The lack of monitoring and treatment of activity events in certain periods of time presents a risk of not identifying errors and misuse in time or not identifying them at all.

4 Conclusions

Governance, operations and outsourcing of "e-procurement"

Despite the fact that the e-procurement department in PPRC is well and clearly positioned, for the full functioning of the department, it must be filled with the planned positions. The lack of sufficient resources puts the PPRC at risk of failing to be transparent and accountable, and it also might fail to achieve the set goals, and risks meeting the needs for the adequate functioning of the E-Procurement system.

The PPRC has not created a strategy to ensure the continuity of operations, since the lack of development of internal capacities and the performance of important/vital tasks for the system's function with external contractors has risked the PPRC creating dependencies to third parties, and there is an internal risk of losing knowledge on the e-procurement application, making it impossible to continue using it over a longer period of time.

Due to the lack of an electronic register/system of the problems and incidents that occur, the PPRC has not managed to categorize and identify the most frequent problems in order to deal with them through guidelines, changes in the system and increase work efficiency or focused trainings based on problems for users of the e-procurement system.

Input controls and security of e-procurement

In the electronic public procurement system, the input controls are not sufficiently designed so that only accurate data is processed. Also, there is no connection with other government systems that would enable the recording of valuable data and increase work efficiency, and there are insufficient actions related to the realization of connections. As a result, system modules, fields for registration allow inserting special characters that may compromise the security of the application and may allow access by unauthorized persons from the outside. Consequently, the possibility of placing inadequate data in the e-procurement system makes it impossible to have an accurate overview of registered persons or users in this system.

The information security policies that the PPRC had approved were not comprehensive in terms of account management. Over 50% of the accounts that appeared active had not been activated at all, instead of official accounts they had used private accounts and moreover the same email was used to open more than one account, while passwords were rarely changed by users and moreover, there was no monitoring of their accounts and activities. As a result, some of the users of this system have not respected the terms of use and the principles of public procurement, increasing the risk of information exposure, misuse of accounts and cyber threats to the e-procurement system. Consequently, account management in this system is weak and quite sensitive.

5 Recommendations

The Public Procurement Regulatory Commission must ensure that:

1. **Organizational Structure.** Make a clear separation of duties and responsibilities for all IT positions, ensuring that there is no conflict of responsibilities and ensure that all the necessary mechanisms are available, including the information security officer to implemented internal IT procedures;

2. **Continuity of operations.** Design appropriate strategies which ensure the continuity of the electronic public procurement system.

3. **Incident Management.** Design a procedure for managing the Help Desk. Also, consider creating a registry/system for managing requests/problems addressed in this division.

4. **Change management.** Review and approve the procedure for managing changes, including emergency ones, for the entire information technology infrastructure and ensure that this procedure is being implemented continuously.

   4.1. In cooperation with the **public institutions of the Republic of Kosovo** that provide IT services ensure the continuous operation of this system, sign the agreements for the provision of services.

5. **Validity of input data.** Ensure that adequate restrictions and controls are set in the e-procurement system, in order to avoid errors during the processing of input data in the application, and in particular, set controls that prohibit the processing of special characters that may endanger security of the system.

6. **Interconnection of systems.** The PPRC, together with the relevant **public institutions of the Republic of Kosovo,** take the necessary measures for interaction between their systems, so that there is harmony between their data, and so that it prevents inserting incorrect data and increase work efficiency.

7. **Management of privileges.** Review the account management policy with the part for closing and monitoring accounts in the system and make the necessary changes in the public procurement system for changing the password of each account at least once every six months and consider the possibility of standardization of all electronic accounts in this system.

   7.1. In cooperation with the **public institutions of the Republic of Kosovo**, they must review the accounts and close/deactivate the accounts that are not used.

8. **Confidentiality.** Create the necessary mechanisms so that the system does not accept more than one active account with one email and take the necessary measures to close all accounts that do not belong to the responsible persons.

   8.1. The PPRC in cooperation with the **public institutions of the Republic of Kosovo** ensure that in particular the main public procurement officials as well as all other officials who open accounts in this system are using the system in full harmony with the rules of public procurement.

9. **Monitoring of audit trails.** Ensure that audit trail logs are regularly reviewed for possible manipulation and unauthorized access to them.

   9.1. Prepare periodic reports on the activities of users, in particular comprehensive reports on the activities of economic operators as well as users with full access to systems and databases.

Annex I: Audit design

Areas of risk and indicators of audit problems

International reports have evaluated the operation of e-procurement. However, according to the PEFA evaluation report for Kosovo, it is emphasized that there is no automatic connection between PIP, KFMIS and electronic procurement. Whereas, the progress report for Kosovo in 2020 has estimated that additional efforts are necessary to ensure the interoperability between the electronic procurement system and other relevant IT systems of the Government. This report for the year 2021 has estimated that the expansion of electronic procurement modules has advanced and increased the connections between this system and the Kosovar financial management information system for commitment control and proper implementation of the budget. However, more efforts are needed to ensure interoperability between the e-procurement system and other relevant government IT systems to increase transparency, including payment tracking.

Meanwhile, in the Public Finance Management Strategy 2022-2026, as well as during the pre-study phase, analysis of documentation, reports and interviews with officials in the PPRC, as well as other reports, in addition to the above-mentioned problems, the following problems were also highlighted:

- The PPRC is faced with a lack of human capacities for the maintenance of the E-procurement system, and the description of job duties is not in harmony with the work performed.
- The PPRC is dependent on third parties, both on the company that developed and maintains the system, as well as on individual contractors.
- Policies designed for the management of incidents and problems are not fully implemented.
- There is not enough monitoring of EO for system maintenance by PPRC.
- Penetration tests have not been done to ensure that this system has optimal security against possible cyber-attacks. There is also no information security officer.

Built on the issues identified above as well as our assessments based on the Active IT Audit Manual to identify areas of greatest risk, we will focus the audit on issues that include the following elements:

- Management of human capacity
- Management of service continuity
- Management of information security
- Management of change
- Management of incidents and problems
- Management of service levels
- Management of input data

The indicators of the problems presented above lead us to the formulation of the audit problem as follows: the institution has not effectively managed IT operations to ensure that the electronic public

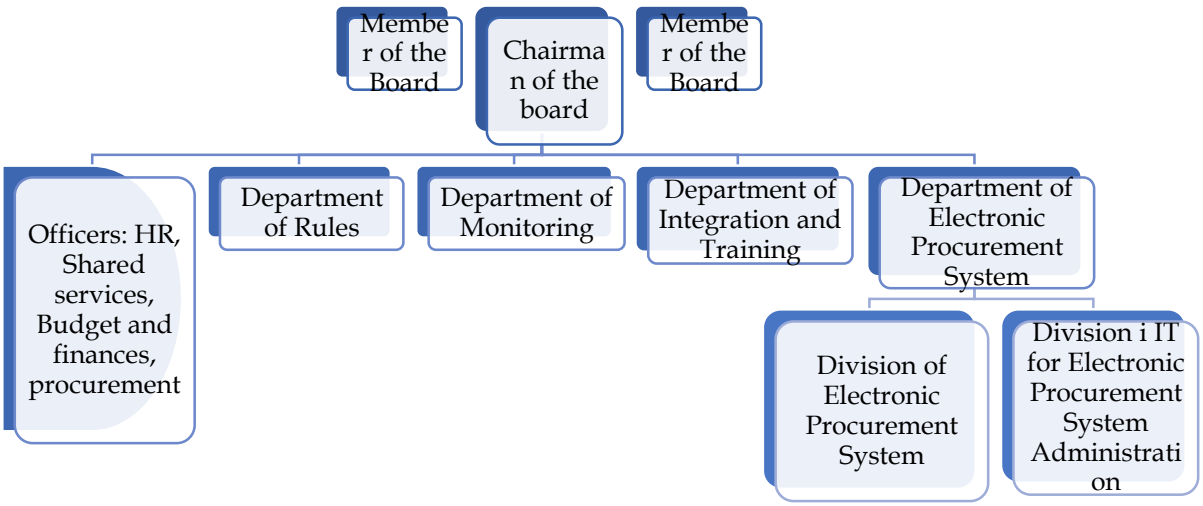
procurement system "E-Procurement" can continuously support procurement services and to maintain its integrity.

System description

According to the Law No. 04/L-042 on Public Procurement of Kosovo, PPRC is responsible for the development, operation and general supervision of the public procurement system in Kosovo. One of the functions given to PPRC by law is to develop an electronic information system throughout Kosovo to improve the publication of notices required by this law and to publish tender documents.

The organizational structure of the Public Procurement Regulatory Commission consists of the PPRC Board[28], the Chairman of the Board, Departments, and Divisions.

Figure 3 ***PPRC organizational structure***



Role and responsibilities for the Electronic e-Procurement System

The e-procurement system department is tasked with leading and administering all IT services that are part of the e-procurement system. Within this department are the IT division for the administration of the electronic procurement system and the division for electronic procurement processes. The number of employees in this department is four full-time employees.

[28] https://PPRCcms.rks-gov.net//uploads/RREGULLORE_Nr_012020_81dd85b299.pdf

Board of Directors

- Supervises the public procurement system in the Republic of Kosovo;
- Prepares and approves the strategy and the action plan of the public procurement system of the Republic of Kosovo;
- Issues and approves secondary legislation regulations for the PPRC procurement and work system;
- The Chairman of the Board represents PPRC and signs documents on behalf of PPRC;

Chairman of the PPRC Board

- The chairman represents, manages and organizes the work of the PPRC and has overall responsibility for the performance of everyday work.
- Signs documents on behalf of PPRC, signs all decisions taken by te Board. No official document should be issued by PPRC which is not signed by the Chairman;
- Responsible for the management of finanfial funds of PPRC;

Department of the Electronic Procurement System

- Ensures the uninterrupted operation and functioning of the services provided by the electronic procurement platform;
- Leads and manages on a daily basis all the IT staff responsible for the administration and support of the electronic procurement system implemented in PPRC;
- Leads and manages on a daily basis the functionalisation, operation and performance of the electronic procurement system implemented in PPRC, including the analysis and approval of proposals for advancement, modification, repair and updating of the modules and functionalities of the public procurement system;
- Plans and prepares in detail the 6-month and annual plans on the updates, improvements, and advancements of the electronic procurement system for the hardware and software part of the system;
- Prepares and updates the security policies and standard operating procedures of the e-procurement platform to be implemented by the IT staff;
- Provides advice to the PPRC management regarding everything related to the electronic procurement system;
- Cooperates with all stakeholders as regards the platform of the electronic procurement system;

Division of IT for Electronic Procurement System Administration

- Administers and continuously maintains the infrastructure of the electronic procurement platform to ensure uninterrupted operation and functioning of the services offered by the platform;
- Verifies technical errors, the impossibility of using the platform, the non-functioning of the platform for the required cases and time periods, and whenever it occurs.
- Implement policies and procedures and regulations for IT strategy, application administration, database administration, business continuity planning, risk management/action plan, disaster recovery planning, back-up policy, archival policy,
- Prepare plans for advancement and updating of the electronic procurement platform for hardware and software, whenever required;

Division of Electronic Procurement Process

- Provides assistance, clarification and advice services on the use of the electronic procurement platform, including the solution of technical problems;
- Provides services through telephone lines, e-mail, etc., for all users of the electronic procurement platform, as part of CA and EO, and advises them on the appropriate action to follow standard procedures;
- Monitors and records problems that may appear more frequently and serve to correct the platform, including identification of situations that require urgent attention
- Informs about repeated problems and prepares reports of the activity in question

Audit questions

In order to answer the objective of the audit, we have presented the audit questions as follows:

1. *Has the PPRC provided sufficient human resources that ensure adequate functioning of the E-Procurement system?*
2. *Does PPRC have sufficient assurance that the E-procurement system and other contracted services can continue even in case of termination of the contract with EO?*

3. *Are user requirements sufficiently supported and change management policies in place?*
4. *Are the application controls designed to accept only valid data?*
5. *Is the process for providing and cancelling access control to E-Procurement users effective and secure?*

Audit criteria

The audit criteria used in this audit are derived from local laws and regulations, international standards of technology/information systems, control objectives for information and technology as well as good practices from the field of information technology as well as standards dealing with management of information security.

In order to assess whether the PPRC has effectively managed human capacity, levels and continuity of e-procurement services, the following criteria will be used:

- To enable the effective operation of the E-procurement system, the department of the electronic procurement system must be clearly positioned within the organization and have separate roles and responsibilities of human resources in order to fulfil its mission;
- The PPRC must have a plan for achieving current and future requirements to meet its needs for the most effective operation of the E-Procurement system;
- The PPRC must have a detailed service level agreement along with all the requirements and must continuously monitor whether the activities of the contract are being implemented;
- The PPRC must have well-defined system ownership as well as sufficient documentation to be able to continue operations within the critical function if contractors or vendors are unable to provide the service.
- The PPRC must have a strategy to ensure the continuity of the E-procurement system either with internal human capacities or other contractors in case of failure of the service provider.

In order to ensure that the IT division has established change and incident management policies, the criteria below have been established:

- The PPRC must establish mechanisms for the detection and documentation of conditions that may lead to the identification of an incident; these mechanisms are intended to prevent the occurrence of similar incidents or problems in the future;
- The IT division should have documented procedures for detecting and recording abnormal conditions. The established mechanisms should at least identify incidents such as unauthorized access of users, intrusions (security), network failures (operational), low functionality of programs (providing services) or lack of skills of end users (training), etc;
- The PPRC must have an incident/problem management system where all incidents that occur are reported;
- Any changes in information systems must follow a defined change management procedure, which must be approved before implementation in the operational environment. The change management process must ensure that changes are recorded, evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in accordance with

documented and approved change management procedures. Also, the PPRC must have and implement the procedure for emergency changes.

In order to assess whether PPRC has effectively managed information security, the following criteria will be used:

- Access policies must exist that provide a basis for controlling access to information and ensure the co-confidentiality of each user account, and these policies must be implemented;
- All users of information systems must have unique and personalized accounts (user IDs) that are used only for individual use;
- The password of the administrator account must be known only by one individual, stored in secure premises and they should be able to use the system when the administrator is not available;
- Accounts with full access should be monitored on an ongoing basis;
- The e-Procurement System implements appropriate technical measures to protect users and their personal data. These technical measures consist of email activation, secret questions, password principles, robot protection ("captcha"). Each user must provide an official e-mail which is used for communication with the system.

In order to assess whether the application controls are designed in such a way that they accept only valid data and save processed changes, the following criteria are established [29]:

- In the E-procurement application, additional controls such as authorized registers should exist to prevent incorrect data from being entered.
- The application and database must have audit trails that capture changes, negligence and authorized logs for critical transactions;
- Audit trails should be reviewed periodically to monitor unusual activities and should be properly maintained and protected;
- Unique and sequential numbers or identifiers must be assigned to each transaction;

Audit methodology

Our approach to auditing uses a variety of techniques to obtain audit evidence and assurance. The relevant documents and legislation will be analysed, the responsible parties will be interviewed, and field tests and observations will be carried out[30].

Analyses will include:

- The legal and regulatory framework applied to the E-procurement system;
- The legal and regulatory framework related to IT (Laws, regulations, administrative instructions);

[29] Information Technology Audit Handbook, product of the EUROSAI Information Technology Working Groups (WGITA) as well as the INTOSAI Development Initiative (IDI) – Chapter 8, Application Controls.

[30] The methodology to be used is detailed in the audit matrix

- Organogram of PPRC;
- Internal policies and procedures for systems development, change and management;
- Application and module manuals;
- Interview with PPRC staff,
- System testing for access management module;
- IT work reports/ Incident/problem reports;
- Structure of data interaction with other systems;
- Internal and external rules related to classified and confidential information;
- Contracted agreements with external parties;
- etc.

Relevant documents

- *Law no. 04/L-042 on Public Procurement of the Republic of Kosovo amended and supplemented by Law No. 04/L-237, Law No. 05/L-068 and Law No. 05/L-092*
- *National Public Procurement Strategy 2017-2021*
- *Guide No. 001/2023 on public procurement*
- *Regulation No.001/2022 on public procurement*
- *PPRC Performance Plan*
- *PPRC Annual Performance Report*
- *Software development policies and processes*
- *Electronic platform security policies*
- *Information security incident management*
- *Business continuity plan*
- *Terms of Use and Eligibility Policies*
- *Logging and Monitoring Policies*

Annex II: Confirmation letter

Republika e Kosovës
Republika Kosova-Republic of Kosovo

KOMISIONI RREGULLATIV I PROKURIMIT PUBLIK
REGULATORNA KOMISIJA ZA JAVNE NABAVKE
PUBLIC PROCUREMENT REGULATORY COMMISSION

REPUBLIKA E KOSOVËS REPUBLIKA KOSOVA-REPUBLIC OF KOSOVO
ZYRA KOMBËTARE E AUDITIMIT
NACIONALNA KANCELARIJA REVIZIJE / NATIONAL AUDIT OFFICE
DATA E PRANIMIT/DOSTAVLJENO: - 1. 08. 2023
DATE RECEIVED/SUBMITTED:

Njësia Org. Org. Jedin. Org. Unit	Shif.klasif. Klasif. Kod Class. Code	Nr. Prot. Br. Prot. Prot. No.	Nr.i faqeve Br. Stranica No. Pages
06	47	1311	1

REPUBLIKA E KOSOVËS
REPUBLIKA KOSOVA
REPUBLIC OF KOSOVA
KRPP - RKJN - PPRC
Nr. 5412023
Dt. 01 08 2023

LETËR E KONFIRMIMIT

Për pajtueshmërinë me të gjeturat e Auditorit të Përgjithshëm për raportin e auditimit të teknologjisë së informacionit **"Sistemi elektronik i prokurimit publik e-prokurimi"**, dhe për zbatimin e rekomandimeve.

Për: Zyrën Kombëtare të Auditimit

Vendi dhe data: Prishtinë 26/07/2023

I nderuar,

Përmes kësaj shkrese, konfirmoj se:

- kam pranuar draft raportin e Zyrës Kombëtare të Auditimit **"Sistemi elektronik i prokurimit publik e-prokurimi"** (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.

Osman VISHAJ

Kryetar i Komisionit Rregullativ të Prokurimit Publik

Zyra Kombëtare e Auditimit
Nacionalna Kancelarija Revizije
National Audit Office

National Audit Office of Kosovo | Arbëria District | St. Ahmet Krasniqi, 210 | 110000 Prishtina

Republic of Kosovo