



Republika e Kosovës
Republika Kosova
Republic of Kosovo



Zyra Kombëtare e Auditimit
Nacionalna Kancelarija Revizije
National Audit Office

Information Technology Audit Report

Kosovo Customs Information Systems - ASYCUDA World



Prishtina, December 2024

The National Audit Office of the Republic of Kosovo is the highest economic and financial control institution vested by the Constitution and the Law¹ with functional, financial and operational independence

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

This audit was conducted in accordance with the International Standards of Supreme Audit Institutions (ISSAI 3000²) and the Guidance on Audit of Information Systems (GUID 5100³).

Information Technology audits undertaken by the National Audit Office are examinations and evaluations of information technology systems and respective controls aimed at obtaining assurance on principles of legitimacy, efficiency⁴, economy⁵, and effectiveness⁶ of the information technology systems and respective controls.

1 Law no.05/L-055 on the Auditor General and the National Audit Office of the Republic of Kosovo.

2 SNISA 3000 – Standards and guidelines for performance auditing based on INTOSAI's Auditing Standards and practical experience

3 GUID 5100 – INTOSAI Guidance on Audit of Information Systems

4 Efficiency – The principle of efficiency implies achieving the maximum from the available inputs. It is about the relationship between input and output in terms of quantity, quality and time.

5 Economy – The principle of economy implies minimising the cost of inputs. Inputs should be available at the right time, quantity and quality and at the best price possible

6 Effectiveness – The principle of effectiveness implies the achievement of set objectives and the achievement of expected outputs.

The Auditor General has decided on the content of the audit report “Kosovo Customs Information Systems - ASYCUDA World” in consultation with the Assistant Auditor General, Myrvete Gashi Morina, who supervised the audit.

The audit team consisted of:

Samir Zymberi, Director of the Audit Department;

Poliksena Berisha, Team Leader;

Gazmend Lushtaku, Team Member;

Besim Lezi, Team Member; and

Naim Neziri, Team Member.

NATIONAL AUDIT OFFICE – Address: St. Ahmet Krasniqi nr. 210, Arbëria District,
Prishtinë 10000, Kosovë
Tel: +383(0) 38 60 60 04/1011
<http://zka-rks.org>

Table of content

List of abbreviations	7
Executive Summary	9
1. Introduction.....	13
2. Audit objectives and areas	17
3. Audit findings	21
3.1.Outsourcing policies	23
3.2.Information Security	25
3.3.Business Continuity Plan – Disaster Recovery Plan.....	31
3.4.Application Controls	33
4. Conclusions.....	41
5. Recommendations	45
Annex I. Audit Design	49
5.1.System description	51
5.1.1.Ministry of Finance, Labour and Transfers	51
5.1.2.Kosovo Customs	52
Annex II: Confirmation letter	68

List of abbreviations

APIS	Advanced Passenger Information System
ATA	Temporary Admission (Admission Temporaire)
AW	ASYCUDA World
EU	European Union
CAAT	Computer Assisted Audit Techniques
CAFAO	Customs and Fiscal Assistance Office
CEFTA	Central European Free Trade Agreement
DETOP	Department of Excise, Tariff, Origin and Procedures
KC	Kosovo Customs
OBD	Operational and Border Directorate
IPR	Intellectual Property Right
DCS	Department for Customs Systems
DJC	Directorate of Joint Services
SAD	Single Administrative Document
LED	Law Enforcement Directorate
ECM	Enterprise Content Management
EDI	Electronic Data Interchange
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
ICIS	Integrated Customs Information System
INES	Software for Intellectual Rights
EC	European Commission
LES	Law Enforcement System
MPA	Ministry of Public Administration
ME	Ministry of Economy
MFLT	Ministry of Finance, Labour and Transfers
MIET	Ministry of Industry, Entrepreneurship and Trade
WTO	World Trade Organisation
AEO	Authorised Economic Operators
PKI	Public Key Infrastructure
DRP	Disaster Recovery Plan
BCP	Business Continuity Plan

RMS	AW Risk Management and Selectivity
AAR	Annual Audit Report
AWS	ASYCUDA World Sector
SEED	Systematic Electronic Exchange of Data
PAS	Procedures and Authorizations Sector
SITS	Sector for Information Technology Support
SRM	Sector for Risk and Monitoring
TARIK	Integrated Tariff of Kosovo
TIR	International Road Transport (Transports Internationaux Routiers)
VAT	Value Added Tax
UNCTAD	United Nations Conference on Trade and Development
WCO	World Customs Organisation
XML	Extensible Markup Language

Executive Summary

Kosovo Customs (KC) is the agency for the management of revenues within the Ministry of Finance, Labour and Transfers. The revenues collected by Customs contribute about 60% of the total revenues collected for the budget of the Republic of Kosovo. KC has a broad mission, starting with the protection of the state, economy and citizens.

In order to discharge its mission more efficiently, the Kosovo Customs has digitalised its processes by developing the information systems and putting them to operation. ASYCUDA World is the Kosovo Customs' fundamental system which is extended to other customs offices, in ports, border stations and free zones. The system's main role is to serve for the management of customs clearance procedures and to manage all types budget revenues, namely around 1.5 billion euros collected annually by the Kosovo Customs.

The National Audit Office has carried out the IT audit to assess whether the ASYCUDA World enables the Kosovo Customs to implement the Customs electronic processes accurately, safely and reliably.

The Customs of Kosovo has continuously upgraded the ASYCUDA World system to ensure the digitalization of the customs processes and to improve the security and accuracy of the data and processes implemented thereof and the security of the system itself. In addition, it has implemented the agreement on ASYCUDA system when it comes to the promotion of gender equality.

Kosovo Customs is suffering shortcomings in the outsourcing policies as they have not addressed the information safety in the agreements/contracts they have entered into with the external parties, hence the responsibility of parties in the project for ASYCUDA system would be undefined should any cybersecurity incidents occur.

The controls implemented by the Kosovo Customs over the information security do not provide sufficient assurance on the integrity, confidentiality and availability of the system because the information security policies have not been updated; there are shortcomings in the staff organisation structure; responsibilities on information security are centralised and conflicting each other; there are shortcomings in the management of access to information systems; and trainings on increasing the staff's awareness on the information security were lacking.

Customs has not provided sufficient mechanisms for business continuity, there is a lack of a plan and structure for the operationalisation of the plan, as well as written procedures for business continuity. In lack of these mechanisms, business continuity would at risk in the event of a disaster, loss, damage to data and the system as well as the dismissal of key staff.

Application controls applied in ASYCUDA do not provide assurance that only true and valid data are entered and updated in the system because some processes are still being implemented manually, such as the calculation of the multiplier for setting the post-revaluation price; and the risk assessment is made through the criteria established in a text only, with no possibility for measuring. It doesn't validate the field for registering the personal/business number and the trademark when there is a lack of interfacing with other systems. The design for some of the modules for the users of risk assessment and tariffs sectors are neither simple nor user-friendly.

Therefore, the risks identified in the outsourcing policies, information security, business continuity and application controls indicate that the Kosovo Customs, which administers and operates the ASUCUDA system, need to be improved in order to ensure that the data in this system is protected and that the digitalised processes are not interrupted. To this end, we have given 13 recommendations to the Kosovo Customs, which we have presented in Chapter 5 of this report.

Entity response

Kosovo Customs agreed with the audit conclusions and committed to implementing the recommendations given.

INTRODUCTION

01

1. Introduction

Kosovo Customs (KC) has been developed based on the EU standards and funded by the Kosovo Budget. It is the main actor in contributing to revenue collection and protecting the citizens from restricted and prohibited goods.

The ASYCUDA World information system - developed by the United Nations Conference on Trade and Development (UNCTAD) - is the Kosovo Customs' main system, which was created in August 2011 and put to operation in September 2012.

It is UNCTAD's largest technical cooperation programme covering 102 countries worldwide, including Kosovo, Bosnia Herzegovina and Albania from our region. ASYCUDA's total implementation cost is only US\$ 1,350,158, excluding equipment and infrastructure. The system is extended

to other customs offices, in ports, border stations and free zones.

The Automated System for Customs Data - ASYCUDA World (AW) - is a computerised customs management system that covers most foreign trade procedures. AW handles manifests⁷ and customs declarations, along with accounting, transit and suspense procedures. It also generates trade data that can be used for statistical economic analysis. ASYCUDA uses international codes and standards developed by the ISO (International Organization for Standardisation), WCO (World Customs Organisation) and the United Nations. ASYCUDA provides Electronic Data Interchange (EDI) between traders and customs using prevailing standards, such as XML. The Kosovo Customs has been using this platform along with its modules since 2012. The KC has, ever since until 2023, managed to collect over 11 billion euros⁸, including the real-time

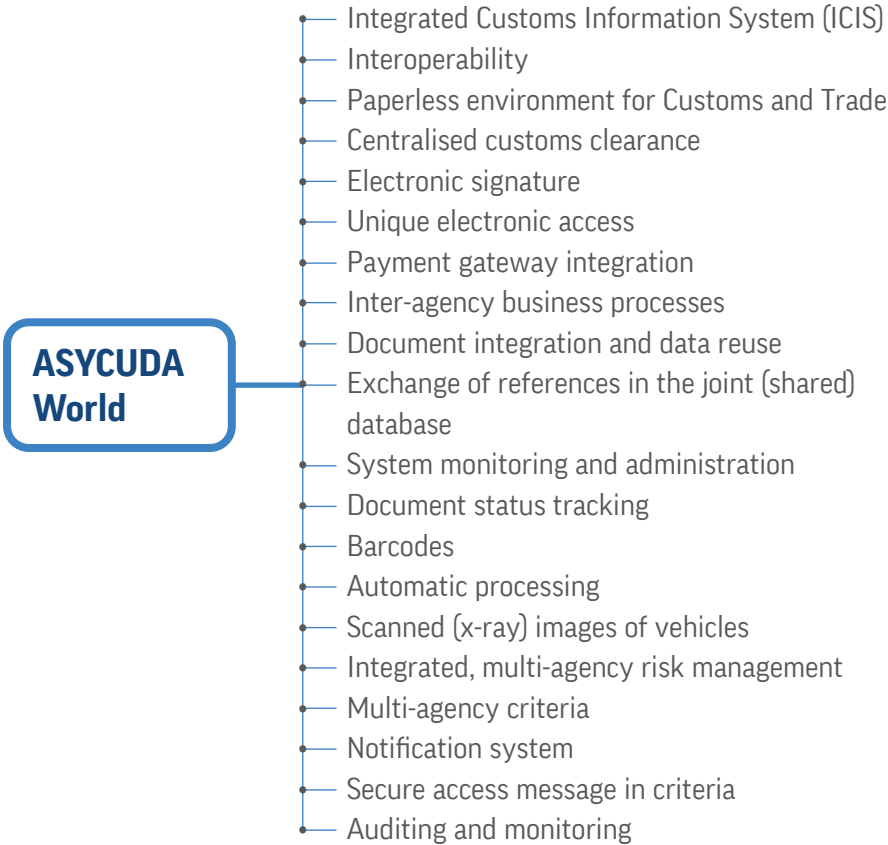
⁷ A customs manifest is an official document used in customs clearance processes that gives a description of the goods being shipped from one country to another. This document gives detailed information of the cargo, including the type, quantity, origine and destination

⁸ Internal document from CK containing data from customs systems - Request for approval of customs systems as state information and communication systems of strategic importance.

automatic confirmations which now take 3 seconds to be done from 45 minutes as it was in 2011.

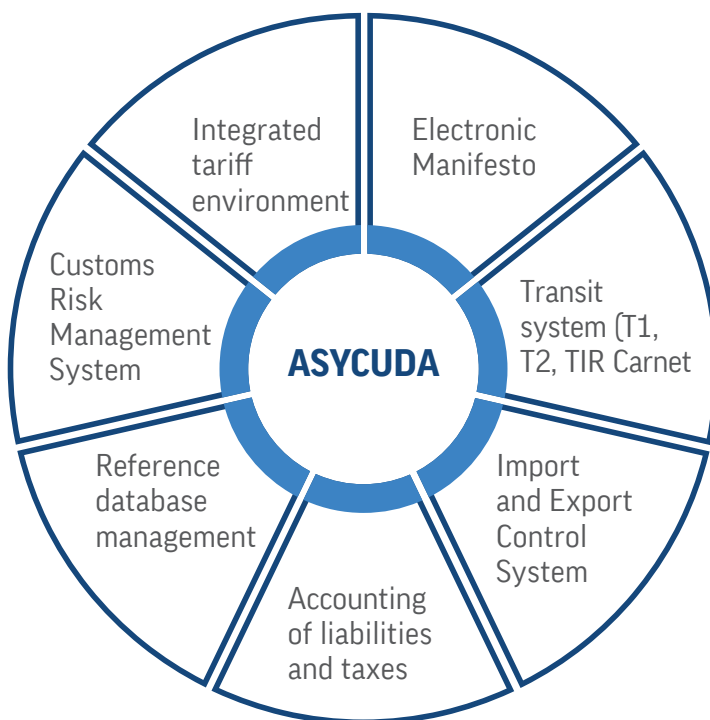
The most important aspects of this system are summarised as the following:

Figure 1. The most important aspects of AW



The main functions of the integrated Customs Management System (AW), through which customs processes are conducted and which were covered during the audit, are:

Figure 2. Main functions of ASYDUC World



AUDIT SUBJECTIVES

02

2. Audit objectives and areas

The objective of this audit is to assess whether the ASYCUDA World system enables the Kosovo Customs to implement the customs electronic processes accurately, sagely and reliably.

With this audit, we aim to give relevant recommendations to the Kosovo Customs in order to improve the information system regarding the information security and application controls.

In order to be responsive to the audit objective, we are focusing on the information security area and application controls as well as matters related to the outsourcing policies and business continuity by selecting the audit topics as follows:

Table 2: Audit areas and matters

Audit areas	Audit matters
1. Outsourcing	1. Outsourcing policies
2. Information Security and Cybersecurity	2. Security
	3. Information security policies
	4. IT security structure
	5. Human Resources IT Security
	6. Access Controls
3. Business Continuity Plan –	7. Structure of the Business Continuity function
4. Disaster Recovery Plan ⁹	
5. Application Controls	8. Input controls
	9. Processing controls

The audit scope covers the Kosovo Customs and the relevant departments for IT management, the ASYCUDA system and the customs functions. The audit covers the 2022 to 2024 period.

9 BCP & DRP – Business Continuity Plan and Disaster Recovery Plan

AUDIT
S
G
N
D
N
S

03

3. Audit findings

The ASYCUDA World system, developed by UNCTAD and used by the Kosovo Customs, represents an important innovation in the customs administration area, by modernising the customs management and procedures more efficiently and sustainably. This system is designed to facilitate and optimise the foreign trade procedures, including the customs declarations, transit operations and shipment accounting. Through this system, the data are saved and managed and the processes involving around 60% of state revenues collected through the digitalised procedures offered by AW are implemented as well.

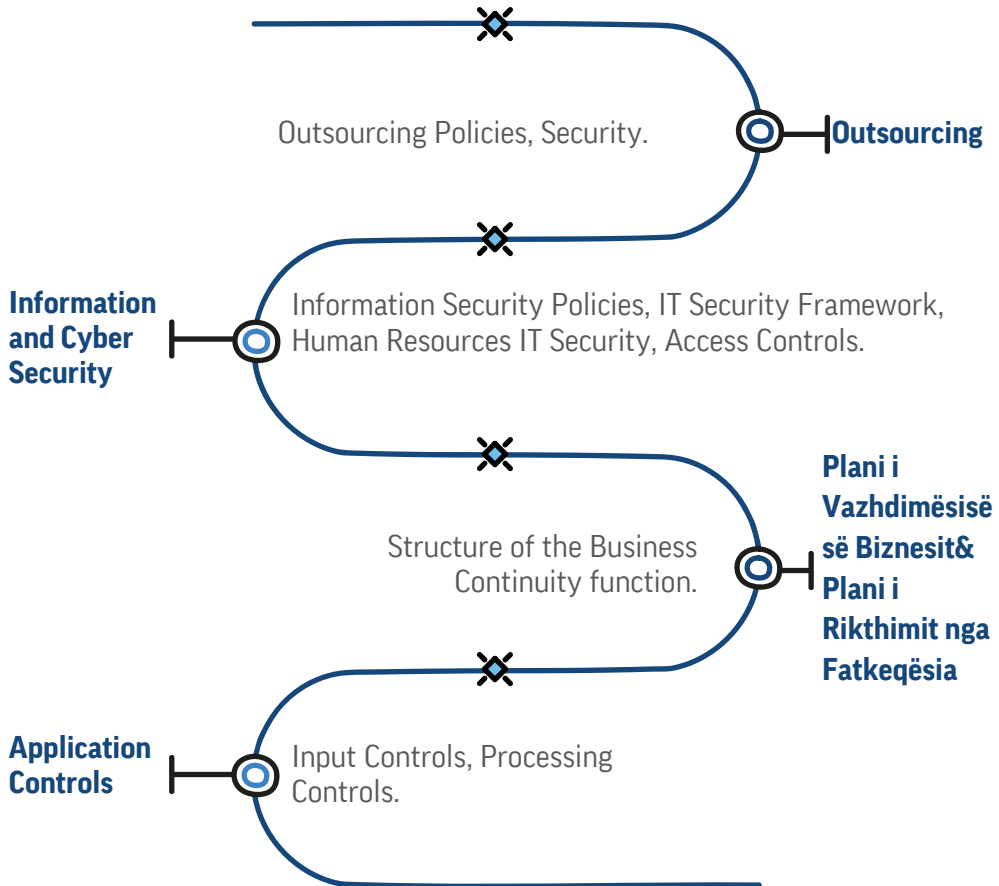
One of the key benefits from this system is the usage of the international standards, which enhance the level of harmonisation and cooperation between the states and international institutions. The system also supports the electronic data interchange (EDI) with KC, thus enabling an uninterrupted flow of information between the parties involved. This increases the accuracy of data and contributes to a clearer and environment-friendly process.

Moreover, AW was developed to digitalise and optimise the processes, which has a direct impact on reducing the time and costs related to international trade. This facilitates the trade and increases the trade partners' and businesses' trust on the efficiency of customs institutions

Ultimately, the implementation of AW system represents an important step towards the modernisation of global trade and strengthening of local economies, namely the administrative and financial stability.

However, apart from the system development, there are shortcomings which we have presented under this Chapter. The audit findings are related to the outsourcing policies and the activities of the parties responsible for the administration, information security, business continuity plan and the application controls in the ASYCUDA World system of KC. The findings are structured according to the audit areas and matters.

Figure 3. Structure of audit matters in KC



The first session presented under Chapter 3.1 covers the identified issues that need to be improved concerning the outsourcing of information systems (1).

The second session presented under Chapter 3.2 covers the identified issues concerning the information and cyber security (2-5).

The third session presented under Chapter 3.3 covers the identified issues concerning the Business Continuity Plan & Disaster Recovery Plan (6).

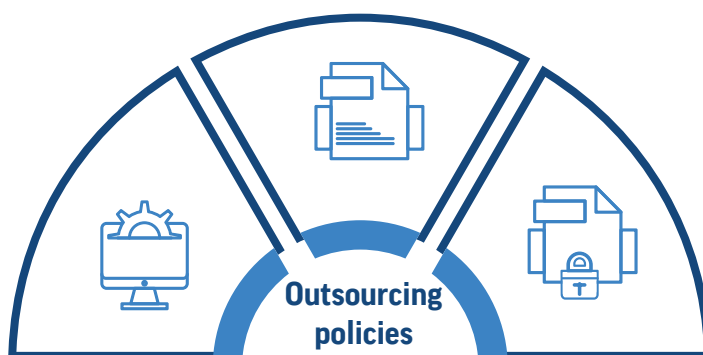
The fourth session presented under Chapter 3.4 covers the identified issues concerning the application control (7-11).

3.1. Outsourcing policies

Organisations should have some policies in place which define the functions that can be outsourced and the functions that must be developed within the organisation. Service outsourcing requires close monitoring and is subject to privacy and security requirements.

KC develops the outsourcing processes in line with the applicable legislation, but it suffers shortcomings when implementing the information security during the outsourcing.

Figure 4. Outsourcing policies (System, information policies and security)



1. Kosovo Customs is suffering setbacks in the outsourcing policies for the development and maintenance of ASYCUDA system

The organisation should implement the organisational outsourcing policies.¹⁰ The organisation's security requirements should be adequately pointed out by the Contractor in the agreements with external parties.¹¹

Kosovo Customs should implement the signed agreement, including the article stipulating the promotion of gender equality, with the participation of women employees in the project.¹²

In order to develop the AW system, KC has entered into an agreement with UNCTAD in 2011. The agreement sets forth the terms for developing this system, but after having analysed the documents¹³ and interviewed the officers, we found that the KC has not managed to address the information security requirements in this agreement, nor has it included them in the base contract entered into on 6 May 2011. To carry out the outsourcing, reference was made to the Law on Procurement and the procedures stipulated therein, which does not provide a separate policy for information security, but rather gives a general description of it. In 2017, KC has drafted information security policies, procedures and standards, which are currently in use, but has failed to address security issues in the subsequent contracts on the AW system's maintenance and upgrading. The officers responsible for the AW system explained this shortcoming with the contractor's access only to the development environment and not to the real one, but we have found that the database contains real data also.

However, KC has managed to implement the gender equality requirements provided in the agreement entered with UNCTAD. The ASYCUDA sector consists of three officers – two males and one female.

Failure to address information security and the shortcomings in outsourcing policies for information security undermine the security of outsourced systems

10 Information Technology Audit Handbook, Outsourcing, Security

11 ISO 27001 – Information Security Policy

12 Annex2 of the Agreement between the Kosovo Customs and the UNCTAD, March 2023.

13 Contract signed between the Government of the Republic of Kosovo, United Nations Specialised Agency, UNCTAD; employment contracts, director's decisions for transfer

and in the event of any information security incident there is no possibility to identify the responsibility of the parties in the contract, for the monitoring and reporting of the incident.

3.2. Information Security

A fundamental aspect of IT governance is the security of the information to ensure the availability, confidentiality and integrity of data. For a better management of information security, the organisation should establish mechanisms that enable managing the security-related risks, taking actions as appropriate and ensuring that the information is available, usable, complete and uncompromised.¹⁴

Figure 5. Principles of information security availability



14 IT Audit Handbook, Information Security

2. Kosovo Customs do not have an updated security policy in place

In order to discharge its mandate, Kosovo Customs should document, approve and communicate appropriate policies and procedures to run the business and IT operations. Information security policies should cover all operational risks and be able to reasonably protect all critical information assets from loss, damage and abuse. The information security management system and other applicable internal policies, procedures or rules should ensure that they are in line with the organisation's latest developments and are regularly reviewed.¹⁵

KC does have an information security policy in place, but it is not updated. Pursuant to the MPA's Administrative Instruction 02/2010 on information security management, the Kosovo Customs drafted information security policies, procedures and standards in 2017, which are currently in use, but the policy has not been updated yet. Therefore, the developments made in KC and information security globally, from 2017 until 2024, have not been included in this policy.

The reason behind the failure to update this policy and the other ones related to the customs procedures and IT is the planning to update them following the entry into force of the Code no.08/L-247 on Customs and Excise in order for them to fit with each other. Thus, they are now in the process of upgrading them to adapt to the new Customs Code.

Failure to update the security policy and the lack of new guidelines on security practices prevents the employees from being informed and makes them incapable of protecting the organisation effectively as well as makes the organisation more vulnerable to cyber-attacks.

15 IT Audit Handbook – Information and Cybersecurity Policies and ISO 27000

3. Shortcomings in the IT security structure and segregation of responsibilities as well as the impact on the management of audit trails in KC information system

Kosovo Customs should have in place clear IT duties and responsibilities related to information security policies, there should be no conflicting areas of responsibility or non-alignment of information security activities. (reference ISO 27000).¹⁶

While conducting our audit, analysing the documents for the organisation of Customs IT and interviewing the responsible officers, we found that KC has not managed to establish a clear information security structure. The Customs' IT officers, who administer the database, have full access in the database and in the AW application. They also have full access in audit trails registers. Meanwhile, they only analyse the audit trails upon request, as it was the case with the external audit. In addition, in the IT Department, focus has been emphasised to be put on the responsibilities and the full dependency on one officer with administrative access to all the systems and databases owned by DK.

Moreover, the organisational structure adopted in 2016, together with its appendix giving details on the duties and responsibilities of each of the KC's sectors and updated in 2019, included the provisions for the systems, security and infrastructure sector. However, it does not specifically define the responsibility for the monitoring of information security, nor does it define a specific role for monitoring the audit trails within the information systems and databases.

During the audit, namely onsite observation at the customs checkpoints, we noticed that after the customs agents entered the information in the ASYCUDA system and the truck arrived, the imports inspection through the red channel would be physically carried out by the customs officer who performed this task alone rather than with his colleagues, as a commission, although during the description of customs processes in the interviews we were told that this process was carried out as a team. In addition, the KC management was convinced that this process was carried out by several officials and not by a single officer, despite the fact that guideline no.17/2015 foresees the implementation of this process by one officer.

16 IT Audit Handbook – Information and Cybersecurity, IT Security Structure

The lack of a well-defined information security structure has led to conflicting responsibilities of officers with access to its systems, thus failing to categorise the level of information security. Full access to audit trails given to the database and applications administrator, based on a single officer only, leads to significant risks. This includes the possibility for unauthorised changes to, errors in and misuse of data, such as the overlooking or deletion of audit trails which threatens the system's integrity.

Meanwhile, physical inspection of goods undermines the transparency of the process and accuracy of the evaluation.

4. Lack of KC employees' awareness and training on information security

Kosovo Customs should ensure that all employees (including contractors or sensitive data users) are qualified to maintain data, use resources, understand duties and responsibilities. The staff should safeguard the information security, from the recruitment until termination of the employment relationship. Their access should be removed as soon as their employment/outsourcing contract is terminated. In addition, refresher trainings should be provided periodically to the employees, whose organisational role is significant for the Information Security and Cybernetics.¹⁷

During examinations in the customs checkpoints we found that the Customs employees are not sufficiently aware of the information security. We have observed that they keep their passwords exposed in workspaces, easily accessible to third parties without being aware of the safeguarding of access and information security.

Although information security notices have been sent by e-mail from the IT Department to all officers, information security training is lacking. The officials' reasoning for exposing the passwords was the difficult policy of password complexity, the frequent changing of passwords, and the large number of passwords they use for different systems.

¹⁷ IT Audit Handbook – Information and Cybersecurity, IT security of human resources

Failure to properly safeguard the access to the system endangers the data and leads to access by unauthorised persons. It also leads to the risk of implementation of any important customs process through access by unauthorised persons and failure to identify them.

5. Kosovo Customs does not have a procedure in place for controlling users access to the information system

The Kosovo Customs policies for access to information systems should provide a basis for the control of interference to information. The information security function monitors the effectiveness of the monitors user account management operations control on a timely basis and reports the operating efficiency and effectiveness.¹⁸ The allocation and use of privileges in the information system environment should be restricted and controlled, i.e. privileges should be allocated on a need-to-use basis, and privileges should be allocated only following the formal authorisation process.¹⁹

Customs officials and customs agents, who are external users and have access to the registration of customs data for carrying out customs processes, have access to the AW system implemented by DK. However, KC does not have a written procedure in place for controlling access to the information systems, because they have not considered it reasonable given that e-mail communication for allowing and changing access was simpler. A procedure, according to them, would cause delays, therefore they do not have a defined process for providing access to the information system, instead they use three methods in practice.

The first method for filling out a form for access to computer systems and applications. This has been used from 2004 to 2020, but, since it caused delays due to the dependency on signatures by chiefs of sectors, this method was removed and they have continued to use the second one.

The second method of changes in approaches is made by decision of the director general, who signs the transfer of staff to different sectors and different positions

18 IT Audit Handbook – Information and Cybersecurity, Access Controls

19 ISO 27001 – Access Controls

and this decision is sent to the AW system administration sector. Based on this decision, they implement changes in customs systems, including the AW system.

The third method of changes in approaches is made upon request of the chief of sector, at customs branches or border crossing points, who sends e-mails with the respective information for changing the access of customs officers.

These three methods have been used for internal users/customs officers only, whilst the customs agents make their requests through the Kosovo Local and International Freight Forwarding Association, as stipulated in the agreement entered into in 2015.

Moreover, due to the lack of a procedure for controlling access to customs systems, access to the users list is not reviewed on a regular basis, in the information system. The most sensitive part of the users list is the customs agents' users list (5250 users with access as customs agents), who, despite the changes, continue to use the accounts of their colleagues, including those who have terminated the employment relationship.

The process of managing access through e-mail requests made is faster, according to them. As for the access review on a regular basis, they have not considered it necessary since every request for the provision and removal of access is fulfilled. Although according to the information security standards, the users access review should be carried out at least once a year. Whilst for customs agents' access, according to KC, it is the 2015 agreement entered between KC and the Kosovo Local and International Freight Forwarding Association that defines the form of customs agents' access, and enables their access accordingly.

The lack of a procedure for controlling the users access to information systems increases the risk of misuse of access and of unauthorised access. It also leads to obscurities as a result of failure to review the users list and of the lack of a clear process for access granting and removal.

3.3. Business Continuity Plan – Disaster Recovery Plan

The organisation should also have a continuity plan to ensure the business continuity of the service provider or take this over from another company. If the recovery from a disaster of a critical function area is threatened, the business continuity will also be at risk. A good continuity plan could become ineffective if the roles and responsibilities are neither clear nor properly understood by the respective staff.²⁰

Figure 6. Business Continuity



²⁰ IT Audit Handbook, BCP – DRP.

6. Kosovo Customs does not have a business continuity plan in place

Kosovo Customs should cover all the organisation's critical areas by a team. Requirements for the duties and responsibilities in the team members.²¹ The Business Continuity Planning tests should ensure that all the recovery team members and the other relevant staff are aware of the plan and their responsibilities on the business continuity and information security as well as recognise their roles when the plan is revoked.²²

KC does not have a policy, procedure or specific manual on business continuity plan, but the ASYCUDA system is configured so that the database is replicated (duplicated) in real time through the Oracle ActiveDataguard platform. KC has two data centres that are connected to each other with optical fibre. Replication is done through the VMware platform as well as through the Storage-to-Storage platform (3PAR8400 – 3PAR8200).

In addition, they do not have a defined structure of the persons in charge, which would serve to the implementation of the business continuity plan should any disaster or emergency cause the disruption of the information system processes, given that there is no business continuity plan defined which would specify this structure either.

Although KC has adapted the AW system's implementation based on the Kosovo Customs legislation as well as its written general procedures, it cannot fully rely the business continuity thereon because these procedures are outdated and have not been updated during the system developing and upgrading.

Every process that is implemented through the ASYCUDA system is made in line with the Kosovo Customs legislation; thus, these processes are numerous and complex. They lack specific diagrams for all the processes and operations, because the system has been adapted depending on the customs legislation in force.

21 IT Audit Handbook, BCP – DRP – Structure of the business continuity function

22 ISO 27001 – Structure of the business continuity function.

The staff of Kosovo Customs is part of the Government's working groups and the Customs data are stored in the databases in the Government's premises. However, technical actions for business continuity have also been undertaken by conducting data replication and storage in two different locations. As for the structure, it has not been defined due to the lack of a plan, but IT officers do monitor the backup copy on a regular basis. When it comes to the updating of procedures, we also obtained information from the internal audit that they had suggested drafting and updating the procedures that explain the customs processes and those of the information system, but they have not managed to implement them yet.

In the event of a disaster, data loss, system damage, or key staff leaving, the lack of a comprehensive business continuity plan poses a significant risk to the operations. This includes the lack of a defined structure for the implementation of such a plan and the lack of written procedures for customs activities carried out through the ASYCUDA system, which manages critical customs data and processes. These gaps jeopardize the Customs' ability to keep the operations during emergencies uninterrupted.

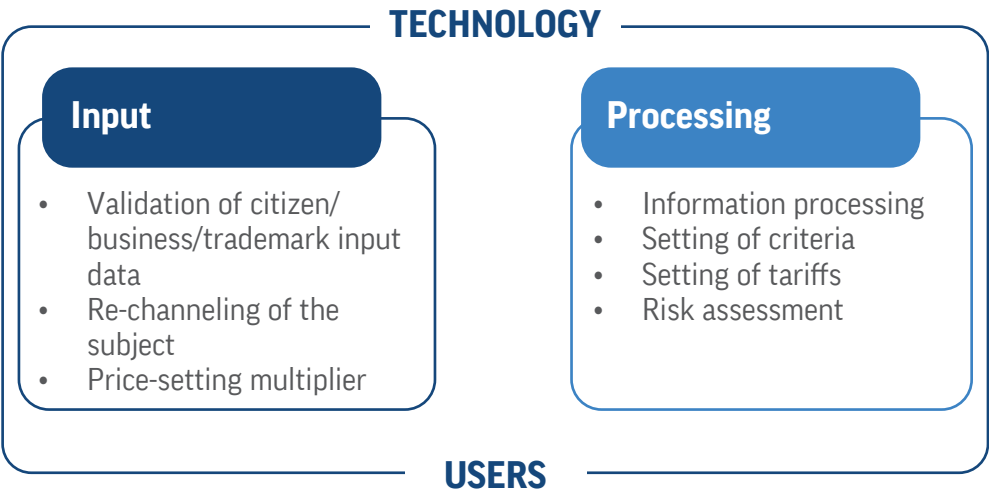
3.4. Application Controls

Application controls are: control over the functions of input, processing and output. They include methods to ensure that: only complete, accurate and valid data is entered and updated in an information system, the processing performs the correct task and the processing output meets the expectations and that the data is stored.²³

The **ASYCUDA World** system used by Kosovo Customs includes a number of computerised and manual controls aimed at ensuring the customs' data integrity and security. In general, these controls help in facilitating the system functioning and in assuring compliance with regulations, but there are shortcomings in the input controls and processing in the AW information system.

23 IT Audit Handbook – Application controls

Figure 7. Data entry-processing model in the AW information system



7. The price-setting multiplier is calculated manually in ASYCUDA

Validation rules are well-designed and implemented into entry (input) interfaces; invalid data is properly rejected by the application; compensating controls such as logs and authorisation rules in case of the possibility of overriding input controls are in place; there is proper control and documentation of application entries.²⁴

During the customs clearance process, goods that go through the control process are assessed based on the risk-profiling criteria which enable the channelling of high-risk consignments (red channel), medium-risk consignments (yellow channel) and low-risk consignments (green channel). The red channel consignments are subject to physical inspections, the yellow channel consignments are subject to documentation inspections and the green channel consignments are released without being subject to any controls. Afterwards, the sector for assessing the yellow channel consignments, located in the headquarters, analyses the source documents and assesses the compliance of the price declared in the Single

24 IT Audit Handbook – Application controls, Input controls

Administrative Document (SAD) by the parties with the respective Kosovo Customs Code articles on the evaluation.

As soon as the customs officer finds that the price declared in SAD should be changed following the comparison with internal and external prices, he should calculate the price-setting multiplier manually, outside the system (description 45 in SAD – regulation). He should then enter it into the ASYCUDA without applying input controls in the system in order to validate the accuracy of data so that the SAD can be generated with the price of goods as changed/valuated by the Customs.

The ASYCUDA system does not enable the automatic calculation of the price-setting multiplier within the system, given that it has not been requested by the business unit, and no examples on how to apply it have not been given either.

Since the customs officers calculates the price-setting multiplier manually, errors could be made during the calculation thus not setting the correct value.

8. Re-channelling of consignments from the green channel to the red one

Documentation of different methods of data entry; invalid data should be properly rejected by the application; validity criteria are updated as appropriate and authorized; compensating controls such as logs and authorisation rules in case of the possibility of overriding input controls should be in place; there is proper control and documentation of application entries.²⁵ Documents and physical inspection of goods labelled for the red channel (observation teams) as well as documents inspection of goods labelled for the green channel should be in place.²⁶

The customs officer (could also be the shift leader/unit leader) - 15 minutes after the system has channelled the consignment to the green channel - can re-channel it to the red one when he finds that additional examinations are required and there is information that needs to be validated, without having the documents on the

²⁵ IT Audit Handbook – Application controls, Input controls

²⁶ Kosovo Customs – Identification of risks for Kosovo Customs, 2023.

reasoning for re-channelling or the possibility of control by the system in the event of an error in the consignment re-channelling.

Based on the tested cases, the customs officer or the person that re-channelled the consignment to the red channel had not given any comments or reasoning on such action. There is no procedure obliging the customs officer to write any comment on such action, and neither is there any field in the system to write the reason behind the re-channelling - although the standards for application input controls suggest verifying and documenting the data entry into the system.

This leads to risk management sector to lack an overview on risky cases and to lack of transparency and accountability of the officer at the custom crosspoint. It also leads to incomplete situation reports serving the management for decision-making.

9. ASYCUDA system does not validate the data on personal/business number and trademarks

Invalid data should be properly rejected by the application; validity criteria are properly updated and checked with the basic data register,²⁷ including the personal and business number. Trademarks should be identified in SAD during the custom clearance phase, section 31 of SAD, so that - after having written it - the AW system warns whether it is a protected trademark.²⁸

We found that, when registering the declaration, the customs agents describe the personal number and the business number manually in all the cases and do not check it with the database of the civil register or business register.

The personal number and the business number are data of the Civil Registry Agency and Business Registration Agency, whilst Customs has not created an interface for some of the fields used by the ASYCUDA system. Even though they provided us

²⁷ IT Audit Handbook – Application controls, Input controls

²⁸ Kosovo Customs – Identification of risks for Kosovo Customs, 2023.

with a written agreement they had with the Business Registration Agency, there was no technical interfacing implemented in the system.

We also found that the ASYCUDA system does not give a warning on the protected trademarks when inspections are carried out by the customs officers. However, they do have a separate system (INES) where the protected trademarks are listed by the KC and lists of documents wherewith, they manually check whether the commodities are protected trademarks.

Moreover, the trademarks data entered into the INES system used by the KC cannot technically interface with the ASYCUDA system. The basic system that safeguards these data, INES, is limited and restricts the possibility of data exchange with AW system.

The lack of these data validation interfaces may result in intentional or unintentional error and failure to verify it in real time. If goods enter without prior verification of the protected trademark by KC, it would cause damages to the trademark and the citizen and also constitute non adherence to the agreement with the list of traders that KC has for the protection of trademarks.

10. The modules for placing the criteria and the tariffs in the ASYCUDA system are neither suitable

The application correctly identifies the transactional errors. A suitable mechanism for addressing processing errors is in place.²⁹ Officers from respective sectors continuously update the risk assessment, receive information and process it into the ASYCUDA World system, which will afterwards be read as criteria during the examination stage and by any user of AW. Based on these criteria (risk levels) the consignments will be re-channelled by SW system itself to the yellow, green and red channels.³⁰

29 IT Audit Handbook – Application controls, Input controls.

30 Kosovo Customs – Identification of risks for Kosovo Customs, 2023.

The ASYCUDA's criteria setting module is not user friendly. The risk sector officers in charge should be careful to understand the databases and the syntax of programming languages, as setting the criteria in ASYCUDA requires specific knowledge. Therefore, when introduced to this module, we realized that syntax errors had occurred when setting the criteria due to the way the module is designed, which have also resulted in the criteria in the real system.

The tariff setting module is not user friendly either. The officers have to write the calculation formulas in each field for changing one tariff. Whilst, when they have to change many tariffs, the ASYCUDA system does not allow for the automatic replacement of all the tariffs simultaneously, instead they have to change them one by one which takes time and leaves room for errors, which we encountered during the execution.

These modules have been implemented as such because the ASYCUDA system is a ready-made one and the options it provides are universal for all the AW users worldwide. The Customs officers claimed to have discussed about the risk criteria module at a UNCTAD conference and asked for changes, but the KC has not submitted any formal written request for this matter.

This current way of changing and setting the criteria and tariffs in the AW system affects the efficiency of work of these two sectors and of all AW users who use the criteria and tariffs, thus enabling the possibility of errors in the data recorded by the relevant sectors and having an adverse impact on the system operation.

11. ASYCUDA system does not carry out a risk assessment automatically and measurably

Officers from respective sectors should continuously update the risk assessment, receive information and process it into the ASYCUDA World system, which will afterwards be read as criteria during the examination stage and by any user of AW. Based on these criteria (risk levels) the consignments will be re-channelled by SW system itself to the yellow, green and red channels.³¹

31 Kosovo Customs – Identification of risks for Kosovo Customs, 2023

The risk sector within the Kosovo Customs sets the criteria to be taken into consideration during the custom clearance process on certain categories, based on the internal researches as well as imports and economic operators' background.

The risk sector enters all the criteria, as a text, in a certain field of the system. The customs officer then reads these criteria and compares them with the documents submitted by the party subject to the custom clearance process. All this is performed manually, with a comment given by the customs officer who fills out the "inspection act" field with a briefing text. But there is no parameter set to notify the level of risk from applying these criteria – which criteria have been applied and which not – by giving an accurate statistical figure automatically, measurably and timely.

KC does not have procedure in place to define how to carry out the risk assessment and the setting of criteria, which would help in the development of this process in the system as well. In addition, the segregation of duties and the lack of formal approval in the criteria setting process has not been defined.

Lack of formal approval and unclear segregation of responsibilities regarding the setting of risks criteria may affect the resilient decision-making, thus leaving room for unequal treatment of cases and leading to challenges in addressing the risk priorities. Moreover, this situation may limit the complete feedback and the risk sector's efficient period on the set criteria, thus making the criteria analysing and monitoring process more challenging. This may also affect the efficient decision-making and allocation of resources.

04

4. Conclusions

Kosovo Customs has made significant progress towards the digitalisation of custom processes, improving efficiency and transparency in the management of its operations. Such progress has been achieved through the implementation of the ASYCUDA World system, which enables the automation of a significant part of customs procedures, thus reducing bureaucracy and speeding up processes. The system allows the electronic registration and processing of customs documentation, as well as real-time data interchange between customs agents, economic operators and other relevant institutions. By using this system, Kosovo Customs has managed to improve the monitoring of the flow of commodities. However, digitalisation remains an ongoing process, and challenges such as adapting the risk criteria, full integration of sectors and provision of technological support require continuous engagement in order to reach the complete digitalisation.

Outsourcing

Kosovo Customs has managed to implement the agreement on ASYCUDA system regarding the development, upgrading and maintenance of the system and has also managed to implement the UNCTAD request for promoting gender equality. Kosovo Customs has not managed to clearly define the duties and responsibilities of the parties involved in the information security and protection, thus leaving the information system security unaddressed and vulnerable.

Information and cybersecurity

Kosovo Customs suffers shortcomings in controls over the information security due to the lack of a clear IT security structure. With a low level of employees' awareness on information security, it lacks a users' access control procedure and owns an outdated information security policy. This will continuously expose the information to the risk of damage, change and loss, without giving the possibility of identifying and preventing it in time.

Business Continuity Plan - Disaster Recovery Plan

Kosovo Customs does not have an effective business continuity policy in place. It lacks the business continuity plan and structure which would enable the implementation of the plan and of the customs written procedures that are implemented through the ASYCUDA system.

Application Controls

Kosovo Customs has continuously updated the ASYCUDA World system for the digitalisation of customs clearance processes. But it has not managed to ensure that the data entered into the system are correct, because the data for the calculation of the multiplier for setting the post-revaluation price are processed manually. Neither does it assure that the data are true and valid given that it cannot validate all the data entered into the system. Even when the data can be validated from the existing databases, the KC is not able to have measurable feedback on the risk occurrence because of the way the risks assessment criteria are set into the system. Moreover, this system is not user-friendly, it does not provide simple usage options, especially for the risk and tariffs modules, thus resulting in errors appearing in the system occasionally.

05

5. Recommendations

We recommend the Kosovo Customs on:

1. Outsourcing policy – to ensure that, prior to initiating developing any information technology project, all contracts on information technology have addressed the information security requirements;
2. Information security policy – to update the policies and procedures for protecting the information security;
3. IT security structure, segregation of responsibilities and management of audit trails – to segregate the duties and responsibilities of the roles in information systems and restrict the actions of each of the roles in line with the information security standards, by separating the roles of the database administrator and system administrator from the role of information security officer. The privileges of access to audit trails should be restricted and monitored on regular basis, without causing conflict of responsibility and ensuring the safety data integrity;
- 3.1 To review the customs declaration processing procedure in the ASYCUDA World system, made by the goods physical inspection officers, in order to provide for more accurate and transparent physical inspection;
4. KC employees' awareness and trainings on information security – to hold trainings for all the customs officers regarding the information security and to consider the possibilities of implementing the access to information systems by using the single sign on form;
5. Control over users access to information system – to apply the access control procedure, through which the process for providing and removing access to the information system is defined and all access is reviewed in regular basis;
- 5.1 To revise the 2015 agreement entered between the Kosovo Customs and the Kosovo Local and International Freight Forwarding Association that defines the form of customs agents' access and to review the access of customs agents;

6. Business continuity plan – to draft and approve a business continuity plan; to set forth the structure as well as the roles and responsibilities on plan implementation; to draft a document with written customs procedures and processes implemented through the ASYCUDA World system;
7. Calculation of the price-setting multiplier in ASYCUDA World – to automate this process so that the customs officers will no longer need to conduct such a process manually;
8. Re-channelling of consignments in the ASYCUDA World system – to create mandatory fields in the system so that the customs officer, including the shift leader or unit leader, could give a comment or reasoning in the system regarding the actions taken when re-channelling the consignments from the green to the red channel;
9. Data validation in the ASYCUDA World system – to enter into agreements with the respective institutions that own the databases (Civil Registry Agency and Business Registration Agency) and to establish technical solutions for data interchange with ASYCUDA World system in order to verify them with basic databases;
10. User-friendly modules – to upgrade the system with more user-friendly modules, by finding the most suitable form to facilitate the use of the module for users from the risks and tariffs sector;
11. Risk assessment and setting of criteria – to draft an internal regulation on risk assessment and setting of criteria; to enable the creation of a criteria setting checklist in the ASYCUDA system so that both the management and the risk sector could obtain information and statistics in real time, analyse them and take the right decisions based on the analyses made.

ANNEX

Annex I. Audit Design

Risk areas and audit problem indicators

The Kosovo Customs has a broad mission, commencing from protection of the state, economy and citizens. Therefore, the mission of the Customs Service can be divided into two main categories:

1. For economic issues - The collection of customs duties: such as customs duty, value added tax; excise for the Kosovo Consolidated Budget. Control of import and export, defend the economy; protection of trademarks and others, as well as accurate statistics on foreign trade.
2. For the security - Fighting illegal activities. Increased security presence at border crossings through fighting border crime; fighting drug trafficking, etc. Protection of population and environment, prevention of smuggling of weapons and explosive substances.

Considering the role and importance of KC, the National Audit Office (NAO) and the European Commission (EC) have dedicated special sections in their respective annual reports.

The EC's Report on Kosovo puts an emphasis to the progress of KC, the importance of IT systems and to the progress KC has made in the digitalisation of processes.

Moreover, NAO has, in its annual audit report (AAR) for 2022, found cases of incomplete reconciliation of the customs tariffs between the TARIK and ASYCUDA systems. This had occurred due to the Customs' failure to update the list of tariff codes and sub-codes between the two systems and neither had it updated the full list of customs tariffs in the AW system.

Considering its importance and the fact that this is an IT systems audit topic that requires a special addressing, NAO has deemed it indispensable to conduct an IT audit that is separate from the performance division aimed at addressing the security and accuracy of information system in KC.

During the pre-study phase we examined the documentation on IT systems and customs processes as well as conducted interviews with the KC responsible officers and found the following shortcomings:

- KC suffers shortcomings in its organisation, structure and information security policies;
- KC did not address information security issues in the development agreement and in the subsequent maintenance and advancement agreements;
- Secure access with multiple authentications is not used in the ASYCUDA World system in KC;
- The ASYCUDA World system lacks interfaces with other systems, as a result some of the registrations are done manually, such as the personal number registration.
- Even though it uses the INES system for registering the trademark, the KC is unable to identify the protected trademark, due to the lack of interface of this system with ASYCUDA World and LES ECM systems.

This audit is carried out as part of the IDI's LOTA Program, which aims to develop SAls in IT auditing, IT use and Strategy.

The examined problems' indicators identified from different sources; the meetings held with persons in charge of identifying issues concerning information systems in KC; and our assessments based on the IT Audit Handbook³² for identifying the riskiest areas from the obtained documentation led us to the main problem that is: KC has shortcomings in organising the information security and the application control.

³² IT Audit Handbook - is a platform developed by ITWG/EUROSAl and WGITA/INTOSAl, which is used to identify the riskiest areas, define questions, criteria and work methodology during the IT audit process.

1.1. System description

1.1.1. Ministry of Finance, Labour and Transfers

Ministry of Finance, Labour and Transfers (MFLT), pursuant to the Regulation on the Areas of Administrative Responsibility of the Office of the Prime Minister and Ministries³³, is responsible for: development, drafting, adoption, assessment and oversight of public policies; drafting of legal acts; drafting and adoption of bylaws; determining the mandatory standards on public finance management, internal control and audit for the public sector, standards on accounting and financial reporting for the private sector and publicly owned enterprises, public debt, public procurement, macroeconomic and fiscal policies, property tax, state aid in accordance with the Constitution and the applicable legislation. MFLT consists of the revenue management agencies, including the Kosovo Customs. It operates in close cooperation with the Ministry of Finance, Labor and Transfers and such cooperation is structured in some key areas:

1. Revenues Collection:

Kosovo Customs collects taxes and customs tariffs from imports and exports of goods. These incomes are an important part of the state budget and are reported to the Ministry of Finance, Labor and Transfers.

2. Implementation of Fiscal Policies:

KC is responsible for the implementation of fiscal policies set by the Ministry of Finance, Labor and Transfers. This includes collecting VAT and excise duties on goods entering Kosovo.

³³ Regulation (GoK) no.07/2020 on the Areas of Administrative Responsibility of the Office of the Prime Minister and Ministries.

3. Legislation:

KC works together with the Ministry to draft and improve customs legislation and trade policy. This ensures that the customs policy is in line with international standards and protects the Kosovo's economic interests.

4. Control and Monitoring:

Kosovo Customs and the Ministry of Finance, Labor and Transfers cooperate to ensure accurate monitoring and control of commercial and financial flows. This includes the fight against smuggling and tax evasion.

5. Technology and Training:

There is ongoing cooperation in information technology and staff training to improve the efficiency of customs and financial operations.

6. Reviewing and Reporting:

Kosovo Customs reviews and reports its income and activities to the Ministry of Finance, Labor and Transfers on a periodic basis, ensuring transparency and accountability in the management of public funds.

All of the areas above show the close and indispensable connection between the Kosovo Customs and the Ministry of Finance, Labor and Transfers aimed at optimising the country's fiscal and economic administration.

1.1.2. Kosovo Customs

Kosovo Customs was established in August 1999 by the EU pillar, to ensure the application of fair and uniform customs regulations and other provisions applicable to goods, which are subject to customs supervision. On 12 December 2008 UNMIK Customs Service became Kosovo Customs. The new Customs Code - adopted on 11

November 2008³⁴ by the Assembly of Kosovo – enabled such transition and later in 2012 was amended and supplemented. The Code is fully in compliance with European Union standards and aims, inter alia, the economic development of the Republic of Kosovo.

Besides customs duties generated by the Customs, the VAT and the excise tax are paid at the border. In addition to revenue collection, Kosovo Customs protects the society from smuggling of drugs and other prohibited goods, having a detrimental effect by economic crime and revenue evasion.

Kosovo Customs was built based EU standards and is funded entirely from the Kosovo Consolidated Budget. It is also supported by the EU through the senior professional from EU customs authority. Customs also benefit from technical support of the EU Customs and Fiscal Assistance Office (CAFAO), which has helped in the development of basic legislation, organization, structure and training in staff development. Kosovo Customs is assessed as one of the institutions with the highest organisational values, and, ever since its establishment, it has been the main contributor when it comes to revenue collection and protection of citizens from prohibited and restricted goods. The revenues collected by Customs constitute around 60% of the total of revenues collected for the Budget of the Republic of Kosovo.³⁵

According to the internal regulation, the Kosovo Custom structure consists of the following five directorates:

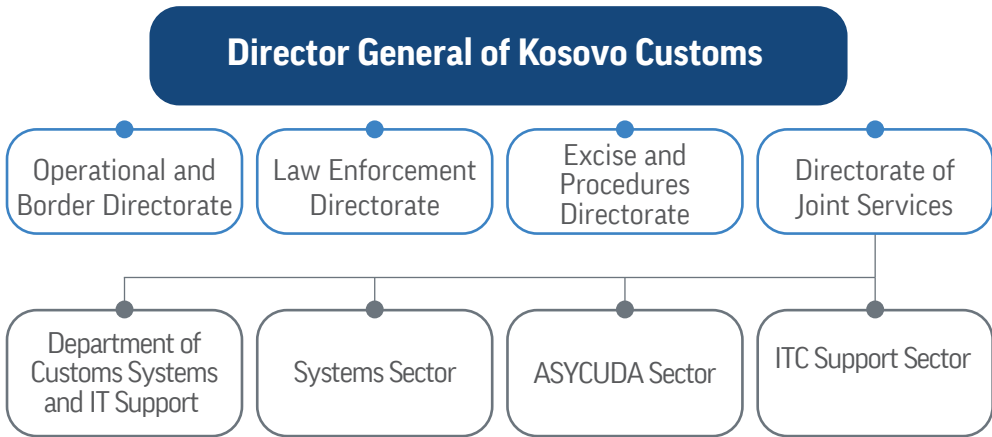
- Director General;
- Operational and Border Directorate;
- Law Enforcement Directorate;
- Excise and Procedures Directorate; and
- Directorate of Joint Services, which includes the Department of Customs Systems and IT Support consisting of the following sectors:

³⁴ Code nr. 03 L-109 on Kosovo Customs and Excise

³⁵ KC Strategic Plan for 2019-2023.

- Systems Sector;
- ASYCUDA Sector; and
- ITC Support Sector

Figure 5. Organisation of directorates, departments and sectors included in the scope



Operational and Border Directorate (OBD) is run by the director of directorate with a customs status who reports directly to the DG. Within its determined competencies, coordinates and monitors the activities of regional directorates and other Customs directorates. It is responsible for planning, strategy-making, decision-making, coordination and monitoring of the implementation of strategies, as well as it undertakes activities for implementation of customs legislation, as assigned for the OBD's competence. It coordinates activities with national law enforcement structures and with third countries customs authorities within the agreements in force. It is responsible for the implementation and further development of the system and procedures dealing with customs procedures, national strategies in cooperation and coordination with certain directorates and departments, in order to collect legal revenues and to support the legal trade facilitations.

Law Enforcement Directorate (LED) is run by the director of directorate who reports directly to the DG. Within the KC's strategies and operational plans and in accordance with the rule of law, LED is responsible for implementation of legislation as assigned to for Customs competence, by ensuring the coordination

with the other departments, those regional in particular. It is responsible for the implementation and development of the national risk management system based on risk analysis and intelligence and in full coordination with the regional units. It provides for and supervises the implementation of the law and procedures related to the protection of Intellectual Property Rights (IPR). Coordinates activities with other national law enforcement agencies, as well as with third countries customs authorities within the agreements in force.

Excise and Procedures Directorate (EPD) is run by the director of directorate with a customs status who reports directly to the DG. Within its competencies assigned to, it coordinates and monitors the EPD and subordinate structures activities. It is responsible for planning, strategy-making, coordination, decision-making and monitoring of the implementation of strategies and of the activities for implementation of customs legislation, trade facilitation, upgraded respective customs procedures, implementation of which is assigned to the EPD. It coordinates with other directorates, customs departments and other agencies, as well as with third countries customs authorities within the agreements in force. It is responsible to develop the systems and institutions within the directorate and support their fair application by other directorates. It provides for the implementation of customs legislation in relation to procedures, excise, rules of origin, customs classification of goods and customs tariffs, customs duties, customs laboratory and debts oversight.

Directorate of Joint Services (DJS) is run by the director of directorate with a customs status who reports directly to the DG. Within its competencies assigned to, it coordinates and monitors the DJS and subordinate structures activities. It is responsible for planning, strategy-making, coordination and monitoring of the implementation of strategies, as well as it undertakes activities for implementation of customs legislation as assigned to. It is responsible for Customs budget policies and obligations regarding the accounting and expenditures. It provides for the development of HR policies and strategies and the implementation of respective legislation. It prepares the annual financial plan for the Customs and its organisational units. Provides for and monitors the procurement and IT policies, including innovations in IT systems and ASYCUDA. DJS consists of departmental and sectoral organisational units under the management of the DJS director or of the respective departments, including the Department for Customs Systems and Information Technology.

Department for Customs Systems and Information Technology is run by the head of department with customs status, who reports directly to the director of DJS. This department is responsible for setting the KS's strategy and operational plans on information technology and communication. It undertakes actions and coordinates the activities for implementation, development and management of IT systems, security and infrastructure as well as coordinates and supports the KS's organisational units at both central and regional levels on using the IT systems, tools and assets.

This department consists of the following sectors:

- Systems Sector;
- ASYCUDA Sector;
- IT Support Sector.

Systems Sector (SS) is run by the head of sector with customs status who reports directly to the CSD-IT. This sector contributes in implementing and developing the customs systems strategy and procedures automation. It manages and administers the Law Enforcement and Case Management Systems, the VMware Virtual Platform and Systems Auditing, the Staff Management Systems and other systems in relation to the electronic presentation and customs procedures. Is responsible to manage and develop all the tools and applications necessary for the automation of customs procedures. It performs analysis on innovations and development of KC technological systems. It suggests changes to and new technical solutions for upgrading customs systems operations. It offers technical specifications and necessary documents and solutions to upgrade the systems operations and customs computerised procedures and the Customs systems infrastructure.

ASYCUDA Sector (AWS) is run by the head of sector with customs status who reports directly to the head of CSD-IT. This sector manages and administers the development of ASYCUDA World (AW) system; administers and develops the BI–Cognos platform, the Systematic Electronic Exchange of Data (SEED)³⁶ and other systems regarding the electronic presentation and customs procedures. It ensures

³⁶ Systematic Electronic Exchange of Data

the regular maintenance of computerised customs systems and various applications and necessary tools to support offices work. It contributes in implementing cross-agency projects and regional cooperation such as SEED, etc. It is responsible to perform the database installation services for Customs Systems and the testing the new versions of the operative system, by saving and following changes to the legislation and procedures with the purpose of including them in the system. Based on respective authorisations and reports received from organisational units, it performs necessary upgrades in the system.

Sector for Information Technology Support (SITS) is run by the head of sector with customs status who reports directly to the head of CSD-IT. Is responsible to develop systems security, network infrastructure, starting from the internal network users, firewall, security certificates and PKI (public key infrastructure), implements the continuous functioning of business (business continuity) for IT infrastructure, systems and security. It organizes, it monitors, manages and assesses the performances of resources, activities and IT infrastructure. It develops, administers, maintains and oversees the implementation of policies, procedures and plans that have to do with systems security administration, infrastructure and server systems, databases, applications and users access in the system. It determines and implements the disaster recovery plan for the network infrastructure, systems servers, databases, applications and systems security. It guarantees the proper functioning of systems and server equipment such as: Domain Controller, Storage-Data file server, Firewall, Backup and other IT systems; as well as camera surveillance systems, depending on the organization's needs, to guarantee appropriate updates and functioning of databases and applications regarding the Finances, Human Resources, Logistics, Procurement and other applications which IT is responsible for, to guarantee necessary technical support for all the KC offices, for installations, maintenance, use of equipment and network.

Audit scope and questions

The audit scope will cover the Kosovo Customs and the respective departments for IT management, ASYCUDA system and customs processes:

Directorate of Joint Services - Department of Customs Systems and ITC Support with the sectors: Systems; ASYCUDA and ITC Support.

Border Operations Directorate with customs departments and sectors including a land border point, air border point and sea border point.

Law Enforcement Directorate - Sector for Risk and Monitoring (SRM).

Excise and Procedures Directorate (EPD) – Department of Excise, Tariff, Origin and Procedures (DETOP) with the Sector of Origin, Sector of Tariff, Sector of Procedure and Authorizations (SPA), Sector of Excise and Sector of Debts.

The audit will focus on information security and input controls and application processing controls for information technology systems used for customs processes, with focus on ASYCUDA World system. The audit will cover the period from 2022 to 2024.

Audit questions

In order to be responsive to the audit objective, we have posed the following questions:

1. Does the Kosovo Customs implement the outsourcing policies?
2. Has Kosovo Customs identified and addressed the security requirements in the developed outsourcing procedures?
3. Does the Kosovo Customs own and implement information security policies?
4. Does Kosovo Customs have a clear IT security structure in place?

5. Are employees aware of the security-related duties and responsibilities and have they been provided with trainings regarding information security?
6. Is the process for granting and removal of access to employees and contractors effective and safe?
7. Does the organisation have an effective business continuity plan in place?
8. Are correct data entered by authorized personnel in the database and in the application?
9. Does the application ensure data integrity, validity and reliability during the transaction processing cycle?

Audit Criteria³⁷

The criteria used in this audit derive from the IT Audit Guideline³⁸, International Standards on Information Security³⁹, and documents of the Kosovo Customs such as the System development and maintenance⁴⁰ and the approved document on risk assessment.⁴¹

37 For more information, please read ISSAI 300, Criteria, p.7

38 IT Audit Handbook is a product developed the IT Working Groups of EUROSAT (WGITA) and INTOSAT (IDI) defining the rules and standards on IT auditing – hereinafter IT Audit Handbook.

39 Information Security Management System ISO/IEC 27000/01.

40 Agreement between the Kosovo Customs and the UNCTAD on the project for Customs software, ratified by the Assembly of the Republic of Kosovo

41 Risks assessment for Kosovo Customs, 2023.

In order to assess the identification of needs and addressing of information security requirements in the projects outsourced by KC, we have set the following criteria:

- The organisation should implement the organisational outsourcing policies.⁴²

Kosovo Customs should implement the signed agreement including the following article: In the project's initial stages, the preparatory activities that will be undertaken, including the efforts to ensure that awareness on and mobilisation of women reach the various groups concerned (customs, merchants); in line with its commitment to promote gender equality/awareness-raising, UNCTAD strongly encourages the participation of female staff in training projects and activities and other events.⁴³

- The organisation's security requirements should be adequately pointed out by the Contractor.⁴⁴

The agreement with external parties involving the access, processing, communication or management of the organization's information or information processing structure, or the introduction of products or services into the information processing system, is in accordance with all appropriate security requirements.⁴⁵

In order to assess that Kosovo Customs has put information security and business continuation mechanisms in place, we have set the following criteria:

- In order to discharge its mandate, Kosovo Customs should document, approve and communicate appropriate policies and procedures to run the business and IT operations. Information security policies should cover all operational risks and be able to reasonably protect all critical information assets from loss, damage and abuse. (Ref. ISO 27000: Information Security

42 Information Technology Audit Handbook, Outsourcing Policies

43 Annex2 of the Agreement between the Kosovo Customs and the UNCTAD, March 2023.

44 Information Technology Audit Handbook, Outsourcing, Security

45 ISO 27001 – Information Security Policy.

Management System and other applicable internal policies, procedures or rules).⁴⁶

- Kosovo Customs should have in place clear IT duties and responsibilities related to information security policies, there should be no conflicting areas of responsibility or non-alignment of information security activities. (reference ISO 27000).⁴⁷

Information security activities should be coordinated by representatives from various parts of the organization who hold relevant roles and job functions. An established management authorization process for new and existing information processing facilities should be defined and put into practice. Confidentiality requirements or non-disclosure agreements reflecting the organisation's needs for the protection of information must be identified, documented and regularly reviewed. risks to the organization's information and information processing facilities arising from business processes involving external parties should be identified and appropriate controls should be implemented before granting access. Information systems must be configured and operational to ensure that audit trails are generated for all transaction data. Reporting of events must be accurate on all the activities performed by the system users. Access to audit trail logs must be limited and controlled, and the integrity of the audit trail data must be protected against modification.⁴⁸

- Kosovo Customs should ensure that all employees (including contractors or sensitive data users) are qualified to maintain data, use resources, understand duties and responsibilities. The staff should safeguard the information security, from the recruitment until termination of the employment relationship. Their access should be removed as soon as their employment/outsourcing contract is terminated.

46 IT Audit Handbook – Information and Cybersecurity, Information security policies

47 IT Audit Handbook – Information and Cybersecurity, IT Security Structure.

48 ISO 27001 – IT Security Structure.

In addition, refresher trainings should be provided periodically to the employees, whose organisational role is significant for the Information Security and Cybernetics.⁴⁹

- The Kosovo Customs policies for access to information systems should provide a basis for the control of interference to information. The information security function monitors the effectiveness of the monitors user account management operations control on a timely basis and reports the operating efficiency and effectiveness.⁵⁰

The allocation and use of privileges in the information system environment should be restricted and controlled, i.e. privileges should be allocated on a need-to-use basis, and privileges should be allocated only following the formal authorisation process.⁵¹

- Kosovo Customs should cover all the organisation's critical areas by a team. Requirements for the duties and responsibilities in the team members.⁵²

The Business Continuity Planning tests should ensure that all the recovery team members and the other relevant staff are aware of the plan and their responsibilities on the business continuity and information security as well as recognise their roles when the plan is revoked.⁵³

In order to assess that the ASYCUDA World information system has application control mechanisms that enable safe logical and reliable access to the information system, we have set the following criteria:

- Validation rules are be well-designed and implemented into entry (input) interfaces; different methods of data input are documented; invalid data is properly rejected by the application; the validation criteria are updated in a timely, appropriate and authorised manner; compensating controls such as logs and authorisation rules in case of the possibility of overriding

49 IT Audit Handbook – Information and Cybersecurity, IT security of human resources.

50 IT Audit Handbook – Information and Cybersecurity, Access Controls.

51 ISO 27001 – Access Controls

52 IT Audit Handbook, BCP – DRP – Structure of the business continuity function

53 ISO 27001 – Structure of the business continuity function.

input controls are in place; there is proper control and documentation of application entries.⁵⁴

- Documentation and physical inspections of commodities coming out from the red channel (observation teams) and documentation inspections in the yellow channel should be in place. Documentation inspection based on risk analysis for consignments coming out of the green and blue channel. Other post documentation controls conducted by the Post Documentation Control Sector.
- Trademarks should be identified in SAD during the custom clearance phase, section 31 of SAD, so that - after having written it - the AW system warns whether it is a protected trademark.⁵⁵
- The application correctly identifies the transactional errors. Data integrity is maintained even during unexpected interruptions to transaction processing. There is an adequate mechanism for handling processing errors, review of suspense files and clearance.⁵⁶
- Officers from respective sectors continuously update the risk assessment, receive information and process it into the ASYCUDA World system, which will afterwards be read as criteria during the examination stage and by any user of AW. Based on these criteria (risk levels) the consignments will be re-channelled by SW system itself to the yellow, green and red channels.⁵⁷

54 IT Audit Handbook – Application controls, Input controls

55 Kosovo Customs – Identification of risks for Kosovo Customs, 2023.

56 IT Audit Handbook – Application controls, Processing controls

57 Kosovo Customs – Identification of risks for Kosovo Customs 2023.

Audit Methodology

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

In order to assess the needs identification and address the information security requirements in the projects outsourced by Kosovo Customs, we will:

- Review the outsourcing policies and documents to ensure that they have been approved and implemented;
- Review the documents to assess whether the organisation has identified the risks and is aware of them.
- Review the documents to assess whether the organisation has identified the security requirements and drafted in the contract or SLA.
- Verify whether the organisation has obtained assurance on the security mechanisms established by the service provider.

In order to assess whether Kosovo Customs has information security and business continuity mechanisms in place, we will:

- Examine the documents to verify whether IT Strategy adequately addresses the critical role of information security; make reference to the use of IT Governance matrix and the IT Strategy matrix; check whether the IT security plan identifies the duties and responsibilities, staff demands, security awareness and trainings, implementation of practices, needs for investments in needed security sources; review and analyse the diagram to verify whether it refers to an organisational risk appetite on information security and that this diagram clearly includes the purpose and objectives of the security management function.
- Determine whether the IT security responsibilities are well defined; check whether there is a process for prioritisation of proposed security initiatives in place, including the required levels of policies, standards and procedures.
- Check whether the roles critical to the information security are clearly defined and documented; the employees and third parties being assigned to those roles are aware of their responsibilities regarding the protection of the organisation's information assets; review the proper identification of critical

roles for which security validation checks are required; check the proper segregation of duties between the IT security management and operations; check whether the policy of IT staff appointment, transfer and rotation as well as staff dismissal is clear in order to diminish the dependence on the individual; check as to what knowledge transfer mechanisms are followed.

- Check the procedures in order to define as to what frequency users access and privileges are revised; check the way the privileges granted to users are confirmed.
- Interview users and check the instructions, by sampling, in order to verify as to how users are informed of their responsibilities on the protection of sensitive information or assets, if they are granted respective access.
- Examine the documents/interview the responsible staff in order to assess all the organisation's critical areas that need to be represented in the business continuity group; examine the documents in order to assess whether there is ownership and tasks assigned for business continuity responsibilities at the top management, e.g. whether the management has identified the level and emergency of recovery and whether this has been presented in the policies; examine the documents in order to assess whether all the critical departments have appointed the member to the disaster recovery group along with well-defined duties; interview a number of staff in the business continuity group/or equivalent, to assess whether they are aware of their role in business continuity for each critical business unit/department.

In order to assess that the ASYCUDA World information system has application control mechanisms that enable safe logical and reliable access to the information system, we will:

- Check whether validation rules are well-designed and documented; check whether validation controls on input data are in place; observe the application users; observe the application users in real action; implement the application in testing environment and test different interactions for all the input data; analyse the data logs saved in the databases by using CAAT (IDEA); obtain an operational description for each class of input information and design for transaction data logging; inspect the functionality and model about presence of timely and complete controls and error messages.
- Assess whether criteria and validation parameters on input data correspond to business rules and implement the rejection of the ill-fitting types of data;

inspect the managers on the periodic review of the criteria and validity parameters on input data, if they are properly cleared and confirmed; security is maintained through documentation review, coding analysis, and interviews; determine as to what interfaces are in place with the application; these interfaces are in the form of real-time or periodic transmission of data via package processes; review the process flow diagrams and system code.

- Assess whether the application contains accurate validity controls to ensure the integrity of processing; inspect the reconciliations and other documents in order to verify whether the input numbering is coherent with the output numbering, to obtain assurance on the data processing; follow the transactions through the process in order to verify that the reconciliation effectively establishes whether the total files correspond to the terms outside the reported balance.
- Inspect the audit trails and other documents, plans, policies and procedures to verify that system capabilities are effectively designed to automatically maintain data integrity; inspect the functional description and design information for transaction data entry to verify that transactions that fail validation routines are posted to suspension files; confirm that older failed transactions have been properly corrected.

Relevant Documents

Regulations

Regulation (GoK) no.06/2020 on the Areas of Administrative Responsibility of the Office of the Prime Minister and Ministries

This regulation sets forth the administrative responsibilities of the Office of the Prime Minister and ministries in the Government of the Republic of Kosovo.

Relevant Documents

Code no.03 L-109 on Customs and Excise in Kosovo

This code regulates basic elements of the system for customs protection of the economy of Kosovo and the rights and obligations of all operators in applying customs legislation.

KC Strategic Plan 2019-2023

This document sets forth the strategic priorities and objectives as well as the actions that the Kosovo Customs intends to follow for the 2019-2023 period. This strategy aims at implementing the policies; developing the procedures related to the international trade chain, the circulation of vehicles and passengers; and developing border and inland customs inspections by making the most rational use of the available resources.

Annex II: Confirmation letter

REPUBLIKA E KOSOVËS-REPUBLIKA KOSOVA-REPUBLIC OF KOSOVO			
ZYRA KOMBËTARE E AUDITIMIT			
NACIONALNA KANCELARIJA REVIZIJE / NATIONAL AUDIT OFFICE			
DATE PRANORJEVE DOKUMENTI DATE PRANORJEVE DOKUMENTI DATE PRANORJEVE DOKUMENTI			
Niveli Org. Org. Unit	Shif. Klasif. Klasif. Kod Class. Code	Nr. Prot. Br. Prot. Prot. No.	Nr. Faqeve Str. Gramera No. Pages
06	47	22557	1



13.12.2024 DATA E DËSHATIMIT

Nr. Prot. 01/1029/2024

Thema e Dokumentit: Aplikimi i sistemit të ASYCUDA World

Republika e Kosovës
Republika Kosova - Republic of Kosovo
Qeveria - Vlada - Government
Ministria e Financave, Punës dhe Transfereve - Ministarstvo Finansija, Rada i Transfera -
Ministry of Finance, Labour and Transfers



Dogana e Kosovës - Carina Kosova - Kosovo Customs
Zyra e drejtorit të përgjithshëm
LISTË DISTRIBUIMI/ CIRKULARNO PISMO/ ROUTING SLIP

LETËR E KONFIRMIMIT

Për pajtueshmërinë me të gjeturat e Auditorit të Përgjithshëm për raportin e auditimit të teknologjisë së informacionit 'Sistemet e Informacionit në Doganën e Kosovës - ASYCUDA World', dhe për zbatimin e rekomandimeve.

Për: Zyrën Kombëtare të Auditimit

Vendi dhe data: Prishtinë
19 Dhjetor 2024

I nderuar,

Përmes kësaj shkrese, konfirmoj se:


- kam pranuar draft raportin e Zyrës Kombëtare të Auditimit Sistemet e Informacionit në Doganën e Kosovës - ASYCUDA World (në tekstin e mëtejshëm "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.

Agron Llugaj
 Drejtori i Përgjithshëm
 Dogana e Kosovës



Prishtinë

19 Dhjetor 2024



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