Republika e Kosovës
Republika Kosova
Republic of Kosovo

Zyra Kombëtare e Auditimit
Nacionalna Kancelarija Revizije
National Audit Office

AUDIT REPORT ON INFORMATION TECHNOLOGY

MANAGEMENT OF TAX LIABILITIES IN INFORMATION SYSTEMS OF TAX ADMINISTRATION OF KOSOVO

Prishtina, July 2020

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

Our mission is to strengthen, through quality audits, accountability in public administration for an effective, efficient and economic use of national resources. The reports of the National Audit Office directly promote accountability of public institutions as they provide a base for holding managers' of individual budget organisations to account. We are thus building confidence in the spending of public funds and playing an active role in securing taxpayers' and other stakeholders' interests in enhancing public accountability.

This audit has been carried out in line with the International Standards on Supreme Audit Institutions (ISSAI 3000[1]) Guidance on Audit of Information Systems (GUID 5100[2]) and good European Practices.

Information Technology audit undertaken by the National Audit Office is an examination and evaluation of IT systems and related controls to obtain assurance on the principles of legitimacy, efficiency[3], economy[4], and effectiveness[5] of Information Technology system and related controls.

The Auditor General has decided on the content of this report "Management of Tax Liabilities in Information Systems of Tax Administration of Kosovo", in consultation with the Assistant Auditor General, Vlora Spanca, who supervised the audit.

The audit report team consisted of:

Samir Zymberi, Director of Audit Department
Shqipe Mujku Hajrizi, Team Leader
Poliksena Berisha, Team member

[1] ISSAI 3000 – Standards and guidelines for performance auditing based on INTOSAI's Auditing Standards and practical experience.
[2] GUID 5100 – Guidance on Audit of Information Systems issued by INTOSAI.
[3] Efficiency- The principle of efficiency implies achieving the maximum from the available inputs. It relates to the relationship between input and output in terms of quantity, quality and time.
[4] 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 lowest price possible.
[5] Effectiveness - The principle of effectiveness implies the achievement of set objectives and the achievement of expected outputs.

TABLE OF CONTENT

List of Abbreviations

CMS	Case Management System
DWH	Data Warehouse
EDI	Electronic Data Interchange
HRD	Human Resources Division
IEC	International Electro-Technical Commission
ISO	International Organization for Standardisation
IT	Information Technology
ITD	Information Technology Department
NAO	National Audit Office
PA	Payment Agreement
SAD	Systems Administration Division
SIGTAS	Standard Integrated Government Tax Administration System
SQL	Structured Query Language
TAK	Tax Administration of Kosovo
UNIREF	Unified Standard for Reference Numbers
VPN	Virtual Private Network

Executive Summary

Public institutions should assure taxpayers that the systems supporting the collection and recording of revenues and tax debts maintain the integrity, confidentiality and availability of data. Tax Administration of Kosovo is the Executive Agency within the Ministry of Finance, responsible for the administration of tax liabilities. To provide/perform its services, it uses information systems.

The National Audit Office has conducted an audit of the Information Technology in the Tax Administration of Kosovo to assess whether the information systems provide reliable, accurate and complete information. The administration and management of tax liabilities has been conducted through associated information systems, the Electronic Tax Declaration System, the Standard Integrated Government Tax Administration System and the Case Management System.

The Electronic Tax Declaration System has enabled the provision of online services, maintaining and handling tax declarations and has reduced operating costs for the Tax Administration of Kosovo. Whereas, for taxpayers it has reduced the errors in the tax declaration/contributions and has saved time in declaring and paying them. Taxes are managed through the Standard Integrated Government Tax Administration System, however, this system has constantly been advancing in the automation of processes, while the Case Management System has enabled the easier management of tax debts.

During the audit, shortcomings were identified in the above-mentioned Information Technology Systems, related to application controls[6], logical system access controls[7], as well as information security and system continuity[8], exposing systems to the risks of loss of integrity and data confidentiality and system availability.

These shortcomings lead to the presentation of inaccurate and incomplete tax account declarations; risks to the functioning of information systems; loss of data integrity and confidentiality; and risks to information security and system business continuity.

Based on the overall conclusion and the risks identified by the audit, they therefore indicate that there is need for improvements in the management of information systems, through which tax liabilities are administered. Given the importance of tax liabilities to the state budget, we have made a priority recommendation to the Ministry of Finance and Transfers to address specifically issues regarding information security and the capacity/role of the Tax Administration of Kosovo.

While, in order to address quickly the issues of management and control of information technology within the organization, we have made 25 recommendations for the Tax Administration of Kosovo. ***The list of recommendations is given in Chapter 5 of this report.***

[6] Details of these issues are in Chapter 3.1 "Application Control".
[7] Details are given in Chapter 3.2 "Logical Access Management in Information Systems".
[8] Details can be found in Chapter 3.3 "Information Security Management and System Continuity Plan".

Management response on this audit

Director General of Tax Administration of Kosovo has agreed with our audit findings and conclusions and committed to address the recommendations given.

The National Audit Office commends the TAK's management and staff for their cooperation during the audit process.

1. Introduction

The Tax Administration of Kosovo (TAK) is an Executive Agency with full autonomy within the Ministry of Finance, whose responsibility is to administer the applicability of any type of tax applied with tax legislation in the Republic of Kosovo. The main task of TAK is to ensure that proper tax amounts from taxpayers are timely and properly paid, providing the government with revenues for the country's budget.

The central government taxes collected by TAK are:

- Value Added Tax (VAT) on domestic supplies;
- Personal Income Tax;
- Corporate Income Tax;
- Withholding taxes, and
- Pension Contributions.

The collection of revenues through taxes enables fair and transparent financing of public services such as; infrastructure, security, education, health, social welfare programme, etc. The declaration and payment of tax liabilities by taxpayers is important in the economic development of the country, therefore, it is a binding obligation.

The collection of revenues from TAK every year has been increasing, as is seen in the graphic presentation given in the figure 1.[9]

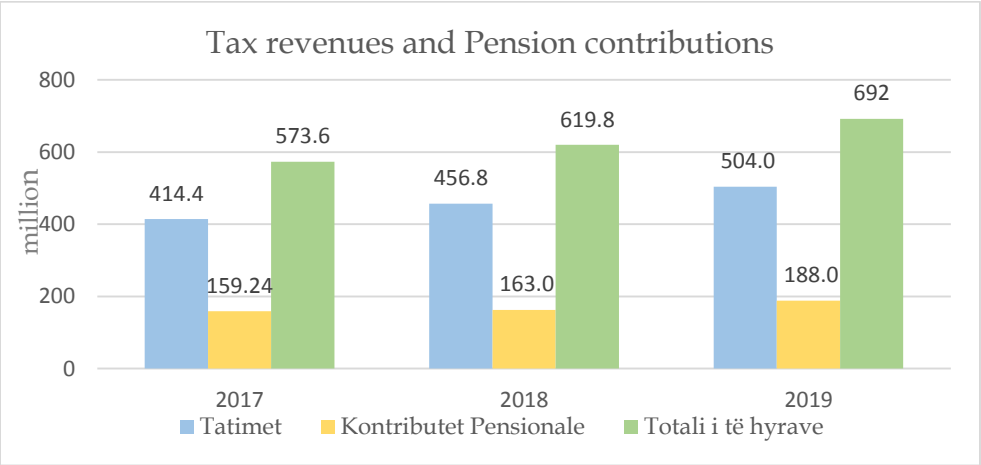

Figure 1. Revenues generated from taxes and pension contributions according to 2017-2019

Outstanding tax debts[10] to TAK during 2017 are 319.5 million, 2018 are 376.1 million and during 2019 they are 357.8 million.[11]

[9] Annual Report of the Tax Administration of Kosovo January - December 2017/2018 & http://www.atk-ks.org/wp-content/uploads/2020/01/20-vjetori-i-ATK.pdf

[10] Taxes constituting an obligation, which must be paid to TAK, are debts to TAK.

[11] Annual Report of the Tax Administration of Kosovo January - December 2017/2018 & TAK, Report of tax debts 2019.

To manage taxes more efficiently and effectively, TAK has used complex information systems to collect, process, store, distribute and use information. The central tax management system is the SIGTAS system (System Integrated Government Tax Administration System). The types of taxes and tax forms presented in Figure 2 are managed through this information system:

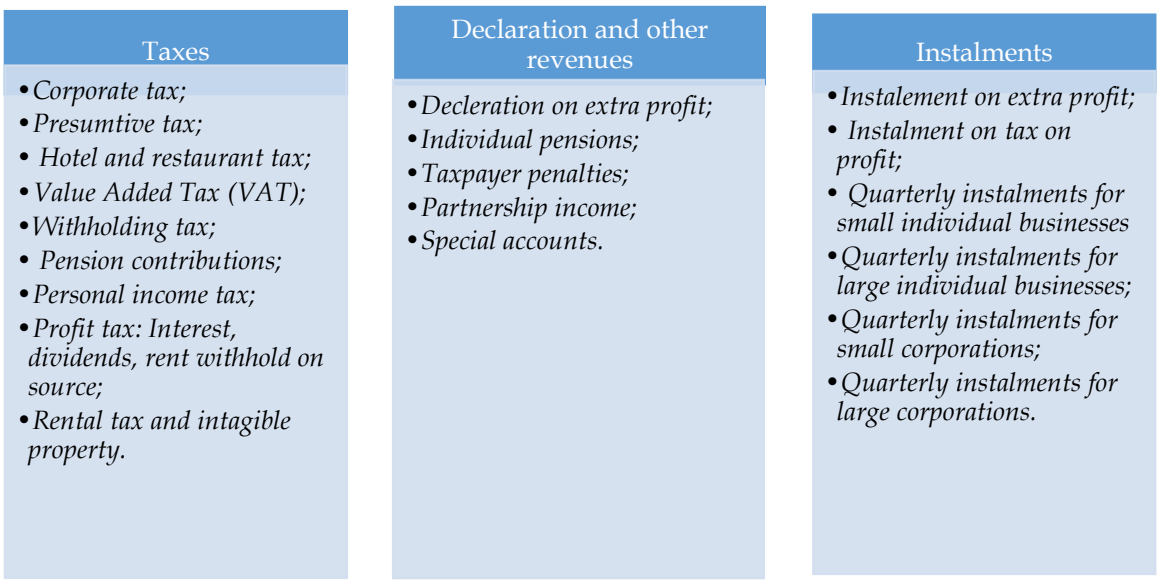

Figure 2. Types of taxes and tax forms managed by the SIGTAS information system

Debt management, payment agreement management, incurring of payments and payment slips are managed through this system.

The SIGTAS information system, which is the basic TAK system, has been in use since 2010. This information system has been developed on the web platform and the database is on the ORACLE platform. This information system is configured for different types of taxes, as well as for calculating tax interests and penalties, according to legal requirements.

The first version of the SIGTAS system has been in use since 2001, when tax collection has begun. This system has been still used for taxpayers' reference and historical data, for cases when passive taxpayers are reactivated, who have not been registered in the new SIGTAS system.

1.1 Risk Areas and Audit Motive

During the audit-planning phase, we have identified several risks that accompany the SIGTAS information system. In the absence of flexibility of the SIGTAS information system, the IT Department within TAK has developed additional information systems that exchange information with each other to manage taxes and the level of tax debts. TAK is also in the preparation phase for the development of the new system for tax management, because the current system is limited to the changes that are necessary for TAK.

As a result, problems related to the SIGTAS system have been identified, which manages taxes, but does not automatically calculate interest and penalty after the last date for declaration/payment. Whereas, the Case Management System (CMS), through which the tax debt collection cases are monitored, does not contain a notification message on the delay for payment of instalments.

Taxpayers' complaints for inaccurate presentation of the Statement of General balance of Declarations and Transactions which are generated by SIGTAS information system; payment processing; and non-transfer of tax declarations from EDI system to SIGTAS system are also considered problems by the taxpayers. These problem indicators have motivated us to conduct this audit.

Examination of the problem indicators identified from various sources and from our assessments based on the Living IT Audit Manual to identify the riskiest areas for the efficiency and effectiveness of debt management in SIGTAS information system leads us to the main problem: the management and control of information systems with particular emphasis on the debt management module.

1.2 Objective and Audit Questions

The audit objective is to assess whether the SIGTAS information system supports the goals and strategy of the institution, providing reliable, accurate and complete information. In this context, we have assessed whether TAK has established the necessary mechanisms for the management and control of information systems with emphasis on the debt management module.

Through this audit, we aim to make relevant recommendations for the responsible parties in order to improve IT services.

Audit questions:

1. *Are effective data validity*[12]*controls established in the information system, which is managing tax debts?*
2. *Has TAK established effective control mechanisms that enable safe logical and reliable access to the information system?*
3. *Does TAK have efficient mechanisms for information security and continuity of the information system in place?*

The scope of this audit is the Tax Administration of Kosovo, namely the Information Technology Department, the Processing Division, within the Department of Registration and Taxpayer Service, as well as the Regional Directorate in Prizren.

The focus of the audit is: SIGTAS Information System, which is the central system for tax administration in TAK, CMS Information System through which taxpayer debt collection management is conducted, as well as the electronic EDI system through which tax declaration and payment connectivity is made with tax declaration via UNIREF[13]. The audit covered the period January 2019 - February 2020.

The applied audit methodology, criteria, methods used, role and responsibilities of the parties and relevant documents are presented in Appendix 1.

[12] The intention of the validity of data is to identify data errors, incomplete or missing data, completeness and accuracy, as well as discrepancies between data.

[13] Unified standard for reference numbers - Instrument used to identify and classify payments, as well as their recording in the SIGTAS information system.

2. System Description

TAK has been operating with full operational autonomy, and conducts administration/applicability of any type of tax applicable with the tax legislation in the Republic of Kosovo.

Within TAK, there is Functional Pillar for Operations, Functional Pillar for Programmes and Procedures, and Pillar for Supporting Programmes and Procedures.

For the implementation of the objectives defined by law, TAK covers ten (10) regional directorates (Prishtina 1, Prishtina 2, Prishtina 3, Prizren 1, Prizren 2, Mitrovica, Peja, Gjakova, Gjilan and Ferizaj).

IT plays a very important role in the main areas of TAK, such as: taxpayer services, registrations, processing, calculations, business automation, tax management and treatment. IT systems and assets are managed by the Information Technology Department. To provide support for the registration and handling of taxpayer requests is the Processing Division, which operates within the Department of Registration and Taxpayer Service.

The systems used for tax management are given in Figure 3.

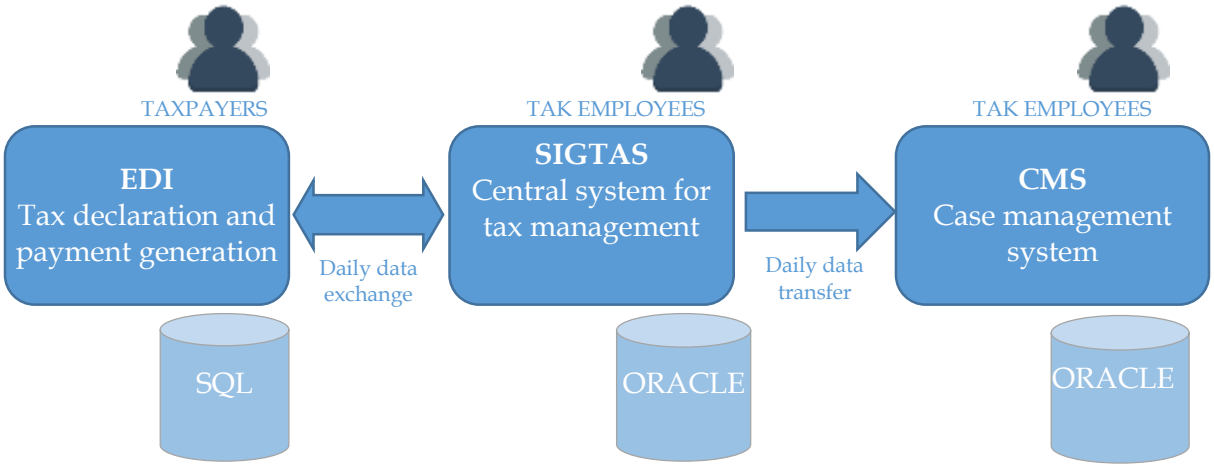

Figure 3: Data flow in information systems

Every person who carries out an economic activity based on tax legislation is obliged to perform the following processes, as in figure 4:

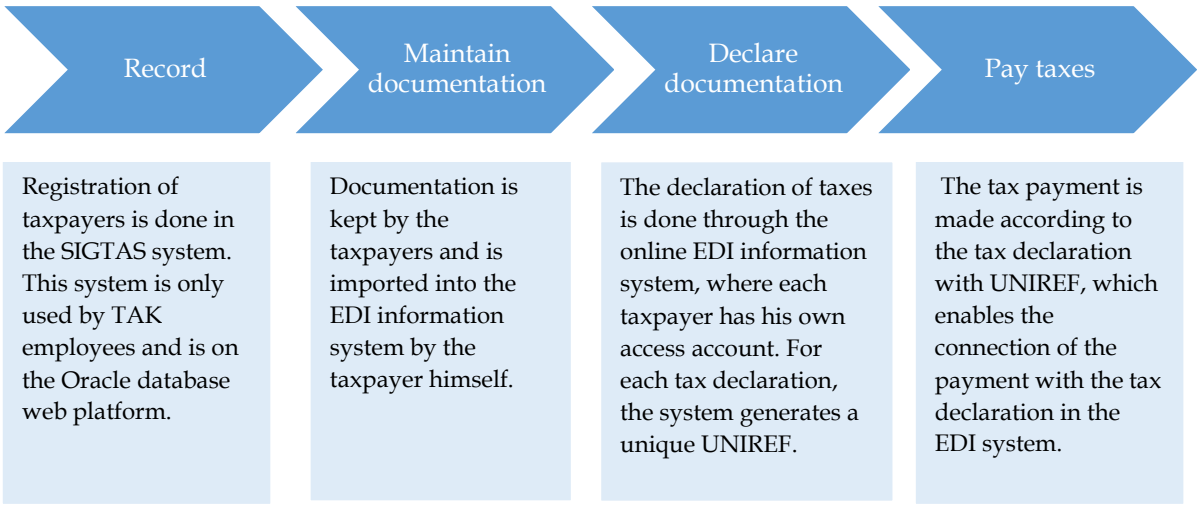

Figure 4. Requirements for meeting tax liabilities

Registration is a process where the Tax Administration collects basic taxpayers' identification information, such as: name, address and type of legal person. This information enables TAK to know who its taxpayers are, where they are located and whether they are active or passive. These activities are recorded in the SIGTAS central information system.
Maintaining documentation is a process that obliges taxpayers to keep documentation, such as books and records in accordance with tax legislation.

Tax declaration is the process where every person who is subject to any type of tax according to the applicable legislation in Kosovo will submit a tax declaration to the TAK within the specified legal deadline. Persons who fail to submit the tax declaration within the deadline set by the applicable legislation in the Republic of Kosovo are subject to administrative penalty.

Tax payment is the process where every person whose obligation is to pay taxes to TAK according to the applicable legislation in Kosovo will pay such tax at the specified time and place, without notice or request from TAK. All taxes that are obligatory and should be paid to TAK are therefore a debt to TAK. If any amount of any tax administered by TAK, according to the applicable legislation in Kosovo has not been paid by the deadline set for payment, the taxpayer will be required to pay the administrative penalty and interest on overdue payments to TAK.

3. Audit Findings

This chapter presents the audit findings related to the activities of the responsible parties in the management and control of the SIGTAS information system as well as the findings for the CMS and EDI information system, which are related to the SIGTAS information system. The findings are structured in three parts, and are interrelated according to audit questions.

- The findings related to application controls, namely related to the validity of the data, the treatment of errors in the system and to the accuracy and completeness of the data are presented in the first part.

- The findings related to logical access controls to ensure the integrity, confidentiality and availability of information systems, including the segregation of roles and responsibilities of users in systems, traceability and monitoring of activities, and role review and user responsibilities in systems are presented in the second part.

- The findings related to information security management and processes for continuity of information systems are presented in the third part.

Key issues and their addressing – *Given the findings presented through this audit for TAK information systems related to the security and continuity of systems and the importance of tax liabilities at the national level, we consider the involvement and support of the Ministry of Finance in addressing these issues to be necessary. The recommendation is made in Chapter 5.*

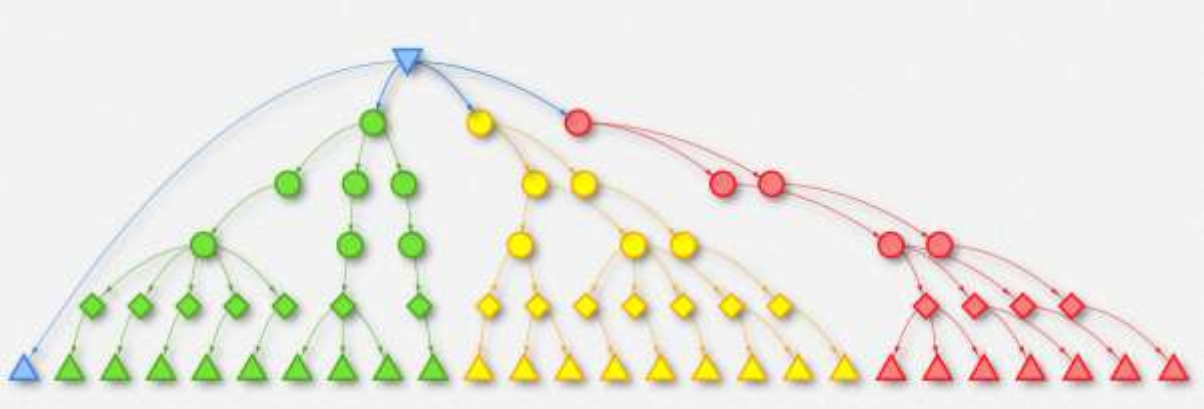

Figure 5. Structure of audit findings by audit questions, and audit objective

3.1 Application control

Application controls are control over the function of input, processing and output. They include methods to ensure that: only complete, accurate and valid data is entered and updated into the information system; processing performs the exact task; the processing result meets expectations and data is stored.

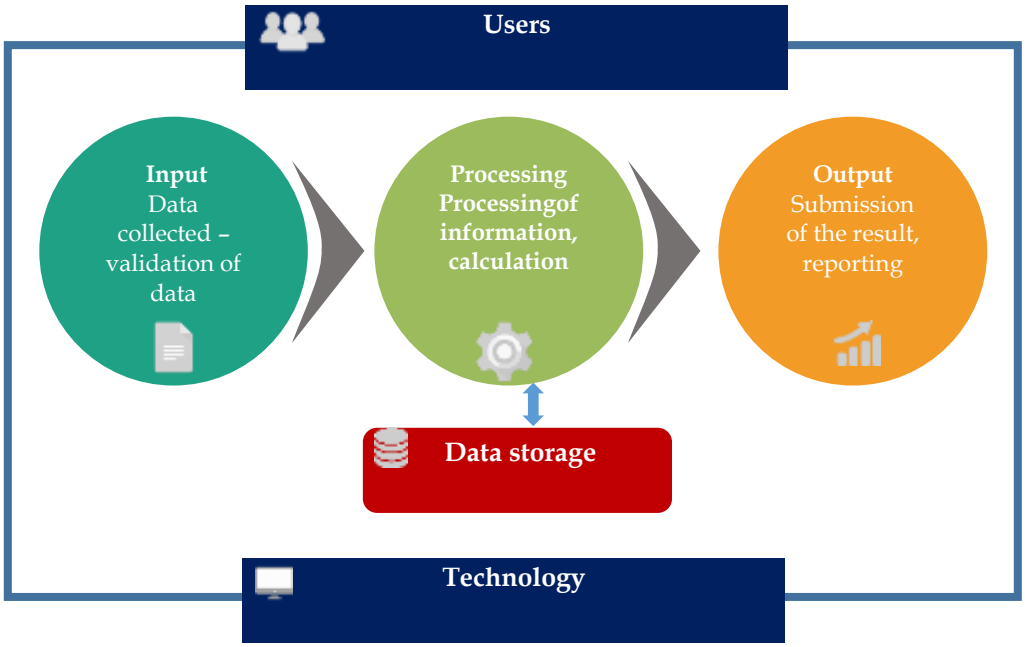

Figure 6. Input – processing – output model of data in information systems

These controls help ensure data accuracy, completeness, validity, verifiability and sustainability, by achieving data integrity and their reliability.

Application controls in the Tax Administration of Kosovo are deficient. Shortcomings in the configuration of the SIGTAS system have been identified by presenting inaccurate and incomplete overview of the accounts of tax declarations and shortcomings of procedures and processes in handling unprocessed data errors.

1. *Handling of errors in TAK information system*

Entry control procedures[14] *should ensure that every transaction to be processed has been entered, processed and fully and accurately recorded. The information system should have clear validity controls for error handling, by communicating problems. Errors that occur when placing data in the relevant fields can be traced and corrected before processing transactions. Error recordings should be reviewed periodically and the necessary corrective action should be taken.*[15]

[14] Audit criteria are presented as a paragraph in italics.

[15] The Information Technology Audit Manual is a product of the EUROSAI Information Technology Working Group (WGITA) as well as the INTOSAI Development Initiative (IDI) for determining the rules and standards of Information Technology Audit standards - hereinafter Information Technology Audit Manual

The audit of the entry application controls has highlighted the following shortcomings:

- Taxpayers' tax declarations are made through the EDI online information system, which after 12 hours, are processed/transferred into the SIGTAS basic system. This is a dynamic process and we have noticed that since the beginning of 2019 there are about 10 thousand un-transferred declarations (of 2,675,900 transferred declarations) from EDI system to SIGTAS. These un-transferred declarations are treated manually from officers, and according to TAK around 5% of them should be processed/transferred to SIGTAS. Furthermore, the EDI information system is not fully linked to the SIGTAS information system for taxpayers' tax declaration accounts and does not return messages to the taxpayer's account, for the taxpayer to be notified of taxpayers' unprocessed declarations and the reason of failing to process in the SIGTAS system. These declaration remain in intermediate[16] database for manual processing. In the absence of automatic processing of tax declarations between systems, TAK has determined the officials to make the necessary improvements and transfer them to the SIGTAS system the following day.

- There are cases when the monthly calculation of interest and the penalty for tax debts of taxpayers is not done for assessments of tax declarations. In these cases of automatic non-calculation of penalty and interest, a script is manually executed in the database to obtain those assessments of tax declarations and make calculations, without identifying the cause of the error and without correcting the error.

- The SIGTAS system does not have error messages for all types of transactions. In the report of unprocessed payments, there were payments without error message, while, for those payments for which the error message was generated, there are messages that are unclear. Even for assessments of tax declarations whose interest and penalty have not been calculated, the error message is not clear. The reason for not addressing transaction errors in information systems is the lack of policies and procedures for rejected data and the procedure for reviewing the pending files. While the lack of a complete list of error messages has occurred due to lack of maintenance of the SIGTAS[17] system. Now, TAK is in the process of finalising the drafting of a detailed list of error messages.

These shortcomings affect the increase of unprocessed declarations and payments and risk that errors are not recorded and error rates can increase continuously. While, the lack of interconnection of tax declarations between systems and non-harmonisation of data across systems affects the presentation of incomplete taxpayer's declarations.

[16] Figure 3 presents the graphical representation of data flow architecture in information systems.

[17] The maintenance and support of the SIGTAS information system expired on 7 September 2016. In October 2018, the tender procedure for the maintenance and support of the SIGTAS system was initiated.

2. *Calculation at the interest level in advance instalments is incomplete and inaccurate*

The application should have procedures to ensure that the completeness and accuracy of the application results is assessed and can be further processed or proceeded with according to predefined criteria. [18]

In analysing samples of the Annual Tax Declaration generated by the SIGTAS system, in cases where taxpayers have not complied with the terms of payment of tax[19] instalments, we have noticed that the calculation of the penalty in instalments is not accurate.In 6 (six) samples, the calculation of the penalty in instalments was not accurate and for 5 (five) samples of tax declarations, the penalty in instalments was not calculated even though the taxpayer did not comply with the payment terms.

The legal requirement for calculating the penalty in instalments for the general outstanding tax liability for the tax period has not been applied in the SIGTAS system, which should include the generated payment of the withholding tax for that period. [20]

Incomplete and inaccurate calculation of the penalty in instalments occurred because the Department for Programs and Policies in TAK did not provide clear details on how to apply the calculation and did not modify the annual tax declaration for recognition of the withholding tax, to implement it in SIGTAS. Once the Tax Analysists identified the problems in the calculation of penalty in instalments, in September 2018, the Department for Programs and Policies drafted the document for the application of this penalty. Whilst, the request for correcting this error in the system was made in March 2019 because the system had not been maintained by that time[21]. In November 2019 it was closed as an issue, however it is still under correction process.

Incomplete and inaccurate calculation of the penalty in instalment will result in taxpayers paying more penalty in the instalment than required, and in the other case, it will affect TAK not to collect the revenues due to it.

3. *Data of tax declaration assessments of payment agreement*

The organization should have control procedures to ensure that transaction data in information systems are harmonised. Output reports should be complete and provide accurate representation of the data source. [22]

[18]Information Technology Audit Manual.

[19] Taxpayers with gross annual income from business activities exceeding fifty thousand euros (€50,000) and taxpayers who voluntarily choose to be taxed on the basis of real income are required to pay instalments in advance. If the advance payment has not been made on time or has been made in the amount less than the requested amount, TAK will apply a penalty in an amount equal to the interest rate in force at the time when the advance payment has been mandatory to be made.

[20] Law no. 05 /L-029 on Corporate Income Tax.

[21] In February 2019, TAK signed the contract for support and maintenance of the SIGTAS information system.

[22] ISACA (Information Systems Audit and Control Association) - CISA Review Manual 27th Edition, 2019.

When analysing five (5) samples of payment agreement [23] in three (3) samples, the accumulated[24] administrative penalty of one percent (1%) of the tax liability (accumulated during the payment agreement period) was not calculated correctly. In analysing samples, we noticed that the accumulated amount is higher than the required one. Tax liabilities (tax, penalty and interest) of assessments of tax declarations in the payment agreement are also not presented accurately, such as in the transactions of the tax declaration account.

The inaccuracy of the calculation of the accumulated administrative penalty is that the schedule of the payment agreement does not present the detailed accumulated administrative penalty during the agreement and the calculation error is not easily identified. In addition, the inaccurate reflection of the data of the tax declaration in the agreement is that in case the payments made for penalties and interest have been transferred to tax; the system does not change the name of the obligation in transactions. After identifying this error during the audit, TAK has taken action to correct it by making a request to the economic operator and it is still in the process of correcting it.

Incorrect calculation of the accumulated penalty during the agreement leads to incorrect presentation of the calculation of tax liabilities in the report on taxpayer payment agreement and to untrue presentation of tax statements.

4. Tax Payments Made through E-banking following the last session of bank reporting

The payment system should provide the necessary information in the sending/ receiving messages of financial payment transactions, including the date and time of the transaction.[25] Tax liabilities for payment should be made within the time limit set. If any amount of any tax administered by TAK according to the applicable legislation in Kosovo has not been paid by the last date set for payment, the taxpayer will be obliged to pay interest[26] and will be subject to an administrative penalty of one percent (1%) of the tax liability.[27]

The taxpayers' payment report is generated by the Central Bank of Kosovo in the Treasury Department of the Ministry of Finance. This report is then submitted to TAK via web services. Payment are processed in SIGTAS on a daily basis. When it comes to payments made by taxpayers for tax declarations through the e-banking service after the last session of daily reporting from commercial bank to the Central Bank, these payments are reported and recorded in TAK as payments made on the following day. Details of payment transaction in the bank payment report do not contain the date of payment order. As a result, although the taxpayer has paid the tax liability within the set deadline, the taxpayer has been charged with administrative penalty and interest.

[23] The payment agreement should include the debt of all tax liabilities according to past tax declarations. It should accurately display tax liability data such as payment tax, interest before payment agreement (PA), penalties before PA, total for payment and accumulated penalty arising after the agreement on tax declarations.

[24] Law no. 03/L222, Article 51.2 When a person required to pay tax under the applicable legislation in Republic of Kosovo fails to pay the full or part of such tax by the due date, such person is subject to an administrative penalty of one percent (1%) of tax due for each month or part of the month that payment is late, up to maximum twelve (12) months.

[25] ISO 20022 Standard for the exchange of electronic data between financial institutions.

[26] Law no. 03/L-222 On Tax Administration and Procedures, Article 28.1.

[27] Law no. 03/L-222 On Tax Administration and Procedures, Article 51.2.

TAK does not have the date of the payment order[28] in the bank payment reports, in the details of the payment transaction, but has the date of the transaction[29] and the date of the bank transaction.[30]

Due to failure to report the date of payment order in the Treasury reports, the date when the payment was executed, TAK registers the date of the banking transaction as the date of payment of the tax declaration, as a result, taxpayers are damaged.

5. Configuration of Tax Debt Remission Transactions in SIGTAS System,

The application should contain validity control procedures to protect it against transaction processing errors. They should be configured to ensure that application transactions are executed in accordance with the expected behaviour.[31]

In SIGTAS system, tax debt remission transactions are performed manually. System configuration for this type of transaction contains shortcomings. In cases where tax debt has been remittedfor a tax declaration and after a period for that tax declaration, there has been a revaluation/recalculation, the system recognises the difference between the remitted debt and the tax liability as an overpayment or credit.

This shortcoming occurs because the procedure has not yet been drafted on the part of the business party on how to handle debt remission cases in cases of change in tax value. Now, the request for correcting this issue has been made to the economic operator, but in the absence of the procedure on how to carry out this process, it is still not corrected.

Failure to design the automated procedure in the system for tax debt remission cases leads to inaccurate tax declaration. It also risks that taxpayers' request reimbursement for overpayments/credits that appear in the tax account declarations.

6. Handling of Tax Liability for Payment from Three (3) Euro or Less

The organization should ensure that all legal aspects are identified, addressed and configured in the information system.[32] *Each tax liability for payment according to a tax declaration is three (3) euros or less, or another such small amount determined by the General Director, TAK will treat the tax payable as zero value.*[33]

In order for TAK to achieve its objectives, the processes in the information system should be configured in accordance with the statutory requirements. In analysing the taxpayers' debts remission report, we found that there are taxpayers who did not fully pay the tax liability,

[28] Payment order means any instruction from the payer or the receiver, given to his or her payment institution where the execution of the payment transaction is required.
[29] Payment transaction means an action, initiated by the payer or the receiver, to place, transfer, or withdraw money, regardless of any relevant obligation between the payer and the receiver.
[30] The date of the banking transaction is the date of transfer of interbank transactions to the Commercial Bank-CBK.
[31] Information Technology Audit Manual
[32] ISACA- Information Technology Control Objectives 2019.
[33] Law No. 03/L-222 on Tax Administration and Procedures, Article 27.7.

thus leaving a liability of €3 or less unpaid.[34] Meanwhile, SIGTAS system does not recognise the remaining debt as a liability but rather as a remitted debt.

This occurs because the system is configured to forgive tax liabilities of €3 or less and does not identify the creation of a tax liability according to a tax declaration for payment of €3 or less, from the outstanding debt of the same value. As a result, TAK has not collected these tax liabilities.

On the other hand, TAK has not defined the procedure for handling the rounding up of the last three numbers after the decimal point to two numbers after the decimal point. There are cases where taxpayers who are subject to real income tax have been fined for not paying tax less than €0.01 tax. Although the taxpayer has made the payment in instalments and has complied with the amount and time limits for payment, the system has calculated them as penalty in the instalment for tax liability in its full amount. This penalty in instalments has come because of non-payment of less than €0.01 for each instalment of four (4) tax periods, where a total of €0.04 has been rounded up.

The system is configurable and the rounding criterion in the system can be set. It is also possible to separate and identify the created tax liability from the outstanding tax debt €3 or less. Yet, TAK does not have an action on how to handle the remaining debt issues for payments of up to three (3) euros.

7. Notification on Cases when the Payment Agreement Is Not Respected in CMS system

The organization needs to ensure that information systems support its goals and strategy. [35] *If the agreement is up to 12 months, the calculation of interest will be stopped from the month following the month in which the agreement was signed. If the taxpayer meets the full agreement, the taxpayer will be entitled to a reduction in sanctions.*[36]

To support the statutory requirements on management of tax debts cases, TAK has developed the CMS system. Cases of payment agreements (PA) of taxpayers' debts are made through this system. To enable easier monitoring of taxpayers who are in payment agreement, the information system should contain notifications/reports for non-compliance with the agreement.

Figure 7. Monitoring the payment agreement

In analysing CMS system and the reports provided by this system, we found that this system is lacking detailed reports for taxpayers who do not meet the terms of the agreement.

[34] There were cases when taxpayers paid €171 instead of €174 of the tax liability, and they were remitted the difference of €3 of unpaid tax liability.
[35] Information Technology Audit Manual.
[36] Law No. 03/L-222 on Tax Administration and Procedures.

Furthermore, in analysing payment agreement samples, we noticed that there are taxpayers who did not comply with the terms of the agreement, i.e., there were delays in payments and the payment agreement was not terminated to the taxpayer.

In the analysis of the document "Business processes and functional requirements of the CMS system" it was requested to alert the collection officer to cancel the payment agreement in case of non-compliance. However, this requirement has not been developed in the system.

The reason for not developing the report or notification in the CMS system, in cases when the taxpayer does not respect the payment agreement is the non-implementation of the policy and procedure for managing the changes in the information systems.

Lack of a detailed report in the system for taxpayers who have not complied with the time limit for payments, according to the payment schedule of the agreement and non-termination of the agreement leads to difficulties in monitoring the agreement and failure to terminate it in time.

3.2. Logical Access Management in Information Systems

Logical access is the ability to interact with computer resource data using identification, authentication, authorisation, and auditing. Access controls are policies, procedures, and techniques used to prevent or detect unauthorised logical access to sensitive resources and are the main tools used to manage and protect information assets.

Figure 8. Logical access processes included in auditing

To ensure the integrity of information stored in information systems, the confidentiality of sensitive data, and to ensure the continued availability of their information systems, the organization should therefore have control over logical access.

Tax Administration of Kosovo has shortcomings in managing controls overs users' logical access in information systems, by exposing systems to risks of loss of integrity and data confidentiality, thus not creating adequate control mechanisms to protect systems information from unauthorised access.

8. Segregation of levels in SIGTAS system for taxpayers' management by tax centres

Confidentiality and integrity of records in the IT system should be protected by controlled access, ensuring that only authorised employees have access to certain resources.[37]

During the physical observation of the authorisation levels for system users and during tests performed in the SIGTAS system, we have noticed that there are users who have access to taxpayer data management for all TAK regions. These are the officials of the Taxpayer Service Division, of the large tax centres, who manage more than one region within a city.

Giving access to all TAK regions is because the SIGTAS system is configured in such a manner that taxpayer management users are allowed to access only one designated TAK region or all TAK regions.

[37]TAK- General Security and Users' Policies of Information Technology System, v.3.2, 2016.

This system configuration shortage does not provide equal access to officers of all tax centres. Moreover, unrestricted access of officers in tax centres leads to the risk that taxpayers' data modified/deleted by officials who are not authorised to intervene.

9. Controls over logical access of users having full access to information systems of TAK

There should be a segregation of responsibilities and controls to prevent unauthorised changes in information systems and system configuration. When unable to segregate responsibilities, there are compensatory controls to reduce the possibility of unauthorised modification or misuse of information or services as well as controls during data processing to ensure that authorised data remains unchanged.[38]

In analysing users' lists with the roles and responsibilities they have in information systems, in the core system SIGTAS and in the CMS and EDI support systems, we have found users with full access both in the application and in the database. Database and application administrators also use general accounts to administer the SIGTAS system. Transaction changes in the database are not made with administrators' personalised accounts, but are made with administrators'' general accounts, which makes it difficult to identify activities done by users (administrators), as this account is used by more than one user.

One developer from CMS system and EDI system each and the Manager of Department administrating these systems have full access to the database of these systems. Users also have full access to the Data Warehouse (DWH), a database that is used by the CMS system and for SharePoint reports (a system for storing and managing documents as well as generating different reports). DWH is reconciled with SIGTAS database every 12 hours.

There are no compensatory controls for system change requirements to ensure that authorised data remains unchanged.

This happened because TAK management did not give relevance to the establishment of policies and procures for controls over users having full access to authorise and control activities in information systems. In April 2020, Management approved the procedure for IT control and access management. In the administration of the SIGTAS system, the application does not have complete independence from the database either. Employees are assigned with double tasks, for system administration, for system development and database administration, which according to good practices should be separate.

Lack of control over users with full access to the system, where data integrity should be carefully maintained risks:

- Carrying out/changing/deleting intentional and unauthorised transactions;
- Transactions may not be identified; and
- Make impossible to maintain the integrity of information and processing infrastructure.

The use of these accounts exposes the entire information system to intentional or accidental risks.

[38] ISACA-CISA Review Manual 27th Edition, 2019.

10. Procedures for allowing remote access through VPN

Remote access to intranet can be done through VPN upon detailed request made by the employee, approved by the relevant supervisor, following approval by the IT Director.[39]

In order to be efficient and flexible, the IT Department in specific cases enables certain officials to connect to the IT intranet even from a distance. However, TAK has not implemented the procedure set out in the "TAK Information Security Policy" for remote access via VPN. TAK officials make the request for access to VPN to the Systems Administration Division via e-mail, without notifying the IT Director. As a result, VPN access was allowed to these officials without formal approval.

Failure to comply with the "TAK Information Security Policy" procedure increases the risk for unauthorised access and intentional or unintentional misuse of remote access, putting the entire TAK internal information system at risk.

11. Users' access rights in cases when job position is changed and contract terminated

Access rights in the use of information systems for all employees, contractors or third parties should be ceased upon contract termination, or adjusted to changes in responsibilities. [40]

When analysing the list of employees who have changed their job position and the changed roles and responsibilities in the SIGTAS system, we have noticed that their roles and responsibilities have not changed immediately in the system, with the change of the position. The non-change of roles and responsibilities in the SIGTAS system is because the Human Resources Division has not immediately notified the IT Department, namely the Systems Management Division (SMD), of the change of employees' position, and the Administrative Instruction (MPA) no. 02/2015 on Official Electronic Accounts is not applied.

We have encountered cases where the IT official of that region has made the request for role changes in the SIGTAS system for the employee who has changed position after 15 days, while the notification from the HRD has been done after 54 days.

We have also noticed that there are employees whose positions have been changed in August 2019 and whose access to the SIGTAS system has not yet been changed, even though the SMD has been notified by the HRD. Furthermore, the TAK Information Security Policy has not been applied to employees whose employment contract has been terminated, which requires that all accounts in the information systems be terminated. In one case of employee's contract termination, the HRD notified the SMD after 5 days and the account at DWH[41] was closed after 15 days.

Failure to terminate the employee's account in the information systems shortly after termination of the employment contract, as well as failure to change roles in the system

[39] TAK, Information Technology Department - General Policies for Security and Use of the Information Technology System V.3.2.

[40] Administrative Instruction (MPA) No. 02/2015 on Official Electronic Accounts.

[41] DWH – data storage, in TAK case there is a set of database where data are consolidated from all used applications.

according to the employee's responsibilities leads to the risk of systems users performing intentional unauthorised activities that affect the functioning of the systems; disclosure of information; financial loss; and loss of institution's reputation.

12. Management of passwords

The password management defined criteria should be configured in the information system. The password should be changed at certain times. The administrator's account password should only be known to an individual, while the organization should be able to use the system when the administrator is not available. User account passwords should be encrypted with HASH algorithm. Password policy should be read and policy recognition should be mandatory for system users.[42]

In verifying and testing password management in systems, we have found that the password for user accounts with full access/administrator, in the SIGTAS system database and in DWH is not configured to be changed in certain periods. In analysing the list of users who have access to the SIGTAS application, we found that there are 85 users, who have not changed the password for more than 6 months, and from these open accounts, 13 are those who have not changed the password since 2013. Moreover, the SIGTAS application administrator account password has not been changed since 2013 as well as the SIGTAS system administrator password (application and database) and DWH is recognised by all employees who have the position of database administrator.

While in the EDI system, a system which is used by taxpayers to declare tax liabilities and generate payment slips, we have found that the passwords of these users/taxpayers are not encrypted, they are readable passwords "plain text". Having been raised as an audit issue, TAK has undertaken actions to encrypt the passwords of taxpayers' accounts.

The cause for the shortcomings of password management is that the management is that the management of TAK has not paid attention to password configuration in information systems by not complying with Administrative Instruction (MPA) no. 02/2015 on Official Electronic Accounts. It has neither approved the password management policy and procedure, which was developed at the end of 2018, and the criteria set in this document have not been fully implemented in the systems. The management of administrator's account password and password encryption has not been defined in IT security policy either. In April 2020, the issue of administrator's account password/ID of the administrator was corrected in the procedure for IT control and access management.

Failure to comply with the criteria set for managing system passwords risks that the account/ID password is detected by unauthorised persons and that these accounts are misused, and the accountability of user activities cannot be implemented.

13. TAK's audit trail mechanisms in system information

Information systems should be configured and should be functional to ensure that audit trails are generated for all transaction data. Event reports should be accurate for all activities performed by system

[42] ISACA – CISA Review Manual 27th Edition, 2019.

users. Access to audit trail registers should be limited and controlled, and the integrity of audit trail data against modification should be ensured.[43]

From our assessment and tests, we have noticed that the audit trails provided by TAK for user activities in the SIGTAS system, are not complete. In cases where a script for ("Stored Procedures") is executed in the database by database administrators, the tool used to monitor user activities is not fully functional and does not identify which user this activity is from. Whereas, in the database, the changes made in the taxpayers' registers by the database administrators who use the same general account, it is does identify the users who made the change.

In the list of assessments, there are ordinal numbers missing and are not even in the table of deleted assessments. There are cases where up to 27 numbers are missing in a series of ordinal numbers. According to the IT Department, this occurs when the sequence exceeds one or more ordinal numbers due to the termination of the session involuntarily, for which trails (logs) from the database server have been submitted/documented.

Even in the CMS system, no audit trails of user activities are provided for data, which is changed or deleted.

During the physical observation, we noticed that all employees who have the position of the database administrator have access to the records of audit trails in the database. The tool "Oracle Audit Vault" for user monitoring is also managed by the database administrator, who has full access to both the SIGTAS system application and the database.

The reason behind the management of Oracle Audit Vault tool by the Application Administration Division is that TAK does not have any security information officer, whilst the lack of completeness of audit trails in Oracle Audit Vault tool is that this tool is still in the process of configuration. When it comes to CMS system, TAK has placed history tables.

The lack of complete audit trails makes identification of unauthorised user activities impossible. Furthermore, the administration of the "Oracle Audit Vault" tool by the database and application administrator, as well as the full access of database administrators to the audit trail can affect changes/misuse of data in systems by not considering or deleting audit trails.

14. Constant control and monitoring of user access

The activities of the account administrator and operator of information technology systems is recorded and monitored on a regular basis. There are mechanisms for controlling the activities of users with full access to systems and users who access from the outside, which are constantly monitored. TAK should also conduct a periodic review of user accounts, including a review of user access rights to ensure that they remain relevant to their function.[44]

TAK did not have a policy and procedure designed and approved for monitoring the administrator accounts. As a tool for controlling user activities in systems, TAK has Oracle Audit Vault tool, which was being updated during our audit. However, activities of

[43] ISO 27001 Requirements for Logging and Monitoring
[44] ISACA, CISA Review 27th Edition, 2019

users/administrator accounts who have full access as well as user activities that access after working hours and users accessing from outside are not monitored.

Lack of continuous monitoring of user activities with administrator accounts (full access account) risks to develop any unauthorised activity, such as changing or deleting data in systems and are not identified.

TAK does not perform a periodic review of the accounts of each user of the privileges in the system to ensure that they are suitable for the job function. From the list of users who have access to the SIGTAS system, we have noticed that there are users whose job position has been changed and their access rights to the system have not, according to their position, but only an additional role has been added on the supervisor's request.

Even the lack of a periodic review of user access rights increases the risk that users will have inappropriate rights with their responsibilities and may use sensitive or unnecessary information.

In April 2020, the issue of monitoring the activities of users with full access to information systems and periodic review of user accounts was corrected in the procedure for IT control and access management.

3.3 Information Security Management and Information System Continuity Plan

Information security is one of the fundamental aspects of IT governance to ensure readiness, confidentiality and data integrity. For better information security management, the institution should establish mechanisms to enable the management of security-related risks, acting appropriately and ensuring that information is available, usable, and complete and is uncompromised.

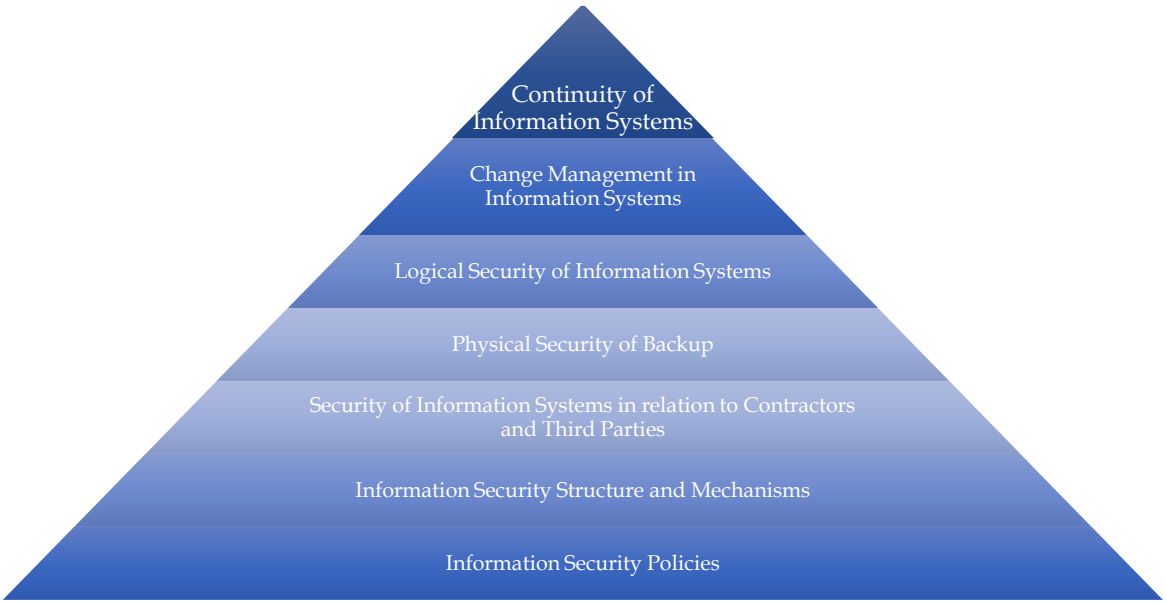

Figure 9. Information security management and information systems continuity plan

The Tax Administration of Kosovo has shortcomings in information security and in the continuity of information systems. There is no unit/official for information security, and there are shortcomings in the process of managing changes in information systems, risking that changes in systems are contrary to the objective of the Tax Administration of Kosovo.

15. Information security mechanisms

Information security policies should cover all operational risks and be able to reasonably protect all critical information assets against loss, damage and abuse, and be reviewed at planned intervals (at least each year).[45] *Staff should understand and maintain information security.*[46] *The organization should continuously monitor the infrastructure of information technology and users of information*

[45] Relevant control objectives for information technology (COBIT) issued by the IT Governance Institute & Information Technology Audit Manual & CISA review manual, 26th edition, 2016.

[46] International Standards of Supreme Audit Institutions issued by the International Organization of Supreme Audit Institutions (INTOSAI) & Standards and guidelines for auditing and providing information technology issued by the Information Systems Audit and Control Association (ISACA).

technology systems.[47] *Information systems should have a security protocol or security certificate installed to protect the identification of data against cyber-attacks.*[48]

- The document approved "TAK Information Security Policy", drafted in 2007 and revised in 2016 is deficient and the contents of this document does not contain all the elements of an Information Security Policy, according to ISO/IEC 27001/27002 information security standards. TAK has also revised this document in early 2020, but which has not yet reached the required level according to standards.

- TAK did not organise training and campaigns for its employees on the importance and awareness raising of information security, and did not plan to hold trainings, hence not prioritising information security for TAK.

- TAK has not established a clear tasks segregation structure for information security; the unit/officer for information security has not been established/appointed. Monitoring of user activities in systems is done by the database and application administrator. The roles of information security administrator and database administrator (DBA) should be separate, while monitoring of user accounts by DBA does not provide adequate controls. In April 2020, TAK approved the new organisational structure, including the information security officer.

- The "SIGTAS" application, which is on the web platform in the internal network does not have a security protocol installed, so it has access via http (open/unencrypted access) and not https (coded/encrypted access). In this system, most TAK users have limited or no access at all, therefore, based on information security standards, such a web application should have a security protocol.

  According to TAK officials, they tried to install the security protocol, but the economic operator does not provide support in the architecture of the old system currently used by TAK.

The lack of these information security mechanisms may increase the vulnerability of TAK systems against risk, reducing its ability to protect IT assets/resources and the information contained in IT systems. It also makes information systems vulnerable to cyber-attacks and leads to the possibility that these attacks are not identified on a timely[49] manner, and may result in an interruption to TAK operations.

16. Change management procedures for SIGTAS system

The organization should have policies and procedures for managing changes in information systems. Requirements for changes should be approved and documented, and the code (in the production environment) should enable the tracking of records for each change. The potential impacts of changes should be assessed and then reviewed and approved by management.[50] *In the procedure for change*

[47] International Standards of Supreme Audit Institutions issued by the International Organization of Supreme Audit Institutions (INTOSAI) & Standards and guidelines for auditing and providing information technology issued by the Information Systems Audit and Control Association (ISACA).
[48] ISO/IEC 27033- Information security management systems.
[49] International Standards of Supreme Audit Institutions issued by the International Organization of Supreme Audit Institutions (INTOSAI) & Standards and guidelines for auditing and providing information technology issued by the Information Systems Audit and Control Association (ISACA).
[50] ISACA – CISA Review Manual 27th Edition, 4. Business Continuity Plan (BCP); 5. Disaster Recovery Plans (DRP).

management, changes based on system sensitivity should be prioritised and considered for compatibility.[51]

For the management of system changes in 2015, TAK has approved "Standard Procedures for Operations for Change Management in the Information Technology System". However, during the change analysis in the SIGTAS system, we noticed that TAK has not implemented the process of requests for changes in the systems.

During 2019 and until February 2020, when the audit was carried out, TAK has initiated 23 requests to the economic operator for changes in the system to improve the system. 12 of these requests were made by the economic operator and the testing of these changes was done in the test environment by the Basic Application Support and Maintenance Division, but the testing and its approval was not done by the Change Management Board.[52]

The execution of changes in the production system is therefore done without obtaining approval for changes and without making documentation for approving the testing of changes in the core system SIGTAS.

In the absence of the implementation of these procedures, as a result of the lack of acceptance tests (by businesses and end users), the change in error correction has also had unintentional effects on taxpayers' data. The identified case is the penalty in instalments that has been calculated late, so the obligation for the taxpayer arises late (after several years). It is about taxpayers to whom the debt was remitted years ago according to the law on debt remission. While years later, in 2019 (after changes in the system with the contract for maintenance and advancement), the penalty appeared to the taxpayer which was remitted years ago and as a result many taxpayers' accounts have suffered changes in their financial situation in the tax declaration. Execution of changes in the production system, without documentation from initiation to testing and approval is because TAK management has not paid attention to the implementation of the procedure for managing changes in information systems.

For the changes made in the code by IT officials, there is no description/explanation in the production environment of what that code does. The scripts developed for the application in the basic system are sent via e-mail to be executed in the real production environment without any documentation with explanations of what that code does and without obtaining approval from the management.

Lack of assessment and testing of all phases including business testing as well as documentation for approving testing of changes in the system risks for uncontrolled and unsupervised changes, damage to the information system and its continuity.

[51] TAK, Information Technology Department - Standard Operating Procedures (SOP) V1.0.

[52] In the SOP for change management in TAK information systems it has been determined that there is also a member from the business for approval of the change in the Board for Change Management.

17. Backup physical security of TAK information system

To ensure that the critical activities of an organization (and support systems) are not interrupted in the event of an accident, secondary media are used to maintain software application files and associated data for backup purposes. To ensure that these data are not lost, it is very important to apply strict physical and logical data controls.[53]

During the physical observation of the backup storage of the information systems, we noticed that TAK has stored the backup copy of the information systems in locations that are not suitable for their storage, as they do not have controls and restriction of access only to responsible persons and have no camera surveillance, an application or a list for physical security monitoring.

TAK has not yet managed to approve a recent drawn up draft for the backup procedure. Resolving the backup maintenance process in tapes is the least costly solution and does not require maintenance of the environment like the data centre. This solution has facilitated it to decide to place it in rooms such as a meeting room, IT inventory storage or IT office.

The current form of storing a backup creates easier possibilities for loss and damage, as it does not provide possibility to identify responsible persons in the event of a potential intrusion.[54]

18. TAK information systems business continuity mechanisms

The organization should have a plan on the business continuity of the information system, which enables the continuation of activities. In order to implement this plan, the main processes of the organization's business should be identified, the time of response, recovery and period of losses should be determined. In order to have an effective plan for the recovery of information systems, the organization should determine an organizational structure in case of need to activate this plan and should test in certain periods to verify whether it can recover work processes in case of any natural disaster or system failure.[55]

TAK systems store and process sensitive and confidential taxpayer's data. Information security and the continuity of business system should therefore have a priority and policies should be put in place to reduce the risk of losing this data and interruption of systems.

However, TAK does not have a business continuity plan of the system to manage the risks associated with unplanned system interruptions. Furthermore, it has not made a logical and physical infrastructural solution for restoring business continuity data, as required by IT[56] standards, respecting the defined geographical distance, physical security, logical security, preparation of organizational structure that will be ready for data recovery and system business continuity.[57] TAK has not established the most critical applications and functions for

[53] ISACA – CISA Review 27th Edition, 2019.
[54] ISO 27001: A.11: Physical & Environmental Security.
[55] ISACA – CISA Review Manual 27th Edition, 4. Business Continuity Plan (BCP); 5. Disaster Recovery Plans (DRP).
[56] ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity.
[57] ISO 27001 Controls and objectives: Security Policies.

assessing the impact on the information system to assess the response time, the time of system recovery and the period of data loss.

TAK has relied on the Ministry of Finance for the implementation of the data recovery centre by initiating the project for such a centre. Subsequently, the Agency of Information Society has initiated such a central project and as a result, TAK management stopped the initiative to draft a plan for the business continuity of information systems.

During the physical observation, we noticed that TAK uses tape to store the backup of information systems. During the testing of the selected copy for audit, we noticed that TAK has not determined the optimal time for data recovery. Subsequently, there was no documented supportive backup test report and successful data recovery. This can lead to complications, delays in data recovery in the event of unplanned interruptions.

The reason for not specifying how to store the backup, the optimal time for data recovery, response time and system recovery in case of system failure or any natural disaster, is that TAK management has not defined these processes in IT security policy.

Lack of a practical programme and continuity of business processes management increases the risk of failure of TAK processes, if a natural disaster or failure of primary systems occurs.

4. Conclusions

Application controls

There are shortcomings in application controls in Tax Administration of Kosovo. Despite efforts to improve processes in the systems, it has not yet managed to provide a fully functional environment. There is a lack of policies and standard operation procedures on IT. These shortcomings lead to the risk that system errors will not be avoided and TAK will not have a complete and accurate report on the tax situation.

There are shortcomings in the system configuration, thus resulting in failure to meet all TAK legal requirements and incorrect and incomplete calculation and presentation of estimates on tax liabilities declarations.

Management of logical access to information system

TAK has not established adequate mechanisms of logical access to ensure integrity, confidentiality and availability of data. There were shortcomings in the division of user levels. Users with full access to information systems have dual responsibilities and use the general account/ID for system administration. The password for these accounts is not required to be changed at certain time periods and is recognized by all employees in charge of the administration of the database. These shortcomings may result in the risk of unauthorized interference and do not guarantee the availability and reliability of data in the information system.

TAK systems used to manage taxpayers do not have complete traceability and the tool used to monitor user activities is not fully operational. Consequently, unauthorized user activities may not be identified.

Users' access is not interrupted by the termination of the employment contract and the user's roles in the system do not change if the official position is changed, and there is no periodic review of user accounts to ensure that they remain suitable for their function. As a result, it cannot be ensured that they have maintained the integrity and confidentiality of the data in the information system.

Management of information security and continuity of information systems

TAK has not established sufficient mechanisms to reduce risks related to information security and guarantee continuity and availability of systems in order to enable safe and uncompromised data at any time.

There are shortcomings in security policy; there is lack of security officer, security-related awareness programs for employees, and of protection mechanisms of physical and logical access to information systems within TAK. Lack of proper information security mechanisms exposes TAK information systems to operational risks and makes them vulnerable to cyber-attacks.

Moreover, TAK has shortcomings in controlling changes to the information system, as documentation, testing and approval of changes in the system are lacking.

TAK has not provided sufficient and efficient mechanisms for the continuity of the information system operation. It has neither developed a plan on the continuity of information systems operation nor found a logical and physical infrastructural solution for the continuity of business and data recovery. Therefore, there is a risk that in the event of a natural disaster or system failure, TAK will not be able to restore the necessary critical data in time and increases the risk of data loss.

5. Recommendations

We recommend the Ministry of Finance to:

Ensure that TAK has information systems configured in line with tax legal requirements and that importance is paid to information security to guarantee continuity and availability of systems in order to enable safe and uncompromised data at any time.

We recommend Tax Administration of Kosovo:

1. **Standard IT Operating Policies and Procedures.** To design, approve and communicate policies/procedures, including the handling of system errors and rejected data, and to periodically review pending files and harmonise data across systems. To establish a control environment in order to ensure that these policies and procedures are understood and followed;

1.1. **Validation.** To validate fields and interconnect the data between the Electronic Tax Declaration System and the Government Integrated Tax Administration System as well as to inform the taxpayer on the declaration processing status. In regard to unprocessed transactions, to identify the transaction error, correct it, have the execution approval and re-process the transactions thereafter;

1.2. **Error messages.** Make a complete and clear list of error messages so that employees can easily identify the error and configure the information systems in order to provide error messages for each level of field or transaction. Those messages must match the data validity;

2. **Data validity procedures.** To design, in order to ensure that completeness and accuracy of applications outcomes has been assessed and can be further processed according to the defined legal criteria;

3. **Tax liabilities reports in tax declarations.** To ensure complete and accurate coverage of outgoing reports on tax declaration.

4. **Report on taxpayers' payments.** In cooperation with Ministry of Finance and Treasury to ensure that the report contains sufficient details on transaction so that the payment is recorded in the Government Integrated Tax Administration System on the tax declaration payment date;

5. **Business procedure for handling debt remission cases.** To draft the procedure and apply the Government Integrated Tax Administration System;

6. **Configuration of Government Integrated Tax Administration System.** To configure the system in accordance with the legal requirements on outstanding tax liability for the value of three (3) EUR or less by clearly defining the processes in the application and the transaction results output;

7. **Warning Report in the system for management of collection cases.** To generate the warning report for taxpayers having agreed to pay in instalments and do not meet the agreement's terms of payment, in order to enable enforced collection officer to cancel such agreement in time;

8. **Configuration in roles definition.** To regulate the configuration in the Integrated Government Tax Administration System, in order to enable the logical access control when defining the regional offices so that only those allowed transactions, which it is authorized for, are executed;

9. **Logical control policy and procedure.** To implement and communicate the policy and procedure for the management, authorization and logical control of users with full access. To have compensatory controls in order to reduce the chances of unauthorized modification or misuse of information or services;

9.1 **User authorization**. To manage user identity and authorization in a standardized manner. Allow access to critical and sensitive data only for authorized users. The user's access rights to the systems and data must be defined and documented in accordance with the needs of the Tax Administration of Kosovo, so that the user profiles are in accordance with the tasks and responsibilities they have;

10. **Allowing remote access.** To continuously implement the requirements for allowing remote access in accordance with the established procedures of the TAK information security policy. Access through VPN to be done with a detailed request by the employee, approved by the relevant supervisor and after approval by the IT director;

11. **Access rights.** In regard to use of information systems, terminate access to employees shortly after contract termination or adapt to changes in responsibilities;

12. **Passwords in information system.** To implement the TAK procedure for password management. Taxpayer's account passwords in the Electronic Tax Declaration System must be encrypted;

13. **Reports on events.** Reports should be complete to enable the identification of changes/deletions of transactions. To fully configure and functionalize the Oracle Audit Vault tool for monitoring user activities. Restrict users access to audit trail to ensure the integrity of audit trail data against modification;

14. **Monitoring and control.** To continuously monitor user activities with full access; to implement and communicate the procedure for information technology controls and access management. To continuously control and monitor the administrators' and operators' account activities in information systems and of users who access remotely via VPN;

14.1 **Periodic review on access rights**. To implement and communicate TAK policies and procedures. To periodically review the users roles and responsibilities to ensure that they are valid and appropriate for the user's operation function;

15. **Information security policy.** To supplement the policy according to standards in the planned intervals (at least every year). This document must meet the information security standards, to ensure its continued compatibility. There should be an effective information security training program for all staff and ensure that officers have the necessary knowledge on information security;

15.1. **Information Unit/officer**. To Activate the unit by clearly defining the tasks and responsibilities and to separate their tasks and responsibilities from the rest of the information technology staff;

15.2. **Security protocol or security certificate**. To install the protocol/certificate in the Integrated Government Tax Administration System, to protect the data from unauthorized access, even within the intranet;

16. **Policy and procedures for information system change management.** To implement the procedure in all steps of control over changes into the systems[58]. To carry out all necessary tests, including those of the business and end user, to ensure that the changes made do not have unintended impacts on the system;

16.1. **Documentation of changes to the code**. To document (in the real production environment) any change in the information system, to enable the tracking of records for each change, and to enable identification of cases of unauthorized changes, as well as to protect the system from being compromised;

17. **Information system backup.** Preserve copies in places with limited physical access only to authorized persons and, at the same time, conduct physical monitoring there on based on information security standards; and

18. **Continuity of operation of information systems.** Develop, approve and implement a continuity plan based on good information technology standards and practices for business continuity.

[58] Request for change – validation – acceptance – prioritisation – change of design – change testing – implementation – documentation.

Annex I. Audit design

Role and responsibilities of parties

IT Department

IT Department operates under the Pillar for Support to Programs and Procedures and aims to provide services and support to all users of IT systems and equipment.

Duties and responsibilities of IT Department are:

- Provides services and support to all users of IT systems and equipment;
- Maintains and supports all systems and subsystems of Information and Communication Technology (ICT) within TAK;
- Processes business requirements and designs information systems implementation processes;
- Designs and develops software systems and applies them in the ICT technical infrastructure;
- Assures process owners that information systems comply with requirements, procedures and applicable laws;
- Develops IT strategy and operation plans to meet Tax Administration objectives;
- Coordinates inter-institutional activities between TAK and Kosovo Customs, Pension Savings Trust, Central Bank of Kosovo in relation to information processing and related processes;
- Runs and supervises decision-making processes in the selection of products and technical solutions, based on TAK requirements;
- Advises senior management on proposed and new legislation, regulations or procedures that have an impact on information system; and
- Ensures that TAK Management, whilst making IT related decisions in line with developing trends, provides for continuity and sustainability in IT processes.

This Department includes:

- System Administration Division;
- Support and Operations Division;
- Basic Application Maintenance and Support Division; and
- Applications Development Division.

Data Processing Division

Data Processing Division operates under the Taxpayer Registration and Service Department established to provide registration support and other services to taxpayers in order to raise the level of taxpayers' awareness to meet tax obligations voluntary.

Regional Directorates

Regional directorates operate within the Functional Pillar for Operations, and their main purpose is to implement tax administration policies by adhering to tax laws and other applicable laws to achieve the annual objectives set by Senior Management for regional directorates and to provide equal treatment of taxpayers in accordance with legal requirements.

Duties and responsibilities of Regional Directorates are:

- To manage continuity of operation of Tax Administration Regional Directorate;
- To coordinate and monitor activities of enforced collection and undertake all actions on implementing the law on debt collection; and
- Supervise activities of IT officer and cooperate with HQ IT Unit on issues related to the respective region.

Regional Directorates consist of:

- Taxpayers service team;
- Inspection team;
- Enforced collection team; and
- Team ZGJONA

Audit question

In order to be responsive to the audit objective, we have prepared the following audit questions and sub-questions:

Does SIGTAS information system provide accurate, complete, reliable and timely data?

1. Are effective data validity [59] controls established in the information system, which is managing tax debts?
   1.1. Does the application contain suitable procedures for tackling errors?
   1.2. Does application control provide accuracy and completeness of its transactions?

2. Has TAK established effective control mechanisms that enable safe logical and reliable access to the information system?
   2.1. Have levels of authorisations for data entry in information system been established?
   2.2. Are there audit tracing mechanisms in information system in place?
   2.3. Are users' access to information system controlled and monitored?

3. Does TAK have efficient mechanisms for information security and continuity of the information system in place?
   3.1. Has TAK established a clear structure of information security?

[59] The validity of data tends to identify data errors, incomplete or missing data, completeness and accuracy, as well as discrepancies between data.

3.2. Does TAK has a standard procedure in place to control all changes to the information system?
3.3. Has TAK provided for mechanism on the continuity of information system, including data storage and recovery?

Audit criteria

Audit criteria applied in this audit originate from domestic laws, international standards on information technology/information systems [60], control objectives on information and technology, good practices on information technology [61], and standards on information security management[62].

To assess the validity of information system data and to ensure that the processing of stored information is complete and accurate, the following criteria are set:

- Validity rules should be designed, documented and implemented while entering data into the information system.
- Entry control procedures should ensure that every transaction to be processed has been entered, processed and fully and accurately recorded. These checks should ensure that only valid and authorised information is entered and that these transactions are processed only once.
- The information system has validity checks in place, that are clear for error handling by communicating problems in order to take corrective action for any type of error. Errors occurring while entering data in the relevant fields can be appropriately adjusted before transactions are processed thus enabling their tracking. Error records should be reviewed periodically and necessary corrective action should be taken.
- TAK should have procedures in place in order to ensure that completeness and accuracy of application output is assessed and can be further processed according to predetermined criteria.
- Taxpayers' data should be reconciled with all systems used for tax administration. Reports must be accurate and provide accurate representation of the data source.
- The payment system should provide the necessary information in the send/receive messages of financial payment transactions, including the date and time of the transaction. Tax liabilities to be paid should be executed within the set deadlines. If any tax amount administered by TAK according to the applicable legislation in Kosovo has not been paid by the deadline set for payment, the taxpayer will be obliged to pay interest and will be subject to an administrative penalty of one percent (1%) of the tax liability.

[60] International Standards of Supreme Audit Institutions issued by the International Organization of Supreme Audit Institutions (INTOSAI) & Standards and guidelines for information technology security and auditing issued by the Information Systems Audit and Control Association, (ISACA).
[61] ontrol Objectives for Information and Related Technology (COBIT) issued by IT governance institute & IT Audit Manual & CISA Review Manual –26th Edition, 2016.
[62] Family of standards ISO/IEC 27000 International Organization for Standardization (ISO) and International Electro-technical Commission (IEC).

- The organisation should clearly define application processes in the transactions output results and in the accurate documentation of the logic in the report extraction. If the advance payment has not been made correctly and on time, TAK applies a penalty in an amount equal to the interest rate applicable at the time when the advance payment had to be made.
- The organisation should ensure that all legal aspects are identified, addressed and configured in the information system. For each tax liability to be paid - according to a tax declaration is three (3) EUR or less - or any other small amount as determined by the Director General, TAK will treat its tax payable as zero value.
- The organisation should ensure that information systems support its goals and strategy. If the agreement is up to 12 months, the interest calculation from the month following the month when the agreement was signed will be stopped. If the taxpayer fully meets the agreement he will be entitled to a reduction in sanctions.

In order to assess whether TAK has put in place efficient control mechanisms that enable safe logical and reliable access to the information system, the following criteria have been set:

- Confidentiality and integrity of records in the IT system must be protected with controlled access ensuring that only authorized employees have access to certain resources.
- Remote access to intranet can be done through VPN upon detailed request from the employee, approved by the line supervisor, following approval by the IT director.
- There are divisions and levels of transactions authorisation and they are implemented through different checks. In cases of inability to segregate responsibilities, there are compensatory controls in place to reduce the possibility of unauthorised modification or misuse of information or services.
- There are checks during data processing to ensure that authorised data remains unchanged.
- The right of access to the use of information systems for all employees, contractors or third parties, terminated at the time of termination of the contract, or adjusted to changes in responsibilities.
- Access rights in the use of information systems for all employees, contractors or third parties should be ceased upon contract termination, or adjusted to changes in responsibilities.
- The information system should meet the criteria set for password management.
- The administrator's account password should be known only to one individual. TAK should be able to use the system in an emergency situation when the administrator is not available. To enable access to the system, administrator passwords are kept in a closed envelope, kept in a locked cabinet and available only for senior managers. Password policy should be read and policy knowledge should be made mandatory to system users.
- Ordinary systems accounts such as Administrator, Admin, and Guest should be renamed or deactivated when technically possible
- There are controls and they work to ensure that the audit trail is generated and maintained for all transaction data. Event reports should be accurate for all activities performed by system users.
- Access to audit trail registers should be limited and should be controlled, and the integrity of audit trail data against modification should be secured.

- The administrator's account activities and those of IT system operator are recorded and monitored on a regular basis. There are mechanisms for controlling user activities with full access to systems and users who access from outside, which are constantly monitored.
- The organisation performs a periodic review of user accounts, including a review of user access rights to ensure that they remain relevant to their function.

In order to assess that TAK has efficient mechanisms for information security and continuity of information system, the following criteria have been set:

- Information security policies should cover all operational risks and be able to reasonably protect all critical information assets against loss, damage and abuse, and be reviewed at planned intervals (at least each year) or when significant changes occur in the organisation, its business operations, or the inherent risk associated with security to ensure its continued compatibility.
- To ensure that the critical activities of an organization (and support systems) are not interrupted in the event of a disaster, secondary media are used to maintain software application files and associated data for backup purposes. To ensure that this data is not lost, it is very important to apply strict physical and logical data controls.
- Duties and responsibilities of IT staff, contractors and third party users are defined and documented in accordance with the Organisation policy on information security. Policies and procedures should form a sustainable managerial environment for internal and external communications. Staff should – from their recruitment day to the work termination - maintain information security. To maintain a secure environment, the organisation should continuously monitor the IT infrastructure and users of IT systems.
- Information systems should have a security protocol or security certificate installed to protect the identification of data against cyber-attacks.
- The organisation should have policies and procedures to manage change to information systems. Best practices on controlling change include: change request - validation - acceptance – prioritisation – design change – change testing – implementation – documentation. Change requests should be approved and documented. Potential impacts of changes need to be assessed. Change requests should be reviewed and approved by management. During the change management procedure, changes should be prioritised based on system sensitivity, and reviewed for compatibility.
- There are procedures for emergency changes to ensure that emergency improvements can be made without compromising system integrity.
- Changes to the code/production environment should be tested and traced in the registers produced by the system, indicating the date and time of the change, and in adequate authorised documentation.
- The organisation should have an information system continuity plan to ensure the continuation of critical services in the event of interruption of activities. This plan should include tasks and responsibilities, purpose, resource allocation criteria/principles, recovery procedure, training requirements, maintenance schedule, testing schedule, data storage plans, and approval levels.
- The organisation should determine the applications critical level according to the importance and functions to assess the impact on the Information System, the defined periodicity of data storage and recovery, as well as documented plans for data storage and recovery.

Audit Methodology

In order to answer the audit questions and support the audit conclusions we have applied the following methodology[63]:

- Analysis of legal and regulatory frameworks of TAK, which are determining criteria for tax administration in the information system;
- Analysis of policies and procedures designed for Information Technology systems;
- Analysis of Use Cases and Workflow documentation, which applies to the tax administration system, as well as the system use manual.
- Testing in the information system to evaluate the validity of the input data;
- Evaluate the application for accurate validation checks to ensure data processing integrity.
- Sampling to assess data completeness and accuracy.
- Analysis of reports obtained from SIGTAS, SMRM and EDI information systems, to assess the harmonisation of taxpayers' data in these systems.
- Assessment of information security and logical access to applications and databases;
- Analysis of system continuity, storage and retrieval of data in information systems;
- Assessment of documentation for information systems change management;
- Conducting interviews with officers in charge in the IT Department, Processing Division and in the Regional Directorate in Prizren.

Relevant documents

- List of laws and regulations relevant to this audit:
- Law No. 03/L-222 on Tax administration and procedures
- Law No. 05/L -037 on Value added tax
- Law No. 05/L -028 on Personal income tax
- Law No. 05/L -029 on Corporate income tax
- TAK draft Regulation No.13/2019 on internal organisation and systematisation of job positions in TAK
- TAK Strategic Plan 2015-2020
- General Policies on Information Security and Use of Information Technology System
- Standard Operation Procedures (SPO), Change Management in IT System
- MPA Administrative Instruction No. 02/2015 on Official electronic accounts

[63] Details on the methodology to be used is found under the audit matrix.

Annex II: Letter of Confirmation

Republika e Kosovës - Republika Kosova - Republic of Kosovo
Qeveria - Vlada - Government
Ministria e Financave - Ministarstvo za Finansije - Ministry of Finance
Administrata Tatimore e Kosovës - Poreska Administracija Kosova - Tax Administration of Kosovo

ARKIVA / ARHIVA / ARCHIVE
09-06-2020
30.06.20

LETËR E KONFIRMIMIT

Për pajtueshmërinë me të gjeturat e Auditorit të Përgjithshëm për raportin e auditimit të performancës **"Menaxhimi i Obligimeve Tatimore në Sistemet e Informacionit të Administratës Tatimore të Kosovës"** dhe për implementimin e rekomandimeve.

Për: Zyrën Kombëtare të Auditimit

Vendi dhe data: Prishtine, 30/06/2020

I nderuar,

Përmes kësaj shkrese, konfirmoj se:

- Kam pranuar draft raportin e Zyrës Kombëtare të Auditimit **"Menaxhimi i Obligimeve Tatimore në Sistemet e Informacionit të Administratës Tatimore të Kosovës"** (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.

Drejtori i Përgjithshëm

Ilir Muxhezaj

REPUBLIKA E KOSOVËS - REPUBLIKA KOSOVA - REPUBLIC OF KOSOVO
ZYRA KOMBËTARE E AUDITIMIT
NACIONALNA KANCELARIJA REVIZIJE / NATIONAL AUDIT OFFICE
1 07 2020

Njësia Org. Org. Jedin. Org. Unit	Shif.klasif. Klasif. Kod Class. Code	Nr. Prot. Br. Prot. Prot. No.	Nr. i faqeve Br. Strana/ca No. Pages
06	47	918	1