Report No: IS-2022-01(E)

22 December 2022

Information Systems Audit -

Use of IT in the Valuation of the Import Duties

Maldives Customs Service

އޮޑިޓަރ ޖެނެރަލްގެ އޮފީސް

AUDITOR GENERAL'S OFFICE

Table of contents

EXECUTIVE SUMMARY

Under the Audit Act (law no: 4/2007), Auditor General is mandated to carry out audits of all government institutions, accounts and government trading bodies in order to promote public accountability and good governance and sound financial management in the administration of government institutions. Carrying out audits of information systems assists the Auditor General to discharge the aforesaid mandate, as most of the financial and integral services in government institutions rely heavily on information systems.

Information Technology (IT) audit usually comprise of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organisational goals to be achieved effectively and uses resources efficiently. In other words, it is the process that helps to draw reasonable assurance that the system and the controls surrounding the use of the systems support a mechanism that ensure the safety of assets essentially related to integrity, confidentiality and availability of data. This is achieved through two distinct types of controls i.e. general controls and application controls. General controls refer to controls that focus on the management and monitoring of the IT environment which affect all IT-related activities.

Maldives Customs Service (MCS) was established as a separate legal entity independent of the Civil Service under the Maldives Customs Act (Law no:08/2011) which was ratified on 11 May 2011 with the main responsibilities to carry out all necessary activities pertaining to customs in relation to import and export of goods to and from the Maldives and to maintain all the concerned accounts and to operate and manage activities of collecting import duties and export duties. Currently, all these services are digitised and major digitisation has been carried out in-house by the IT department of MCS. An important part of this digitisation is the MCS' application of E-valuator, which is used to accumulate and assess historical prices of declarants to review their prices against system-held historical data. Therefore, audit of e-evaluator and surrounding IT environment contribute towards gaining assurance over integrity, confidentiality and availability of the revenue collection system.

In this engagement we mainly focused on reviewing general IT controls of MCS and application controls specific to e-valuator application. In our review, we have found that the main issues in the use of IT and -valuator were related to IT governance; namely lack of essential documentation and procedures that are required to ensure confidentiality, accuracy and integrity of data that is managed throughout the daily operations of MCS.

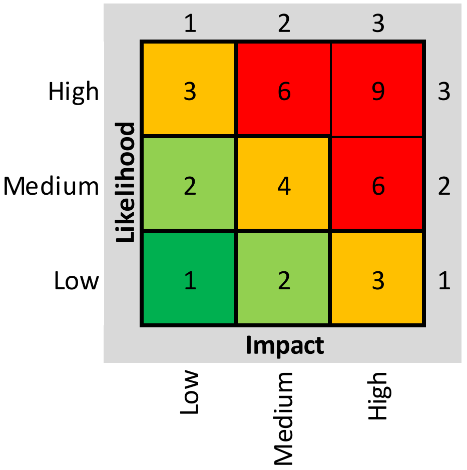
KEY AUDIT FINDINGS

FIND CATEGORY	FINDINGS	Page No.	Finding Ratings		
			H	M	L
GENERAL IT CONTROLS	Lack of a Disaster Recovery Plan (DRP) and a Business Continuity Plan (BCP)	6	X		
	Emergency procedures were not identified/documented	8			X
	Business Impact Analysis are not performed	9			X
	IT Department does not have detailed and measurable objectives	9		X	
	Lack of an incident response policy/plan	10			X
	MCS does not perform IT Risk Assessments	11		X	
	Cost and Benefits Analysis was not carried out	12			X
	Lack of information in the training materials regarding IS policy	12			X
	ICT division SOPs lacked penalties for non-compliance	13			X
	Password policy is not documented/communicated	13		X	
APPLICATION CONTROLS	System documentations related to E-Valuator were not properly maintained	14		X	
	User Management – access and privilege are not reviewed	15	X		
Number of Issues 12			2	4	6

Risk Matrix – Rating of Audit Findings

Findings made during the audit are categorised into high, medium, or low based on its likelihood and severity of impact.

High Risk (H): There is significant vulnerability in the system which needs immediate attention. Controls should be implemented to reduce risk.
Medium Risk (M): There is vulnerability although it is not significant, and it requires attention. Controls should be improved or developed to reduce risk.



Likelihood		1	2	3	
High		3	6	9	3
Medium		2	4	6	2
Low		1	2	3	1
Impact		Low	Medium	High	

Low Risk (L): A vulnerability has negligible chance to occur. And when it occurs, its impact is minimal. Thus, occasional monitoring is sufficient for low risks.

BACKGROUND INFORMATION

Maldives Customs Service (MCS) has a robust IT department that have over the years heavily contributed to the digitisation of several functions of MCS. Currently, all the services given by MCS is processed through IT systems. Therefore, it was necessary to conduct an IT audit of MCS. Thus, this audit was conducted to review the general IT controls and application controls (specific to e-Valuator) in Maldives Customs Service (MCS).

The general controls review helped to understand the mechanisms placed by management to ensure that there are appropriate measures implemented within the organisation to deter unauthorised parties from accessing and modifying critical information assets of the organisation, and whether these measures were strong enough to ensure protection of sensitive data against security vulnerabilities, detect and deter unauthorised changes to programs, and how the management ensures that operations can be restored in the wake of a disaster.

For the Application Controls, we examined a software called e-Valuator (previously called Price Analysis Tool (PAT)). This is an application designed and developed in-house for use in the valuation process of import duties. It has been a handy tool in viewing the historical prices of all the imports since 2004. Thus, the tool is regarded by the MCS as indispensably useful in accurately assessing the import duties due.

Audit Objectives

Information and Communication Technology (ICT) investments is a huge cost for any entity. This is especially true for an entity such as MCS which relies on information technology in their daily operations of the most critical business functions. ICT investments help the organisation to obtain business value through reduced costs, greater effectiveness, enhanced efficiency and/or increased service delivery. It is against these objectives that an IT auditor is required to provide assurance to the management.

This audit is aimed at determining how information technology is used in MCS's import valuation process, and whether related IT controls are adequate and in effect, to assist the organisation to achieve its business objectives (effectiveness) with appropriate use of resources (efficiency). In order to achieve this aim, following objectives are set for the audit.

Audit Objective 1: To assess the effective incorporation of policies and procedures governing MCS.

Audit Objective 2: To ascertain the adequacy and effectiveness of general computer controls across the organisation

Audit Objective 3: Review of the application controls of import duties valuation application (e-Valuator) to gain assurance about their adequacy and effectiveness.

Scope of the Audit

This audit focused on IT environment of MCS around the import valuation process through assessment of general IT controls and specific controls with respect to e-Valuator.

Testing Approach

The audit mainly focused on the adequacy of IT controls in the system to ensure effective use of IT in Import Duties. The following are the focus areas of the audit.

a) General Controls

IT general controls (ITGC) are controls that apply to all systems, components, processes, and data for a given organisation or information technology (IT) environment. The objectives of ITGCs are to ensure the proper development and implementation of applications, as well as the integrity of programs, data files, and computer operations. These, including policies and procedures, segregation of duties, business continuity and disaster recovery, change management and computer operations controls, Network, Internet & computer Controls.

b) Application Controls in e-valuator

The audit assessed application controls in e-Valuator to ensure the privacy and security of data used by and transmitted between applications.

Application control includes completeness and validity checks, identification, authentication, authorization input controls among others. The areas of focus in assessing application control were as follows:

- System Development Life Cycle Controls
- Logical access control;
- Input controls;
- Processing control;

- Master and standing data control;
- Output control; and
- Audit Trails".

The audit team used following methods to gather data and information; analyse data; and derive conclusions:

a) **Document Review**

The documentation related to policies and procedures were reviewed against commonly benchmarked IT Standards/frameworks such as Control Objectives for Information and Related Technology (COBIT) and National Institute of Standards and Technology (NIST), additionally rules, regulations, procedures, and guidelines set forth by MCS were also reviewed.

b) **Walk throughs**

The team carried out walk through tests of the system where necessary to observe and understand the procedures or activities performed in MCS.

c) **Interviews**

Relevant officials or project team involved in the IT development were interviewed to have better understanding of the system.

Statement of Auditing Standards

Currently, Maldives does not have a standard to govern the Information Technology industry. Therefore, during the course of this audit, as a guide, we relied upon international best practices such as COBIT (Information Technology Infrastructure Library ITIL and US government's NIST. Apart from the aforementioned standards/frameworks, as a general guide, Working Group on Information Technology Audit's (WGITA) handbook was extensively utilised in this audit engagement.

Although we performed our work with due care, in the performance of it should not be construed to imply that unreported irregularities do not exist. The prevention of fraud is the responsibility of MCS' management. Audit procedures alone, even when executed with due care, do not guarantee that fraud will be detected. Specific areas for improvement are addressed later in this report.

Audit Limitations

The audit was not able to carry out tests related to system documentation, system access controls and database as these were unavailable or not provided during the course of the audit. Additionally, we did not undertake penetration test and vulnerability assessments for the audited system.

Acknowledgements

We would like place on record our appreciation for the cooperation provided to us by the staff members of MCS during the audit.

FINDINGS, IMPLICATIONS AND RECOMMENDATIONS

Lack of a Disaster Recovery Plan (DRP) and a Business Continuity Plan (BCP)

HIGH RISK

Establishment of a structured process to create a disaster recovery plan that reflects the business needs, in order to resume and recover the required resources, is an essential activity for any organisation, especially for an organisation such as MCS, where the mission-critical operations rely heavily on the use of IT. This process must ensure the existence of a structured setup for management of business continuity that identifies the critical resources and the disaster recovery procedures in detail and appoint accountable parties who will oversee this function. Additionally, regular testing and updating the plan is an important aspect of risk minimisation and mitigation. The main benefit of adopting a Disaster Recovery Plan (DRP) is to ensure there is minimal impact on the business operations in a crisis.

During the audit, we found that MCS does not have a documented DRP or a separate team to plan and carry out the disaster recovery process, if such a need arises. Yet, there was a brief mention of a DRP in the overall IT policy which could further be developed to include the aforementioned point. In addition, there has been some efforts in establishing a disaster recovery site at MCS building. It currently remains abandoned due to the challenges faced (primarily in securing the required budget) in acquiring the required bandwidth and storage to be functional as a Disaster Recovery site.

Furthermore, we also observed that backups are currently being maintained in the same physical location/building of MCS. This is not the ideal practice in terms of minimisation of risks.

Additionally, as per Information Security best practices, an organisation must design and develop business continuity plans with a focus to reduce the impact of a major disruption on key business functions and processes. The plans should be based on understanding of risks, potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover information system and related peripherals usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach.

However, in our audit, we found that MCS does not have a documented Business Continuity Policy/Plan or procedures. In addition, the required IT-related risk assessment to develop the continuity plan is also lacking.

Implication

There are several drawbacks of not having proper procedures to manage business continuity in the face of a crisis, such as the inability to adapt rapidly and continue business operations, and maintain availability of resources and information at a level acceptable to the organisation. This may result in loss of availability of critical services, loss of revenue and organisational reputation.

In the absence of a DRP and procedures, the poor coordination or practices to recover from a disruption might lead to loss of business due to the lack of delays in proper responses, possible data security issues, such data unavailability, corruption or leakage or loss of data.

Recommendations

a) Establish and maintain a plan to enable the business and organisation of IT to respond to incidents and quickly adapt to disruptions. This will enable continued operations of critical business processes and required IT services and maintain availability of resources, assets and information at a level acceptable to MCS.

b) We recommend establishment of a business continuity management process that would designate a separate Disaster Recovery function and a separate team accountable for the disaster recovery process.

c) Prepare a detailed DRP that documents all procedures necessary for MCS to continue critical activities in the event of an incident that may damage, alter or even obliterate physical or digital assets of the organisation. This plan must include the data recovery process in detail, such as frequency of data backups, where and how the data will be maintained and who would be responsible for these procedures.

d) Explore the option of offsite/offshore back up to avoid loss of data in the event of any physical damages to existing setup.

e) We further recommend to periodically review and update the DRP in order to keep it aligned with the business requirements, and tested regularly to ensure its effectiveness.

f) We recommend to carry out the IT-related risk assessments and to formulate a comprehensive plan on how to respond to the potential risks before a major disruption occurs.

Emergency Procedures were not identified/documented

LOW RISK

IT department should develop an emergency plan for IT-related incidents such as cybersecurity incidents to ensure a prompt response to security breaches due to system bugs, computer viruses, network attacks and intrusions. An emergency plan may include a response team and their responsibilities, a data breach notification mechanism, strategies for response, details of internal decision makers etc. Network operators when encountered with such a risk must address it immediately and after resolving the issue as per the plan, must promptly report to higher authorities about the risk, its likely cause, impact/severity and the actions taken to mitigate the risk.

During the audit, we found that MCS does not have a plan to act on emergency instances. The strategy used is to find an alternative way to provide services in emergency instances and risk is managed in an ad-hoc manner.

Implication

Without a policy or defined procedures to tackle emergencies, there could be service disruptions that may not be resolved in a timely manner, thus leading to service unavailability for internal and external users and may even lead to loss/damage of data.

Recommendation

Develop a clear policy or a set of procedures to deal with emergencies.

Business Impact Analysis is not prepared

LOW RISK

A Business Impact Analysis (BIA) helps to identify important services to the organisation and helps to map these services and resources to business processes and identify business dependencies. Additionally, BIA ensures that the impact of unavailable resources is fully agreed upon and accepted. For vital business functions, it ensures that availability requirements can be satisfied by establishing capacity baselines and monitoring the effectiveness of the operations.

However, MCS has neither performed a BIA nor established capacity baselines to monitor the effectiveness of the operations.

Implication

Business Impact Analysis would help to clearly understand which assets would be impacted and the severity of emergencies, and what procedures to follow when an emergency is encountered. Hence, without a proper BIA and clear procedures in place to deal with emergencies, the organisation might adopt ad-hoc procedures~~,~~ which may result in lengthy recovery times, whilst leaving the organisation vulnerable longer and unable to resume services promptly. For an organisation such as MCS where data backup facility is in a critical state due to storage shortages, having a BIA is of greater importance. The main reason for this shortage as per MCS was unavailability of budget for the expansion.

Recommendation

Conduct a comprehensive Business Impact analysis to;

a) Identify scenarios that could potentially cause losses to the organisation; and

b) Identify and evaluate the potential risk scenarios and devise a plan of investment for recovery and mitigation strategies along with outright prevention.

IT Department does not have Detailed and Measurable Objectives

MEDIUM RISK

As per best practice, an enterprise's strategy should be translated into objectives related to IT-enabled initiatives (the organisational goals for IT). These objectives should lead to a clear definition of IT's own objectives (the IT goals), which in turn defines the IT resources and capabilities (the enterprise architecture for IT) required to successfully execute IT's part of the organisation's strategy. The way to ensure that the IT objectives effectively support the organisation's strategy is through systematic performance measures mapped to the IT goals. They often measure the availability of appropriate capabilities, practices and skills, and the outcome of underlying activities. Thus, by assessing and establishing capacity baselines for IT operations and monitoring them against actuals help the management identify clearly where the IT function requires more attention and where the function is effective in creating value for the organisation by aligning itself with the organisation's overall strategy.

However, we found that MCS does not have detailed and measurable IT-related objectives, and there are no pre-established baseline capacities for IT department to monitor their performance. Therefore, we are unable to conclude on the effectiveness of the current practices in IT operations.

Implication

Without proper detailed and measurable objectives, it will be difficult to assess whether the overall goals of IT are achieved.

Recommendation

Set detailed and measurable objectives for IT department with quantifiable Key Performance Indicators (Example of KPIs: Service duration, Number of tickets open, Total downtime per month, Total time to resolution and Number of tickets closed) and monitor the IT operations regularly to keep the IT operations' goals aligned with the overall organisational strategy.

Lack of an Incident Response Policy/Plan

LOW RISK

An incident response policy/plan sets out procedures to follow during the aftermath of an incident and helps to establish who, where and how to respond to an incident. This is an important document as without one, the organisation may not address the incident in a timely manner and in the process, lose critical information related to the incident such as the cause and severity of the incident. An incident response policy usually includes (i) documenting the procedures to be taken by the organisation in case of an incident; (ii) ensuring that the incident is systematically handled and communicated; (iii) allowing the quick recovery of the affected core systems; (iv) finding out the cause of the incident; and (v) adopting preventive measures aiming to address future incidents.

However, MCS does not have an incident response policy/plan despite the critical nature of the information managed by the MCS and the current challenges faced in securing adequate bandwidth and storage.

Implication

The absence of an incident response policy/plan could amplify the damage caused by an incident by increasing response time and system down time.

Recommendation

We recommend to prepare an incident response policy/plan, identifying the responsible persons and detailing their roles and responsibilities in case of an incident.

MCS does not perform IT Risk Assessments

MEDIUM RISK

IT security Risk Management is the process of identifying, understanding, assessing and mitigating risks related to information security. This process helps organisations to forecast and evaluate the potential risks they may face (identification), and from there, devise procedures through further understanding and assessing the said risks to avoid or mitigate them.

We note that MCS prepares incident reports related to incidents encountered whilst using ASYCUDA and has a separate risk management function tasked with the responsibility of managing risks associated with processing of Customs declarations. However, the overall IT operations do not have a risk assessment mechanism or a documented risk register related to IT. Therefore, there is no mechanism to assess the risks prior to implementing new information systems, rolling out new versions, or performing other IT-related operations.

Implication

Failure to adequately assess, foresee and device procedures to deal with business risks may result in the organisation having to face hefty losses. Apart from the financial losses, these may include operational or service disruptions and loss of sensitive data. Therefore, establishing a sound risk assessment mechanism that considers internal as well as external risks is an integral function.

Recommendation

a) Establish a system to identify the potential risks related to IT and assess and device procedures to mitigate these risks before a critical incident is encountered.

b) Maintain a risk register for IT and update it regularly.

Cost and Benefits Analysis was not carried out

LOW RISK

It is imperative for organisations to understand the costs and benefits of their decisions, including IT-related decisions that involve significant infrastructural and software development. Cost-benefit analysis helps to compare the total cost of a project/programmes and analyse the benefits derived out of it. Thus, it helps the organisation to choose the right approach and evaluate the quantitative and monetary impact of the decision. Additionally, by carrying out such an analysis, the number of projects that are abandoned could be reduced.

Despite the majority of applications utilised in MCS being developed in-house by the IT department, MCS has not carried out a proper cost-benefit analysis prior to development of these applications.

Implication

Without proper cost-benefit analysis, management will not be aware of the actual costs involved in going ahead with the project. Even though software is developed in-house, by documenting a cost-benefit analysis, MCS will be able to request for funds from the relevant authorities to acquire the required capacity (manpower, expertise and hardware). Additionally, ensure MCS does not decide to abandon projects halfway through development, after having invested valuable time of IT staff members.

Recommendation

We recommend carrying out proper need and cost-benefit analyses prior to commencement of IT-related projects.

Lack of Information in the Training Materials about IS Policy

LOW RISK

System security awareness and ethical conduct whilst using information systems is integral to maintain the confidentiality, integrity and availability of information utilised within the organisation. Thus, it is essential to regularly keep fresh and seasoned employees informed about the information security policies set by the organisation by incorporating the security policies into the training materials. Additionally, the employees must also be educated on consequences of non-compliance with security policies set by the organisation.

However, the training materials provided to us during the audit for verification did not contain information related to information security.

Implication

Without proper awareness about the IT-related policies, the organisation may be open to vulnerabilities and may face accidental or intentional data breaches by employees. In addition, without clearly set specific disciplinary measures for such negligence or intentional data breaches, the organisation will face difficulties in making employees accountable.

Recommendation

We recommend to design training materials covering the aspects of Information Security related policies, so that employees are aware of them from the commencement of their job. In addition, regularly provide refresher training to ensure the employees are up to date on the IT security related policies of the organisation.

ICT division SOPs lacked Penalties for Non-compliance

LOW RISK

Information Security policies are more effective if there is a way to ensure employees are aware of penalties/consequences they would face if they choose to disregard the policies. This is a critical element for an organisation such as MCS with a vast database of sensitive information that is accessed and utilised extensively by the employees on a daily basis.

During the audit, we found that even though MCS have a confidentiality clause in the Employees Regulation, the SOPs of the ICT division do not specify any penalties for misuse of systems or information.

Implication

Not having a clear consequence for non-compliance may result in diminished attention towards carrying out tasks as per the policies, rules and regulations set by the MCS, which in turn would put the organisation in a vulnerable state, should there be an attempt to misuse the given access.

Recommendation

Set out clear consequences of non-compliance with ICT policy.

Password Policy is not documented/communicated

MEDIUM RISK

A password is the first line of defence for an entity's information assets. Thus, it is imperative to focus on strengthening the process for generating, changing, storing and managing the passwords. Additionally, the passwords must adhere to a set of rules (documented policies), and these policies must be clearly communicated to the users. Setting password complexities, passwords durations, limiting use of old passwords are commonly used policies to strengthen passwords. Additionally, the employees must also be educated on safe use of passwords by making sure passwords are not being shared for convenience.

During the audit, we found that MCS does not have a documented password policy.

Implication

Without documented password policy, enforcing the baselines for security management related to users will be very difficult.

Recommendation

Establish and formalise a password policy with the approval of management and to inform and educate the users about its importance and the consequences for breaching the policy.

System documentation related to e-Valuator were not properly maintained

MEDIUM RISK

System related documentation such as Data Flow Diagrams (DFDs), data models or descriptions, system operating manuals and program change management are vital to understand the application schema required to map the data flows, and the connected interfaces and the procedures within the system. Therefore, not keeping proper documentation would result in a cumbersome task to understand the controls designed and embedded in the system. Furthermore, without proper documentation the data types, classes and the requirement for collection may not be established. Thus, as access is granted to users depending on the data classifications and sensitivity, without a detailed document outlining the information related to data may ultimately leave confidential data unprotected. Another significant problem may be documentation related to change management, without proper documentation unauthorised change may be deployed.

e-Valuator has been in use since 2004 (previously called PAT), but there was no documentation related to the software especially the data flow diagrams depicting the flow of data within the system and the related interfaces. Additionally, there has been several instances of changes brought to the system, but there is a lack of related documentation to follow and track these changes and the authorisations for these changes.

Implication

Without proper documentation the data may not be classified as per the requirements of the organisation. The users may be given access to data they do not require, as the classes of data are not identified prior to granting access. Furthermore, the organisation will face complications in bringing required changes to the system should the program developers were to leave the organisation.

Recommendation

practice maintaining proper and adequate documentation related to software developed in-house, namely; the Data Flow Diagrams (DFDs), system operating manuals and change management documentations.

User Management – access and privilege are not reviewed

HIGH RISK

User access management is a critical area for any entity as this process could make or break the other controls. Though user access management is usually regarded as creating users and managing the users accounts, this is not the beginning of the process. The initial phase of user access management is tying the user levels to the pre-defined business rules (or pre-established information classifications) that will help administrators to provide access to users based on who requires how much access to which networks and services.

Currently, access and privileges are provided by the IT Department based on a request from the respective section of the MCS. Similarly, an access right is changed as per request from a respective section. Access rights are managed by tying the access to required programs or functional areas using Active Directory Groups. However, there is no document to show the access categories; which class of users have what rights. Additionally, after granting access to users, it is not reviewed by the organisation to terminate the access when their role changes or they leave the organisation.

Implication

Without documented pre-established information classification there is a no way to map who should be provided with which information. Additionally, without regular reviews of access, unwanted/unauthorised parties may have access to sensitive information of MCS and this may lead to misuse, or data tampering or even data leaks in extreme cases.

Recommendation

Carry out the task of identification of the information classes aligned with business requirements, and then followed by setting proper levels of access to the classified information.

22nd December 2022

H. Niyazy

Auditor General
Hussain Niyazy

Ghaazee Building, Ameeru Ahmed Magu
Male', Republic of Maldives
Tel: +960 332 3939
Email: info@audit.gov.mv
www.audit.gov.mv