OFFICE OF
THE AUDITOR GENERAL
OF THE FEDERAL REPUBLIC OF SOMALIA

INDEPENDENT AUDIT REPORT ON THE SOMALI CUSTOMS AUTOMATED SYSTEM OF THE FEDERAL GOVERNMENT OF SOMALIA

For the Year Ended 31st December 2023

Table of Contents

Abbreviations

BCP	Business Continuity Plan
DRP	Disaster Recovery Plan
EDI	Electronic Data Interchange
FRS	Federal Republic of Somalia
GITC	General IT Controls
ICT	Information and Communication Technology
IRP	Incident Response Plan
IS	Information Systems
ISO	International Organization for Standardization
IT	Information Technology
MIS	Management Information System
OAG	Office of the Auditor General
SOMCAS	Somali Customs Automated System
WCO	World Customs Organization
XML	Extensible Markup Language

AUDITOR GENERAL'S OVERVIEW

I am pleased to share the summarised results of my detailed audit of the Somali Customs Automated System (SOMCAS). This summary report outlines the key areas examined during my audit to assess the security and effectiveness of the system.

The Ministry of Finance, particularly the Revenue Directorate relies heavily on a variety of ICT applications, these are hosted both on internal servers and in the cloud, and they play a crucial role in delivering essential services to the public. These applications are fundamental to supporting key decision-making and operational activities, making the security and integrity of the data they handle extremely important.

Our audit focused on evaluating the effectiveness of controls in place for SOMCAS, assessing how data is managed, stored, and protected, both on internal servers and in the cloud, and reviewing the governance structures and risk management practices to ensure they align with organizational processes and broader IT controls. We also analyzed the security measures implemented to protect the integrity and confidentiality of the data.
Effective controls need to be carefully aligned with the organization's existing processes and broader IT controls. A comprehensive approach that includes governance, risk management, and security is crucial to maintain operations that are both secure and efficient.

We are optimistic about the ongoing improvements in these areas and are dedicated to assisting the Ministry of Finance in strengthening the resilience of its financial management systems.

Yours sincerely

H.E. Avv. Ahmed Isse Gutale
Auditor General, Federal Republic of Somalia

Executive Summary

Introduction

Under the Law of the Office of the Auditor General of the Federal Republic of Somalia (Law No. 14 of 10th September 2023) OAGS is mandated to carry out audits of all government institutions, 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 (IS) assists the Auditor General of the FRS to discharge the aforesaid mandate, as most of integral services in government institutions rely heavily on Information System (IS).

Information Technology (IT) audit usually consists 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 ensures the safety of assets essentially related to integrity, confidentiality, and availability of data.

SOMCAS Background

The Somali Custom Automated System (SOMCAS) is an advanced system designed to manage and optimize foreign trade processes. Developed by the Revenue Directorate with donor support, SOMCAS integrates essential functions necessary for Customs declarations, duty and tax assessments, accounting, warehousing, and oversight of procedures like transit. This system enhances the integrity, confidentiality, and availability of the revenue collection process.

Key Features:

- **Customs Declaration and Processing -** Efficiently handles cargo and goods declarations, facilitating accurate duty and tax assessments.
- **National Characteristics Integration -** Adaptable to individual Customs regimes, national tariffs, and legislation, allowing for effective policy management related to importation and exportation.
- **Risk Management -** Includes tools for targeting non-compliant declarations, creating and maintaining risk profiles, and applying selectivity criteria.

- **Reporting and Analysis -** Generates detailed user-defined reports for financial and economic analysis, with a Management Information System (MIS) dashboard for monitoring Customs activities and key performance indicators (KPIs).
- **Compliance with International Standards -** Aligns with international codes and standards set by organizations such as ISO and the World Customs Organization (WCO).
- **Electronic Data Interchange (EDI) -** Facilitates EDI between traders and Customs using XML standards.
- **Web-Based Access -** Secure, web-based system accessible through a user-friendly portal.

SOMCAS aims to provide robust audit trails, enhancing administrative accountability and improving the accuracy and timeliness of trade facilitation processes.

AUDIT FOCUS AND SCOPE

The office of the Auditor General of the Federal Republic of Somalia's audit focused on the implementation of the SOMCAS by the Revenue Directorate. The audit assessed the effectiveness of controls related to the General IT environment, Application, and database. The audit period covered 2023, and an on-site visit to the Revenue Directorate was conducted to assess the level of system implementation and controls.

OBJECTIVE

The objective of the audit was to evaluate the effectiveness of the controls in place for the SOMCAS implemented by the Revenue Directorate of Somalia.

SPECIFIC OBJECTIVES OF THE AUDIT

- To ascertain that the development of the system followed and adhered to international system development standards.
- To establish that necessary application controls were implemented and applied during the period under review.
- To establish that the controls around the database of the system were implemented and applied during the period under review.
- To review the governance aspects of the system
- To ascertain the integrity of the data processed and output by the system.

AUDIT CRITERIA

Our audit was planned and performed in accordance with Law No. 14 and internationally recognized Information Technology/Information Systems Standards for audit, governance, and security. These standards include the Information Technology Audit and Assurance Standards and Guidelines issued by the Information Systems Audit and Control Association (ISACA) and the Control Objectives for Information and Related Technology (COBIT) issued by the IT Governance Institute. These standards and guidelines provide benchmarks and best practices within the Information and Communications Technology (ICT) sector, enabling us to compare and test the effectiveness of the Revenue Directorate's general computer controls.

METHODS OF DATA COLLECTION

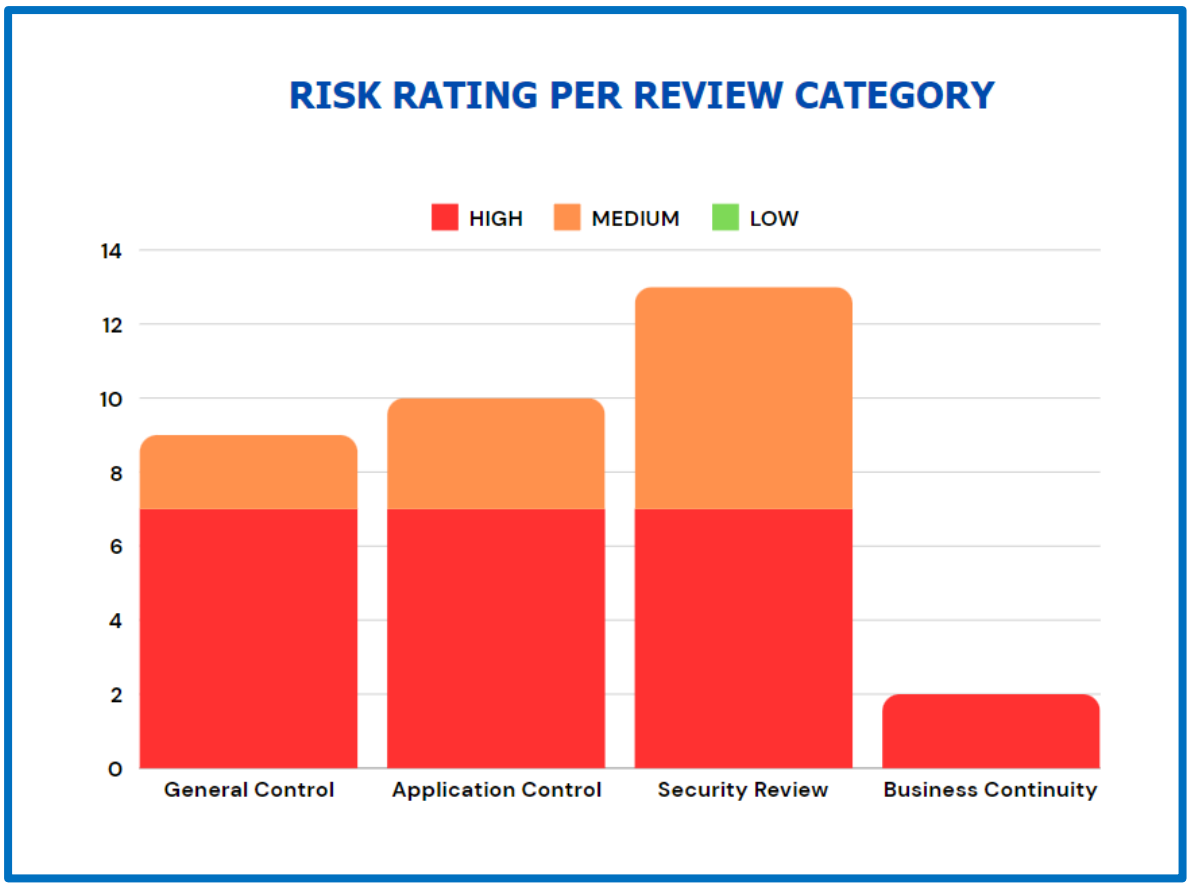
To ensure the accuracy and validity of our findings, the audit team used the following methods to gather data and information; analyze data; and derive conclusions:

- Interviewed staff members from the Revenue Directorate and reviewed documents concerning the SOMCAS.
- Assessed security controls for the application by validating user access appropriateness, evaluating password strength controls, and reviewing the process for periodic user access reviews.
- Conducted examinations on the security of the system's database and backups.
- Reviewed privileged user access to the system.
- Reviewed the existing change management processes.
- Assessed the effectiveness of the system's backup and recovery procedures.
- Performed tests on the system's data validation and integrity controls.
- Reviewed policies and procedures associated with system management.

By using these methods, we were able to thoroughly evaluate the controls in place for SOMCAS, ensuring they align with best practices and provide a robust framework for secure and efficient operations.

SUMMARY OF KEY FINDINGS AND OBSERVATIONS

The findings and observations have been categorized into four key areas: Application control Review, General IT Controls Review, Security Controls Review, and Business Continuity Review. A total of 34 findings have been identified and are detailed in the subsequent sections. The review highlighted 23 high-risk findings and 11 medium-risk findings. The stacked bar chart below displays the distribution of risk ratings (High, Medium, Low) across different review categories.



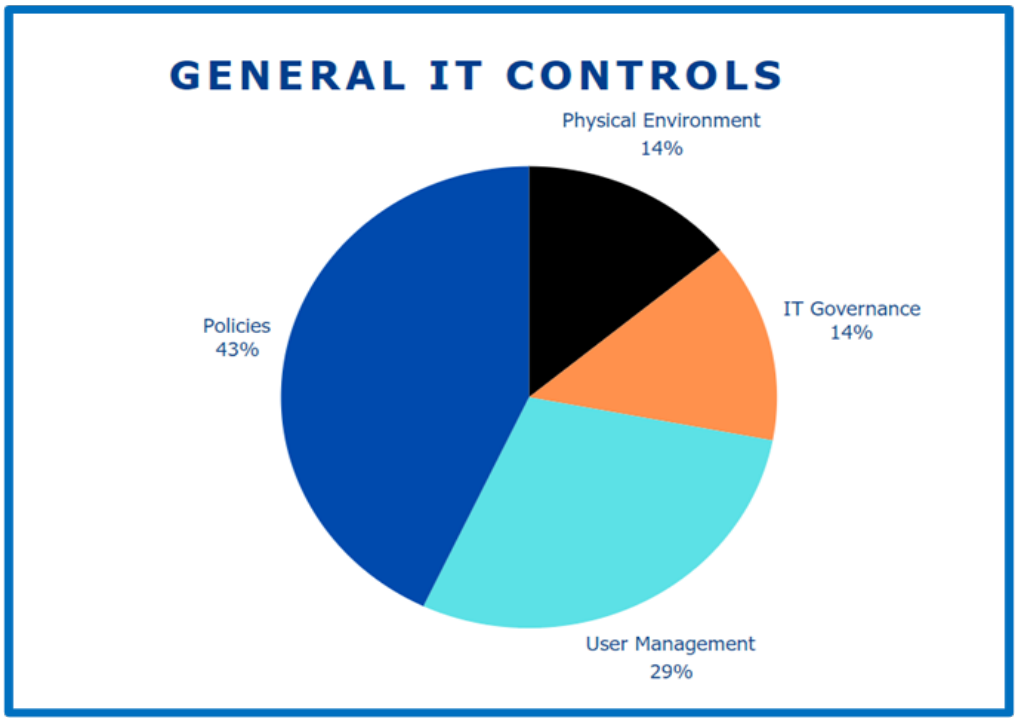
GENERAL IT CONTROLS REVIEW

IT General Controls (ITGCs) are essential safeguards that govern the design, implementation, and utilization of technology within an organization. These controls influence a wide range of activities, from configuration management and password policies to application development and user account creation. ITGCs also address critical issues such as the acquisition and development of technology and the deployment of security protocols across the enterprise.

Auditing IT General Controls focuses on key areas crucial for ensuring the security, efficiency, and reliability of the IT environment. These areas are vital for evaluating the overall health and risk posture of the IT infrastructure.

GENERAL IT CONTROLS (GITC) FINDGINS

The comprehensive review of the SOMCAS IT General control mechanisms has revealed several critical findings, the majority of which have been categorized as high risk. The identified risks encompass a range of issues that pose significant challenges to the system's operational controls. Common weaknesses we found included:



APPLICATION CONTROLS REVIEW

Applications are software programs that support an organization's essential business processes, such as, finance, human resources, case management, licensing and billing. They also enable specialized functions that are unique and essential to individual entities. Each year we review a selection of important applications that agencies rely on to deliver services. We focus on the key controls that ensure data is completely and accurately captured, processed and maintained. Failings or weaknesses in these controls have the potential to affect other organisations and the public. Impacts range from delays in service and loss of information, to possible fraudulent activity and financial loss.

The audit assessed application controls in SOMCAS to ensure the. 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:

- Logical access controls.
- Input controls.
- Processing controls.
- Master and standing data controls.
- Output control; and
- Audit Trails

The absence of IT governance and formal IT policies, along with a lack of formal controls in data centre operations, poses high risks, including potential misalignments with organizational strategies and inconsistent IT practices. Additionally, the lack of integration between SOMCAS and revenue collection systems leads to inefficiencies and data discrepancies. What Should be done?

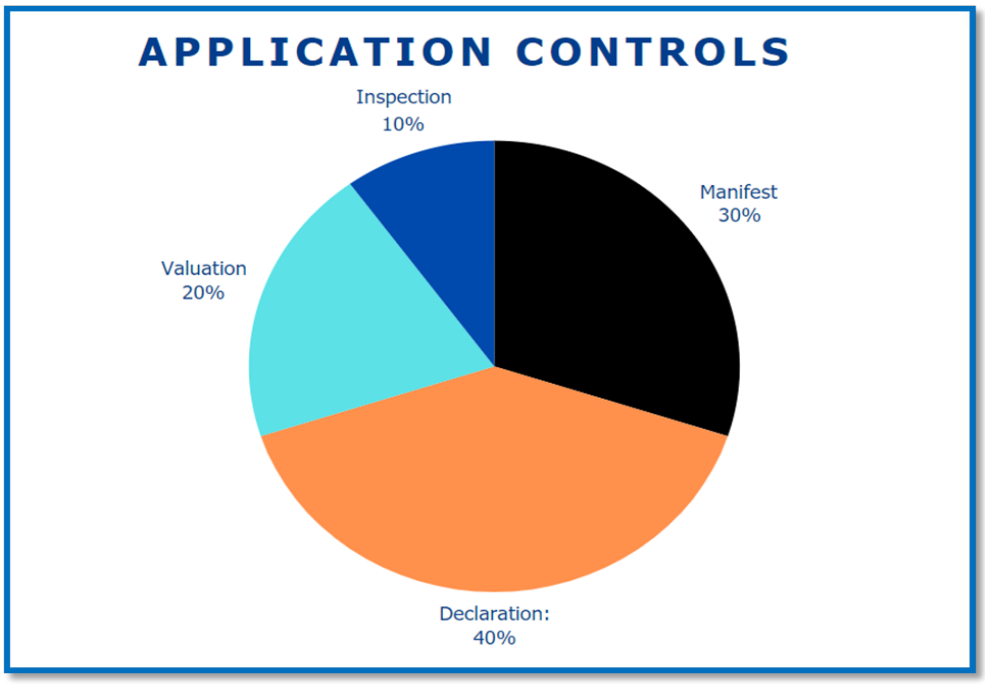
To address the high risks and enhance IT governance, we have shared with the responsible entity a comprehensive guideline of what needs to be done. This includes developing a comprehensive IT governance framework and formal IT policies to ensure alignment with organizational strategies and consistent IT practices. Implementing formal controls in data center operations will improve security, reliability, and efficiency. Integrating SOMCAS with revenue collection systems will eliminate inefficiencies and data discrepancies. We are now awaiting the implementation of these actions, which will be assessed in the next follow-up audit to determine whether the recommendations have been successfully implemented.

APPLICATION CONTROLS FINDINGS

The review of the SOMCAS application's control mechanisms has revealed 34 critical findings, the majority of which have been categorized as high risk. These identified risks encompass a range of issues that pose significant challenges to the system's integrity and efficiency, as illustrated in the pie chart below.

Common weaknesses identified include:

- Lack of reconciliation between manifests and cleared declarations, resulting in data discrepancies and undermining the accuracy of customs operations and financial reporting.
- Incomplete data in the duty exemption process and inadequate input validation, leading to incorrect duty calculations and the submission of incomplete declarations.
- Failure to detect duplicates, posing risks of data redundancy and inaccuracies.
- Discrepancies between package counts on manifests and declared gross weights, along with the absence of supporting documents, indicating procedural non-compliance and inconsistencies in cargo documentation.
- Inconsistencies in weight, description, and value in item declarations, coupled with variable inspection processes, presenting risks of errors and non-uniform customs enforcement.
- Utilization of an external system for customs valuation and non-compliance with regulatory requirements, posing significant legal and operational risks.

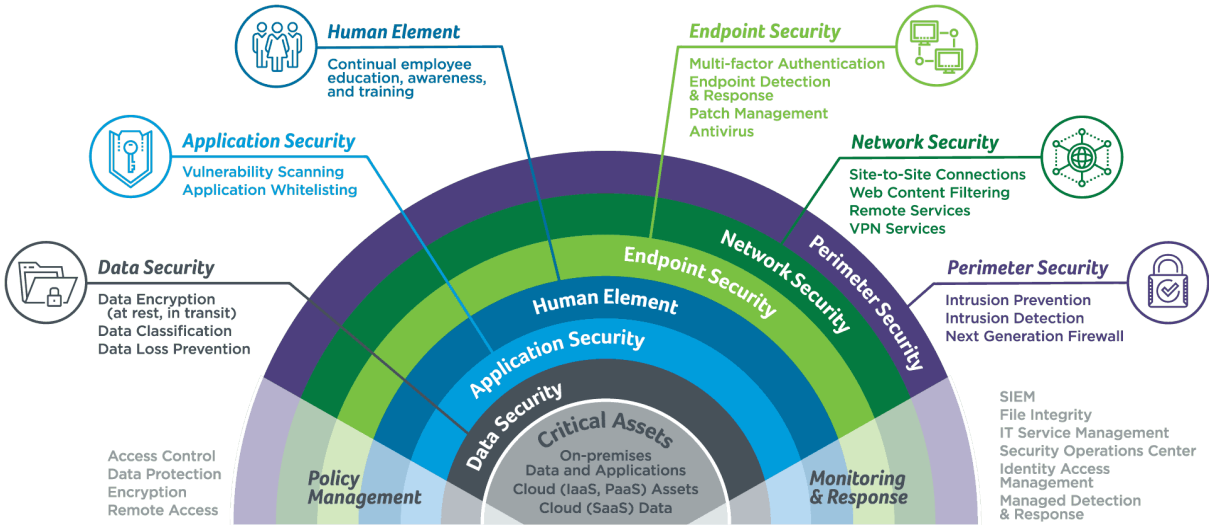


To address these findings, a complete guideline of what needs to be implemented has been shared with the responsible entity to ensure the Ministry of Finance continues to receive the information it relies on accurately and completely. The effectiveness of these measures will be assessed in the next follow-up audit to determine whether the recommendations have been successfully implemented.

SECURITY CONTROLS REVIEW

We evaluated whether SOMCAS controls were administered and configured to protect information systems and IT environments from internal and external threats. This assessment included an examination of operations, information systems, and security policies, along with an evaluation against best practice controls for information and cyber security. The key areas of control reviewed included:

- IT Security Policy: Assessing the existence of an overarching policy that guides and informs the management approach to IT security.
- Administrative Controls: Reviewing security checks, confidentiality, and acceptable use agreements.
- Network Security: Evaluating access controls, account management, and the logging and monitoring of users.
- Application and Database Security: Checking access controls, account management, and the logging and monitoring of users.
- Sensitive Information Handling: Ensuring the proper handling of sensitive information.



Examination Approach

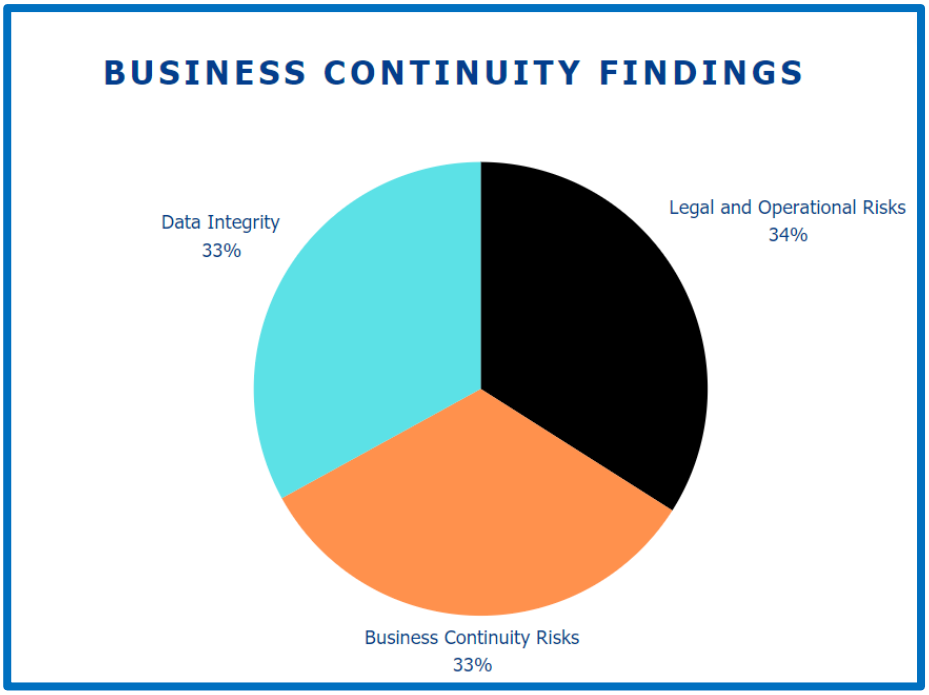
Our approach began with identifying the personal and sensitive information stored within the agency. Based on an assessment of the most significant risks and vulnerabilities, we tested the adequacy of the controls in the key areas.

Findings

The findings of the cybersecurity assessment conducted on SOMCAS have been confidentially documented and categorized. The recommendations to address these findings have been shared with the responsible entity for urgent action. The effectiveness of these measures will be assessed in the next follow-up audit to determine whether the recommendations have been successfully implemented.

BUSINESS CONTINUITY REVIEW

Interruptions to business can have serious impacts on the critical services entities deliver to the public. To ensure business continuity, we have tests to see if the revenue directorate have an up-to-date business continuity plan (BCP), disaster recovery plan (DRP) and incident response plan (IRP) Common weaknesses we found included.



The absence of an escrow agreement for source code ownership poses significant legal and operational challenges, potentially impacting software management and continuity. Furthermore, the lack of formalized backup and recovery processes introduces considerable risks to data integrity, as there are no established protocols to restore data in the event of system failures.

This deficiency is compounded by the Ministry of Finance's lack of a comprehensive disaster recovery and business continuity plan for critical business operations. Without such a plan, the Ministry of Finance is highly vulnerable to disruptions, as there are no measures in place to ensure the continued functioning of essential services during emergencies. These combined shortcomings create a precarious situation, threatening both the operational stability and legal compliance of the organization.

To address the significant legal and operational challenges posed by the absence of an escrow agreement for source code ownership, it is essential to implement such an agreement. This would ensure that the software management and continuity are safeguarded, reducing the risk of operational disruptions and legal complications. Additionally, the current lack of formalized backup and recovery processes introduces considerable risks to data integrity, as there are no established protocols for data restoration in the event of system failures. To mitigate these risks, it is crucial to develop and formalize comprehensive backup and recovery processes. These processes should be designed to ensure that data can be reliably restored, thus protecting the organization from potential data loss.

What Should Be Done

The Ministry of Finance should follow the guidelines and recommendations provided by the Office of the Auditor General of the Federal Republic of Somalia. These recommendations are designed to address identified risks and enhance the overall effectiveness, security, and resilience of the SOMCAS. By adhering to these guidelines, the Revenue Directorate can ensure that SOMCAS operates more efficiently, accurately, and securely, supporting the goals of effective customs management and robust revenue collection. It is crucial for the entity to implement these improvements promptly and thoroughly to align with national and international standards.

CONCLUSION

SOMCAS offers significant promise for improving customs operations in Somalia, realizing its full potential requires addressing its current operational and security deficiencies. By implementing the recommended improvements, the Revenue Directorate can ensure that SOMCAS operates more efficiently, accurately, and securely, thereby supporting the overall goals of effective customs management and robust revenue collection. These steps are essential for creating a reliable, transparent, and resilient customs system that aligns with both national and international standards.

OFFICE OF THE AUDITOR GENERAL

OF THE FEDERAL REPUBLIC OF SOMALIA

Mogadishu, Somalia

www.oag.gov.so | oag@oag.gov.so