THE UNITED REPUBLIC OF TANZANIA
NATIONAL AUDIT OFFICE

ISO 9001:2015 Certified

ANNUAL GENERAL REPORT ON INFORMATION SYSTEMS AUDIT FOR THE FINANCIAL YEAR 2022/23

CONTROLLER AND AUDITOR GENERAL
MARCH 2024

THE UNITED REPUBLIC OF TANZANIA

NATIONAL AUDIT OFFICE

ISO 9001:2015 Certified

Controller and Auditor General, National Audit Office, Audit House, 4 Ukaguzi Road,
P.O. Box 950, 41104 Tambukareli, Dodoma. Telephone: 255(026)2161200, E-mail:
ocag@nao.go.tz, Website: www.nao.go.tz

Ref.No.CGA.319/421/01B. **28 March 2024**

H.E. Dr. Samia Suluhu Hassan,
The President of the United Republic of Tanzania,
State House,
P.O.Box 1102,
1 Julius Nyerere Road,
11400 Chamwino,
40400 DODMA.

RE: ANNUAL GENERAL REPORT OF THE CONTROLLER AND AUDITOR GENERAL ON THE AUDIT OF INFORMATION SYSTEMS FOR THE FINANCIAL YEAR 2022/23

I am pleased to submit my Annual General Report on the audit of Information Systems for the Financial Year 2022/23 in accordance with Article 143(4) of the Constitution of the United Republic of Tanzania of 1977 and Sect. 34 of the Public Audit Act, Cap. 418.

This report presents audit findings and the recommended measures of redress which aims at fostering accountability in collection and use of the public resources.

I humbly submit,

Charles E. Kichere
Controller and Auditor General
United Republic of Tanzania

ABOUT THE NATIONAL AUDIT OFFICE

Mandate

The statutory mandate and responsibilities of the Controller and Auditor-General are provided for under Article 143 of the Constitution of the United Republic of Tanzania of 1977 and in Section 10 (1) of the Public Audit Act, Cap 418

NAOT Vision, Mission & Motto

01 **Vision**

To be a credible and modern Supreme Audit Institution with high-quality audit services for enhancing public confidence.

02 **Mission**

To provide high-quality audit services through the modernisation of functions that enhance accountability and transparency in the management of public resources.

03 **Motto**

Modernising External Audit for Stronger Public Confidence

Independence and objectivity

We are an impartial public institution, independently offering high-quality audit services to our clients in an unbiased manner.

Teamwork Spirit

We value and work together with internal and external stakeholders.

Results-Oriented

We focus on achievements of reliable, timely, accurate, useful, and clear performance targets.

CORE VALUES

Professional competence

We deliver high-quality audit services based on appropriate professional knowledge, skills, and best practices

Integrity

We observe and maintain high ethical standards and rules of law in the delivery of audit services.

Creativity and Innovation

We encourage, create, and innovate value-adding ideas for the improvement of audit services.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviation	Full Name
ATMIS	Agriculture Trade Management Information System
BCP	Business Continuity Planning
CBMS	Central Budget Management System
CCTV	Closed-circuit television
CFMS	Core Fund Management System
CIMIS	Computerized Integrated Management Information System
CMVRS	Central Motor Vehicle Registration System
CRB	Contractors Registration Board
DRP	Disaster Recovery Planning
ERMS	Enterprise Resource Management Suite
ERP	Enterprise Resource Planning
GovESB	Government Enterprise Service Bus
FiRCIS	Fisheries Revenue Collection Information System
GePG	Government Electronic Payment Gateway
GFS	Government Finance Statistics
GLICA	Gaming Licensing, Inspection and Compliance Application
GovNET	Government Communication Network
GRN	Goods Received Note
HCMIS	Human Capital Management Information System
iCHF-IMIS	Community Health Fund Management Information System
IFMS	Integrated Financial Management System
LIMS	Laboratory Information Management System
MAJI IS	Maji Integrated and Unified Billing System
MASSEMS	Maritime Safety Security and Environment Management System
NEST	National e-Procurement System of Tanzania
NPMIS	National Project Management Information System
POAS	Port Operations Application System
POS	Point of Sales
PSSN-MIS	Productive Social Safety Net -Management Information System
RIMS	Regulatory Information Management System
RRIMS	Railway & Road Information Management
SARIS	Student Academic Register Information System
SBMS	Shipping Business Management System
SLPS	Special Load Permit System
SMBS	Shipping Business Management System
SPLS	Special Load Permit System
TAUSI	Local Government Revenue Information System
TOS	Terminal Operating System
WIMS	Workplace Information Management System

STATEMENT OF THE CONTROLLER AND AUDITOR GENERAL

I am delighted to present the audit report for the financial year ended on 30 June 2023, which encompasses Information Systems. I would like to acknowledge the Government's initiatives, led by H.E. Dr. Samia Suluhu Hassan, the President of the United Republic of Tanzania, in promoting accountability and transparency in public resource management. I also appreciate the cooperation from the management of audited entities, who provided the necessary information and clarification for the preparation of this audit report.

The audit findings reveal a diverse array of Information Systems management practices among the Government Entities. While some have shown commendable Information Systems management, others have faced challenges in maintaining Information Systems stability and performance. It is crucial for the Government to intervene and ensure these entities operate efficiently and effectively, contribute to the economy, and deliver top-notch services to the citizens.

The report is organised into nine chapters, each delving into different facets, including Information Technology General Controls, Accounting systems, Revenue Systems, Human resource and Payroll systems, Application systems and administration, System Optimization and Process Automation, Operation Efficiency of e-GA. The report also identifies areas where these entities need to improve their operations and execute their mandate more efficiently.

In the report, I have provided recommendations on how to boost the operations of the reported entities, increase transparency and accountability, and foster good governance. I trust these recommendations will be beneficial for the Government, and other stakeholders in guaranteeing the provision of high-quality services.

Lastly, I extend my heartfelt thanks to the audit staff for their relentless efforts in carrying out the audits and compiling this report. Their commitment and hard work have been key in the preparation of this report, and I am grateful for their input.

Charles E. Kichere
Controller and Auditor General
United Republic of Tanzania

EXECUTIVE SUMMARY

Introduction

This report summarizes the findings, recommendations, and conclusions from audits of information systems across various public authorities, departments, agencies, and institutions in the United Republic of Tanzania for the financial year ending 30 June 2023. The primary objective was to assess the effectiveness and adequacy of internal controls related to information and communication technology (ICT) and application systems to ensure data integrity, confidentiality and availability.

Key findings from the audits include:

(a) Information Technology General Controls

The evaluation of e-government standards and guidelines compliance for 22 organizations (detailed in Appendix II) revealed varying levels of achievement across different IT general control domains. Notably, National Social Security Fund (NSSF), Roads Fund Board (RFB), Ministry of Finance (MoF) and Tanzania Insurance Regulatory Authority (TIRA) achieved high compliance in most areas, with only a few domains showing moderate compliance. Conversely, Ministry of Work (MoW), Occupational Safety and Health Administration (OSHA), Open University of Tanzania (OUT), Rural Energy Agency (REA), National Institute of Transport, Tanzania Posts Corporation (TPC) and Exports Processing Zones Authority (EPZA) exhibited consistently low compliance across most IT general control domains.

My analysis shows that most organizations are effectively implementing measures to physically protect their IT infrastructure (e.g., secure access, cameras) and have established clear policies and procedures for managing IT systems and data.

On the other hand, areas like Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP), Change Management, Incident Management, Database Management, and Software Acquisition and Development show a lower compliance rate. This suggests that fewer organizations are following best practices in these critical areas. This could be due to factors like lower awareness of their importance, the complexity of implementation or a lack of resources.

The evaluation highlights the need for improvement in ICT management practices across most organizations. While some achieved compliance in some domains, very few attained the required level in all areas which underscores the importance of implementing comprehensive enhancements in ICT management practices. (*Refer to Chapter 2)*.

(b) Accounting System

(i) Mismatch between Purchase Order and Requisition Quantities

The Epicor system at Medical Stores Department (MSD) lacks adequate controls to match purchase order quantities with corresponding requisitions. This has resulted in 287 orders having more quantities than their corresponding requisitions, and 3,137 MSD-funded purchase orders lacking corresponding requisitions. This could lead to fraudulent activities such as the creation of inflated or unauthorized purchase orders, leading to potential financial losses. *(Refer to Para 3.4)*

(ii) Receiving items without Requisition and Purchase Orders

In auditing the Epicor system at MSD, I found 37 items that were delivered without ever being a requisition and not included in a formal purchase order (PO). There were also four additional items whose requisition exists but never formally ordered (PO missing). This lack of controls could lead to having wrong items in the inventory or understocking of items that are highly needed. As a result, this can disrupt operations and budget. *(Refer to Para 3.5)*

(iii) Invoices raised without Goods Received Note

In auditing the Epicor system at MSD, I found 148 invoices that were created without a corresponding goods received note (GRN). Reference numbers for purchase orders, including PO number, line number and release number, listed on these invoices could not be matched to any existing GRNs. This stems from inadequate system controls that fail to demand that invoices be linked to GRNs. Without the GRN to verify that goods or services were received, MSD is at risk of paying for items it never received. *(Refer to Para 3.6)*

(iv) Inadequate segregation of duties in payment processes

The audit of the Ministry of Finance (MoF) and the Ngorongoro Conservation Area Authority (NCAA) payment processes revealed critical weaknesses. Specifically, there is a lack of segregation of duties, allowing individuals to perform multiple critical steps in the payment process without proper oversight. This situation increases the risk of errors, fraud and compromises transaction integrity. Addressing this concern is essential for financial accuracy and accountability within both institutions. *(Refer to Para 3.10)*

(v) MUSE allows overspending beyond the Allocated Budget

The system allowed exceeding the approved budget because expenditures paid directly by MoF on behalf of other entities were not automatically reflected, creating an artificially inflated available balance and allowing entities to spend more than the exchequer amount. Also, the budget allocated for wages was used for unauthorized construction expenses, compromising financial management and reporting best practices. (*Refer to Para 3.14*)

(vi) Inappropriate system usage

The audit identified some concerning instances of inappropriate system usage across government agencies, raising concerns about financial transparency, accountability, and process integrity. Specifically, the Ministry of Finance (MoF) was found to bypass procurement controls for stock items in MUSE accounting system by posting payment to suppliers direct to the general ledger, while at the Ministry of Livestock and Fisheries automated bills exceeding TZS 1.4 billion were generated through the "miscellaneous" module with limited oversight, and lack of proper tracking for permits paid through the same module.

In a related instance, Tanzania Medicines and Drugs Authority (TMDA) also generated bills manually that should have been automated, potentially leading to revenue loss. These findings necessitate stricter controls within application systems, specifically to prevent purchase order bypasses and limit use of the "miscellaneous" module to ensure proper system utilization. *(Refer to Para 3.16)*

(vii) Unauthorized Access and Activity in Financial System

My audit revealed a serious security breach in the financial system of the Rural Energy Agency (REA). In one case, an unauthorized individual was granted access to the system and used it to create invoices and payment vouchers. This individual lacked proper accounting expertise and bypassed established authorization procedures. This has an impact to increased risk of fraud due to unauthorized access and transactions. Also, there is potential inaccuracies in financial records due to the user's lack of expertise. *(Refer Para 3.18).*

(c) Controls in the revenue system

(i) Multiple receipt generation from single payment at TSN

In the **Sage Pastel** being used by Tanzania Standard Newspapers, the system allows a single payment to be used to generate multiple receipts and clear various customer invoices, falsely indicating that they have been paid *(Refer to Para 4.3).*

(ii) Registration fees not configured in TMA Integrated Weather Portal

The TMA Integrated Weather Portal used by Tanzanian Meteorological Agency (TMA) is not configured to collect registration fees from meteorological stations. This is due to lack of configuration within the system. This anomaly can lead to incorrect charges related to meteorological services. (*Refer to Para 4.15*)

(iii) Inadequate segregation of duties in revenue system (TASAC, TMDA, LATRA)

My audit of revenue systems at Tanzania Shipping Agencies Corporation (TASAC), ,TPA, TMDA and Land Transport Regulatory Authority identified critical internal control weakness: a lack of segregation of duties within the billing process workflow. This means that in some instances, the same person was responsible for both creating and approving various applications hence raising concerns about the integrity of the process. The review found a concerning number of instances where this occurred, including over 8,000 certificate applications across MASSEMS, SBMS and TOS; PSV license applications in RRIMS; and even clinical trial certificates in RIMS. This lack of segregation of duties appears to be caused by inadequate validation controls when assigning user access rights. By allowing a single person to handle both creation and approval, these systems increase the risk of errors, misuse of sensitive data and potential fraud. (*Refer to Para 4.20*)

(d) Human resources and payroll system

(i) Segregation of duties weakness in HCMIS

My audit of the HCMIS system revealed a lack of approval functionality for changing employees’ date of birth and amending personal emolument (PE) budgets. Only one user from PO-PSMGG can alter such details. This was caused by insufficient system design which failed to incorporate appropriate approval workflows. A single user performing critical human resources tasks increase the risk of undetected errors and unauthorized activities. (*Refer to Para 5.3*)

(ii) Computer system analyst performing HR officer duties

My review found out that a principal computer system analyst, not a designated human resource officer, was updating personal user details in the Management Information System (MIS) database at Roads Fund Board. The reason is likely due to inadequate data migration plan or insufficient human resources staff. This deviation from protocol raises concerns about data accuracy and accountability within the system. (*Refer to Para 5.9*)

(e) Application System Administration

(i) Excessive privilege to ICT officers

My recent government institutions' audit identified a serious security risk: widespread inappropriate privilege assignments for Information and Communication Technology (ICT) officers. This action grants them excessive control which potentially compromises data integrity and operational efficiency. The audit found examples across various agencies, including at TMDA's RIMS system which allows bypassing approval stages for product registrations; staff at NSSF's BCMS creating and cancelling bills beyond their designated roles; and nine ICT staff at PORALG having unauthorized financial access in TAUSI. Furthermore, e-Government Authority assigned business roles (accounting, procurement, etc.) to staff meant for technical support; and a Roads Fund Board analyst entered employees' data instead of an HR staff. These widespread anomalies stem from inadequate access controls and a lack of segregation of duties which potentially leads to process inefficiencies, data discrepancies, security breaches, and even financial losses. (*Refer to para 6.1*)

(ii) Uncontrolled vendor access in Subsidy Management Systems

The auditing of Tanzania Fertilizer Regulatory Authority's Subsidy Management System found that the vendor retains uncontrolled access to servers and databases, contrary to requirements. This creates data security risks. Additionally, TFRA's ICT officers cannot even extract data due to insufficient access, highlighting the potential for unauthorized access or breaches. The vendor's uncontrolled access to a live server and database creates a significant risk against breaches by the vendor or its employees (*Refer Para 6.3).*

(f) Information Systems optimization and process automation

(i) Integration between Systems

Audits across government agencies identified widespread system integration issues hindering efficient financial management and data exchange. For instance, Tanzania Social Action Fund (TASAF) and Roads Fund Board (RFB) lack integration between core process and accounting systems, requiring manual data entry hence raising error risks. Similarly, billing systems at TSN, Air Tanzania Company Limited and Tanzania Petroleum Development Corporation (TPDC) are not integrated with the central accounting system, necessitating manual transaction transfers and potentially inaccurate reporting. These inadequacies were also found in management systems, like the Ministry of Works' SPLS which is not integrated with Tanzania Revenue Authority's TIN application system which leads to errors in permits issuance. To improve transparency, efficiency and reduce human error, I recommend system integration across government institutions, along with data integrity checks for entities like OSHA and TMDA. (*Refer to Para 7.3*)

(ii) Duplication of Systems hinders e-Government efficiency

My audit revealed ICT initiative and application system duplication across various entities. Notable examples include **Gaming Board** which utilizes both ERMS and Sage Pastel for accounting processes; **NSSF** which has developed an in-house Asset Management System, alongside the existing Oracle ERP; **Tanzania Postal Corporation** uses MUSE alongside Sage Pastel for accounting; and **Tanzania Ports Authority** has an enhanced POAS but initiated a TOS tender and thus duplicating functionalities. The **e-Government Authority's ERMS** overlaps with HCMIS and NEST in various areas. These duplications result from inadequate access control and pose risks to efficiency and data integrity. *(Refer to Para 7.6*)

(g) Operational efficiency of e-Government Authority.

(i) Delayed provision of Government's e-mail services

Requests for government mail services submitted by public entities experienced delays ranging between 24 and 132 days, surpassing the stipulated response time of delivering services on the Government Mail System (GMS) of within three working days upon receiving the requests as outlined in Para 5.3 of e-GA Client Service Charter. Delays in service delivery can tarnish the reputation of e-GA as a reliable and efficient service provider by public entities which may perceive the Authority negatively, impacting its standing in the e-Government ecosystem. (*Refer to Para 8.5*)

CHAPTER ONE

INTRODUCTION

Recognizing the transformative power of ICT for social and economic progress, the United Republic of Tanzania government established a National e-Government Strategy. This strategy aims to leverage ICT opportunities and address challenges in public service delivery. The e-Government Act of 2019 further strengthened the goal by creating the e-Government Authority to oversee the Strategy's implementation and develop standards and guidelines.

This report summarizes key findings from 57 information systems audits. 35 of the audits were conducted alongside financial audits, while the remaining 22 focused solely on information systems. All audit reports were submitted to the relevant accounting officers.

1.0 Audit Objectives

The audit aimed to evaluate the effectiveness of information systems and technology in supporting government entities' goals and objectives. The evaluation focused on three key areas:

- **General Controls:** This assessed the overall security and management framework surrounding the systems and ICT operations.

- **Project Management Efficiency:** This examined how effectively information and communication technology projects are planned, executed, and monitored.

- **Application Controls and Systems Efficiency:** This evaluated the effectiveness of controls within government applications and the overall efficiency of these systems.

1.1 Audit Scope

I conducted a thorough audit of the information systems and technology used by government entities by looking at four key areas to ensure everything is functioning smoothly: how well information is protected within each system; how is the government managing its overall IT infrastructure; how well are IT projects planned and carried out; and how efficient does the e-GA operate. In total, I reviewed 57 information systems, including 35 as part of financial audits and 22 as standalone IT systems audits. The findings are based on records, documents and information made available during the audit.

1.2 Audit Methodology

I conduct audits of information and communication technology (ICT) systems and processes in accordance with the International Standards of Supreme Audit Institutions (ISSAI) issued by the International Organisation of Supreme Audit Institutions (INTOSAI). In performing these audits, I adhered to established audit procedures and guidelines, including the AFROSAI-E Information Technology Audit Guideline, Tanzania e-Government standards and guidelines, COBIT 5, and ISO/IEC 27001 for information security management systems.

My approach to ICT audits is comprehensive, considering system efficiency, effectiveness, and security. I assess the risks associated with ICT systems and identify control measures to mitigate these risks. The objective of my audits is to ensure that ICT systems and processes operate effectively, efficiently and securely to support government objectives.

CHAPTER TWO

INFORMATION TECHNOGY GENERAL CONTROLS

2.1 Introduction

Information Technology General Controls (ITGCs) are set of rules that help to ensure a company's computer systems are safe, can run smoothly, and the information they produce can be trusted. These controls cover things like making sure only the right people can get into the system, that there is a backup in case something goes wrong, and that any changes to the system are done properly. They are not about specific tasks or processes, but about the overall environment that supports these systems.

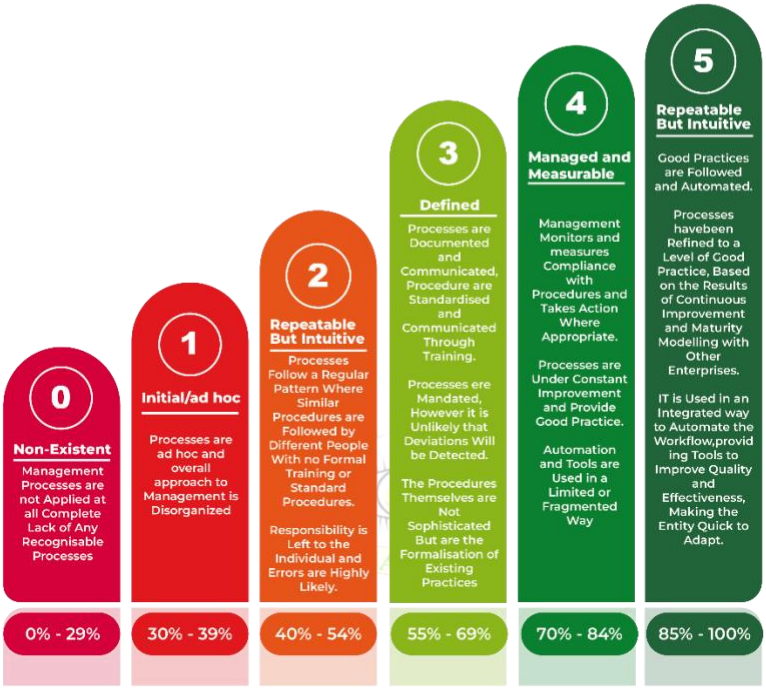
When auditing Information Technology General Controls (ITGCs) in the public sector, the goal is to make sure that the government's computer systems are working as they should be. This means I check if the systems are secure, reliable, and being used properly. The audit also looks at whether the systems are helping the government follow all rules and regulations as provided for by e-Government Act, guidelines, standards and best practices that apply. By conducting these assessments, I help to reduce the risk of problems like data loss or security breaches, and make sure that the government can provide services effectively and efficiently.

During my audit of ICT general controls effectiveness, I used the "ITGCs Compliance Assessment" model, which has 11 key domains. These domains include: ICT Governance, Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP), Network Management, Incident Management, Database Management, Third-Party Management, Change Management, Application Access Management, Physical and Environmental Control, Acquisition and Development, and Information Security.

My assessment aimed to evaluate the overall compliance level of these domains against the e-Government Act, relevant guidelines, standards and best practices established by ISO 27001. This assessment model defines five compliance levels, ranging from zero to five (as detailed in Figure 1).

According to the model, entities should strive to achieve at least a compliance level of 3 (Defined) or higher across all domains.

Figure 1: Rating scale and Criteria



0 Non-Existent
Management Processes are not Applied at all Complete Lack of Any Recognisable Processes
0% - 29%

1 Initial/ad hoc
Processes are ad hoc and overall approach to Management is Disorganized
30% - 39%

2 Repeatable But Intuitive
Processes Follow a Regular Pattern Where Similar Procedures are Followed by Different People With no Formal Training or Standard Procedures.

Responsibility is Left to the Individual and Errors are Highly Likely.
40% - 54%

3 Defined
Processes are Documented and Communicated, Procedure are Standardised and Communicated Through Training.

Processes ere Mandated, However it is Unlikely that Deviations Will be Detected.

The Procedures Themselves are Not Sophisticated But are the Formalisation of Existing Practices
55% - 69%

4 Managed and Measurable
Management Monitors and measures Compliance with Procedures and Takes Action Where Appropriate.

Processes are Under Constant Improvement and Provide Good Practice.

Automation and Tools are Used in a Limited or Fragmented Way
70% - 84%

5 Repeatable But Intuitive
Good Practices are Followed and Automated.

Processes havebeen Refined to a Level of Good Practice, Based on the Results of Continuous Improvement and Maturity Modelling with Other Enterprises.

IT is Used in an Integrated way to Automate the Workflow,providing Tools to Improve Quality and Effectiveness, Making the Entity Quick to Adapt.
85% - 100%

2.2 ITGCs Compliance Assessment

2.2.1 ICT Governance

ICT governance is a structured framework that helps businesses align their IT strategy with their goals by focusing on performance measurement and clear communication. It covers key areas like the overall function of the IT department, key performance indicators (KPIs), and measuring the value of technology investment.

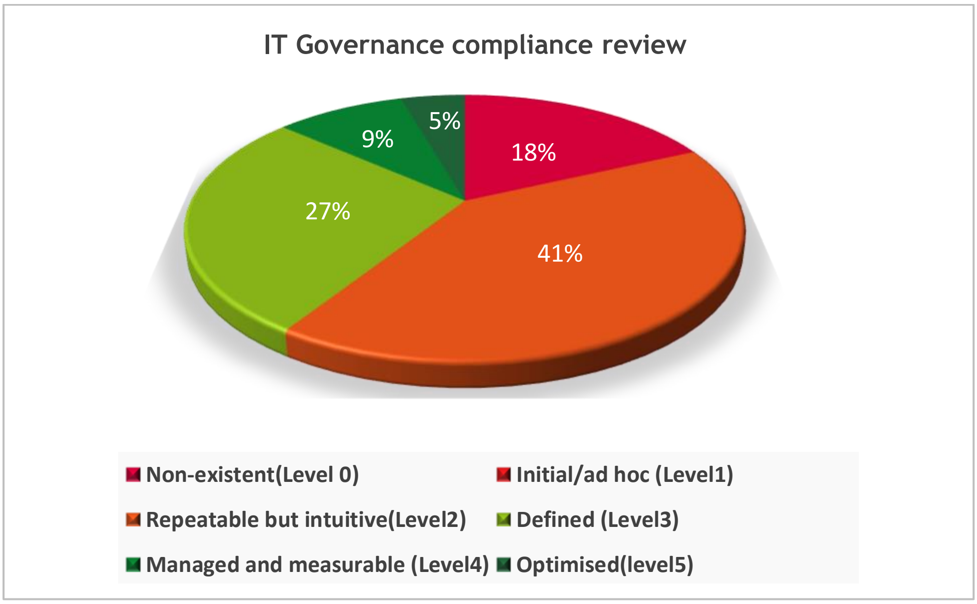
The audit of ICT governance looked at several things, including:

- How the ICT steering committee, which guides the ICT work, is operating.
- The roles of ICT staff

- The policies that have been approved in relation to ICT
- How the internal audit of ICT is being done.
- The procedures for ICT budgeting
- How the ICT strategic document, which outlines the ICT plans, aligns with the goals of the business.

The audit also checked how well 22 public entities were following the standards and guidelines for ICT governance set by e-Government. The level of how well they were following these standards is shown in Figure 2.

Figure 2: ICT governance and compliance review



I audited the ICT governance in 22 entities and found several areas requiring improvements. Here are the main concerns:

(i) Ineffective ICT steering committees

Among the 22 audited entities for the fiscal year 2022/23, it was revealed that 11 have issues with their ICT steering committees. The issues include:

- Lack of a steering committee altogether

- Failure to meet as often as recommended.

Considering the pivotal role of the ICT steering committee in supervising ICT initiatives which encompasses reviewing and offering guidance on investment portfolio and priorities, as well as ensuring the alignment of ICT with the organization's business needs, an ineffective committee raises concerns about a possible misalignment between objectives and core business goals. Entities ought to establish and operationalize an ICT steering committee and ensure regular meetings as per guidelines.

(ii) Misalignment and inadequate monitoring of ICT Strategic Plan

Among 22 audited entities, 13 face challenges in aligning ICT investments with institutional business objectives. Their ICT strategies diverge from organizational plans and lack systematic monitoring. This misalignment hampers resource efficiency and impedes technology support for business objectives. Continuous monitoring of the ICT strategic plan is essential to prevent misalignment with business objectives, averting wastage of resources and ensuring progress.

(iii) Non-performance of ICT internal audit

The audit also revealed that six entities did not conduct ICT internal audits, potentially failing to effectively address risks associated with IT-dependent processes. ICT internal audit is important to ensure ICT related controls are adequate, effective and compliant with regulations and industry standards.

2.2.2 Business Continuity and Disaster Recovery Planning

In today's fast-paced and interconnected world, it is crucial for organizations to be prepared for unexpected events that could disrupt their operations. Two key strategies that help ensure this preparedness are **Business Continuity Planning (BCP)** and **Disaster Recovery Planning (DRP)**.

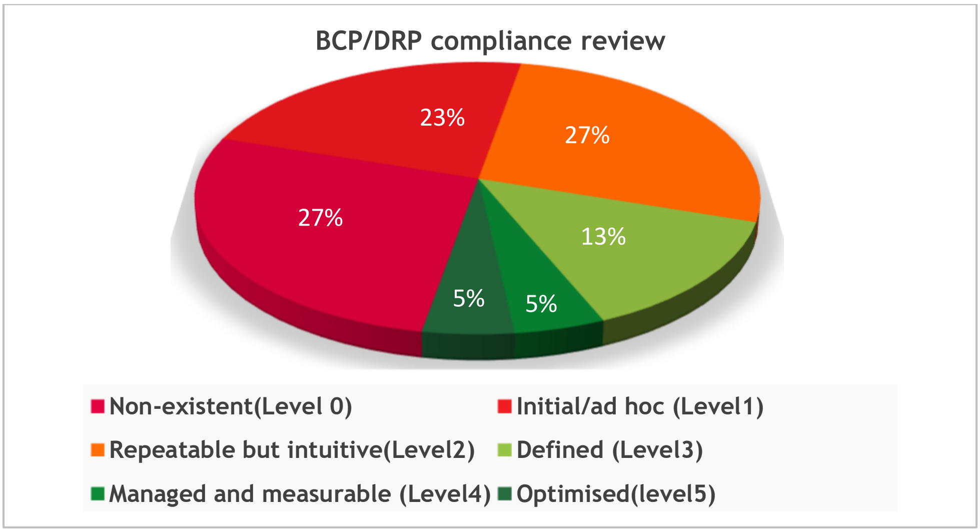
BCP is a proactive plan that enables an organization to maintain essential functions during, as well as after, a disaster has occurred. It is all about ensuring that the business can continue to operate and adapt swiftly to disruptions, minimizing the impact on services, customers and stakeholders.

While BCP is about keeping the business running, DRP is focused on getting things back to normal after a disaster. DRP is a set of detailed instructions to recover and protect a business IT infrastructure in the event of a disaster.

While BCP and DRP have different focuses, they are closely related and often work hand in hand. Together, they form a cohesive strategy to safeguard against challenges to stability and operational continuity.

I audited 22 entities to assess their compliance with e-Government standards and guidelines for BCP and DRP. Figure 3 visually depicts this, providing an overview of their preparedness for disruptions.

Figure 3: BCP and DRP compliance review



I assessed the BCP and DRP processes among 22 public entities and unveiled common issues, which are detailed below:

(i) Lack of Business Continuity and Disaster Recovery Plans

In my audit of 22 entities, I found that 10 had neither a Business Continuity Plans (BCP) nor a Disaster Recovery Plan (DRP). This lack of planning raises concerns about their ability to navigate disruptions effectively and maintain operational stability during unforeseen events. It is crucial for these organizations to establish comprehensive BCP and DRP plans to mitigate risks, protect critical functions and ensure a swift recovery from disruptions. To enhance their overall resilience, these entities should prioritize addressing this gap urgently.

(ii) Non-performance of BCP and DRP tests

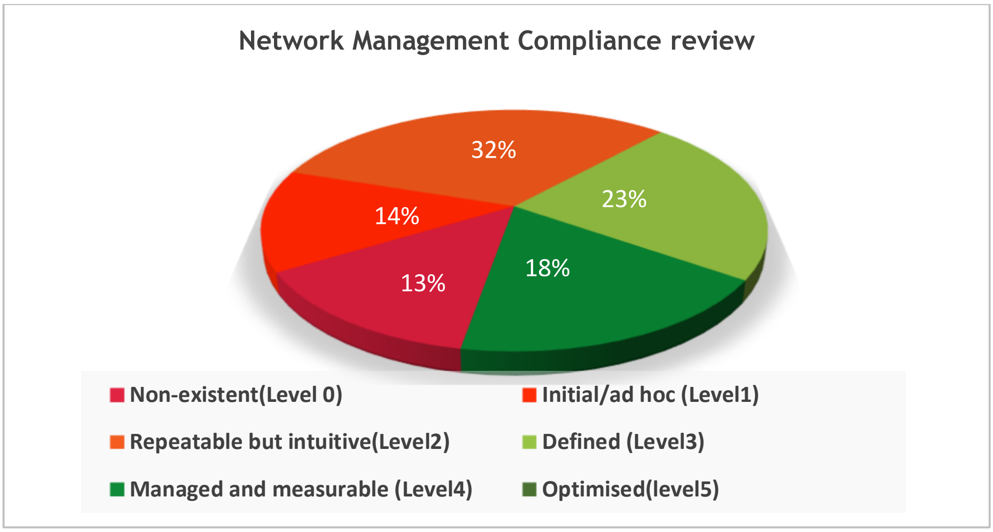
In my audit of 22 entities, I found that 12 did not perform BCP and DRP tests. This was due to a lack of business impact analysis and the absence of defined Recovery Point Objective (RPO) and Recovery Time Objective (RTO). The lack of these tests
raises concerns about their readiness for potential disruptions. Regular testing is crucial to validate the effectiveness of BCP and DRP measures and to ensure alignment with predefined recovery objectives. Addressing these issues will significantly strengthen the overall resilience and preparedness of these entities.

2.2.3 Network management

In a Network Management audit, I evaluated the performance and security of a computer network, which includes hardware, software, security protocols and user access. My goal was to find potential problems, security risks and areas for improvement by analyzing the network's architecture, configuration and protocols.

I examined how well 22 public entities followed e-government standards and guidelines related to network management in this audit. The overall level of compliance is shown in Figure 4 below.

Figure 4: Network management compliance review



In the audit of network management across 22 entities, several concerns were noted as presented below:

(i) Non-monitoring of network performance

I reviewed 22 entities and found that eight of them do not monitor network performance, which puts their security and performance at risk. For optimal functionality, issue resolution and improved security plus user experience, entities should monitor their networks.

(ii) Uncontrolled remote network access

In my review, I found that four entities often allow remote network access without any documented policies or procedures for authorization. This practice increases risks of unauthorized data access and data breaches. To safeguard sensitive data and uphold the integrity of the organization's network infrastructure, entities should establish documented policies and procedures governing remote network access.

(iii) Non-performance of network security assessment

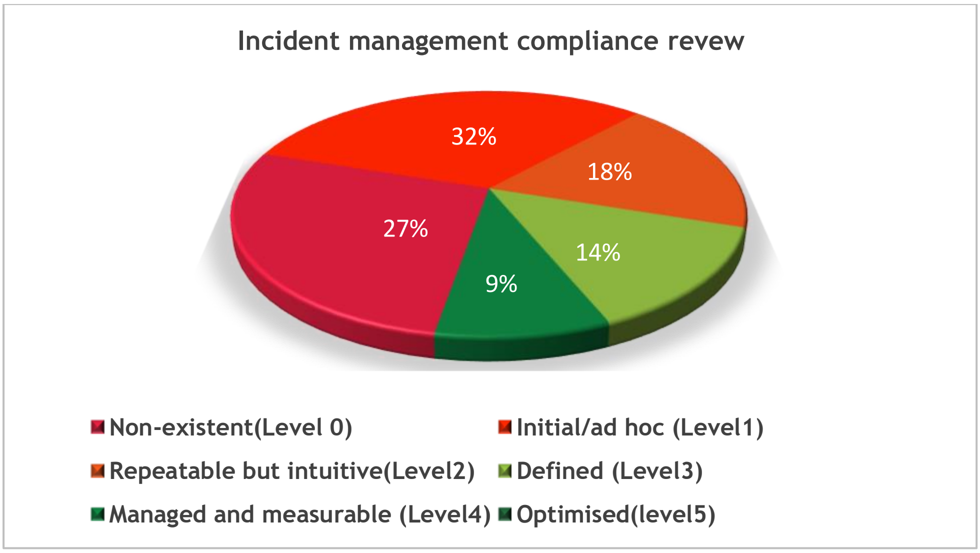
During my audit, I found that three entities have not conducted network security assessments. Lack of network security assessment exposes entities to the risk of unidentified vulnerabilities and compromises their overall information security. For timely detection and resolution of network vulnerabilities, entities should conduct network security assessments regularly.

2.2.4 Incident management

Incident management involves managing ICT service disruptions reported by end users and restoring services within agreed-level agreements. The audit in incident management focused on the availability of incident management procedures, timely incident resolution, regular incident reviews and the presence of Operational Level Agreement (OLA) between ICT and the organization.

The audit evaluated the adherence to e-government standards and guidelines for incident management across 22 public entities. The analysis of compliance levels is depicted in Figure 5 below.

Figure 5: Incident management compliance review



In the course of the incident management audit, the following anomalies were identified:

(i) Absence of incident management procedures

The audit revealed that five entities lack incident management policies and procedures, which indicates a significant gap in the organizations' capacity to respond effectively to ICT incidents. In order to provide a structured framework for responding to incidents effectively, entities should establish incident management procedures.

(ii) Absence of Operation Level Agreement (OLA)

Five entities lacked the OLA between the ICT department and other user departments, raising concerns about coordination, communication and efficiency in ICT service management. In order to have defined roles, responsibilities and accountabilities between ICT department and other departments, entities should formulate Operational Level Agreements without failure.

(iii) Delays in handling of ICT incidents

The audit revealed that four entities are delaying the resolution of ICT incidents, deviating from the agreed-upon resolution time outlined in the OLA. This delay not only risks the effectiveness of incident management but also disrupts business operations. To address the delays in resolving ICT incidents, entities should allocate required resources, provide training and support to staff on incident management but also conduct regular reviews for continuous improvement.

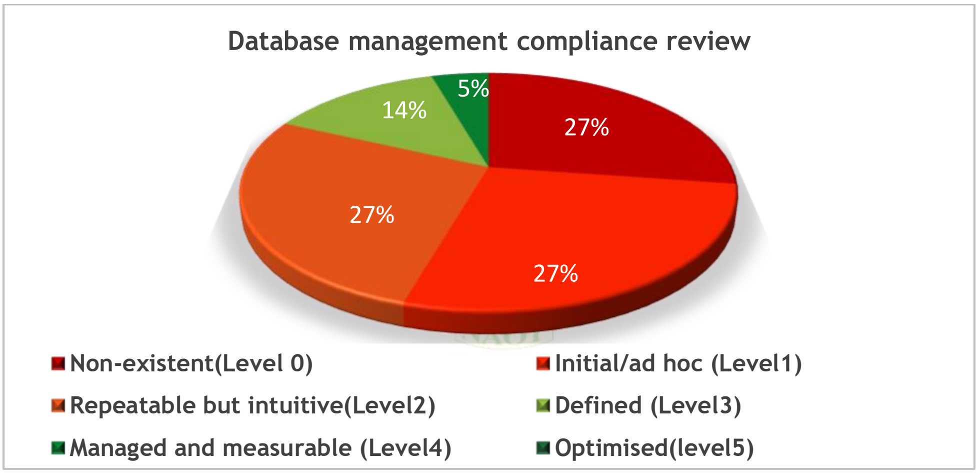
2.2.5 Database management

Effective database management is key to ensuring the security and integrity of organizational data stored in databases. It mitigates risks such as unauthorized access and data breaches. To prevent potential cyber-attacks and ensure the confidentiality, availability and integrity of sensitive information, organizations must manage their databases properly.

In my assessment, I evaluated the configurations of database audit trails and the performance of system activity monitoring. I checked whether the database management systems were operating on supported versions. I also reviewed user authentication, password management and the maintenance of default user accounts for secure practices.

My audit scrutinized the compliance of 22 public entities with e-Government standards and guidelines related to database management. Figure 6 represents the collective level of compliance.

Figure 6: Database management compliance review



In the assessment of database management across 22 public entities, the following vital issues surfaced:

(i) Database Audit trail and log review deficiencies

In the 2022/23 audit, I found that 16 of the 22 entities had not set up the audit trail and had not conducted regular reviews of audit logs. This oversight creates vulnerability in monitoring unauthorized access or activities within ICT systems. Such a lapse increases the risk of security breaches and potential threats to data integrity. It’s crucial that these entities address this issue by setting up audit trail and conduct regular reviews.

(ii) Default database user accounts

During the audit, I found that eight of the 22 entities audited were maintaining default database user accounts. These default accounts, with their standard settings and passwords, pose a security risk. If these accounts are not modified or deactivated, they increase the potential for unauthorized access.

(iii) Existence of outdated database version

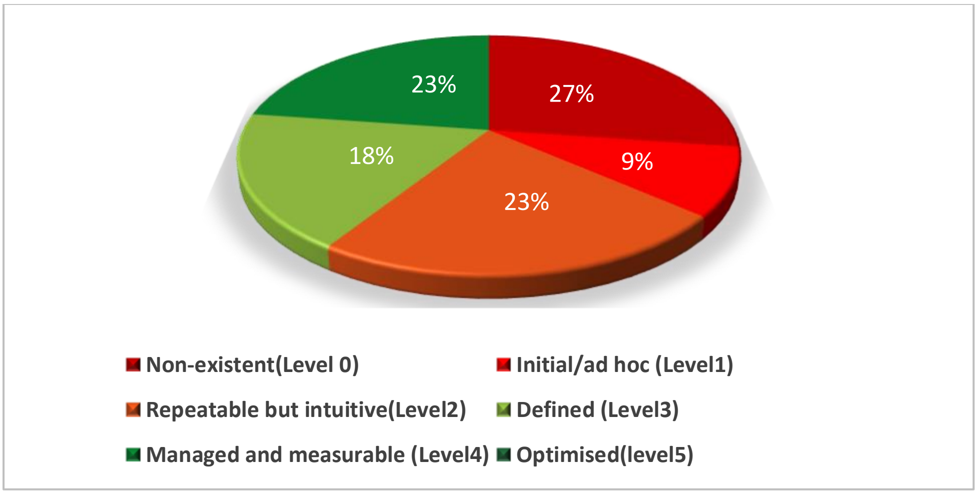
Among the 22 entities audited, I observed that three of them were using an outdated version of the database management system. This lack of effective version control exposes the organization to risks associated with the use of obsolete software or applications. Such a situation can result in security vulnerabilities, lack of support and compatibility issues, thereby threatening the overall stability and security of the ICT environment. To resolve this issue, entities should update their database management system to the latest version available.

2.2.6 Third-party management

Third-party vendor management is vital for companies that depend on external vendors. While there are benefits, the relationship between the entity and the vendor introduces risks, including cybersecurity threats due to access to computer network and application systems. To mitigate these risks, it’s essential to implement third-party management practices.

In my audit of the 22 entities, I evaluated the availability of contracts and Service Level Agreements (SLAs) between ICT vendors and entities. I also assessed supplier service delivery management and change management for third-party services. These evaluations were against the e-Government standards and guidelines for Third-Party Management. The audit results are visually represented in Figure 7.

Figure 7: Third-party management compliance review



During my audit of third-party management, I identified the following primary anomalies:

(i) Absence of contracts and Service Level Agreements between entities and ICT vendors

In the audit of the 22 entities, I found that 12 of them are operating with multiple vendors without any formal contracts or Service Level Agreements (SLAs). This practice poses risks of undefined terms and legal uncertainties. It also impacts service quality and delivery timelines. Entities should establish formal contracts and service level agreements (SLAs) for all services provided by service providers.

(ii) Non-monitoring of vendor performance

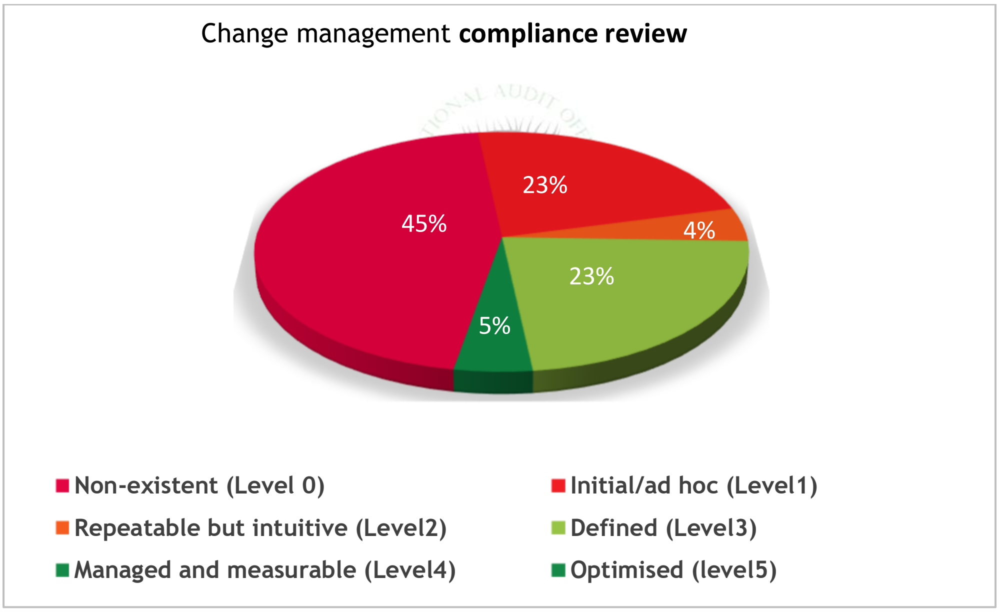
In my review, I found that 10 of the 22 audited entities did not monitor the performance of their suppliers/vendors. This lack of monitoring indicates potential risks such as quality issues and compliance breaches. To ensure that the quality of services provided by vendors aligns with the terms outlined in contracts and service level agreements, entities should conduct regular monitoring of these services.

2.2.7 Change management

Effective change management is crucial for the controlled implementation of system enhancements. Inadequate change management practices can pose inherent risks to both system stability and security. In the 2022/23 audit, I evaluated the entities' adherence to change management procedures and guidelines. This evaluation included established procedures, authorized system changes, post-implementation reviews and the segregation of development, test, and production environments.

I assessed the adherence of 22 public entities to e-Government standards and guidelines on change management. The overall level of compliance is visually represented in Figure 8.

Figure 8: Change management compliance review



The audit highlighted key challenges in change management across the audited public entities:

(i) Absence of change management procedures

Four out of 22 entities lacked essential change management procedures, compromising the controlled implementation of system modifications and increasing the risk of errors, instability and unauthorized changes. Implementing robust protocols is crucial to mitigate these risks and ensure a secure environment for system modifications.

(ii) Non-separation of test and live environments.

One out of 22 entities lacked proper separation between development, test, and production environments, posing a significant risk to system stability and security. This deficiency may lead to unintended interferences during testing, increasing the potential for errors, data corruption and unauthorized access. To address these anomalies entities should separate development, test, and production environments to ensure the integrity of the system.

(iii) Non-performance of security tests before deploying changes

Seven out of 22 entities had not performed security tests before deploying changes, posing an increased risk of potential vulnerabilities in their systems. This leaves the organization exposed to security threats and compromise the integrity of its systems. It is essential for entities to implement security testing procedures to identify and address potential risks before deploying any changes.

(iv) Lack of post-implementation review

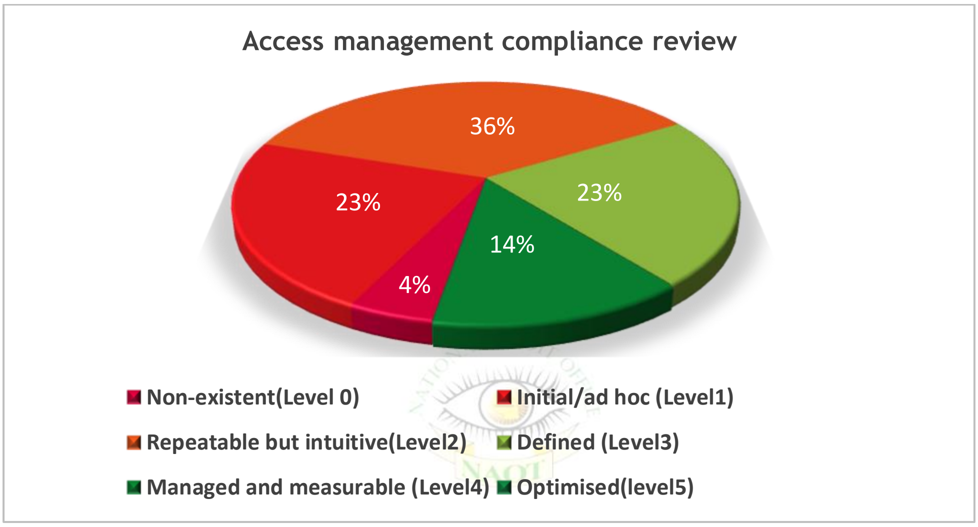
I found that nine of the 22 entities had not conducted post-implementation reviews. This lapse in evaluating the effectiveness and impact of system changes hinders the assessment of changes' effectiveness. It could potentially lead to unresolved issues, inefficiencies and increased vulnerabilities. These entities should prioritize the establishment of a post-implementation review process to refine and optimize system changes, ensuring they align effectively with organizational goals and standards.

2.2.8 ICT Systems Access Management

The role of access management is to control and monitor authorized user access to ICT systems, using various policies, processes, methodologies and tools to maintain information system security. The focus of my audit was to validate the existence and execution of procedures concerning user access provisioning, authorization, authentication and revocation. It also encompassed a review of the rights of user access and the corresponding user system activities.

The audit assessed the compliance of 22 public entities with e-Government standards and guidelines pertaining to ICT Systems Access Management. The overall level of compliance is illustrated in Figure 9.

Figure 9: ICT Systems Access Management compliance review



Critical issues identified during the auditing of ICT Systems Access Management include the following issues:

(i) Absence of systems access provision and revocation procedures

My audit revealed that among 22 entities, 14 lacked documented procedures for granting and revoking system access to users, leading to unauthorized access, in violation of e-government guidelines. To safeguard sensitive data and uphold the integrity of the information systems, entities should establish documented policies and procedures governing provision and revocation of access to information systems.

(ii) Non-review of user access rights and activities

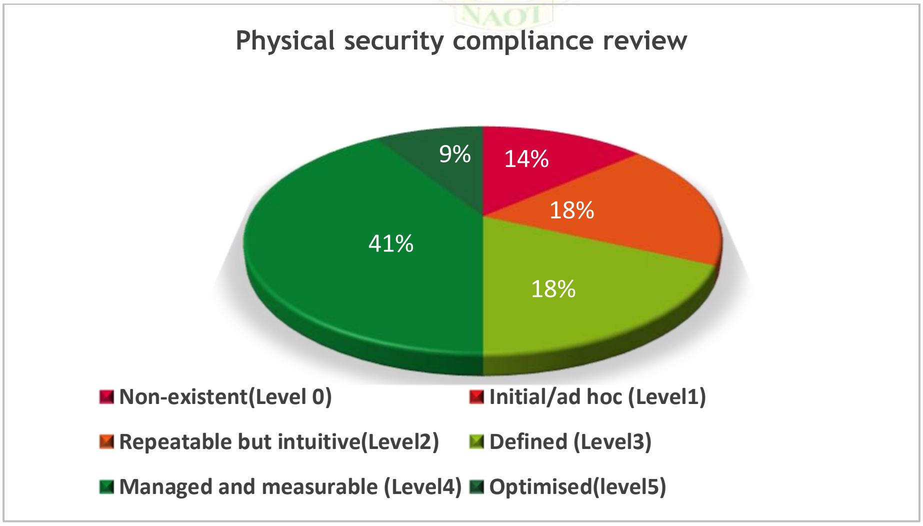
During my review, I noted that 13 entities did not assess system user access rights and review of user activities, highlighting security risks within the information system, particularly those associated with unauthorized access that may go undetected. To address this issue, entities should perform regular user access right and activities review.

2.2.9 Physical environmental control

Physical and environmental control is vital for securing sensitive areas and facilities, encompassing measures like door access management, CCTV surveillance and regular maintenance in line with regulations. Neglecting these measures increases the risk of unauthorized access and compromises the physical environment. In the current year audit, I assessed entities for adherence to physical access controls, including door access management, presence of CCTV cameras and facility maintenance procedures.

The audit evaluated the compliance of 22 public entities with e-Government standards and guidelines regarding physical environmental control and the level of adherence is illustrated in Figure 10.

Figure 10: Physical environmental control compliance review



In the audit of physical environmental control, the following pivotal concerns emerged with all the 22 public entities:

(i) Ineffective physical access control

I noted that four out of 22 entities lack effective physical access control, with unrestricted door access and the absence of server room visitors log register. This facilitates unauthorized access by individuals who should not have entry privileges, and it is hard to keep track of what visitors are doing. Mitigating these risks necessitates implementing access control measures within the entities.

(ii) Absence of CCTV cameras in Sever room/data center

I found that two out of the 22 audited entities lack security cameras in their data centers, posing challenges in monitoring the premises. To enhance data center security and monitoring capabilities, it is important for these entities to install security cameras.

2.2.10 ICT Systems acquisition and development

Getting new software for government agencies (ICT systems acquisition and development) involves figuring out what is needed, designing and building it. This can be done by the agency itself or by hiring an outside company. Following established rules (standards) is crucial when developing these systems.

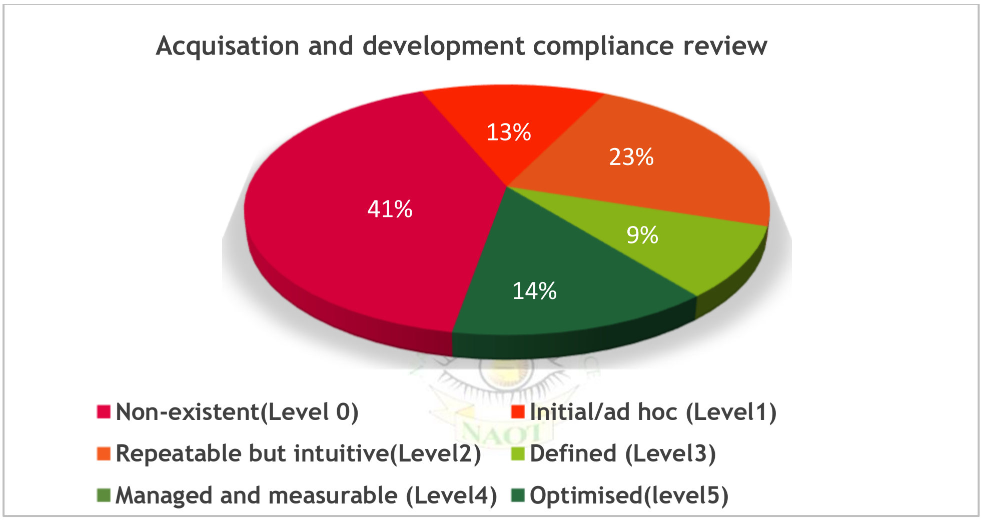
My review focused on making sure several key things were done properly:

- Clearly documenting what users need from the system
- Following coding rules
- Thoroughly testing the system
- Planning and assessing security
- Having a plan for launching the system, including moving from old systems (legacy system migration)
- Having a backup plan in case of problems (rollback plans)
- Training users on the new system
- Continuously monitoring how well the system is working

- Overseeing and keeping track of the work done by any outside companies involved in development (outsourced system development)

My audit checked if 22 government agencies followed the established rules (e-Government standards and guidelines) when getting and developing new software. Figure 11 shows an overall picture of compliance.

Figure 11: ICT Systems acquisition and development compliance review



During the audit of ICT systems acquisition and development processes, I identified notable concerns as follows:

(i) Inadequate documentation of system requirement documents

One government entity developed five new systems, but I could not find any proof that the people who use them (business users) reviewed and approved the initial plans (Software Requirements Specification, or SRS). This raise concerns that the systems might not be well-made or meet the real needs of the agency. Entities should prioritize the formulation of system requirement documentation and ensure its reviewed by business users prior implementation.

(ii) Non-performance of User Acceptance Test (UAT)

Six government entities did not test their new systems with the people who will actually use them (user acceptance testing). This raised concerns that the systems might not work well, be reliable or meet the real needs of the users in everyday situations (real-world scenarios). Entities should ensure user acceptance testing is performed by business users prior to deployment.

(iii) Non-performance of source code review

Four government entities skipped a crucial step (source code review) during the process of building new software. This means no one else checked the code that makes the systems work, which could lead to problems like:

- Security vulnerabilities: the code might have weaknesses that hackers could exploit.
- Bugs and errors: the systems might not work correctly or as intended.
- Poor overall quality: the code might be messy or inefficient, making the systems difficult to maintain or update in the future.

Skipping this step increases the risk that the systems will not be reliable or suitable for their intended use. Entities should ensure source code review is performed during the process of building the new software.

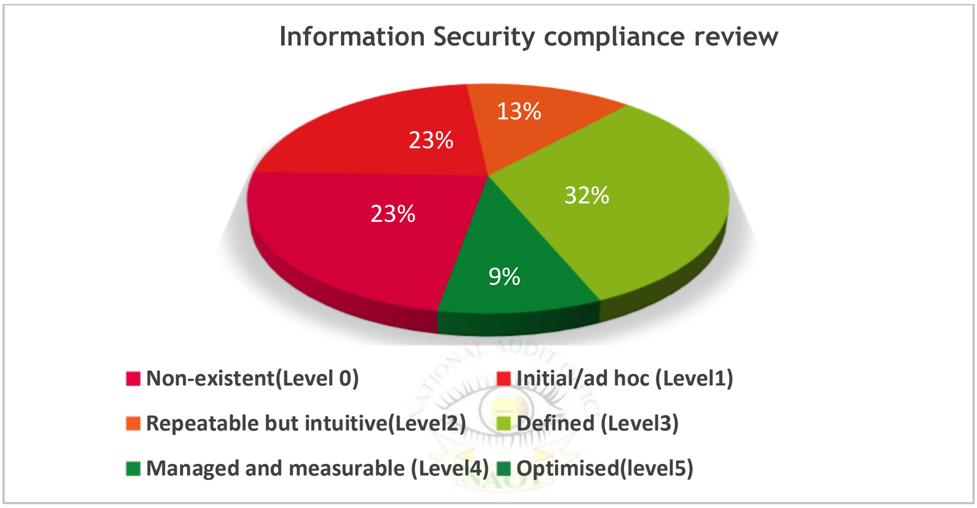
2.2.11 Information security

Protecting sensitive government information (information security) is crucial to prevent unauthorized access and ensure the information stays private, accurate and accessible. Weak security practices increase the risk of cyberattacks and data breaches. To assess this, I reviewed several key aspects in my audit:

- Does the organization have a dedicated information security officer (ICTSO)?
- Do they regularly conduct vulnerability assessments and penetration tests to identify weaknesses in their systems?
- Do they provide information security awareness training to employees?

The audit checked if 22 government agencies followed the established information security rules (e-government standards and guidelines). Figure 12 shows an overall picture of how well they followed these rules.

Figure 12: Information security compliance review



The following prevalent issues came to light in the audit of information security:

(i) Absence of ICT security officer

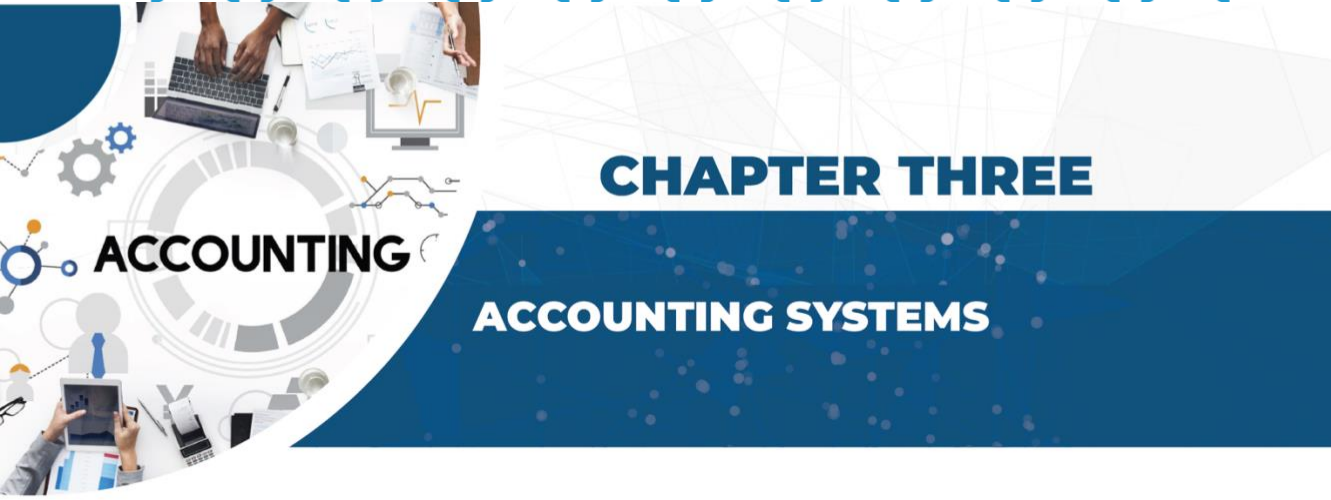
During the audit, I noted that four out of 22 entities did not have an ICT security officer. The absence of such a position result in a lack of oversight for implementing and monitoring security protocols, conducting risk assessments and responding to security threats. This deficiency poses a threat to the organization's ability to uphold an effective approach to information security. Entities should ensure the presence of ICT security officers.

(ii) Non-performance of vulnerability assessment and penetration testing

Five out of 22 entities did not conduct thorough security checks (vulnerability assessments and penetration tests) on their systems, which could leave them vulnerable to cyberattacks. Regularly checking for weaknesses is essential for strong information security. For timely detection and resolution of vulnerabilities, entities should conduct security assessments.

(iii) Lack of information security awareness training

I noted that 12 out of 22 entities did not provide essential information security awareness training, raising concerns about an elevated susceptibility to security threats. This deficiency may heighten the risk of social engineering attacks and security incidents. Entities should conduct regular awareness training sessions to foster a security-conscious organizational culture, thereby mitigating potential risks stemming from insufficient security knowledge among personnel.



CHAPTER THREE

ACCOUNTING SYSTEMS

3.0 Introduction

As per the Accounting Procedure Manual of 2021 (Second Version) for Ministry of Finance, the United Republic of Tanzania accounting system refers to the system implemented and followed by all government institutions in collecting, classifying, recording, summarizing, communicating, and interpreting financial information. The system aggregates all transactions in detail and other economic events involving receipt, spending, transfer, usability and disposition of assets and liabilities.

In my audit of the accounting systems, I primarily focused on evaluating the efficiency of system controls in MUSE, Epicor used by MSD, Serenic Navigator used by REA, and Sage Pastel used by TSN, Advanced Financial System used by Ngorongoro, ERMS system used by e-GA. I scrutinized key aspects such as validation and processing controls, accessibility of critical business reports, and enforcement of segregation of duties. In my audit, I noted the following anomalies:

3.1 Inadequate integration design in MUSE and revenue systems

In my assessment of MUSE and government revenue systems, I noted that the current setup only records paid bills as received from Government electronic Payment Gateway (GePPG). The current integration setup does not facilitate automatic posting of unpaid bills from revenue collection (billing) systems in MUSE accounting system, which is necessary for proper accounting of receivables. As a result, there is a reliance on manual journal entries.

I attribute this issue to the inadequate design of the integration, which did not take into account the recording of unpaid bills from revenue collection systems to corresponding accounting systems.

This dependence on manual journal entries to capture total receivables in MUSE introduces a significant risk of errors and inconsistencies. The risk in question exposes the institutions to financial inaccuracies and challenges with information integrity.

I recommend that the Ministry of Finance improve the integration between the institutions revenue systems and the accounting system (MUSE) to enable better tracking of receivables and enhance overall financial management.

3.2 Inadequate system control to manage applied exchange rates for supplier payments

Para 10.12.(Transactions and balances) of The Ministry of Finance and Planning (MoFP) Accounting Procedure Manual of 2021(Second Version) requires that foreign currency transactions be translated into local currency at prevailing exchange rates. Gains/losses from settlement and year-end translation are recognized in the statement of financial performance.

The review of MUSE General Ledger (GL) transactions at EPZA identified an issue in control over used exchange rates, leading to the application of different rates on the same date for transactions with the same bank during supplier payments. This inefficiency poses a risk inaccuracy of financial reports and potential impact on the organization's overall financial performance.

I recommend that EPZA's management in collaboration with MoF to strengthen controls in MUSE to ensure accuracy of exchange rates

3.3 Irregular Sequential Numbering

Serenic Navigator system has irregularity in the sequential numbering patterns. This is due to flaws in the sequence algorithm design. There were gaps in invoice numbering. This could lead to difficulties in tracking invoices and reconciling accounts, potentially resulting in inaccurate financial reporting.

I recommend a thorough review and enhancement of the sequence algorithm for generating purchase order numbers and invoices.

3.4 Mismatch between purchase order and requisitions quantities

The Epicor system at MSD lacks adequate controls to match purchase order quantities with corresponding requisitions. This has resulted in 287 orders having more quantities than their corresponding requisitions, and 3,137 MSD-funded purchase orders lacking corresponding requisitions. This could open up opportunities for fraudulent activities, such as the creation of inflated or unauthorized purchase orders, leading to financial losses.

I recommend management of MSD: (a) Implement robust system controls to ensure strict matching of Purchase Orders with their corresponding Purchase Requisitions; and (b) Configure system settings to restrict the creation of POs with quantities exceeding those in the purchase requisitions or to send alerts for any discrepancies.

3.5 Receiving Items without purchase and requisition orders

Epicor system at MSD has inadequate control to prevent receiving of items without purchase requisition (PRs) and purchase orders (POs). This resulted in existence of 37 items received without corresponding evidence in both PO and PR with 4 items received having a PR but not found in the PO.

This issue stems from system design deficiencies that allows receipts to be processed without corresponding requisitions and purchase orders.

The receipt of mismatched items can lead to inventory and procurement errors, causing overstocking or understocking, impacting operations and budgets. Inconsistent records among Goods Received Note (GRN), Purchase Order and Purchase Requisitions compromise data integrity and thus hampering procurement tracking and informed decision-making.

I recommend management of MSD to implement appropriate controls that restrict item number changes to authorized personnel and enforcing consistency between GRNs, POs, and requisition records to ensure the accuracy and integrity of procurement data.

3.6 Invoices raised without a Goods Received Note

The Epicor system at MSD has inadequate control that ensure invoices are raised from Goods Received Note. My review revealed the existence of invoices for 148 items raised without the GRNs. The specified GRN reference number, Purchase Order (PO) number, PO line and PO release number for these invoices were not found in the list of all GRNs. This is caused by inadequate system controls to enforce creation of accounts payable invoice based on GRN. Without a GRN to verify the receipt of goods or services, there is a risk the organization could pay for items it did not receive.

I recommend management of MSD strengthen Epicor controls to effectively match invoices with GRN such that invoices are raised based on GRN.

3.7 Mismatch between goods receiving note and purchase order

There is inadequate control within **Epicor system** to enforce matching of goods received with corresponding purchase order. This resulted in mismatch in quantity and amount whereby there are goods received with quantity greater than quantity ordered, similarly, there exist goods received that have amount greater than ordered. This is caused by inadequate system control to enforce matching of GRN with PO.

Discrepancies in GRN and PO quantities and amounts can cause financial discrepancies, impacting financial statement accuracy and potentially leading to financial losses. Over-receiving goods can lead to overstocking, impacting inventory management, storage, and increased carrying costs, affecting operational efficiency.

I recommend Management of MSD enhance system controls in Epicor to enforce strict matching of GRN with PO to prevent discrepancies in quantities and amounts.

3.8 Manual entering of payment amount

Manual entering of payment amount is practiced instead of using the purchase order amount from the system. My audit revealed that for supplier payments in **Advanced Financial System** used by Ngorongoro Conservation Area Authority (NCAA), the system fills in PO details, but the accountant manually enters the payment amount instead of using the PO amount directly. Manual entering of payments is caused by system design deficiency not to include auto-fetching of purchase orders. This lack of cross-verification for amount entered risks payments exceeding the approved PO value. Manual data entry for payments raises error risks, potentially leading to inaccurate supplier payments, discrepancies, and disputes.

I recommend that NCAA Management enhance the system to automate the extraction of payment amounts from the PO upon selection of the supplier; and for partial payments, the system should crossmatch the entered payment amount with the PO amount to avoid overpayment.

3.9 Inadequate system controls in managing staff imprest

The examination of staff imprest management has revealed the following irregularities:

a) ERMS system managed by e-GA has inadequate control in preventing the issuance of imprests to staff members who have not retired outstanding imprests.

b) MUSE allows creation of more than one payment voucher for the same imprest resulting to payment more than approved imprest amount.

The noted anomalies are caused by inadequate design of the systems which does not enforce the legal provisions which emphasizes retirement of imprests prior to issuance of new imprest.

Inadequate system controls to prevent granting of new imprests to staff prior to retirement of outstanding imprests undermine the internal controls that ensure timely retirement.

I recommend that management of MoF and e-GA enhance system control that ensures imprests are issued to only staff members who don’t have any outstanding imprests, payments do not exceed imprests and imprest payments match authorized amounts while maintaining strict adherence to approved and legitimate transactions.

3.10 Inadequate segregation of duties in payment processes

This audit identified weaknesses in the way the Ministry of Finance (MoF), Medical Store Department (MSD), Rural Energy Authority and Ngorongoro Conservation Area Authority (NCAA) manage their payment processes. Specifically, the audit found inadequate controls to enforce segregation of duties, which means that some individuals can perform multiple critical steps in the process without proper oversight which increases the risk of errors or fraud. Other issues observed are listed below:

- There were instances in MUSE where individuals could create and approve payment vouchers themselves.

- Two instances in MUSE where individuals could create and approve vendor records themselves.

- Individuals could reverse journal vouchers without review in Serenic Navigator system at REA.

- Purchase orders in MUSE lacked an assigned approver.

- Staff creating purchase orders in Epicor System at MSD did not have supervisors assigned in the system, allowing them to bypass the approval stage.

- At NCAA crucial processes including Budget adjustments, stock adjustments, and purchase/invoice reversals within the system have no approvals.

The noted anomalies are caused by inadequate requirement gathering process during the development and customization of the systems.

Lack of segregation of duties increases the risk of fraud or errors due to lack of oversight. Also, it compromises the integrity of transactions and affects accountability.

I recommend that management of Mo, MSD, REA and NCAA enhance the control design that ensure that processing of transactions incorporate segregation of duties.

3.11 Inaccurate reports and inefficient financial statement generation

The ERMS system used by e-GA generate reports with errors as detailed below:

- Discrepancies were found in cumulative expenses for specific GFS codes in the itemized report compared to actual expenditures.

- Negative opening and closing balances for food and beverages were identified in the Stock report.

This anomaly is due to inadequate review of system reports during system testing. Errors in reports can lead to misstated financial figures and misinformed business decisions.

I recommend that e-GA (a) review all reports in the ERMS report module in collaboration with user departments, and (b) Ensure the accuracy of database queries generating reports.

3.12 Manually generated financial statements

Key financial statements like the statement of financial position, statement of performance and cash flow statements are not automatically generated by the Serenic Navigator accounting system used by REA.

The noted anomaly resulted from a lack of proper user requirement specification during system implementation. Manual preparation of financial statements increases the risk of errors and reduces efficiency.

I recommend that REA (a) emphasize and prioritize using the Serenic Navigator system for preparing financial statements; and (b) Explore customization options to automate the generation of key financial statements.

3.13 Inadequate Integration between MUSE and HCMIS

There were differences found in net salary and statutory deductions between HCMIS and MUSE. The noted anomaly leads to inaccurate financial statements.

I recommend that MOF implement data integration improvements to ensure synchronization of payroll information between HCMIC and MUSE.

3.14 MUSE allows overspending beyond Allocated Budget

The system allowed exceeding the approved budget because expenditures paid directly by MoF on behalf of other entities were not automatically reflected, creating an artificially inflated available balance allowing entities to spend more than the exchequer's approved amount. Also, the budget allocated for salaries and wages was used for unauthorized construction expenses, compromising financial management and reporting.

I recommend that MoF: (a)enhance MUSE to automatically recognize all MoF payments, preventing overspending; (b) strengthen system controls to prevent misclassification of expenditures and enforce proper budget allocation.

3.15 Deficiencies in dummy salary accounting in MUSE

Dummy expenses were entered directly through the general ledger window, bypassing required authorization and potentially masking fraudulent activity.

Also, dummy salaries for some months were not posted in MUSE, leading to misstated financial statements. This was due to manual posting of dummy salary in MUSE instead of having MUSE automatically post in General Leger after payment of the salary paylist.

I recommend that MoF must: (a) redesign the adjustment window in MUSE to restrict unauthorized posting of dummy expenses; and (b) automate dummy salary posting to ensure accurate financial reporting.

3.16 Inappropriate system usage

My audit identified several instances of inappropriate system usage in various government entities, raising concerns about financial transparency, accountability, and process integrity.

a) **Ministry of Finance**

Bypassing Purchase Orders: Payments for stock items were posted direct to the general ledger without purchase orders and GRN, potentially circumventing procurement controls within the system.

I recommend that the MoF implement controls to prevent using the normal voucher window for payments requiring purchase orders.

b) **Ministry of Livestock and Fisheries - Fisheries sector**

- **Manual Revenue Generation:** Automated bills totaling over TZS 1.4 billion were generated manually through the "miscellaneous" module, raising concerns about efficiency and potential misuse.
- **Lack of Permit Tracking:** Permits and licenses paid for through the "miscellaneous" module were not tracked within the system, raising compliance and data accuracy concerns.

I recommend that the Ministry of Livestock and Fisheries to restrict the use of the "miscellaneous" module for automated bills and monitor system usage for compliance.

c) **Tanzania Medicines and Drugs Authority (TMDA)**

Manual Bill Generation: Bills suitable for automatic processing were created manually in the non-automated module, lacking proper approvals and potentially leading to revenue loss.

I recommend that TMDA strengthen oversight to ensure proper use of the system and adherence to established procedures.

3.17 Late transaction posting in MUSE System

My audit revealed a weakness in MUSE related to late transaction posting. The system allowed 827 transactions to be posted after the designated deadline of the 15th of the following month without approval, ranging from 3 days to 4 months late. These late postings lacked evidence of proper approval.

This weakness resulted from inadequate system controls to validate and approve the posting date. The noted discrepancy compromised integrity of financial reporting due to unreliable data in the General Ledger.

I recommend that MoF strengthen system controls by implementing validation checks to enforce the posting deadline of the 15th of the following month and prevent unauthorized late postings.

3.18 Unauthorized access and activity in financial system

My audit revealed a serious security breach in the financial system of the Rural Energy Agency (REA). An unauthorized individual gained access to the system and used it to create invoices and payment vouchers. This individual lacked proper accounting expertise and bypassed established authorization procedures. The noted anomaly resulted from inadequate access controls and user role management.

This has an impact to increased risk of fraud due to unauthorized access and transactions. Also, there is potential inaccuracies in financial records due to the user's lack of expertise.

I recommend that REA (a) grant access to financial systems based on the "principle of least privilege," meaning users should only have the minimum access level required for their job duties; (b) ensure employees understand their roles and responsibilities, including proper data handling procedures; and (c) separate the tasks of initiating, authorizing and recording financial transactions to minimize the risk of unauthorized activity.

3.19 Manual transfer of unspent balances in MUSE

The Bank of Tanzania (BoT) system automatically transfers unspent balances from the Treasury Single Account (TSA) to the Consolidated fund (CF) at the end of the fiscal year (30th June). However, MUSE requires manual data entry to reflect this transfer in the TSA Cash Book.

The impact of this manual entry is that: (a) it increases processing time and effort; (b) it is prone to errors, potentially impacting the accuracy of financial records; and (c) inconsistencies between systems can raise concerns about the reliability of financial data.

I recommend that MoF management should prioritize enhancing the MUSE system to automate the transfer of unspent balances, eliminating the need for manual data entry.

3.20 Absence of data migration at Tanzania Meteorological Authority (TMA)

My audit revealed that TMA has not migrated data from their old accounting system (Epicor) to the new Government Payment System (MUSE). This is due to the absence of a formal data migration plan.

Lack of migrated data can lead to inaccurate financial information in the new system.

I recommend that Tanzania Meteorological Authority (TMA): (a) outline the process for moving data from Epicor to MUSE, ensuring adherence to e-Government guidelines; and (b) implement the plan to migrate the necessary data from the old system to the new one.

CHAPTER FOUR

REVENUE SYSTEMS

4.0 Introduction

This chapter identifies opportunities for improvement in Tanzania's government revenue collection systems. It focuses on weaknesses observed across various entities. These weaknesses contribute to revenue loss, operational inefficiencies, and potential non-compliance with regulations. This report outlines specific recommendations to address these critical issues.

4.1 Fisheries Export Permits Issued without payment

A review of the FiRCIS system implemented by the Ministry of Livestock and Fisheries revealed an instance where an export permit was issued without the required payment being received. This was attributed to a system malfunction. This incident highlights the potential for loss of revenue to the government if proper controls are not in place to ensure payments are collected before permits are issued.

I recommend that management of the Ministry of Livestock and Fisheries (fisheries sector) conduct regular reviews to identify and address technical glitches, system errors and unauthorized staff actions while ensuring strict oversight and staff training to maintain the system's integrity and security.

4.2 Students admitted without application fees

In Online Application System (OAS) implemented by The Open University of Tanzania (OUT) there were 50 applicant records with a total fee of TZS 500,000 which had duplicated control numbers (bills). This means that, payment for one control number could settle the application fee of the other applicants.

Similarly, in SARIS implemented by Open University there were 40 student records with total exam fee of TZS 1,670,000 and 71 student records with a total tuition fee of TZS 20,455,500, which had duplicated payment receipt numbers.

The anomaly is caused by inadequate validation controls in SARIS; and online admission systems allow for the duplication of payment control and receipt numbers, coupled with a lack of integration between GePG and SARIS. The noted anomalies can result in the loss of government revenue.

I recommend that OUT management (a) enhance the validation controls in its billing systems to prevent the duplication of control and receipt numbers; and (b) follow up on the noted payment deficit to ensure that the required payments are settled accordingly.

4.3 Multiple receipt generation from single payment

In the **Sage Pastel** implemented by TSN, the system allows a single payment to be used to generate multiple receipts and clear various customer invoices, falsely indicating that they have been paid. The weakness stems from a system design and implementation deficiency which do not prevent tampering with payments.

I recommend that TSN management integrate with GePG for automatic updates and acknowledgment of payments and that they enforce the association of a payment with a single, specific invoice, which would enhance the system's capacity to prevent erroneous or fraudulent activities related to payment processing.

4.4 Manual calculation in updating VISA charges

The immigration e-services implemented by Immigration Department requires manual calculation of new VISA fees by the accountant upon changes in visitor details, introducing the risk of errors. This was caused by inadequate system design which does not accommodate the process for updating visitors' VISA details.

The manual computation and entry of the bill amount by the accountant introduce the potential for miscalculations, introduces a risk of errors and inconsistencies in the corrective billing process.

I recommend management of Immigration Department to implement automation within the system to establish additional fee amount when individuals have paid for an incorrect visa type.

4.5 Duplicate transactions in RRIMS

The RRIMS system implemented by LATRA records single transactions multiple times, leading to an inaccurate representation of revenue collected. This gives the impression that the system has collected more than the actual paid amount.

This is caused by an inadequate system design that permits the duplication of billing transactions. Duplicate transactions can lead to financial discrepancies, potentially causing incorrect billing, payments, and financial reporting.

I recommend LATRA's management to enhance the RRIMS system to prevent the occurrence of duplicate transactions; and perform time-to-time review and monitoring to ensure such anomalies do not appear again in the future.

4.6 Unpaid compound fines in RRIMS

There were 32 offenses issued in 2022/23 where paid amount was less than billed amount indicating unpaid fines and potential loss of government revenue. This anomaly stems from insufficient system design controls regarding the alignment of billed and paid amounts.

I recommend that LATRA's management enhance the RRIMS system by implementing controls that ensure the paid amount matches the billed amount accurately.

4.7 Inadequate offline collections controls in TAUSI MIS

The TAUSI system lacks control over offline collections through Point of Sale (PoS) devices. No limits are set for offline float amounts or timeframes, allowing excessive offline collection of revenue and prolonged offline operation. The anomaly arises due to lack of guidance on maximum allowed offline float amounts and timeframes resulting to non-consideration of limits during system design.

I recommend that PORALG establish comprehensive guidelines for limitation of offline float amount and timeframe, enhance the system to accommodate requirements of the guidelines.

4.8 Manual bill generation in TAUSI

TAUSI does not generate bills automatically for banking processes. Bills are manually created by collectors or revenue accountants, leading to potential delays in bill generation and untimely revenue collection.

The detected anomaly is a result of an insufficient system design that denies automation of bill generation process.

I recommend management of PORALG to automate bill generation in TAUSI by developing and integrating an automated bill generation feature within the system.

4.9 Synchronization Issues between billing systems and GePG

TMDA's RIMS and TPA's TOS billing systems lack controls for validating transaction synchronization with the Government electronic Payment Gateway (GePG). This resulted in the status of 20 cancelled invoices from RIMS and 132 from TOS not reflecting in the GePG. As a result, active control numbers persisted, allowing payments for cancelled invoices. The noted weakness could result in financial discrepancies between the billing systems and MUSE.

I recommend managements of TMDA and TPA implement validation controls and establish routine monitoring to ensure seamless synchronization of transactions between the TOS and RIMS billing systems with the GePG system.

4.10 Product registration billing process prone to errors due to manual input

The product registration billing process is only partially automated, requiring manual input for cost categories and subcategories, increasing the risk of errors and inaccuracies. The root cause of this anomaly lies in the deficiencies in the specification and implementation of system requirements.

I recommend that TMDA management implement a fully automated process for determining cost categories and subcategories in compliance with the TMDA fees and charges regulation.

4.11 TAUSI System fails to prevent PoS collections beyond assigned float

TAUSI MIS System does not adequately control PoS devices, allowing them to collect more than their assigned float amount. This has resulted in 114 PoS devices recording transactions exceeding their assigned floats, contradicting the system's design where revenue collection transactions should deduct from the assigned float. This anomaly arises from insufficient system design, rendering the system unable to effectively monitor and control the devices collections against the assigned float amount. This weakness significantly impacts financial reconciliations, making it challenging to accurately track and manage revenue collected through the POS devices.

I recommend that the President's Office Regional Administrations and Local Governments (PORALG): (a) review and rectify the noted instances of PoS having recorded transactions more than their assigned floats; and (b) enhance the system to ensure that the devices cannot transact more than assigned float amount.

4.12 Inaccurate sewerage tariffs in MAJI IS

MAJI IS at MWAUWASA lacks controls to verify configured tariffs against approved tariffs. This resulted in incorrectly configured sewerage tariffs for residential (domestic) customers. This is due to inadequate levels of review during configuration of approved tariffs in the application system. Incorrect sewerage tariffs in the system results in a misstatement of revenue and overcharging of residential customers.

I recommend that MWAUWASA (a) review all tariffs configured in MAJI IS and ensure they are consistent with the approved tariffs; and (b) establish system configuration change management procedures to set control to ensure accurate and authorized changes of tariffs configurations in the system.

4.13 Missed billings and revenue loss in MAJI IS System

A review of the MAJI IS billing system identified weaknesses in handling different customer statuses, leading to missed billing opportunities and revenue loss as follows.

Unbilled active customers: firstly, the system failed to bill 539 active customers with the "no reading" status in June 2023. These customers, despite having no recent meter reading, were not billed based on their average consumption from the previous three months.

Unbilled meter status "Unknown": secondly, the system malfunctioned for customers with an unidentified meter status ("unknown"). This resulted in unbilled water consumption totalling 8,397 cubic meters, incurring a revenue loss of TZS 11,839,770.

Unbilled sewer service: customers who were reconnected to sewer services consumed 54,748 cubic meters of sewage but were not billed due to an error in parameter settings. This oversight led to a revenue loss of TZS 29,748,003.

Furthermore, a similar anomaly was identified in the DAWASA, where the MAJI IS system malfunctioned for customers with specific meter statuses:

Stack meters: The system failed to accurately calculate charges for customers using stack meters.

Closed gates: The system did not account for customers with closed gates, potentially leading to inaccurate billing.

No readings status: Similar to the issue identified in the broader review, 98 active customers with "no reading" status were not billed based on average consumption, resulting in an uncharged amount of TZS 2.92 million.

I recommend that MWAUWASA and DAWASA should address the identified weaknesses within the MAJI IS billing system to ensure proper handling of various customer statuses and prevent further revenue loss.

4.14 MWAUWASA billing system Issue with meter readings

MAJI IS system, used by MWAUWASA has a flaw in its logic for handling reconnections. When a customer's water service is reconnected, the system uses the meter reading on the reconnection day as the "previous reading" instead of the actual previous reading before disconnection. This has resulted in incorrect billing for 1,295 customers.

I recommend that MWAUWASA: (a) conduct a thorough review of meter readings to identify all affected customers; (b) recalculate bills for affected customers based on their correct water usage; and (c) update customer

statements and financial statements to reflect the corrected billing information.

4.15 Registration fees not configured in TMA Integrated Weather Portal

The TMA Integrated Weather Portal being used by Tanzanian Meteorological Agency (TMA) is not configured to collect registration fees from meteorological stations. This is due to inadequate management of charges within the system. This anomaly can lead to incorrect charges related to meteorological services.

I recommend that TMA add the missing registration fees for meteorological stations to the TMA Integrated Weather Portal.

4.16 Overcharging of new fishing and fishing vessel llicenses in FiRCIS

The Fisheries Revenue Collection Information system (FiRCIS), used by Ministry of Livestock and Fisheries-Fisheries sector, cannot distinguish between new and renewal applications for licenses. As a result, the system applies a 50% penalty fee to new licenses, mistakenly treating them as late renewals.

This is caused by inadequate system design lacking distinction between new and renewal applications. Applying a 50% penalty fee to new license results in overcharging, potentially discouraging new entrants to the fishing industry and placing an undue financial burden on new licence holders.

I recommend that the Ministry of Livestock and Fisheries-Fisheries Sector enable the FiRCIS system to distinguish between new and renewal applications.

4.17 Inefficiencies in SBMS resulting in uncollected revenue

Shipping business management System (SBMS) fails to automatically charge commission and compounded interest on late payment of levy bills, leading to a loss of government revenue. Specifically, the system has the following deficiencies:

- **Uncharged commission**: the system missed charging commission on 53 late bills, totaling TZS 361,353.22.

- **Incorrect interest**: 165 customers who didn't pay bills on time were supposed to be charged a 10% monthly compound interest, but the system failed to charge them.

These inefficiencies stem from the system's reliance on manual intervention for imposing commission and interest. This manual process is susceptible to errors and inconsistencies.

I recommend that TASAC enhance the SBMS application to automatically charge interest and commission on the due date, eliminating the need for manual intervention and ensuring all applicable charges are levied.

4.18 Unauthorized Licensing and System Failure to Differentiate Cargo from Packages

There were two weaknesses in control systems that allowed the issuance of licenses and parcels exceeding established weight limits.

The **Fisheries Special Licenses System**, which is responsible for issuing fishing products special licenses, failed to prevent the issuance of 14 licenses which exceeded the 7-kilogram limit mandated as per the 2009 Fisheries Regulations. This breach violates regulations.

The **ATCL Cargo Management System** allowed the entering of 2,591 parcels exceeding the 16-kilogram weight limit established by their policy. This resulted in incorrect charges being applied, violating the company's management guidelines. Both instances stem from the same root cause: ineffective validation of product weight.

I recommend that:

a) **The Ministry of Livestock and Fisheries (Fisheries Sector) strengthen the validation process for special license applications to guarantee that quantities do not exceed the 7-kilogram limit during the submission stage.**

b) **ATCL reinforce the validation process within the cargo management system to prevent parcels exceeding 16 kilograms from entering the system altogether.**

4.19 Overcharging and inconsistent billing in license renewals

The GLICA System, used by the Gaming Board of Tanzania had several control weaknesses impacting the billing process for license renewals. Specifically, my audit revealed the following:

Non-standard charges: In the first instance, 2,108 licenses were renewed with charges deviating from the system's prescribed rates; and in the second case, 1,163 licenses issued to both key and support employees were charged differently from the standard rate.

Incorrect penalty billing: 742 penalty payments for late renewals resulted in overcharges totalling TZS 379,320,125.

These anomalies stem from incorrect configurations of the license renewal formula within the GLICA System.

These anomalies led to: (a) licensees paying more than intended for renewals and penalties; (b) lack of adherence to established fee structures; and (c) incorrect billing potentially leading to undercharged fees.

I recommend that the Gaming Board of Tanzania takes immediate action to review and rectify the GLICA system configurations to correct errors contributing to the overcharging of penalty fees and to ensure that all renewed licenses are charged according to prescribed rates.

4.20 Inadequate segregation of duties in the revenue systems

My audit of revenue systems used by TASAC, TPA, TMDA, and LATRA revealed inadequacies related to enforcement of segregation of duties in billing process workflow.

The review identified instances where the same individual held both creation and approval roles for various processes:

- **for 2,398** certificate applications through **MASSEMS** at TASAC, **the same person acted as creator and approver.**

- **another 6,432** certificate applications at TASAC through **SBMS also involved same person.**

- **It was the same experience with 152 invoices** in **TOS** application at TPA**.**

- **This was also the case for PSV license applications** through RRIMS at LATRA where the **same person played the role of verification and approval.**

- **so too were clinical trial certificates** through **RIMS** at TMDA**.**

This lack of clear separation of duties is attributed to inadequate validation controls when granting user access rights.

This situation increases the tendency of individuals having excessive access privileges, potentially compromising the security and integrity of the applications. This could lead to potential misuse or mishandling of sensitive data.

I recommend that TASAC, TPA, TMDA, and LATRA take action to enhance MASSEMS, SBMS, TOS, RIMS and RRIMS systems to enforce segregation of duties, so that no single individual can both create and approve applications or documents.

4.21 Ineffective validation controls

In my audit of information systems used by PORALG, LATRA and TSN, it has revealed inadequacies related to validation of payment and data entry. The review identified the following shortfalls:

- In the iCHF-IMIS System used by PORALG, 89 and 314 members in Kigoma and Arusha regions, respectively, were activated without payments which enables them to continue using health services without completing the renewal/payment process. Additionally, there were 739; 13,209; 42,803; 1,783 and 1,366 CHF-enrolled members in Arusha, Dar es Salaam, Dodoma, Kigoma and Mbeya, respectively who had validity periods that exceeded 12 months.

- The RRIMS System used by LATRA issued 32 short-term permits with incorrect expiry dates which resulted in their being mistakenly considered valid.

- The circulation system used by TSN lacked a validation mechanism for declared returns. This allowed officers to enter return quantities exceeding allocated amounts, potentially impacting both invoicing and commission calculations.

- In FiRCIS used by the Ministry of Livestock and Fisheries's Fisheries Sector, I found three instances where the system permitted a single license to be used to request permits for two different exporters/companies. This enabled unauthorized permit requests leading to revenue loss of USD 800 for the government.

- In the e-visa system used by the Immigration Department, I identified 11 instances where the same individual was issued two visas with different numbers, but with the same validity period and visa type.

- In the Online Registration System (ORS) used by TIRA, I observed 35 instances where a single license certificate was issued to multiple insurers, resulting in a financial loss of TZS 55,775,000 due to undercharging.

- In Tanzania National Business Portal systems used by BRELA, 6 duplicated business license numbers were assigned to distinct lines of businesses.

I recommend that the managements of PORALG, LATRA, TSN, the Ministry of Livestock and Fisheries, BRELA, the Immigration Service Department and TIRA strengthen system validation controls to ensure proper data entry and process validation. Additionally, PORALG should specifically review and update membership status within the system to ensure it accurately reflects the corresponding payment contribution.

4.22 Ineffective system verification controls

My audit of information systems used by the Ministry of Works, TMDA, Ministry of Agriculture, OUT and TSN, revealed deficiencies related to the configuration of verification controls. The review identified the following shortfalls:

- The Agricultural Trade Management Information System (ATMIS) used by the Ministry of Agriculture fails to verify the billed amount against the configured currency rates. This results in inaccurate charges because the system accepts all amounts as valid, regardless of the currency used for payment. Consequently, the Ministry undercharged fees totaling TZS 2,005,000.

- In the SARIS System at The Open University of Tanzania, 27 undergraduate and 6 postgraduate student records for the 2022/23 academic year were absent from their respective applicant lists. This led to the admission of ineligible students and potential financial losses due to non-payment of admissions fees.

- In the circulation system utilized by TSN, discrepancies in invoicing were noted, involving both over-invoicing and under-invoicing of newspapers. This issue arises from inadequate system design permitting unauthorized discounts and manual invoice amount input. The total over-invoicing amounts to TZS 45,183,960, while under-invoicing totals TZS 1,092,865.

I recommend that:

(a) The management of MOA enhances ATMIS System controls for verifying billed amounts.

(b) The management of OUT enhances SARIS controls over students' application, selection and admission process to ensure that only eligible students who have applied are admitted.

(c) The management of TSN enhances circulation system controls by verifying the input of returned newspapers beyond allocated limits and introducing an approval functionality for the reported quantity of returned newspapers.

4.23 Anomalies noted in system computations

My review of FiRCIS at Ministry of Livestock and Fisheries' Fisheries Sector, and MAJI IS at MWAUWASA and DAWASA, to assess system computations noted the following:

- In FiRCIS System, I noted inadequate change management of system parameters, particularly in the configured exchange rates and export royalty fees per fisheries products that resulted in incorrect computations of permit fees. This has been caused by inadequate system design that did not consider the implementation of input validation. This resulted in 20 export permits being undercharged, amounting to TZS 510,800, and six export permits being overcharged, amounting to TZS 55,700.

- In MAJI IS System used by MWAUWASA, 1,994 active customers experienced inaccurate computations for sewer bills, resulting in a revenue loss of TZS 22,952,882. Moreover, at DAWASA, 870 customers had their meters replaced without payment, resulting in unpaid charges totaling TZS 43,450,000. Additionally, the system lacks controls to prevent new connections from being activated without full payment, leading to outstanding balances totaling TZS 1,915,536,123.06 between September and June.

I recommend that the management of the Ministry of Livestock and Fisheries' Fisheries Sector implement change management controls to manage configuration changes for export royalty fee computation. Additionally, MWAUWASA and DAWASA should collaborate with the Ministry of Water to enhance the MAJI IS System for accurate billing. Furthermore, they should strengthen controls to ensure proper approval of meter replacements and verification of payments for new connections while taking measures to recover outstanding debts from customers.

4.24 Absence of key-generated system reports

My review of MASSEMS, M-BILL, Integrated Weather Portal, ORS, and WIMS noted that the systems do not generate key reports. The missing reports are explained below:

- The MASSEMS system utilized by TASAC lacks revenue collection report, issued licenses report, applications report and registered vessels report.

- M-BILL system used by TASAC lacks a licensed services provider report, revenue collection report, shipping report, levy quarterly report, border shipping report, reports for agencies/companies changing names and monthly report of manifests.

- Integrated Weather Portal system used by TMA lacks key reports such as a list of registered weather stations, list of issued permits for meteorological services and a register of all stakeholders (miners, contractors, agriculture and maritime) requesting meteorological packages from TMA.

- Online Registration System utilized by BRELA lacks an in- built report for clients’ unpaid annual maintenance fees.

- CIMIS system used by Contractors Registration Board lacks a summary report detailing the total inspections conducted within a specific time frame, including project regions or zones.

- WIMS System used by OSHA lacks a report for workplaces and projects that were not billed for ergonomic and general inspections during the registration process.

These shortcomings have been caused by inadequate user requirement gathering during the initial stage of system development. I am concerned that the noted anomalies hinder management's ability to access real-time information essential for making informed decisions.

To address the noted shortfalls, I advise the management of TASAC, TMA, BRELA, CRB and OSHA to gather, review and implement key system reports that will enhance visibility and decision-making.

CHAPTER FIVE

HUMAN RESOURCE AND PAYROLL SYSTEMS

5.0 Introduction

Human Resource and Payroll Systems automate workforce management tasks, including employee data management and payroll processing. Leveraging these systems helps government entities improve efficiency, compliance with regulations, data accuracy and resource allocation.

In my audit of the Human Resource and Payroll Systems, I primarily focused on evaluating the efficiency of system controls in HCMIS, Microsoft Navision used by Tanzania National Parks Authority (TANAPA) and SAGE PASTEL used by ATCL. I scrutinized key aspects such as validation and processing controls, deduction of employee salaries, promotion, and demotion of employee but also enforcement of separation of duties in payroll processing. In my audit, I noted the following defects:

5.1 Inadequate controls for minimum salary threshold

My review of HCMIS and Microsoft Navision revealed inadequate controls to prevent staff from earning less than one-third of their basic salary after deductions. This resulted in employees falling below the threshold in each system, respectively. Inaccurate deductions could lead to non-compliance with labour laws and regulations, potentially resulting in legal and financial consequences.

I recommend that President's Office Public Service Management and Good Governance (PO-PSMGG) and TANAPA management enhance system controls to ensure deductions are reasonable and comply with regulations.

5.2 Payroll deduction errors in Sage Pastel System

My review of the Sage Pastel System used by ATCL identified weaknesses in payroll deductions. 10 staff had their Social Security Fund (SSF) deductions exceeding 5%, 3 staff members had discrepancies in their Higher Education Students Loan Board (HESLB) deductions of salaries below the mandated 15% for some, while others were above the threshold. Another 112 employees lacked the required National Health Insurance Fund (NHIF) deductions. This was caused by insufficient system design controls that were unable to ensure deductions are accurately applied according to regulations.

Excessive Social Security Fund deductions can strain employees financially and lead to legal issues. HESLB misapplications can disrupt loan repayment hence affecting staff finances. The absence of NHIF deductions risks employee health coverage and well-being.

I recommend that ATCL Management should: (a) enhance system controls for payroll deductions, implementing validation checks and ensure accurate application of deduction rates for Public Sector Social Security Fund (PSSSF), HESLB and NHIF; and (b) perform regular reviews and reconciliations of their payroll to maintain ongoing compliance and accuracy in the deduction process.

5.3 Segregation of duties' weakness in HCMIS

The audit of HCMIS system revealed a lack of approval functionality for changing employee date of birth and amending personal emolument (PE) budgets. Only one user from PO-PSMGG can alter these details.

This was caused by insufficient system design which failed to incorporate appropriate approval workflows. A single user performing critical HR tasks increases the risk of undetected errors and unauthorized activities.

I recommend that PO-PSMGG Management enhance the system by incorporating a structured approval workflow for managing changes to employee date of birth and PE budget verification.

5.4 Promotion and demotion management issues in HCMIS

My review of the HCMIS System identified weaknesses in managing staff promotions and demotions which resulted in:

- 487 employees experienced grade progression deviation during the normal promotion process.
- 248 employees lack records specifying the grade from which they were promoted.
- 20 employees promoted without meeting the minimum three-year tenure requirement.
- 10 demoted employees whose salaries remained unchanged.

This was caused by the system lack of controls for enforcing minimum tenure requirements and ensuring salary adjustments after demotions. Inadequate management of promotions and demotions leads to financial losses due to incorrect payment of salaries.

I recommend that PO-PSMGG's management should enhance the HCMIS system by implementing: (a) an automated workflow that triggers salary adjustments upon demotion approval (b) controls to restrict and validate normal promotions, preventing ineligible individuals from being promoted and skipping salary grade steps.

5.5 Inaccurate calculation of extra duty charges

A review of the system used to process extra duty requests (MIS application) found errors in how it calculates the charges for 26 requests. These errors caused the system's calculated amounts to be different from the results I obtained when I recalculated them.

This was caused by the ineffectively designed calculation logic, which led to both overcharging and undercharging of extra duty payments. Errors in calculating extra duty payments have led to financial issues for both employees and the organization.

I recommend that the Roads Fund Board automate the controls for calculating extra duty weekend days to ensure accurate calculations.

5.6 Staff loan exceeding a limit of TZS 1,000,000

My review of loans issued to TANAPA staff identified 19 employees who received loans exceeding the TZS 1,000,000 limit set by regulations. The system lacks controls to prevent loan issuance above the prescribed limit due to insufficient requirement gathering and design.

Exceeding the loan limit could disrupt budget planning and allocation, potentially depriving other eligible staff members of loans.

I recommend that TANAPA enhance system controls to restrict loan issuance to staff members above the specified limit.

5.7 Leave management system weaknesses

My review identified weaknesses in leave management systems across different organizations:

- **HCMIS:** 34 employees on unpaid leave were mistakenly included in the payroll and received salaries.

- **ERMS (e-GA):** The system allows leave accumulation exceeding two years, contravening regulations. I found 153 employees with accrued leave exceeding the limit.

- **PMIS (TPC):** I observed incorrect tracking and calculation of leave durations.

This was caused by deficient system design which failed to ensure leave management aligns with regulations.

These weaknesses resulted in: (a) incorrect payroll disbursements to employees on unpaid leave; (b) accumulation of leave exceeding the two-year limit; and (c) inaccurate tracking and calculation of leave durations.

I recommend that PO-PSMGG, e-GA and TPC collaborate to enhance the leave functionality in HR management system. This includes: (a) automatically excluding employees with approved unpaid leave from payroll; and (b) accurately tracking and calculating employee leave days according to public service standing orders.

5.8 Duplicate check numbers and form four index numbers in HCMIS

My audit of HCMIS identified weaknesses in employee data validation:

a) Some employees have been assigned multiple check numbers, which may lead to confusion or errors in processing payments.

b) 238 employees share the same form four index number.

This was caused by inaccurate and ineffective validation of employee details during the hiring process. Duplicate data compromise's reliability and hinders accurate identification of individual employees.

I recommend that PO-PSMGG enhance the system's logic and validation mechanisms to: (a) restrict the assignment of multiple check numbers to the same employee; (b) integrate with National Examinations Council of Tanzania (NECTA) system for verification and validation of new employee form four index numbers.

5.9 Computer system analyst performing HR officer duties

My review identified that the principal computer system analyst, instead of the designated human resource officer, was updating personal user details in the Management Information System (MIS) database.

The reason is likely due to either an inadequate data migration plan or insufficient HR staff. This deviation from protocol raises concerns about data accuracy and accountability within the system.

I recommend that the Roads Fund Board establish a formal procedure for granting and revoking access rights to staff performing duties outside their designated departments.

CHAPTER SIX

APPLICATION SYSTEMS ADMINISTRATION

6.0 Introduction

System administration encompasses tasks like user account management; access control; security implementation and troubleshooting; ensures the efficient and secure operation of application systems within an organization.

This review of application system administration controls identified the following key findings from the audit conducted within various government entities: excessive privileges granted to ICT officers; deviations from protocol in the performance of duties; and uncontrolled access of vendors to system servers and databases.

6.1 Excessive powers to ICT officers

My recent audit of various government institutions revealed widespread concerns regarding excessive powers granted to Information and Communication Technology (ICT) staff. These findings highlight a critical security risk, potentially compromising data integrity and operational efficiency.

Here are specific examples identified by the audit:

- The evaluation of TMDA's Regulatory Information Management System (RIMS) highlighted that ICT staff have excessive powers enabling them to bypass crucial stages, like invoicing and approval, during product registration and certificate generation thereby facilitating direct application submission to the final stage.

- In NSSF's Bridge Collection Management System (BCMS), ICT officers have been granted excessive powers which has enabled them to create and cancel bills, as well as register vehicles, actions which go against their defined roles.

- Nine ICT staff at PORALG were assigned finance roles in TAUSI system which would enable them to misuse that privilege.

- ICT officers designated for ERMS System knowledge transfer and technical support at e-GA were assigned business roles, covering areas such as accounting, procurement and fleet management in the live instead of test environment.

- A computer system analyst entered employee details into the Management Information System (MIS) used by the Roads Fund Board, instead of the human resource officer.

The anomalies are caused by inadequate access control and a lack of segregation of duties. This leads to process inefficiencies, potential data discrepancies, security risks and financial consequences.

I recommend that management of e-GA, PORALG, NSSF, TMDA and RFB re-assess and define the ICT staff excessive privileges to align with their roles.

6.2 Back-end adjustment of the penalties by the database administrator

Penalties collected through the Railway & Road Information Management System (RRIMS) cannot be paid once the control number expires. The only option is to pay through a new control number manually generated in a separate system called the GePG Generic portal. However, RRIMS is not linked to the GePG Generic portal to automatically update the status of the penalty as paid. To finalize the payment, a database administrator needs to update the status of the original (expired) control number in the RRIMS back-end to "paid."

This process poses a risk of unauthorized and unpaid transaction adjustments by the database administrator without compensating controls such as approval mechanisms or regular activity reviews.

I recommend that the managementof LATRA:

(a) enhance the RRIMS system to automatically regenerate control numbers for late payment of offenses. This will streamline the payment process and eliminate the need for the database administrator to make back-end adjustments.

(b) regularly review and monitor the actions performed by database administrator accounts to ensure adjustments are no longer made through the back end.

6.3 Uncontrolled vendor access in Subsidy Management Systems

The review of Tanzania Fertilizer Regulatory Authority (TFRA)'s Subsidy Management System found that the vendor retains uncontrolled access to servers and databases, which is contrary to regulations and creates data security risks. Additionally, TFRA's ICT officers cannot even extract data due to insufficient access, highlighting the potential for unauthorized access or breaches.

The vendor's uncontrolled access to the live server and database creates a significant risk that data could be copied, disseminated or misused by the vendor or its employees.

I recommend that TFRA: (a) revoke the vendor's access to the production server and database; and (b) identify and document all accounts with access to the production server and database.

6.4 Access controls inefficiencies in Cargo Management System

A review of ATCL's cargo management systems noted that ATCL has no access to modifying currency exchange rates and user account creation which results in reliance on email communication with vendors who update these rates on behalf.

This has been caused by inadequate access management which did not consider handing over these functionalities to ATCL management. This weakness results in operational inconveniences, leading to delays in updating the exchange rate and user account creation.

I recommend that the ATCL board review the service level agreement (SLA) with the vendor and ensure that functionalities, including exchange rate updates and user account creation, are under ATCL's control.

CHAPTER SEVEN

SYSTEMS OPTIMIZATION AND PROCESS AUTOMATION

7.0 Introduction

Achieving operational excellence in the public sector necessitates a rigorous evaluation of ICT system implementation and strategic process automation. This chapter delves into the current state of automation within various government entities, focusing on the level of system integration, effective technology utilization and the transformative potential that optimized ICT systems and automation offer for the audited public sector entities.

7.1 Lack of integration between billing systems and GePG

My review of business process flows identified integration issues with the Government electronic Payment Gateway (GePG) in several entities:

- **Universal Communications Services Access Fund (UCSAF):** The SAGE Evolution application in use lacks integration with GePG, potentially leading to inaccurate bill amounts.

- **TMA:** The Integrated Weather Portal is not integrated with GePG, necessitating manual billing through a generic portal, which increases the risk of errors.

- **TSN:** Despite implementing automation systems like Circular and ePaper, bills are generated through the generic GePG portal due to its lack of integration with the GePG platform. Additionally, the e-paper system is integrated with Selcom as a payment gateway, contradicting the purpose of GePG and potentially reducing transparency in government revenue collection.

Furthermore, SARIS at Open University of Tanzania, lacks integration with GePG, requiring manual bill generation for fees. Discrepancies were found between SARIS and GePG generic portal, with 20 examination fees and 34 tuition fees recorded in SARIS but missing from GePG.

7.2 Discrepancies Identified in GePG integration with billing systems

My audit of the GePG integration with various billing systems identified discrepancies in recorded payments:

- **Posta Kiganjani:** The system displayed inconsistencies in payee details and duplicated control numbers, leading to potential revenue loss and challenges in financial reporting.

- **RIMS:** Transactions totalling TZS 1,729,407 had lower amounts recorded in GePG compared to RIMS, while others totalling TZS 920,000 had higher amounts in GePG.

- **RITA:** 526,115 bill records were found in GePG but missing from RITA's billing system, while conversely, 114 bill records were present in RITA's system but absent in GePG.

- **Law School of Tanzania:** A comparison of GePG and MUSE Cashbook records revealed transactions with different amounts, with a total difference of TZS 115,644,139 between the two systems (TZS 3,092,299,998 recorded in GePG and TZS 3,207,944,137 in MUSE).

7.3 Lack of system integration

This report examines a critical issue plaguing various government entities on the United Republic of Tanzania caused by lack of integration between different application systems. This deficiency hinders efficiency, data accuracy and financial transparency which potentially may lead to errors, discrepancies, and even financial losses.

The report delves into five key areas where a lack of integration poses significant challenges:

- **Management systems and accounting systems:** This section highlights the inefficiencies caused by the disconnect between systems used for managing core processes and the accounting system responsible for finalizing payments.

- **Billing systems and accounting systems:** This section examines the manual data transfer required due to the absence of integration between billing systems and the central accounting system, leading to a risk of human error and inaccurate reporting.

- **Billing systems and business management systems:** This section analyzes the challenges arising from the lack of integration between billing systems and systems used for managing business processes, affecting tasks like verification and validation.

- **Accounting system and banks:** This section highlights the risk of discrepancies between approved payments and actual bank transactions due to the manual transfer of data between the accounting system and the internet banking portal.

- **Management systems:** This section focuses on the lack of integration between management systems across different entities, hindering information exchange and verification processes.

7.3.1 Management systems and accounting systems

Reviews of system integration at TASAF and RFB identified an operational issue. Both entities rely on separate systems (PSSN-MIS for TASAF and MIS for RFB) to manage core processes, particularly in the initial stages of payment procedures. However, these systems lack seamless integration with MUSE, the central accounting system. This lack of integration hinders the automatic transfer of payment details which are critical for finalizing payments. As a result, data must be transferred manually, introducing the risk of discrepancies in payments and inconsistencies in records.

7.3.2 Billing systems and accounting systems

My assessment of integration at TSN, ATCL and TPDC revealed a lack of integration between their billing systems (Circulation System, Cargo Management System, Crane Revenue System, and LAPIS) and the central accounting system, SAGE. As a result, these entities must manually transfer transactions, introducing the risk of human error and potentially leading to inaccurate financial reporting.

Similarly, at T-PESA, the lack of integration between the TTCL mobile money system and the ERMS system necessitates manual posting of transactions for revenue recognition. This manual process introduces the same risk of human error and inaccurate reporting.

7.3.3 Billing systems and business management systems

My review identified that the Fisheries Revenue Collection Information System (FiRCIS) lacks integration with several crucial systems:

- **National Identification Authority (NIDA):** This hinders effective verification and validation of individual nationalities.

- **TAUSI and BRELA**: These systems are essential for issuing collection license numbers which are a prerequisite for granting fishing business licenses. The absence of integration prevents FiRCIS from verifying business licenses effectively.

- **Bank of Tanzania (BoT)**: Lack of integration with BoT prevents automatic updates on daily exchange rates used in permit and license fee calculations. This can lead to undercharging or overcharging as evidenced by our analysis revealing an undercharge of TZS 379,932.

Furthermore, TMDA's Regulatory Information Management System (RIMS) also faces a similar integration challenge. Its lack of connectivity with the Bank of Tanzania prevents real-time updates on exchange rates resulting in inaccurate fee configurations and affecting the final payment amount.

7.3.4 Management systems

My review identified a lack of integration among entities' management systems, hindering effective information verification, validation and seamless data exchange across systems and entities, as detailed below:

Entity	Non-Integrated Systems	Reason for Integration	Implication
Ministry of Works	SLPS with TRA TIN application system	Automatic verification of TIN numbers for special load permits	human errors, issuance of permits with invalid TIN numbers
OSHA	WIMS with CRB system	Seamless sharing of crucial project information	Inaccurate billing, errors, inefficiencies.

Entity	Non-Integrated Systems	Reason for Integration	Implication
TASAC	SBMS with TRA and M-BILL with TRA, BRELA	Automatic exchange of pre- and final assessments of imported goods and assets and business license verification	Errors resulting in inaccuracies in business license verification
	Dar es Salaam Maritime Institute System and NIDA	Automatic certificate recognition, DMI number provision, and citizenship recognition during seafarer registration	Errors and compromise the integrity of information between systems.
PO PSMGG	HCMIS with PSRS	Sharing of information crucial for placement of newly hired employees and issuance of recruitment permits	Errors and forgery.
Tanzania Immigration Department	Emergency Travel Document (ETD) system with Border Management Control (BMC) system and Passport system	Validation of document authenticity and automatic sharing of information for registered individuals in the passport system	hindering automatic validation of document authenticity, potential errors, and misuse.
MoF	Dfund with NPMIS, commercial banking systems, MUSE, and CBMS	Verification and validation in NPMIS, recording payments to suppliers, automated transfer of donor fund information and project budget verification	Errors, delayed recording of payments and challenges in project budget verification
	GERAS with e-Office	Permit verification from PST	Risk of unauthorized or inappropriate exchequer issuance
CRB	CIMIS with CMVRS and BRELA	Efficient verification of motor vehicle registration, owner details, and company information during contractor registration process	inefficiencies, delays, and potential inaccuracies, posing risks to the reliability of contractor data
Mzumbe, NIT, SUA, UDOM	students' management systems with HESLB LMS	Integration between students' management system and loans management system	data discrepancies and delays in the disbursement of loans to students.

Entity	Non-Integrated Systems	Reason for Integration	Implication
NSSF	CFMS Plus with Oracle ERP	Synchronization of benefit data	Delayed synchronization of benefit data, discrepancies in financial statements, inaccurate assessment of the Fund's stability
OUT	SARIS with HESLB	Sharing student fee payment data	Manual processing led to delays and increases the potential for errors in data entry.
PORALG	CHF with FFARS/MUSE	Updates for claims payments transmitted to the accounting system.	Manual entry of information into the accounting system can lead to errors and forgeries.
	CHF with GOTHOMIS	Membership status verification before service consumption	Manual verification leading provision of services to undeserved individuals and loss to government revenue.

To promote transparency, efficient bill generation and mitigate potential revenue loss from human error, I recommend system integration for the identified institutions.

7.4 Under-utilization of application systems

During my evaluation of information system implementation in REA, STAMIGOLD, TFRA, HESLB, TMDA, RFB, NSSF, PO-PSMGG and the Ministry of Water, it became apparent that these entities deploy information systems customized to meet user requirements. However, the underutilization of functionalities within these systems is impeding the achievement of intended objectives and hindering the realization of a satisfactory return on investment. The functionalities/modules underutilized are detailed in the table below.

Table 1: Underutilized modules/functionalities

Entity Name	System Name	Underutilized Functionality/Module
TMDA	Regulatory Information Management System (RIMS)	Tracking imports under conditional release
PO-PSMGG	Human Capital Management Information System (HCMIS)	Employee replacement, placement, transfer and leave
NSSF	Property Management System (PMS)	Expenses management and one-time tenant portal
RFB	Management Information System (MIS)	Leave tracking, functionalities
HESLB	Employer Repayment Portal (ERP)	Compliance module
TFRA	Fertilizer Information System (FIS)	Inspection and stock management
STAMIGOLD	Sage Evolution accounting system	Project, contract, purchase, inventory and fixed assets
REA	Serenic Navigator System	Budget performance monitoring, human resources, procurement, reconciliation, purchase orders and requisition processes
e-GA	ERMS System	Item receiving module
MOFP	Dfund	Expenditure reporting module

I recommend that these institutions ensure full utilization of developed or acquired systems with the ultimate goal of driving desired business outcomes and ensuring optimal returns on investments made.

7.5 Non-automation of business process

The section presents a comprehensive overview of audit findings conducted on various government entities, shedding light on critical aspects of their operational processes. The focus of this examination was to assess the level of automation within these entities, aiming to identify non-automated processes and their potential implications. The audit, spanning across different sectors, explores the details of organizational functionalities, pinpointing areas where automation could enhance efficiency, accuracy, and transparency.

My analysis of the automation levels across ATCL, UCSAF, TFRA, TIRA, REA, LATRA, IMMIGRATION, TPC, TASAC, Ministry of Livestock and Fisheries, NSSF, and Gaming Board identified various potential unautomated business process summarized in **Table 2** below:

Table 2: Non automated business process by entities

Entity	Non-Automated Processes	Implications
ATCL	Billing process for cargo charges	Inefficiencies, errors, inconvenience, risk of loss of revenue.
UCSAF	Computation of Universal Service Levies	Reliance on Excel for calculations poses the risk of incorrect levy amounts.
	Tracking of communication service provider licenses' status and gross revenue collected	Inaccurate remittance of levies and failure to collect levies from all license holders.
TFRA	Fertilizer registration process	Difficulty in monitoring and tracking fertilizer-related activities.
	Billing Process for cargo charges	Manual billing introduces inefficiencies, errors and inconvenience to customers.
TIRA	Life and health insurance processes	Increased likelihood of errors and delays in processing tasks.
ATCL	Cargo payment process	Cargo services could be provided without proper payment, potentially leading to revenue losses
	Refund approval process	Manual verification delays refunds introduce errors and poses financial risks.
	Cargo tracking functionality	Impacts customer experience, causing delays and dissatisfaction
REA	Core business functions	Manual processes diminish productivity and are prone to human error.
	Levy collection process	Manual calculations may lead to errors and financial losses. Absence of a tracking mechanism for outstanding debts.
LATRA	Semi-automation of offenses waiver process	Manual steps introduce delays, and errors, and limit audit trail, affecting efficiency.
Immigration Department	Issuance of special and business passes process	Manual procedures may lead to delays, errors, and under/overcharging of related charges.

Entity	Non-Automated Processes	Implications
TPC	Charging demurrage and handling fees process	Can lead to inefficiencies, inaccuracies, and delays in bill generation and revenue recognition
	Payroll processes and leave payment	inefficiencies and human errors, affecting operations and overall performance.
TIRA	Computation of premium levies, stickers, and penalties	Manual computation poses risks of errors and delays in penalty processing.
TASAC	Currency conversion	Manual conversion introduces potential errors and inconvenience to system users.
	Verification and approval of certificates process in MASSEMS	Non-automation reduces transparency and accountability, impacting the tracking of certificates/licenses.
	Manifest exportation process	The manual procedure raises concerns about operational efficiency and potential human errors.
	Calculation of days spent by seafarers at sea	Lack of automation results in inaccurate records for seafarers' time at sea.
	Partial automation of penalty generation process	Manual initiation may cause delays and affect the overall efficiency and accuracy.
Ministry of Livestock and Fisheries	Movement permit usage	Potential misuse, loss of government revenue due to reused permits.
MOF	Purchasing requisition process in MUSE	Data entry errors which can impact the accuracy of procurement-related data and subsequent reports.
NSSF	Real Estate Business Operations	Risks of errors, inconsistency, and delays in various real estate processes.
GBT	Currency convention process	Increased risk of human error in currency transactions and billing inaccuracies.
NCAA	Billing process for non-tourism revenue sources	Inefficiencies, inaccuracies, and delays in bill generation and revenue recognition.
OUT	Verification of students' eligibility for graduation	Risks of errors, inconsistency, and delays.
	Selection process for postgraduate students	
Ministry of Work	Computation of penalties charges	Risk of inaccuracies, inconsistencies in penalty and calculations, financial losses,

To ensure effective business management, streamlined processes and reduced human error, I recommend automating the identified processes in these institutions.

7.6 Duplication of systems hinders e-Government efficiency

Section 25(a) of the e-Government Act (2019) emphasizes several principles for sustainable and reliable digital systems, including avoiding duplication and utilizing centralized systems whenever feasible. However, audits across various institutions revealed instances where these principles were not strictly followed as listed below:

- **Gaming Board**: The organization uses both an Enterprise Resource Management Suite (ERMS) and Sage Pastel for accounting, leading to unnecessary duplication.

- **National Social Security Fund (NSSF)**: NSSF developed an in-house Asset Management System (AMS) for asset management, even though their existing Oracle ERP system already possesses these capabilities.

- **Tanzania Postal Corporation (TPC)**: TPC uses both MUSE and Sage Pastel for accounting, creating unnecessary complexity.

- **Tanzania Ports Authority (TPA)**: TPA implemented an enhanced Port Operations Automation System (POAS) but also initiated a tender for a Terminal Operating System (TOS) with similar functionalities.

- **e-Government Authority (eGA)**: Their ERMS system duplicates functionalities present in the NEST system, particularly in procurement and contract management. Additionally, ERMS includes an unused Human Resource module, while HR functions are already handled by the HCMIS system.

These duplications increase maintenance costs and hinder the national goal of a unified government system for procurement and human resources.

My recommendations are as follows:

- **The Gaming Board, NSSF, TPC and TPA should evaluate and streamline their systems to eliminate duplication and optimize existing processes.**

- **TPA should reassess the need for the TOS considering the functionalities already present in POAS.**

- **e-GA should review and update the ERMS, considering existing government initiatives and removing unused functionalities in procurement and human resources.**

7.7 Lack of automation in public services hinders convenience for Tanzanians

An examination of various Tanzanian government entities, including the Immigration Department, NCAA, NSSF, TMDA, TPDC, TASAC and TPA, revealed deficiencies in their automated systems which cause inconvenience to stakeholders. These inconveniences are explained below:

- **Immigration Department:** requires physical submission of resident permits for deactivation upon contract termination between employers and foreign workers thus hindering online use.

- **Ngorongoro Conservation Area (NCAA):** processes aircraft landing permits in attraction sites after landing due to the absence of online self-service options, leading to manual form completion and email submissions.

- **National Social Security Fund (NSSF):** lacks self-service options for property management and real estate operations, requiring manual initiation of contracts, invoices and application forms from tenants and hire-purchase applicants.

- **Tanzania Medicines and Medical Devices Authority (TMDA):** continues manual handling of laboratory test requests and product alterations leading to potential errors and delays.

- **Tanzania Shipping Agencies Corporation (TASAC):** lacks self-service options for applying for seafarers' certificates thereby creating unnecessary hurdles.

- **Tanzania Petroleum Development Corporation (TPDC):** Lapis system restricts gas purchases via USSD code for mobile numbers not registered in their system which limits accessibility.

- **Tanzania Ports Authority (TPA):** lacks a harmonized customer service management system, forcing customers to interact with multiple systems (Harbour View, TePP, and Cargo System) for a single service which leads to data redundancy and inefficiency.

I recommend that these institutions prioritize system enhancements for complete process automation. Implementing online self-service options for stakeholders will eliminate the need for physical visits, improving convenience and accessibility.

7.8 Project delays at Ministry of Works and TFRA

My review identified delays in two key projects:

- **The Laboratory Information Management System (LIMS) at the Ministry of Works:** this system, which is critical for streamlining laboratory operations, is over four years behind schedule.

- **The Subsidy Management System at the TFRA:** Designed to enhance subsidy distribution efficiency, the system has been delayed for over eight months.

These delays pose a significant risk of cost overruns and can hinder the projects' intended benefits from being realized.

To mitigate these risks and ensure the projects' success, I recommend timely completion of both LIMS by the Ministry of Work and SMS by TFRA management.

7.9 Missing project documentation hinders success at EPZA and NIT

Section 2.3 of the Standards and Guidelines for Government ICT Project Implementation mandates public institutions to create an approved ICT Project Document for all projects. This document typically includes project proposals, business cases, timelines, and financial considerations.

However, an examination of ICT project management at the EPZA and NIT revealed concerning deficiencies. Both institutions implemented the Business Facilitation Portal (BFP) and Student Information Management System (SIMS), respectively without proper documentation. This lack of documentation can lead to:

- **Unsustainable systems:** without a clear plan and objectives, maintaining and updating the systems in the future may become difficult.

- **Missed objectives:** without a documented business plan, it's challenging to determine if the project is achieving its intended goals.

- **Delays:** the absence of a defined timeline can lead to unforeseen delays and disruptions in project implementation.

- **Cost overruns:** unforeseen costs can arise without proper financial planning and documentation.

To address these issues, I recommend that EPZA and NIT management establish and implement approved project documentation for the BFP and SIMS projects in accordance with the e-Government guidelines.

7.10 Non-performance of source code review

A review of project management at the Ministry of Works identified the absence of a source code review for the implemented Monitoring and Evaluation (M&E) project. This omission carries significant risks as it can lead to:

- **undetected bugs**: without review, hidden errors (bugs) may remain in the code causing unexpected behavior and potential system failures.

- **compromised code quality**: unreviewed code may lack proper structure, efficiency, and maintainability which in turn may increase development and maintenance costs in the long run.

- **security vulnerabilities**: unidentified security flaws can expose the system to potential attacks and data breaches.

- **inconsistency in coding standards**: the absence of review can lead to inconsistent coding practices, hindering collaboration and future code modifications.

- **diminished opportunities for continuous improvement**: skipping code review misses opportunities to identify areas for improvement and enhance the software's overall quality and efficiency.

These factors ultimately contribute to a less reliable and maintainable software product, hindering the effectiveness of the M&E project.

To mitigate these risks and ensure the quality and reliability of the M&E system, I recommend that the Ministry of Works mandate and implement source code reviews for the ongoing M&E project and all future software projects.

CHAPTER EIGHT

OPERATION EFFICIENCY OF E-GOVERNMENT AUTHORITY

8.0 Introduction

This chapter looks into the effectiveness of the eGovernment Authority in fulfilling its crucial responsibilities. Firstly, it assesses how well the Authority optimizes online government services offered by public institutions. This involves evaluating factors like efficiency, accessibility, and user-friendliness of these services. Secondly, the chapter examines the Authority's performance in ensuring public institutions adhere to established internet governance policies and standards. This analysis is crucial for maintaining online integrity and upholding best practices. While the chapter also acknowledges the e-Government Authority's responsibility for data security and privacy, the primary focus here is on their effectiveness in optimizing services and enforcing governance policies.

8.1 Inefficient application system acquisition processes

My audit of the application system acquisitions across government entities identified the following issues:

- absence of clear e-Government guidelines and procedures slows down the acquisition process, especially when similar systems already exist in other entities.

- difficulties in coordinating with entities already possessing comparable systems further contribute to acquisition delays.

- the current mechanism for identifying the most suitable application system is inadequate.

I recommend that e-GA management implement the following: (a) develop clear guidelines and procedures for seamless collaboration between public entities, the e-GA and acquiring entities; (b) establish well-defined approval processes to expedite the acquisition process; and (c) implement a

structured mechanism for identifying suitable existing application systems within government entities to promote resource efficiency.

8.2 Regulatory obstacles hinder government data sharing initiatives

The e-Government Authority implemented the Government Enterprise Service Bus (GovESB) to facilitate seamless data sharing among public institutions. However, diverse laws and regulations governing data sharing have emerged as significant obstacles. These challenges include regulations that mandate charges for accessing information hence hindering e-Government integration efforts.

One specific example is item number 6 of the second schedule of NIDA Regulations, which imposes a fee of TZS 500 per click for accessing information. This regulatory fee has created a financial barrier for institutions like the Ministry of Water and LATRA, hindering their ability to integrate with NIDA and BRELA and ultimately impeding their operational efficiency. Consequently, broader efforts to achieve comprehensive e-Government integration across public entities are undermined.

I recommend that the e-GA collaborate with relevant regulatory bodies to eliminate or revise charges hindering e-Government integration efforts. Also, e-GA should play an active role in establishing a systematic follow-up process to monitor progress and reach conclusive agreements.

8.3 Low compliance with e-Government Act

My audit which was based on the May 2023 report on "Customers' Perception of e-Government Authority Service Delivery" among 21 public institutions, revealed suboptimal compliance with the e-Government Act of 2019. This Act mandates the creation and implementation of essential ICT management documents by public institutions.

While 79.7% of institutions possess an ICT policy, the compliance rates for other crucial documents remain considerably lower:

- ICT security policy: 57.3%

- ICT strategy: 45.1%

- Disaster recovery plans: 45.9%
- Project implementation procedures: 17.5%
- Enterprise architecture: 10.1%
- Development, acquisition, operation, and maintenance procedures: 16.6%

These low percentages indicate significant gaps in essential ICT management practices across public institutions. This lack of compliance is likely attributed to inadequate enforcement mechanisms by e-GA. This, in turn, can lead to:

- governance challenges: without proper ICT management documents, public institutions are vulnerable to inefficiencies and security risks.
- impeding digital transformation: the absence of a clear ICT strategy can hinder efforts to modernize and improve public services through technology.

In view of such shortcomings, I recommend that e-GA reinforce compliance enforcement mechanisms to guarantee the creation and implementation of essential ICT management documents by public institutions.

8.4 Limited GovESB utilization and missing SLAs hinder data sharing efficiency

The e-GA developed the GovESB to facilitate seamless data sharing and integration across public entities. However, the platform's utilization is less than optimal thus hindering its full potential as detailed below:

- **institutions:** 71% of 81 connected institutions exchanged data during the year under review.
- **systems:** 79% of 88 registered systems on the platform exchanged data.
- **connections:** Only 66% of 375 registered connections were active.

Furthermore, the audit identified a critical gap: the absence of Service Level Agreements (SLAs) between e-GA and the public entities using GovESB. This lack of SLAs creates ambiguity in several areas and include: it is unclear who is responsible for various aspects of platform management, operation and maintenance; without defined performance metrics, it is difficult to effectively monitor, evaluate and improve the platform's availability and effectiveness; and the absence of SLAs weakens accountability mechanisms for both e-GA and the participating entities.

I recommend that the e-GA: (a) promote broader adoption of GovESB to ensure active participation from all connected entities, and (b) establish SLAs that define roles, responsibilities and performance metrics for enhanced accountability and support.

8.5 Delay in provision of government e-mail services

Requests for government electronic mail services submitted by public entities experienced delays ranging from 24 days to 132 days, surpassing the stipulated response time of delivering services on the Government Mail System (GMS) within 3 working days as outlined in Para 5.3 of e-GA Client Service Charter.

Delays in service delivery can tarnish the reputation of e-GA as a reliable and efficient service provider. Public entities may perceive the Authority negatively, impacting its standing in the e-Government ecosystem.

I recommend that e-GA evaluate and optimize internal processes to ensure timely responses to government mail service requests.

8.6 Suboptimal Government Communication Network (GovNET) connectivity and service availability

Availability report on Government Communication Network (GovNET) for the year under audit revealed that the Authority managed to connect 293 nodes out of planned 390 nodes (**75%**). e-GA did not promote and enforce connectivity to 97 nodes, which are critical for service delivery, during the audited year.

It was also noted that 150 out of 293 entities had network availability below 97%, which is contrary to e-GA Client Service Charter. Furthermore, it was found that there was no SLA between e-GA and public entities utilizing GovNet services. This lack of availability may cause public institutions to fail in delivering digital services due to the unavailability of the shared platform.

I recommend that eGA management: (a) establish Service Level Agreement with public entities utilizing GovNet services to ensure service availability of more than 97% for the GovNet to all entities (b) ensure the target of connecting 390 entities to the GovNet is attained.

8.7 e-GA not assessing hardware/software procurement during compliance checks

During compliance assessments of public institutions, the e-GA has not been evaluating whether public entities submit hardware and software procurement for approval. This oversight stems from inadequate controls ensuring compliance with the e-Government Authority Act, 2019.

This presents two potential risks to the government:

1. **inability to ensure integration and interoperability:** without assessing procurement, the e-GA cannot guarantee compatibility between government ICT systems and other systems providing services.

2. **increased security risks and substandard hardware:** unapproved procurement raises the risk of security vulnerabilities and potentially substandard hardware being used in government systems.

I recommend that the e-GA tighten controls to ensure compliance of public institutions to the e-Government Authority Act, 2019 by including in its compliance assessment checklist verification of public entity submission of procured hardware and software for approval.

CHAPTER NINE

CONCLUSION

9.0 Conclusion

The audit findings highlight the need for the public entities to address weaknesses and deficiencies within their information and communication technology (ICT) internal controls. These weaknesses increase the risk of revenue loss, operations inconveniences, fraudulent activities and security breaches.

To strengthen operational integrity, minimize revenue losses and enhance organizational trustworthiness, public entities must prioritize improving their system controls, updating policies and procedures and implementing measures to ensure compliance with the e-Government Act Number 10 of 2019 and its accompanying regulations.

The e-Government authority should enhance operations by streamlining collaboration with government entities to eliminate system integration barriers, strengthening compliance enforcement for effective ICT management and closely working with public entities to address deficiencies in system acquisition procedures while streamlining internal processes for timely service responses.

Similarly, it is essential to tackle identified shortcomings within the government's ICT systems to promote transparency, accountability and efficient service delivery. By taking proactive steps to address these concerns, entities can overcome deficiencies, enhance service provision and maximize the effectiveness of ICT systems across public institutions.

9.1 Recommendations

Following the noted weaknesses, a series of recommendations have been outlined in the individual reports directed to the relevant government entities. Nonetheless, this general report captures key recommendations directed towards the Ministries and Agencies tasked with supervising ICT integration nationwide, aimed at fostering security, efficiency and effectiveness, thereby facilitating economic advancement.

I recommend that the management of Ministry of Finance:

1. **Integration of revenue systems with Financial Systems**: enhance the integration between revenue systems and accounting systems (MUSE) across institutions to enable better tracking of receivables and enhance overall financial management.

2. **Procurement controls and system settings**: enhance a robust matching system to ensure accuracy and integrity in procurement processes. Accounting systems should reconcile purchase requisitions, purchase orders, receipts, invoices and payment records to validate that the goods or services were received as ordered, invoiced correctly and paid for accurately. By enforcing this matching process, organizations can enhance financial control, mitigate risks of over-payment or fraud and maintain compliance with procurement policies and regulations.

3. **Imprest management controls**: improve the existing imprest management controls to ensure accountability and transparency. Implement features that restrict imprest issuance to staff with outstanding balances, prevent imprest over-payments and associate payments with authorized imprests. Additionally, maintain strict adherence to approved transactions and regularly reconcile imprest accounts to detect discrepancies promptly.

4. **Segregation of duties and system usage monitoring**: implement measures such as regular monitoring of user activities, automated alerts for suspicious transactions and periodic rotation of duties to prevent collusion or circumvention of controls. Provide regular training and awareness programs to sensitize employees on the importance of segregation of duties and the consequences of misuse of the same.

5. **Financial reporting and system usage**: enforce entities on the usage of financial systems for preparing financial statements to enhance efficiency.

6. **Salary recording and payment recognition**: enhance reconciliation between HCMIS and MUSE to ensure salary paylist and salary paid in MUSE and ensure the dummy salary in the system cannot be used/disbursed after payment of the paylist.

7. **Budgetary system controls (planning, budgeting and compliance controls):** Strengthen budgetary controls within the system to ensure effective management and oversight of financial resources. Enhance the controls that enforce adherence to approved budgets, including pre-authorization requirements for expenditures that exceed predefined thresholds.

I recommend that the management of e-GA:

1. **Entities IT General Controls compliance**:

   a) **conduct assessments**: initiate thorough evaluations of ICT governance frameworks across all entities to identify areas of non-compliance and assess the maturity levels of existing controls.

   b) **prioritize strategic enhancements and bridge compliance gaps**: strategically allocate resources to address areas of lower compliance, focusing on domains like acquisition and development, and change management. Implement targeted measures from assessments to bridge compliance gaps, elevating overall compliance levels and aligning with industry e-GA standards and guidelines.

   c) **enhance IT governance practices**: implement measures to fortify IT governance practices across all entities. This includes conducting awareness training on e-government policies and procedures to ensure alignment and adherence.

   d) **ICT project management and handover**: ensure that ICT projects across entities are executed within the planned time and budget. For projects involving vendors, ensure that system handover is conducted according to the established plan and contract.

2. **Entities acquiring systems within government**: implement clear guidelines and procedures for streamlined engagement between public entities, the e-GA and acquiring entities, including defined approval processes and a structured mechanism for identifying suitable existing application systems within government entities.

3. **E-Government data sharing initiatives**: collaborate with relevant regulatory bodies to eliminate or revise charges hindering e-government

integration efforts; and optimizing GovESB utilization and establishing SLAs for enhanced accountability and support.

4. **Human resource and payroll systems compliance with Public Service Laws and Regulations**: collaborate with PO-PSMGG and other entities to implement controls within human resource and payroll systems that address the requirements stipulated in public service regulations concerning salary deductions, promotions and demotions.

5. **Automation and optimization of processes**: collaborate with entities to accelerate business process automation through a structured approach. Conduct a thorough assessment of existing workflows to prioritize automation of repetitive and manual tasks, saving valuable time and inconveniences.

6. **Systems configuration and validation controls:** collaborate with respective entities on thorough review and enhancement of internal revenue and management systems with focus on validation controls and system configurations to ensure accuracy, consistency and compliance with regulatory requirements.

I recommend that the management of PORALG:

1. **Management of CHF**: conduct a comprehensive review of the iCHF-IMIS system's data validation and processing logic to enhance system control in preventing misuse of the services through excessive usage of member IDs and ensure accurate health utilization services while ensuring data integrity.

2. **Management of TAUSI:** undertake a comprehensive review and enhancement of the TAUSI system, focusing on configuration, validation, and integration aspects. This includes improving system design to accommodate verification features, implementing controls for accurate data authentication, defining specific user roles and automating bill generation processes.

LIST OF APPENDICES

Appendix I: Overall level of compliance per entity

SN	Entity	Overall Weighted Score	Overall Compliance Level
1	NSSF	69.78	Level 3
2	MOFP	66.96	Level 3
3	RFB	63.1	Level 3
4	TIRA	58.63	Level 3
5	TASAC	54.21	Level 2
6	TMDA	48.95	Level 2
7	TAMISEMI	48.28	Level 2
8	LATRA	48.12	Level 2
9	TMA	45.44	Level 2
10	ATCL	43.29	Level 2
11	CRB	42.77	Level 2
12	IMMIGRATION DEPARTMENT	42.34	Level 2
13	GAMMING BOARD OF TANZANIA	42.18	Level 2
14	FISHERIES SECTOR	40.97	Level 2
15	MOW	39.02	Level 1
16	PO-PSMGG	37	Level 1
17	OUT	37	Level 1
18	NIT	31.67	Level 1
19	REA	31.36	Level 1
20	OSHA	**37.28**	Level 1
21	TPC	26.22	Level 0
22	EPZA	12.5	Level 0

Appendix II: Detailed level of compliance

Entity	ITGC Domain	Compliance Level
TMA	IT Governance	Level 3
	Database Management	Level 1
	Network Management	Level 2
	Information Security	Level 2
	Incident Management.	Level 2
	Physical Security Controls	Level 3
	Acquisition and Development	Level 0
	Application Access Management	Level 1
	Change Management	Level 3
	BCP and DRP	Level 2
	Third Party Management	Level 3
RFB	IT Governance	Level 5
	Database Management	Level 3
	Network Management	Level 4

Entity	ITGC Domain	Compliance Level
	Information Security	Level 3
	Incident Management.	Level 4
	Physical Security Controls	Level 4
	Acquisition and Development	Level 2
	Application Access Management	Level 4
	Change Management	Level 1
	BCP and DRP	Level 3
	Third Party Management	Level 2
NSSF	IT Governance	Level 4
	Database Management	Level 2
	Network Management	Level 4
	Information Security	Level 4
	Incident Management.	Level 4
	Physical Security Controls	Level 4
	Acquisition and Development	Level 3
	Application Access Management	Level 4
	Change Management	Level 4
	BCP and DRP	Level 4
	Third-Party Management	Level 3
TMDA	IT Governance	Level 3
	Database Management	Level 1
	Network Management	Level 2
	Information Security	Level 3
	Incident Management.	Level 1
	Physical Security Controls	Level 3
	Acquisition and Development	Level 3
	Application Access Management	Level 2
	Change Management	Level 0
	BCP and DRP	Level 2
	Third-Party Management	Level 3
TAMISEMI	IT Governance	Level 0
	Database Management	Level 3
	Network Management	Level 3
	Information Security	Level 2
	Incident Management.	Level 3
	Physical Security Controls	Level 0
	Acquisition and Development	Level 5
	Application Access Management	Level 3
	Change Management	Level 0
	BCP and DRP	Level 5
	Third-Party Management	Level 0
REA	IT Governance	Level 2
	Database Management	Level 2
	Network Management	Level 1
	Information Security	Level 0

Entity	ITGC Domain	Compliance Level
	Incident Management.	Level 0
	Physical Security	Level 4
	Acquisition and Development	Level 2
	Application Access Management	Level 2
	Change Management	Level 0
	BCP and DRP	Level 0
	Third Party Management	Level 1
CRB	IT Governance	Level 3
	Database Management	Level 2
	Network Management	Level 3
	Information Security	Level 0
	Incident Management	Level 2
	Physical Security	Level 4
	Acquisition and Development	Level 0
	Application Access Management	Level 3
	Change Management	Level 0
	BCP and DRP	Level 0
	Third Party Management	Level 4
TASAC	IT Governance	Level 4
	Database Management	Level 2
	Network Management	Level 1
	Information Security	Level 3
	Incident Management.	Level 1
	Physical Security	Level 4
	Acquisition and Development	Level 1
	Application Access Management	Level 3
	Change Management	Level 1
	BCP and DRP	Level 2
	Third-Party Management	Level 4
LATRA	IT Governance	Level 2
	Database Management	Level 3
	Network Management	Level 2
	Information Security	Level 3
	Incident Management	Level 1
	Physical Security	Level 4
	Acquisition and Development	Level 1
	Application Access Management	Level 2
	Change Management	Level 2
	BCP and DRP	Level 2
	Third-Party Management	Level 1
TPC	IT Governance	Level 2
	Database Management	Level 0
	Network Management	Level 1
	Information Security	Level 1
	Incident Management.	Level 0

Entity	ITGC Domain	Compliance Level
	Physical Security	Level 2
	Acquisition and Development	Level 0
	Application Access Management	Level 1
	Change Management	Level 0
	BCP and DRP	Level 0
	Third Party Management	Level 0
PO-PSMGG	IT Governance	Level 2
	Database Management	Level 1
	Network Management	Level 2
	Information Security	Level 1
	Incident Management.	Level 0
	Physical Security	Level 2
	Acquisition and Development	Level 2
	Application Access Management	Level 1
	Change Management	Level 3
	BCP and DRP	Level 2
	Third-Party Management	Level 0
GAMMING BOARD OF TANZANIA	IT Governance	Level 2
	Database Management	Level 1
	Network Management	level 0
	Information Security	Level 1
	Incident Management	Level 1
	Physical Security	Level 3
	Acquisition and Development	Level 1
	Application Access Management	Level 2
	Change Management	level 0
	BCP and DRP	level 1
	Third Party Management	level 4
IMMIGRATIO N DEPARTMEN T	IT Governance	Level 2
	Database Management	Level 0
	Network Management	Level 4
	Information Security	Level 3
	Incident Management	Level 3
	Physical Security	Level 4
	Acquisition and Development	Level 0
	Application Access Manag ement	Level 2
	Change Management	Level 3
	BCP and DRP	Level 2
	Third Party Management	Level 0
MINISTRY OF LIVESTOCK AND FISHERIES -	IT Governance	Level 3
	Database Management	Level 0
	Network Management	Level 2
	Information Security	Level 2
	Incident Management	Level 1

Entity	ITGC Domain	Compliance Level
FISHERIES SECTOR	Physical Security	Level 4
	Acquisition and Development	Level 5
	Application Access Management	Level 2
	Change Management	Level 1
	BCP and DRP	Level 0
	Third Party Management	Level 0
MINISTRY OF FINANCE	IT Governance	Level 2
	Database Management	Level 4
	Network Management	Level 4
	Information Security	Level 3
	Incident Management	Level 3
	Physical Security	Level 5
	Acquisition and Development	Level 5
	Application Access Management	Level 4
	Change Management	Level 3
	BCP and DRP	Level 1
	Third Party Management	Level 3
MINISTRY OF WORKS	IT Governance	Level 3
	Database Management	Level 1
	Network Management	Level 2
	Information Security	Level 1
	Incident Management	Level 1
	Physical Security Controls	Level 3
	Acquisition and Development	Level 0
	Application Access Management	Level 1
	Change Management	Level 1
	BCP and DRP	Level 1
	Third Party Management	Level 2
OSHA	IT Governance	Level 0
	Database Management	Level 1
	Network Management	Level 3
	Information Security	Level 0
	Incident Management	Level 1
	Physical Security	Level 0
	Acquisition and Development	Level 2
	Application Access Management	Level 3
	Change Management	Level 0
	BCP and DRP	Level 3
	Third Party Management	Level 4
ATCL	IT Governance	Level 3
	Database Management	Level 2
	Network Management	Level 3
	Information Security	Level 1
	Incident Management	Level 2
	Physical Security	Level 5

Entity	ITGC Domain	Compliance Level
	Acquisition and Development	Level 0
	Application Access Management	Level 2
	Change Management	Level 1
	BCP and DRP	Level 0
	Third Party Management	Level 2
NIT	IT Governance	Level 2
	Database Management	Level 0
	Network Management	Level 0
	Information Security	Level 0
	Incident Management	Level 0
	Physical Security	Level 2
	Acquisition and Development	Level 0
	Application Access Management	Level 1
	Change Management	Level 0
	BCP and DRP	Level 1
	Third Party Management	Level 2
TIRA	IT Governance	Level 2
	Database Management	Level 2
	Network Management	level 3
	Information Security	Level 4
	Incident Management	Level 2
	Physical Security	Level 4
	Acquisition and Development	Level 2
	APP-ACCESS Management	Level 2
	Change Management	level 3
	BCP and DRP	level 3
	Third Party Management	Level 4
EPZA	IT Governance	Level 0
	Database Management	Level 0
	Network Management	Level 0
	Information Security	Level 0
	Incident Management	Level 0
	Physical Security	Level 0
	Acquisition and Development	Level 0
	APP-ACCESS MGT	Level 0
	Change Management	Level 0
	BCP and DRP	Level 0
	Third Party Management	Level 0
OUT	IT Governance	Level 0
	Database Management	Level 0
	Network Management	Level 2
	Information Security	Level 3
	Incident Management.	Level 0
	Physical Security	Level 2
	Acquisition and Development	Level 0

Entity	ITGC Domain	Compliance Level
	APP-ACCESS MGT	Level 3
	Change Management	Level 0
	BCP and DRP	Level 1
	Third Party Management	Level 2

ANNUAL GENERAL REPORT ON INFORMATION SYSTEMS AUDIT FOR THE FINANCIAL YEAR 2022/23

National Audit Office,
Audit House, 4 Ukaguzi Road,
P.O. Box 950, 41104 Tambukareli, Dodoma.
☎ +255(026)2161200,
✉ ocag@nao.go.tz,
🌐 www.nao.go.tz