



THE UNITED REPUBLIC OF TANZANIA NATIONAL AUDIT OFFICE



ANNUAL GENERAL REPORT OF THE CONTROLLER AND AUDITOR GENERAL FOR THE FINANCIAL YEAR 2021/22

INFORMATION SYSTEMS

IT GENERAL
CONTROLS

APPLICATION
CONTROLS

ICT
PROJECTS

OPERATIONAL EFFICIENCY
OF THE E-GOVERNMENT
AUTHORITY

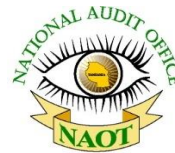


MARCH
2023

INFORMATION SYSTEMS AUDIT



**THE UNITED REPUBLIC OF TANZANIA
NATIONAL AUDIT OFFICE**



Controller and Auditor General, National Audit Office, Audit House, 4 Ukaguzi Road,
P.O. Box 950, 41104 Tambukareli, Dodoma. Telegram: "Ukaguzi", Telephone: 255(026)2161200,
Fax: 255(026)2117527, E-mail: ocag@nao.go.tz, Website: www.nao.go.tz

Ref.No.CGA.319/421/01B

29 March 2023

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

**RE: ANNUAL GENERAL REPORT OF THE CONTROLLER AND AUDITOR
GENERAL ON THE AUDIT OF INFORMATION SYSTEMS FOR THE
FINANCIAL YEAR 2021/22**

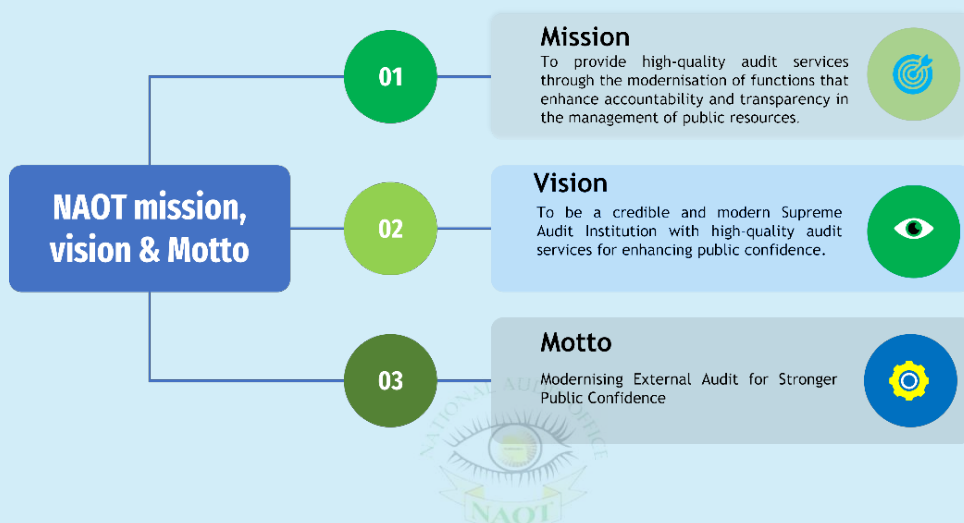
In accordance with Article 143(4) of the Constitution of the United Republic of Tanzania and section 36(1) of the Public Audit Act, Cap 418, I am pleased to submit the Annual General Report on the audit of Information Systems for the Financial Year 2021/22.

I humbly submit,

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

About National Audit Office Tanzania

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, 1977 and in Section 10 (1) of the Public Audit Act, Cap. 418.



Independence and objectivity

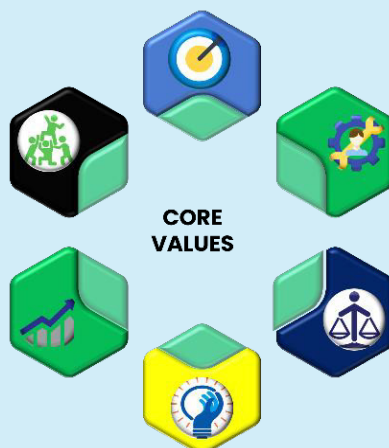
We are an impartial public institution, independently offering high-quality audit services to our clients in an unbiased manner.

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.



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 V

LIST OF FIGURES..... VI

ABBREVIATIONS VII

STATEMENT OF THE CONTROLLER AND AUDITOR GENERAL X

EXECUTIVE SUMMARY XI

CHAPTER ONE1

 INTRODUCTION 2

CHAPTER TWO4

 APPLICATION SYSTEMS CONTROLS..... 5

CHAPTER THREE23

 INFORMATION TECHNOLOGY GENERAL CONTROLS 24

CHAPTER FOUR39

 ICT PROJECT MANAGEMENT 40

CHAPTER FIVE44

 OPERATIONAL EFFICIENCY OF THE E-GOVERNMENT AUTHORITY 45

CHAPTER SIX48

 CONCLUSION..... 49

APPENDIX I: COMPLIANCE LEVELS AND ENTITIES FOR VARIOUS ICT MANAGEMENT DOMAINS50

APPENDIX II: LIST OF AUDITED PUBLIC ENTITIES.52

LIST OF TABLES

Table 1: Inadequate validation controls in various systems	6
Table 2: Issues with GIMIS	8
Table 3: Information System Issues in NIMR	9
Table 4: Unreconciled transactions between Billing systems and GePG	13
Table 5: Applications not intergrated	13
Table 6: Underutilisation of financial and operational systems.....	18
Table 7: Issues with MMMIS and MIMS at Mining Commission	18
Table 8: Application systems lacking reports or key details.....	21
Table 9: Anomalies in Strategy Management for ICT Services.....	26
Table 10: Anomalies in ICT service continuity management	27
Table 11: Anomalies in ICT incident Management.....	30
Table 12: Lack of Service Level Agreements with ICT Service Providers.....	34
Table 13: Anomalies in application systems change management	36
Table 14: Anomalies noted in user access management	38
Table 15: Delay in projects implementation	41



LIST OF FIGURES

Figure 1: Key elements of application systems controls	6
Figure 2: Transaction generated on 6 January 2023 when POS date reads 11 January 2023 11	
Figure 3: Rating scale and Criteria	24
Figure 4: IT strategy management compliance review	25
Figure 5: ICT service continuity management compliance review	27
Figure 6: ICT infrastructure management compliance review	29
Figure 7: Incident management compliance review	30
Figure 8: System management compliance review	31
Figure 9: Third party management compliance review	33
Figure 10: Application system change management compliance review	36
Figure 11: User access management compliance review	37



ABBREVIATIONS

ABS	Aeronautical Billing System
AFROSAI-E	African Organisation of Supreme Audit Institutions-English speaking countries
ATCL	Air Tanzania Company Limited
BCP	Business Continuity Plan
BOT	Bank of Tanzania
CASIP	Civil Aviation System Integrated Portal
CBE	College of Business Education
COBIT 5	Control Objectives for Information and Related Technology
CRIMS	Civil Registration Management Information System
CRS	Civil Registration System
DIT	Dar es salaam Institute of Technology
DRP	Disaster Recovery Plan
EA	Enterprise Architecture
e-GA	electronic Government Authority
ERMS	Enterprise Resource Management System
EWURA	Energy And Water Utilities Regulatory Authority
FAAS	Foreign Award Assessment System
FCC	Fair Competition Commission
FOB	Free On Board
GePG	Government Electronic Payment Gateway
GIMIS	GPSA Integrated Management Information System
GPSA	Government Procurement Services Agency
GRMS	Government Real Estate Management System
HESLB	Higher Education Students' Loans Board
ICT	Information and Communication Technology
INTOSAI	International Organisation of Supreme Audit Institutions
IPD	ICT Project Document
IPSAS	International Public Sector Accounting Standards
ISO/IEC	International Organization for Standardization
ISSAI	International Standards of Supreme Audit
JOT	Judiciary of Tanzania
JSDS	Judiciary Statistical Dashboard System
LGRCIS	Local Government Revenue Collection Information System
LIMS	Laboratory Information Management System
LPMS	Land and Properties Management System
MAC	Member Administration System
MC	Mining Commission
MCIMS	Mining Cadastre Information Management System
MEMS	Members and Examinations Management System

MIIT	Ministry of Investment, Industry and Trade
MIMS	Mineral Information Management System
MLF	Ministry of Livestock and Fisheries
MMMS	Minerals Markets Management Information System
MNH	Muhimbili National Hospital
MOCLA	Ministry of Constitutional and Legal Affairs
MOHCDGEC	Ministry of Community Development, Gender, Women and Special Groups
MOI	Muhimbili Orthopaedic Institute
MORUWASA	Morogoro Urban Water Supply and Sanitation Authority
MoU	Memorandum of Understanding
MSD	Medical Stores Department
MUSE	Mfumo wa Ulipaji Serikalini
MWAUWASA	Mwanza Urban Water Supply and Sanitation Authority
NAOT	National Audit Office of Tanzania
NBAA	National Board of Accountancy and Auditors
NCAA	Ngorongoro Conservation Area Authority
NECTA	National Examination Council of Tanzania
NHC	National Housing Corporation
NIDC	National Internet Data Center
NIMR	National Institute for Medical Research
OLA	Operational Level Agreements
OTR	Office of Treasury Registrar
PCCB	Prevention and Combating of Corruption Bureau
PEs	Procuring Entities
PML	Primary Mining Licence
PMO-LYED	Prime Minister's Office - Labour, Youth, Employment and Persons with Disabilities
POAS	Port Operations Application System
PO-RALG	President's Office - Regional Administration and Local Government
POS	Point of Sale
PSSSF	Public Service Social Security Fund
REIMS	Research Ethics Information Management System
RGS	Revenue Gateway System
RITA	Registration, Insolvency and Trusteeship Agency
RMMS	Road Maintenance Management System
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RUWASA	Rural Water Supply and Sanitation Agency
SLA	Service Level Agreement
SOFIA	Safety Oversight Facilitated Integration Application

SOP	Standard Operating Procedure
STAMICO	State Mining Corporation
TAA	Tanzania Airports Authority
TAESA	Tanzania Employment Service Agency
TAMIS	TCU Asset Management Information System
TANCIS	Tanzania Customs Integrated System
TANROADS	Tanzania National Roads Agency
TASAC	Tanzania Shipping Agencies Corporation
TBA	Tanzania Buildings Agency
TCAA	Tanzania Civil Aviation Authority
TCU	Tanzania Commission for Universities
TCRA	Tanzania Communications Regulatory Authority
TEMESA	Tanzania Electrical, Mechanical and Electronics Services Agency
TESWS	Tanzania electronic Single Window System
TIN	Taxpayer Identification Number
TOS	Terminal Operating System
TPA	Tanzania Ports Authority
TPDC	Tanzania Petroleum Development Corporation
T-PESA	TTCL Pesa
TR	Treasury Registrar
TRA	Tanzania Revenue Authority
TRC	Tanzania Railways Corporation
TTCL	Tanzania Telecommunications Company Limited
TTE	Travelling Ticket Examiner
TTMS	Tele-Traffic Monitoring System
TZS	Tanzanian Shillings
UAT	User Acceptance Test
USD	United States Dollar
WCF	Workers Compensation Fund





STATEMENT OF THE CONTROLLER AND AUDITOR GENERAL

Auditor General

I am delighted to present the Information Systems Audit Report which complements the government's efforts in execution of the National e-Government Strategy. The report highlights the findings and recommendations on the Information Systems controls and management of ICT projects within the government and their adherence to the e-Government Act of 2019, relevant standards, and guidelines.

I would like to commend the Government for its efforts and initiatives in harnessing the potential of ICT for socio-economic growth, however, there are areas for improvement identified in this report, and I would like to emphasize the importance of implementing the recommendations provided. This includes improving application controls, strengthening IT general controls, enhancing ICT project management, and optimizing the Operational Efficiency of the e-Government Authority.

I would like to express my sincere appreciation to the Parliament, Boards of Directors, Accounting Officers, Management, and all staff for their support and cooperation in making this audit a success. I would also like to acknowledge the hard work and dedication of the auditing team in conducting a comprehensive evaluation in accordance with the International Standards of Supreme Audit Institutions (ISSAIs) and other relevant audit procedures.


In conclusion, I hope that this report will serve as a valuable resource in the effective use of ICT in the public sector, under the leadership of Her Excellency Dr. Samia Suluhu Hassan.

The Government of Tanzania has developed the National e-Government Strategy to guide the exploitation of ICT opportunities and address challenges in delivering public services. The e-Government Act of 2019 established the e-Government Authority to oversee the implementation of the strategy and develop e-Government standards and guidelines. I conducted 40 information system audits comprising of 21 standalone information system audits and 19 as part of financial audit. I also conducted audit on operation efficiency of the e-Government Authority.

Below are key audit findings that provide insight into the effectiveness of the National e-Government Strategy's implementation and the compliance of information systems with established standards and guidelines.


(a) Application controls

- (i) The Member Administration System (MAS) has inadequate validation and detection mechanisms, resulting in inaccurate contribution records. (Refer Para 2.1.1)
- (ii) Medical items at MSD have expired items and items without expiry dates due to inadequate validation of expiry dates in the system during the receiving process. (Refer Para 2.1.1)
- (iii) The loan repayment verification process of HESLB lacks adequate validation controls to prevent repayment without receipt, leading to the posting of repayments in the system which have not been banked, potentially impacting the loan repayment process, and resulting in incorrect loan balance information. (Refer Para 2.1.2)
- (iv) The RITA billing system allows payments below or above the configured rate and issues certificates without payment, causing revenue loss. (Refer Para 2.2.4)
- (v) Several government organizations, including TRC, GPSA, RITA, NECTA, Mining Commission, Ministry of Constitutional and Legal Affairs, TBA, PO-RALG, and HELSB, had missing or inadequate key reports in their computer systems, resulting in a lack of transparency and accountability. (Refer Para 2.3)

- 
-
- (vi) TANCIS has configuration issues and lacks harmonization of tariffs, leading to undercharged or overcharged vehicle transit road fee. (Refer Para 2.2.5)
 - (vii) Procuring Entities (PEs) ordering items from GPSA had negative balances in their wallet accounts in the GIMIS application, resulting in GPSA losing funds due to excessive spending beyond the deposited amount. (Refer Para 2.2.1)
 - (viii) There were several unreconciled transactions between billing systems and GePG at TRC, GPSA, RITA, TCAA, TBA, TANROADS, and the Judiciary, which could lead to revenue loss. (Refer Para 2.2.9)
 - (ix) Lack of adequate control and harmonization of application systems at TANROADS, RITA and NIMR resulting to duplication of application systems that increase the cost of support and maintenance. (Refer Para 2.2.11)
 - (x) My review of Tele-Traffic Monitoring System (TTMS) controls at Tanzania Communication Regulatory Authority (TCRA) found discrepancies exist in the chargeable rates and levies for mobile money transactions, with TTMS capturing transactions fees and levies from operators' systems without verifying if they are correct. Additionally, I noted inadequate reconciliation for government levies on mobile money transactions result in discrepancies between reported levies in TTMS and the levies filed to TRA by operators. (Refer Para 2.2.15)

(b) IT general controls:

The evaluation of compliance with e-government standards and guidelines for 21 organizations (Appendix II) indicates varying levels of compliance across different domains of IT management. PSSSF, EWURA, and WCF have demonstrated high compliance levels in most domains except for a few areas of moderate compliance while MIIT, TRC, RITA, Mining Commission, PMO-LYED, Ministry of Livestock, TBA, NIMR and JOT have consistently low compliance levels across most domains.



ICT infrastructure management and third-party management have the highest percentage of organizations that have achieved the required levels of compliance. On the other hand, application systems change management and ICT service continuity management have the lowest percentage of organizations that have achieved the required level of compliance.

Overall, there is a lot of scope for improvement in various IT management areas for most organizations, as the percentage of organizations that have achieved the required levels of compliance in all domains is only 14%. (Refer Chapter 3)

(c) ICT project management:

There is a lack of clear vision and ICT strategy for Tanzania Ports Authority (TPA), resulting in significant amounts of money being spent on developing systems that are discarded before completion. (Refer Para 4.5)

ICT projects across multiple entities have experienced significant delays ranging from several months to over two years due to various reasons, including lack of funds and incomplete user requirements. Additionally, some of entities lack a mechanism for tracking the costs associated with developing their application systems, which could result in the misstated values of reported intangible assets. (Refer Para 4.1 and 4.3)

(d) Operational efficiency of eGA:

During two assessments to evaluate eGA compliance enforcement, eGA completed only 30% of the planned 61 assessments, and conducted monitoring visits in only one (1) entity, which is 1.6% of the total assessments. (Refer Para 5.1, 5.2)

Based on the findings presented, it is evident that there are significant gaps in the controls, processes, and systems of various government organizations in Tanzania. These gaps pose a significant risk to the efficiency and effectiveness of government operations and could lead to financial losses and inaccuracies in financial statements.



To address these gaps, the following recommendations are suggested:

(i) **Application Controls:**

- Input, processing, and output controls should be strengthened to prevent inaccuracies and potential frauds in financial records. Organizations should prioritize implementing adequate validation mechanisms and detection controls in their systems. Also, should ensure that key reports are available in their computer systems to enhance transparency and accountability.
- Organizations should develop an enterprise architecture framework to establish a common understanding of the organization's current and future needs, identify redundancies in the current systems, and ensure that future systems are developed in a coordinated manner. This can help to avoid the duplication of systems and reduce the cost of support and maintenance.
- Organizations should ensure that their systems are adequately integrated and controlled, and harmonization of tariffs across various systems should be prioritized. The use of GePG should be encouraged to reconcile transactions between billing systems and GePG.

(ii) **IT General Controls:** Organizations scoring low compliance level should take steps to improve their compliance with e-government standards and guidelines while Organizations that scored high should continue to prioritize e-government compliance. Also, the Government through e-Government Authority should strength monitoring of compliance of public entities.

(iii) **ICT Project Management:** Organizations should develop clear ICT strategies and vision to avoid investing in systems that will be discarded before completion. ICT project management should be improved to ensure that systems are delivered on time, within budget, and meet users' requirements.

-
- (iv) **Operational Efficiency of eGA:** eGA should prioritize completing compliance enforcement assessments and conducting monitoring visits to various entities to ensure that they comply with regulatory requirements.

By implementing the above recommendations, government organizations can enhance their controls, processes, and systems' efficiency and effectiveness, and minimize the risk of financial losses and inaccuracies in financial statements.



CHAPTER ONE

INTRODUCTION



INTRODUCTION

1.0 Background

This report presents the findings of an extensive audit of various government entities in Tanzania, aimed at assessing the implementation of the e-government strategy and the role of the e-Government Agency (eGA) in driving its implementation. The audit included 40 information systems audits, comprising 19 conducted as part of financial audits and 21 standalone audits.

The purpose of this report is to inform the public on the progress of e-government implementation, identify any challenges encountered, and provide recommendations to improve the implementation process. The report also sheds light on the role of eGA in supporting government entities to adopt e-government and enhance service delivery to citizens.

1.1 Audit Objectives

The objective of the audit was to assess the performance of the information systems and technology in helping the government entities meet their goals and objectives. The audit evaluated various aspects of the information systems and technology, including: (a) Assessing the efficiency and effectiveness of application controls and systems (b) Examining the general controls surrounding the systems and ICT operations; and (c) Evaluating the efficiency of project management for information and communications technology.

1.2 Audit Scope

The scope of the audit included a comprehensive evaluation of the information systems and technology used by government entities. The audit focused on the review of Systems' Application Controls, Information Technology General Controls, ICT Project Management, and the Operational Efficiency of the e-Government Authority. A total of 40 information systems were reviewed. The audit findings are limited to the extent of records, documents, and information made available during the audit.

1.3 Audit methodology

I conducted my audits of 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 followed 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 multi-faceted, considering the efficiency, effectiveness, and security of the systems and processes. I evaluated the risks associated with ICT systems and identified control measures implemented to mitigate these risks.



CHAPTER TWO

APPLICATION SYSTEMS CONTROLS



APPLICATION SYSTEMS CONTROLS

2.0 Introduction

Application controls refer to policies, procedures, and techniques used to ensure the reliability, accuracy, completeness, confidentiality, and security of the data processed by computer applications. These controls are critical for organizations to maintain the integrity of the information and to comply with internal and regulatory requirements.

Audits of application systems controls focus on eight key areas of control categories, as follows.

Policies and procedures, evaluates the appropriateness of the existing policies and procedures in assuring reliability of processed information.

Security of sensitive information, focuses on ensuring the integrity, confidentiality, and availability of information at all times through proper controls.

Data input is evaluated to ensure the information entered is accurate, complete, and authorized.

Data output is evaluated to ensure that online or hard copy reports are accurate and complete.

Data processing is also audited to ensure that information is processed as intended and within acceptable time frames.

Segregation of duties is an important aspect of application controls and auditors ensure that no staff member performs or can perform incompatible duties.

Audit trail is evaluated to ensure that controls over transaction logs ensure the history is accurate and complete.

Masterfile maintenance, interface controls, and data preparation are audited to ensure that controls over data preparation, collection, and processing of source documents ensure that information is accurate, complete, and timely before the data reaches the application.

The figure below illustrate these elements.

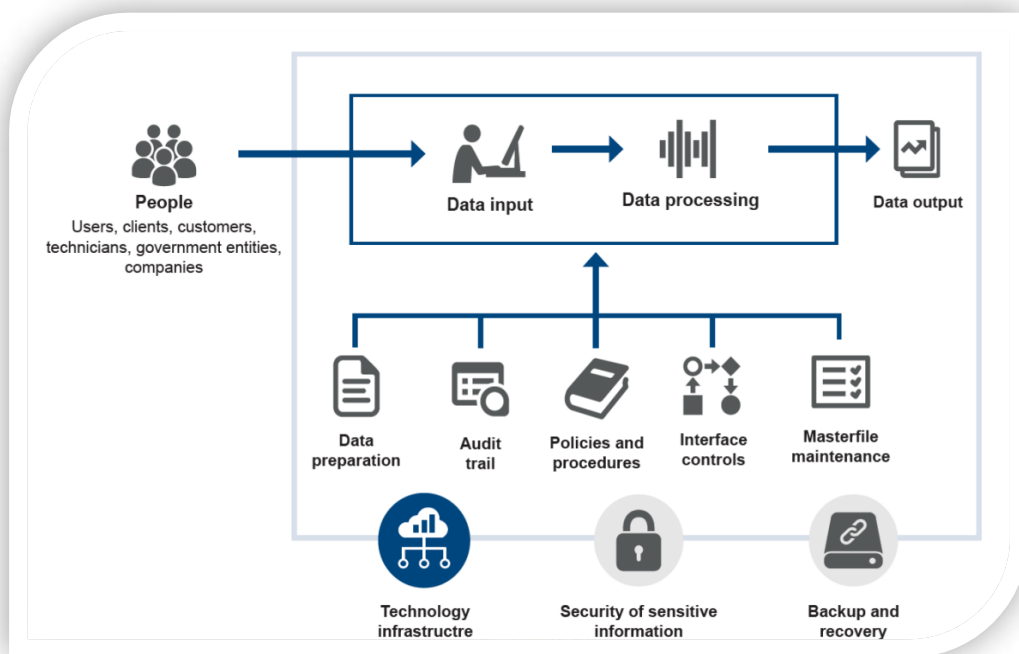


Figure 1: Key elements of application systems controls

This chapter highlights findings and recommendations from the tests performed on application controls in 2021/22, as follows.

2.1 Input controls

2.1.1 Inadequate validation controls in various systems

A review of different systems utilized by various agencies has revealed inadequate validation controls that can result in inaccurate data and potential loss of revenue or harm to the public.

Table 1: Inadequate validation controls in various systems

Entity	Information System	Issues identified	Impact
Public Service Social Security Fund (PSSSF)	Member Administration System (MAS)	17,715 recorded contributions had amounts that did not align with the required 20% of an employee's monthly salary.	Revenue loss and potentially fraudulent activity.

Entity	Information System	Issues identified	Impact
Public Service Social Security Fund (PSSSF)	Member Administration System (MAS)	Monthly contribution receipts lacked proof of payment from 34 employers.	Revenue loss for the Fund.
Medical Stores Department (MSD)	Epicor system	5 items had an expiry date that matched the manufactured date, and 171 items were recorded without an expiry date.	Potential harm to patients and financial loss to MSD.
Mining commission	Mineral Information Management System (MIMS)	The MIMS allows mineral auditors to adjust mineral quantity at inspection points without restrictions, resulting in incorrect charging.	Potential loss of revenue for the mining commission.

I recommend that PSSSF implement proper validation and detection mechanisms in the Member Administration System (MAS) to ensure the accuracy of contribution records. Also, enhance system controls that verifies existence of proof of payment before issuing receipts to maintain the accuracy of the recorded contributions.

I recommend that MSD reviews and cleans the information in their systems, including the manufactured and expiration dates of medical items, and enhance the system validation controls for entering medical expiration date.

I recommend that the Mining Commission integrate MIMS with TRA for automatic weight determination and implementing an approval process for quantity modifications.

2.1.2 Anomaly in the Integrated Loan Management System (ILMS)

Walkthrough of integrated loan management system on the process of verification of loan repayments noted an anomaly in the loan repayment verification process of HESLB. The process was lacking adequate input validation controls, leading to the possibility of posting unreceived repayments in the system without a receipt number.

This is attributed to inadequate input validation controls on the payments posting process. Posting payments without receipt number may lead to the posting of unreceived repayments in the system, which could result in incorrect loan balance information and potentially impact the loan repayment process.

I recommend that HELSB review and enhance system control in the loan repayments verification process to ensure that the system validates all the inputs and restricts posting of payments without a receipt number.

2.2 Processing Controls

2.2.1 Shortcomings on GPSA Integrated Management Information System (GIMIS)

The GPSA Integrated Management Information System (GIMIS) is a crucial application system utilized by public procuring entities (PEs) to manage the procurement of frequently used items, services, fuel, and the purchase of public vehicles. However, the audit revealed several issues and their impact on the GPSA's financial performance and operations.

Table 2: Issues with GIMIS

Issues identified	Description	Impact
Negative balances in PEs wallets	69 entities had negative balances in their wallets in GIMIS.	Financial loss of TZS 32,842,636.7 to GPSA.
Incorrect computation of closing stock balances	The GIMIS system produced incorrect closing stock balances during the inventory review from 1 March 2022 to 31 August 2022.	Misguided product re-ordering and requisitioning decisions.
Undercharge and overcharge of agency fees	There was an undercharge of TZS 65,363.89 and an overcharge of TZS 1,145,017.41 of the agency fee charged to clearing and forwarding services.	Revenue loss and incorrect charging of fees.
Lack of integration between fuel pumps and GIMIS	There was a lack of integration between fuel pumps and the GIMIS application, leading to unreconciled quantity of fuel dispensed from the pump with the recorded quantity in GIMIS.	Potential fuel mismanagement and loss.

I recommend that GPSA conduct regular reviews and audits of its procurement processes and systems to identify any potential issues and ensure that systems are functioning efficiently. Also, put in place appropriate measures to address any identified discrepancies, such as implementing stricter adherence to recharge policies, ensuring tariff schedules are being followed, and integrating systems to reconcile fuel dispensing quantities.

2.2.2 Information System Issues in National Institute for Medical Research (NIMR)

Table 3 provides a detailed account of the issues that were identified in the information systems and applications used by the National Institute for Medical Research (NIMR) and the potential impact they may have on the institute's operations.

Table 3: Information System Issues in NIMR

Information System	Issues Identified	Description	Impact
NIMR Store Management System	Issuance of items without proper request and approval	11 items were issued in the NIMR Store Management System without proper request and approval, posing a risk of fraudulent activity.	Potential for fraudulent activity.
NIMR Store Management System	Inaccurate calculation of product balance	The balance of each product in the store was not being accurately calculated in the system.	Potentially misguided store ordering decisions.
Research Proposal Application Process in REIMS	Missing required documents and under collection of fees	Seven out of 34 research proposals submitted to NIMR were missing required documents, and seven proposals were submitted with lower fees, resulting in under collection of USD 1,800 and TZS 9,584,650.	Possibility of unqualified research proposals being approved and revenue loss.
DISA Lab System	Lack of sample tracking mechanism	The current DISA Lab system used by NIMR to manage the laboratory process for tracking medical research samples from reception to testing lacks a mechanism to track the number of samples tested in accordance with the research contract agreed between NIMR and the researcher.	Potential for non-compliance with the research contract.

I recommend that NIMR act on: (a) improving the accuracy of product balance recording, reinforcing controls for proper request and approval processes in the Store Management System; (b) improving system controls and automation for document validation in the Research Proposal Application Process, and (c) implementing a sample tracking mechanism in the DISA Lab System to maintain compliance and improve efficiency in research.



2.2.3 Inadequate system controls over management of medical items with low shelf life

A review of MSD medical items stock in Epicor system revealed 4,894 expired medical items worth TZS 235,4967,2892.78 prior to distribution. This is non-compliance with the SOP for receiving stock which requires stock position analysis from demand and planning unit before accepting medical items with a shelf life below 80% or 24 months. This weakness is attributed to inadequate system controls to validate shelf life and approval process for the receipt and recording of medical items with a shelf life below 80%.

I recommend that MSD enhance system control to validate shelf life and ensure the approval process for such items is properly accommodated.

2.2.4 Inadequate system controls in billing process

My audit of RITA billing system noted that the system can receive payment below or above the configured rate and that the system can print certificates without payment. I noted 47,419 certificates which were issued without payment between 5 January 2021 and 21 October 2022.

My analysis noted that the anomaly is attributed to misuse of waiver functionality which is used during birth registration's campaigns only. Also, it was due to lack of control in configuration of rates. These anomalies have led to a loss of revenue of TZS 165,963,000.

I recommend that RITA: (a) implement controls to prevent payment below or above the configured rate; (b) review and tighten the waiver functionality to ensure that it is used only during birth registration campaigns, as intended.

2.2.5 Inaccurate computation of foreign vehicles transit charges in TANCIS

Tanzania Customs Integrated System (TANCIS) is the system built on hi-tech principles with a view to increasing effectiveness, efficiency, transparency, and reliability in the Customs administration. Being a web-based system TANCIS progressively facilitates paperless operations leading to a significant reduction in costs of doing business.

I reviewed the vehicle transit charges in TANCIS to verify accuracy of computed charges in accordance with Section 6(1) and 7(2) of the Foreign



Vehicles Transit Charges Act, [CAP 84 R.E 2019] and noted the following anomalies:

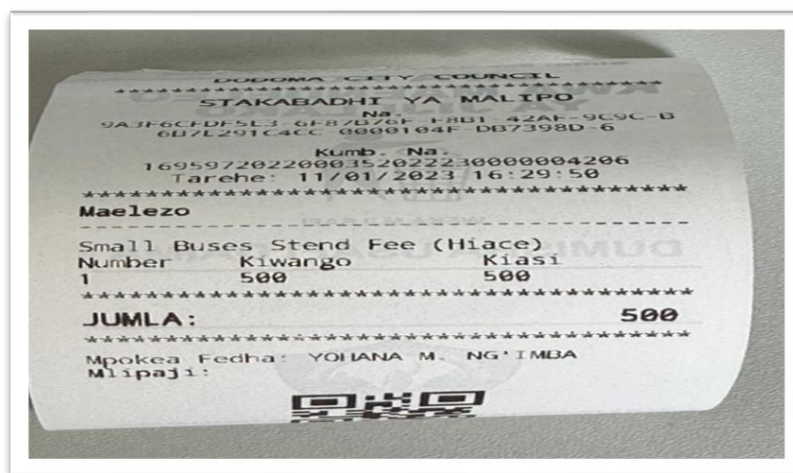
- 11,526 out of 143,792 equivalents to 8% of total number of transit vehicles undercharged road fee by USD 2,020,270.
- 7,501 out of 143,792 equivalents to 5% of total number of transit vehicles overcharged road fee by USD 698,528; and
- There were inaccurate driver names which may not be traceable in case of breaching applicable transit regulations and procedures.

I recommend that TRA: (a) Establish data completeness and computation accuracy review workflow for the foreign transit road charges assessments in TANCIS to have preparer, verifier, and authorizer; and (b) Validate distance between the border points in TANCIS system.

2.2.6 Manipulation of POS device date by revenue collectors

Review of TAUSI revenue application system at President's Office Regional Administrative and Local Government (PO- RALG) found out Point of Sale (POS) devices allow changing of transaction dates to later or earlier than the actual transaction date. As a result, transactions with later or earlier dates than the current financial year can lead to inaccurate financial statements and incorrect revenue recognition. This was attributed to non-restriction to change date settings in POS devices. Example of the changed transaction POS date is as shown in Figure 2

Figure 2: Transaction generated on 6 January 2023 when POS date reads 11 January 2023



I recommended that PO- RALG implements controls to prevent changing of transaction dates to later or earlier dates than the actual transaction date by restricting access to change transaction dates to authorized personnel.

2.2.7 Anomalies noted in House lease Payments Report against Payment guideline

Review of the Government Real Estate Management system (GRMS) at Tanzania Building Agency (TBA) found out 1,302 house leased contracts uploaded in the system had anomalies in payments made against approved rates as per guidelines. Of which 789 contracts payments were less than the required rates by TZS 770,509,450 and 513 contracts payments were greater than the required rates by TZS 359,657,608.

I recommend that TBA ensures lease payment rates are configured in GRMS as per payment guideline.

2.2.8 Inaccurate charging of total overloaded weight fee at TANROADS

A review of the overloading weight fees charged by TANROADS from 13 weighbridges for the financial year 2021/22 found out 11,594 vehicles were undercharged by USD 466,449, and 134 vehicles were overcharged by USD 10,958. This inaccurate charging was due to noncompliance with Para 11 of the third schedule of the East African Community Vehicle Load Control.

Under and overcharging of overloading weight fees at TANROADS results to loss of revenue for the organization and potential legal implications for non-compliance with regulations which may damage the organization's reputation and its credibility.

I recommend that TANROADS reviews and rectifies the system's logical function for calculating all axles weights and gross weight to ensure accurate charging of overloading weight fees in line with the East African Community Vehicle Load Control.

2.2.9 Unreconciled receipt amount between Billing System and GePG

A review of billing systems and GePG at TRC, GPSA, TCAA, RITA, TBA, TANROADS and Judiciary identified several instances of unreconciled transactions between the two systems.

Table 4: Unreconciled transactions between Billing systems and GePG

Organization	Transactions	Discrepancy	Amount (TZS)
TRC	27	Higher amount in e-ticketing system than in GePG	662,994,919
GPSA	58	Higher amounts in GePG than in GIMIS	1,318,970,961
GPSA	1	Higher amount in GIMIS than in GePG	480,000
RITA	65,531	Higher amounts in billing system than in GePG	1,540,040,705
TCAA	15	Higher recorded paid amount in billing systems than in GePG	4,646,620
TBA	60	Higher amounts in GePG than in GRMS real estate management system	40,468,284
TBA	2	Lower amounts in GePG than in GRMS real estate management system	2,400
TANROADS	682	Overpaid bills between Databridge billed amount and GePG settled amount	16,601,526
TANROADS	487	Underpaid bills between Databridge billed amount and GePG settled amount	7,557,402
Judiciary	40	GePG recorded payment transactions higher than in JDS 2	555,245

These noted discrepancies could lead to revenue loss, misstatement of revenue in financial statements, and misstatement of cash collected.

I recommend that the respective organizations investigate and rectify the anomaly, establish the root cause of the discrepancy, and implement a reconciliation module between the billing system and GePG to ensure accurate and transparent recording of transactions and efficient data exchange.

2.2.10 Lack of Integration between Institutions' Applications

My audit of application controls at ATCL, GPSA, Judiciary of Tanzania, Mloganzila Hospital, MSD, NECTA, NIMR, TANROADS, TCAA, TCU, Treasury Register (TR) and TRA noted lack of systems integration as summarised in the **Table 5**:

Table 5: Applications not intergrated

S/N	Institution	Applications not integrated	Impact of non-integration
1.	NIMR	<ul style="list-style-type: none"> Votebook accounting system with PlanRep budget management system. 	<ul style="list-style-type: none"> Non-tracking of expenditure against the budget set.

S/N	Institution	Applications not integrated	Impact of non-integration
		<ul style="list-style-type: none"> Votebook (Accounting System) with REIMS system, which collects revenue for research permits. Votebook with TANEPS 	<ul style="list-style-type: none"> Hinders the visibility of supplier payments from the procurement process.
2.	NECTA	SAGE Accounting System with Bank payment applications.	Human errors, incompleteness and inaccurate transactions, lack of accountability for action performed by users in the system, and potential misstatements in financial statements.
3.	GPSA	GIMIS with Electronic Single window, TANEPS, and MUSE	<ul style="list-style-type: none"> Hinders the visibility of tax assessments. Unqualified suppliers in GIMIS; and Payment of an ineligible supplier and/or overpayment to suppliers.
4.	TCAA	SOFIA-Landing and Overfly Permits System, CASIP- License issuance System, and Billing System with the accounting system (ERMS) for the automatic posting of collected revenues.	Incorrect reporting of collected revenue to intentional or unintentional human error.
5.	TANROADS	<ul style="list-style-type: none"> RMMS application system used to keep and monitor the road projects information including with TANEPS; and Databridge application system that installed in 13 weigh bridge stations with revenue system (Epicor) and GePG. 	<ul style="list-style-type: none"> Unqualified contractors in RMMS; Loss of collections from overloading charges; and Misstatement of revenue
6.	MSD	<ul style="list-style-type: none"> Epicor with Bank Applications. Epicor with Tanzania electronic Single Window System (TESWS) 	<ul style="list-style-type: none"> Overpayment of supplier claims compared to approved amounts; and Failure to detect overcharging caused by under or over-declaration of extra cost.
7.	TCU	<ul style="list-style-type: none"> SAGE PASTEL with Asset Management Information System (TAMIS) 	<ul style="list-style-type: none"> Causes asset and depreciation values to be manually posted from

S/N	Institution	Applications not integrated	Impact of non-integration
		<ul style="list-style-type: none"> SAGE PASTEL with banking systems. SAGE PASTEL with the budgeting system (PlanRep). SAGE PASTEL with billing portal - GePG. 	<p>TAMIS into PASTEL through a journal.</p> <ul style="list-style-type: none"> Can result into overpayment. Can result overriding of budget controls during budget execution; and Can result in the posting of incorrect revenue in the accounting system
8.	Judiciary of Tanzania	<ul style="list-style-type: none"> JSDS 2 with NIDA system to validate the applicant's information 	<ul style="list-style-type: none"> Manual verification and validation of submitted information resulting in inefficiencies and inconveniences.
9.	ATCL	<ul style="list-style-type: none"> SAGE Accounting System and Cargo Management System 	<ul style="list-style-type: none"> Manual posting of cargo related revenue into Sage accounting system which may lead to unrecognized revenue amounting TZS 8,978,231.24 in sage accounting system.
10.	Treasury Register	<ul style="list-style-type: none"> PlanRep with HCMIS and PlanRep with TANEPS. 	<ul style="list-style-type: none"> Insufficient and unauthorised payments to suppliers and employee; and Procurement executed out of budget.
11.	Mloganzila Hospital	<ul style="list-style-type: none"> Wellsoft and Jeeva Hospital Information Management System 	<ul style="list-style-type: none"> Human errors in recording patients' payments details.
12.	MOCLA	<ul style="list-style-type: none"> Legal Aid and Arbitration with GePG; Arbitration and NGOs Information System of the Ministry of Community Development, Gender, Women and Special Groups (MOHCDGEC) 	<ul style="list-style-type: none"> Loss of revenue due to failure in payment verification Certifying unregistered NGOs due to intentional or unintentional human error.
13.	Mining Commission	<ul style="list-style-type: none"> MMIS and MIMS systems which are used for management of mineral sales are not integrated with MCIMS for automatic validation of licences. 	<ul style="list-style-type: none"> License details are manually filled in the 2 systems without verification and approval. use generic GePG portal and manually update payments details in these systems.



S/N	Institution	Applications not integrated	Impact of non-integration
		<ul style="list-style-type: none"> MCIMS and MMMIS are not integrated with GEPG to automate the bill generation process during licence processing. 	
14.	PMO - LYED	<ul style="list-style-type: none"> ePermit System with TIN and BRELA 	<ul style="list-style-type: none"> Provision of work permits to unqualified individuals and illegal companies.
15.	TBA	<ul style="list-style-type: none"> GRMS and HCMIS GRMS and GePG 	<ul style="list-style-type: none"> Sales of houses to non-public servant Settling house debt for ineligible payments.
16.	EWURA	<ul style="list-style-type: none"> CAP Price Computation Information System (CPS-IS) is not integrated with Bank of Tanzania (BOT) systems. CPS-IS is not integrated with Platts API for the automatic transfer of Free on Board (FOB) prices. LOIS is not integrated with BRELA Systems for automatic business license verification. 	<ul style="list-style-type: none"> Manual importing of exchange rates and FOB prices into CPS-IS is subjected to human errors and delays; and Manual verification of business licenses is subjected to human errors which could result into issuing license to unqualified applicants.
17.	TRA	CMVRS and RGS	501 motor vehicle payment transactions worth 4.68 million recorded in CMVRS could not be traced in RGS

Source: 2021/22 Management letters of the respective entities

I recommend that, NIMR, NECTA, GPSA, TCAA, TANROADS, MSD, TCU, Judiciary of Tanzania, ATCL, Treasury Register, Mloganzila Hospital, MOCLA, Mining Commission, PMO - LYED, TBA, and EWURA to collaborate with the e-Government Authority and integrate their application systems with the identified systems using a government enterprise service bus.

2.2.11 Non-harmonization of Application Systems at TANROADS, RITA, and NIMR

I have identified several issues related to the harmonization of application systems in TANROADS, RITA and NIMR.

TANROADS is using three different weighing application systems, namely Data bridge, Smart scale, and Tload, for the same weighing purpose. Further, I noted, only 13 out of 63 weighbridges are connected to the



central server, which poses a risk of fraudulent activities due to ineffective monitoring.

I recommend that TANROADS adheres to Enterprise Architecture guidelines and ensures that all standalone weigh software is connected to the central server for effective monitoring.

RITA has four different application systems for birth and death registration, namely Civil Registration System (CRS), under-five birth registration system, the civil registration management information system (CRIMS), and online registration system. This duplication of systems increases administration, maintenance, and support costs and overhead.

I recommend that RITA Management formulates an Enterprise Architecture plan to deploy IT application systems, reviews existing systems and processes, and establishes a roadmap and timeline to ensure the usage of a single Birth and death registration system across the country, and plans for effective data migration from other systems to the selected one.

In my review of NIMR's ICT initiatives, I found that the organization has two different lab application systems, one used by Mbeya center and the other used by Mwanza center, which perform the same function but were acquired independently without coordination. Additionally, while Mbeya center has a store management system to manage inventory, Mwanza center uses Microsoft Excel for this purpose.

I recommend that NIMR standardize the laboratory application systems used by its different centers to ensure uniformity and efficiency. Mwanza center should implement a store management system to manage its inventory, similar to the one used by Mbeya center. Also, develop and implement guidelines for the acquisition and deployment of ICT systems across its different centers.

2.2.12 Underutilization of financial and Operation system

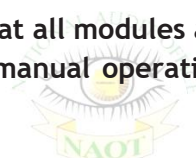
My review of the financial and operational systems used by NIMR, TRC and ATCL observed that there is significant underutilization of some of the modules.

Table 6: Underutilisation of financial and operational systems

Institution	Underutilized Modules/Functionality
NIMR	Procurement, Vehicle, Payroll, and Fixed Assets modules
NIMR	Payments to suppliers not made within the system
TRC	Cargo transshipments, cargo delivery and offloading, cargo storage, cargo diversion, stoppage and extension, cross-border cargo management, and adjustments functionality in the Cargo Management system not in use
TRC	LPMS: Some properties are registered outside the system
TRC	LPMS: Leasing bills for properties are generated in the miscellaneous bill module of the E-ticketing system
ATCL	Cargo Management Revenue system: International cargo are processed outside the system

Underutilization of systems can lead to inefficiencies in payments, leasing bills, and missed opportunities to improve processes and increase efficiency.

I recommend that both NIMR, TRC and ATCL take steps to assess and establish the reasons for the reluctance to use these modules and systems effectively, ensure that all modules and functionalities are fully utilized, and discourage the manual operations for already automated business processes.



2.2.13 Ineffective application controls in MMMIS and MCMS at Mining Commission

The Mining Commission is responsible for managing and regulating the mining industry and ensuring that mining activities comply with the relevant laws and regulations. The review of its two information systems, namely, Minerals Markets Management Information System (MMMIS) and Mineral Information Management System (MIMS) revealed the following issues and their impact.

Table 7: Issues with MMMIS and MIMS at Mining Commission

System	Issue	Impact
MMMIS	<ul style="list-style-type: none"> Market officer responsible for inspection could manually define the indicative price when filling out the sales entry form, instead of using the already defined prices in the system. The officer manually entered details from weighing machines into the system, which determined the loyalty fee, inspection fee, and government service levy. More than one indicative price used on the same day 	Inconsistent prices used, potential for inaccuracies in fees and levies

System	Issue	Impact
MIMS	1060 Primary Mining Licence (PML) licenses missing from Mining Cadastre Information Management System (MCIMS)	Confusion surrounding validity of licenses, potential loss of government revenues
MIMS	311,910 transactions had incorrect calculated selling prices, 198,824 transactions had undercharged loyalty and inspection fees, 113,086 transactions had overcharging of loyalty and inspection fees	Loss of revenue due to incorrect selling prices and fees

I recommend that the Mining Commission: (a) conduct a thorough review of licenses, (b) integrate MMMIS with BOT to automatically capture the purity and weight of minerals, and (c) implement control enhancements to ensure accurate and effective system calculation and configuration of selling prices and mineral indicative prices.

2.2.14 Irregularities in POS management at TEMESA

I found out the POS machines used at TEMESA revenue collection centres were not connected to a central server, therefore in case of a machine breakdown, revenue data are lost and cannot be traceable. This could lead to a possibility of revenue loss and misappropriation.

I recommend that TEMESA implement a centralized system for the management of POS machines to ensure that all revenue data are recorded in real-time and are easily accessible for reconciliation and auditing purposes.

2.2.15 Anomalies of the Tele-Traffic Monitoring System (TTMS)

Reg. 4 - (2) (i) of the Electronic and Postal Communications (Tele-Traffic) Regulations, 2021 requires Tanzania Communication Regulatory Authority (TCRA) to implement a monitoring system for mobile money transactions in compliance with the National Payment System Act. Further, Reg 4 - (2)(j) of the same Regulations requires the Authority to implement revenue assurance system for telecommunication services in the United Republic.

My review of TTMS controls found the following anomalies:

(i) Discrepancies in Chargeable Rates and Levies for Mobile Money Transactions

The Tanzania Telecommunications Regulatory Authority is required to implement a monitoring system for mobile money transactions to provide revenue assurance in compliance with the Reg. 4 - (2) (i) of the Electronic



and Postal Communications (Tele-Traffic) Regulations, 2021. However, I noted differences between the stated chargeable rates and charged rates caused by TTMS capturing transactions fee and levy as they are from operators' systems and not having a mechanism to re-compute levy to confirm and verify that operators' systems are using the correct charge and accurately computing fee and levy. This discrepancy may lead to under or overcharging of the required levy, which may go undetected.

I recommended that TCRA develop a mechanism to re-compute levies to ensure that the correct charge is used and that the fee and levy are accurately computed.

(ii) Inadequate Reconciliation of Government Levies on Mobile Money Transactions

The audit found that there were discrepancies between the reported levies in TCRA Tele-Traffic Monitoring System and the levies filed to TRA by operators. The cause of these anomalies was attributed to inadequate reconciliation processes. As a result, the accuracy of government levies collected by the operators cannot be fully assured.

I recommend that TCRA enhance the reconciliation process by considering the reported figures to TRA by Mobile Operators. Also, implement integration with TRA e-filing system for a more efficient reconciliation and verification.

(iii) Non-monitoring of mobile money rollback transactions

I found that unsuccessful mobile money transactions "rolled back transactions" are not captured in the TTMS. I was informed that design of TTMS did not consider such transactions since they are unsuccessful transactions and are not supposed to have transactions fees other than network costs associated with the use of USSD channels. However, TCRA is mandated to monitor and provide revenue assurance for telecommunication services as per Reg. 4 - (2)(i) and 4 - (2)(j) of the Electronic and Postal Communications (Tele-Traffic) Regulations, 2021. This includes all fees charged and costs incurred by operators for the purpose of tax verification and government's visibility.

I recommend that TCRA enhance TTMS to include monitoring of "rolled back" transactions to ensure completeness and accuracy of the captured data.



2.3 Output Controls

Reliable reporting systems are crucial for organizations to make informed decisions and maintain transparency and accountability. A thorough review of the application systems output controls in Public Entities noted the following challenges.

Table 8: Application systems lacking reports or key details

Organization	Application system	Missing Reports/key details
TRC	E-Ticketing system	Real-time monitoring of POS machines and the failure to identify the collected amount versus the banked amount per TTE.
GPSA	GIMIS	<ul style="list-style-type: none"> Clearing and forwarding report: Arrival date of cargo. Clearance and forwarding statements report: Receipt numbers for deposits and fund balance after account deposits. Issued items report: Corresponding draft indent identification number. Depot transfer reports: Information on the depot to which items were transferred. Depot transfer receipts: Donor depot details.
RITA	Registration systems	Revenue collection reports, annual reports for birth and death registration, and reports for children with or without birth certificates
NECTA	SAGE software	a statement of cash flows and a statement of change in equity
Mining Commission	MIMS application system	Dashboard/report indicating daily POS transactions and online status of POS
Ministry of Constitutional and Legal Affairs	Legal aid and arbitration system	Revenue collection, certificates issued, application status, timeline, services provided, number of cases handled, case type and court, clients receiving legal aid and their location, and outcome of legal aid for the indigent.
TBA	GRMS	Sales reports, lease reports on government houses, non-government houses and lease debts reports, construction project reports and consultancy reports

Organization	Application system	Missing Reports/key details
PO-RALG	TAUSI's application controls	POS collector's cash on hand
HELSEB	Employer portal system	Outstanding loans balance

Lack of key reports in the systems can result in a lack of transparency and accountability such as untimely detection of revenue loss, difficult for organizations to make informed decisions and manual interventions which may increase the risk of errors.

I recommend that the mentioned organisation conduct a thorough review of the existing systems and identify the key reports that are missing or inadequate and enhance the systems to include such reports. Also, ensure that the systems are configured to generate the necessary reports in a timely and accurate manner.



CHAPTER THREE

INFORMATION TECHNOLOGY GENERAL CONTROLS





INFORMATION TECHNOLOGY GENERAL CONTROLS

3.0 Introduction

Following assessing the effectiveness of ICT general controls, I established the overall level of compliance with e-Government act, guidelines, standards, and best practices in the following areas: Strategy Management for IT Services, ICT Service Continuity Management, ICT Infrastructure Management, ICT Incident Management, System Management, Third Party Management, Application systems Change Management, User Access Management. Compliance level is rated on a scale of zero to five, detailed in Figure 3.

The assessment model provides a reference for comparing entity results from year to year. I expect the entity to achieve a level 3 (Defined) rating or better across all domains.

Figure 3: Rating scale and Criteria



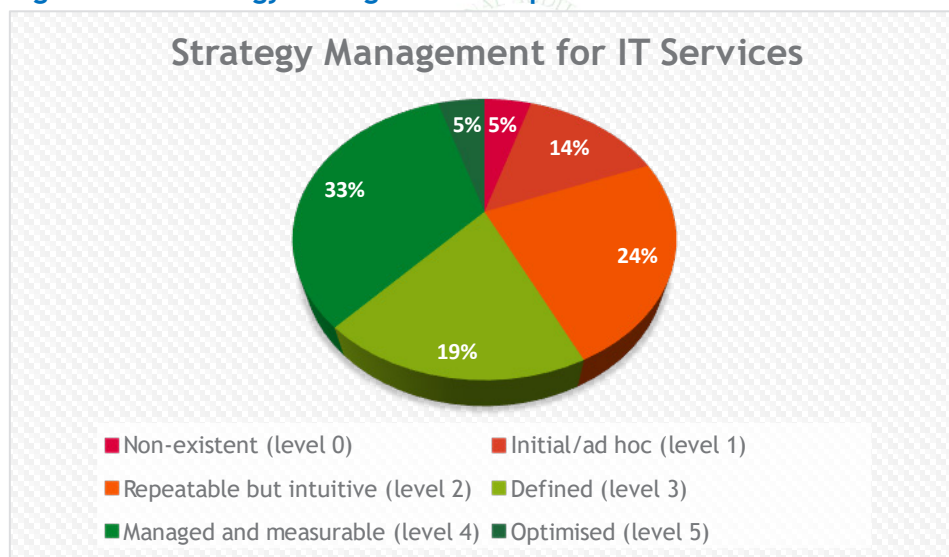
The result of my compliance assessment of 21 public entities (Appendix II) in eight domains of IT general controls are as follows:

3.1 Strategy Management for IT Services

Strategy Management for ICT Services involves developing and executing a plan to achieve organizational goals and objectives through the effective use of ICT. It involves aligning technology with business needs and making decisions on technology investments, policies, risks management and service offerings. Effective strategy management ensures the successful delivery of ICT services that support and drive business growth.

The audit assessed the compliance of 21 public entities with e-government standards and guidelines for Strategy Management for ICT Services. The overall level of compliance is shown in **Figure 4** and the details of its results is summarized in **Appendix I**.

Figure 4: IT strategy management compliance review



Alongside the assessment of compliance level for Strategy Management for ICT Services in audited public entities, my audit also evaluated the implementation of Strategy Management for ICT Services in other entities without ranking and identified various anomalies and weaknesses in their ICT strategic plans, steering committees, reporting structure of ICT departments, ICT management documents, and ICT security functions. The

following **Table 9** summarizes the entities with anomalies and weaknesses found during the audit:

Table 9: Anomalies in Strategy Management for ICT Services

Anomalies	Entities
No approved ICT strategic plan	MNH, MORUWASA, STAMICO, STAMIGOLD, MIIT, MLF (Livestock sector), PO-RALG, RITA
No annual evaluations of ICT strategic plan	TANROADS, MOCLA, NIMR
No establishment of ICT Steering Committee	TRC, STAMICO, STAMIGOLD, TPDC
Less than four meetings by ICT Steering Committee	MSD, TCU, NECTA, TCAA, RUWASA, RITA, TAA, TBA, PMO-LYED, MoCLA, MC, EWURA, PO-RALG, MWAUWASA
Unclear ICT Steering Committee charters	TAA, RUWASA, TBA, MIIT, TCU
Non-compliance with e-Government Act in ICT Steering Committee composition	RITA, MLF (Livestock sector), MWAUWASA
Non-compliant reporting structure of ICT department	MC
Non-review of ICT controls by internal audit	GPSA, MORUWASA, NECTA, NIMR, RITA, TANROADS, TBA, MC, MIIT, TRC

These anomalies and weaknesses may hinder the effective use of ICT to support organizational objectives, as well as increase the risk of security breaches and data loss.

I recommend that these entities; (a) develop ICT strategic plan and ensure it is approved by relevant stakeholders; (b) establish an ICT steering committee to oversee the alignment of ICT initiatives with the organization's strategy; (c) compose ICT steering committee, define the roles and responsibilities of the committee and ensure it convenes at least four meetings annually; and (d) Ensure internal audit functions review ICT controls regularly.

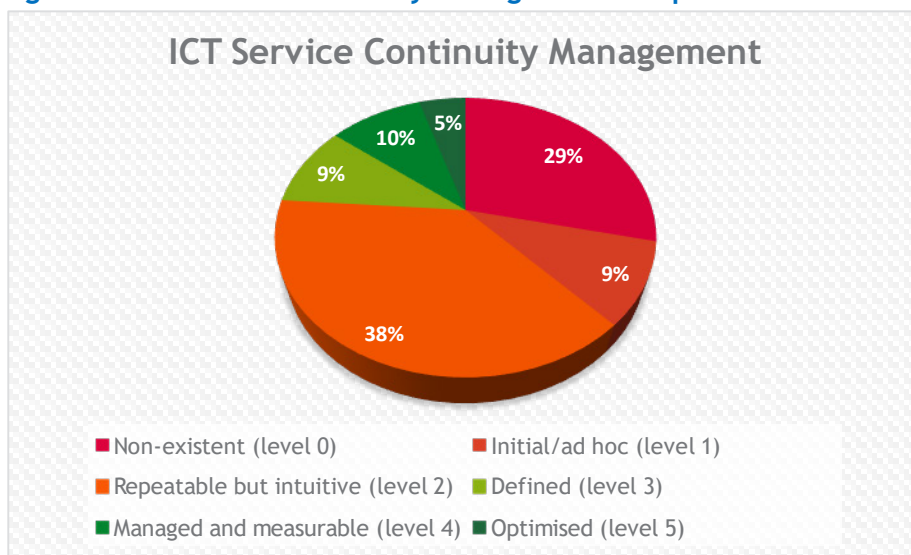
3.2 ICT Service Continuity Management

In today's dynamic business environment, organizations need a strong Business Continuity Plan and Disaster Recovery plan to cope with unexpected disruptions caused by natural disasters, cyber-attacks, and other disruptive events. These disruptions can have severe consequences, including extended outages and disruption to service delivery. BCP&DRP can

help entities recover critical business processes and ICT operations quickly, minimize the impact of the disruption, and continue delivering services to their customers and stakeholders.

The audit assessed the compliance of 21 public entities with e-government standards and guidelines for IT service continuity management. The overall level of compliance is shown in **Figure 5** and the details of its results is summarized in **Appendix I**.

Figure 5: ICT service continuity management compliance review



In addition to assessing the level of compliance with ICT service continuity management in audited public entities, my audit also evaluated the implementation of service continuity for ICT services in other entities without ranking. The audit identified several anomalies and weaknesses in their business continuity planning (BCP), disaster recovery planning (DRP), and data backup practices, which are summarized in the **Table 10**.

Table 10: Anomalies in ICT service continuity management

Anomalies	Entities
Lack of BCP and/or DRP documents	TCAA, TANROADS, JOT, TRC, STAMICO, TPDC, RITA, MLF, TBA
Outdated DRP documents	MNH, MLF, MIIT
Inadequate BCP and DRP documents (lack of defined RPO and RTO in BCP documents, critical application systems not covered in the BCP documents, lack of a	NECTA, GPSA, NIMR, JOT, STAMICO, STAMIGOLD, MoCLA, PO-RALG, MORUWASA



Anomalies	Entities
defined disaster recovery team in DRP documents, and lack of defined recovery procedures for critical application systems in DRP documents)	
Untested DRP and lack of awareness training	NECTA, TCU, GPSA, NIMR, MSD, RITA, MNH, STAMIGOLD, NCAA, MC, MoCLA, PO-RALG, MORUWASA
Lack of data backups	TCAA, TANROADS, RITA, PMO-LYED
No offsite backup location	PSSSF, STAMIGOLD, T-PESA, TEMESA
No offline backup	MSD, Mining Commission, NCAA
No defined backup restoration testing procedures	NIMR, MOI, PMO-LYED, STAMIGOLD
No backup restoration tests	TCU, GPSA, TANROADS, TAA, MoCLA, PO-RALG, TBA, MNH

The noted anomalies and weakness can lead to prolonged recovery times and significant data loss during a disaster.

I recommend that the management of these entities (a) develop and operationalize BCP and DRP documents, review, and update DRP documents, define RPO and RTO, cover all critical application systems in BCP documents, define recovery teams, define recovery procedures for critical systems, test Disaster Recovery Plans, and conduct awareness training of the Disaster Recovery Plans (b) ensure backup is taken frequently, prepare an offsite backup environment, establish an offline backup mechanism, define backup restoration testing procedures, and conduct backup restoration testing regularly.

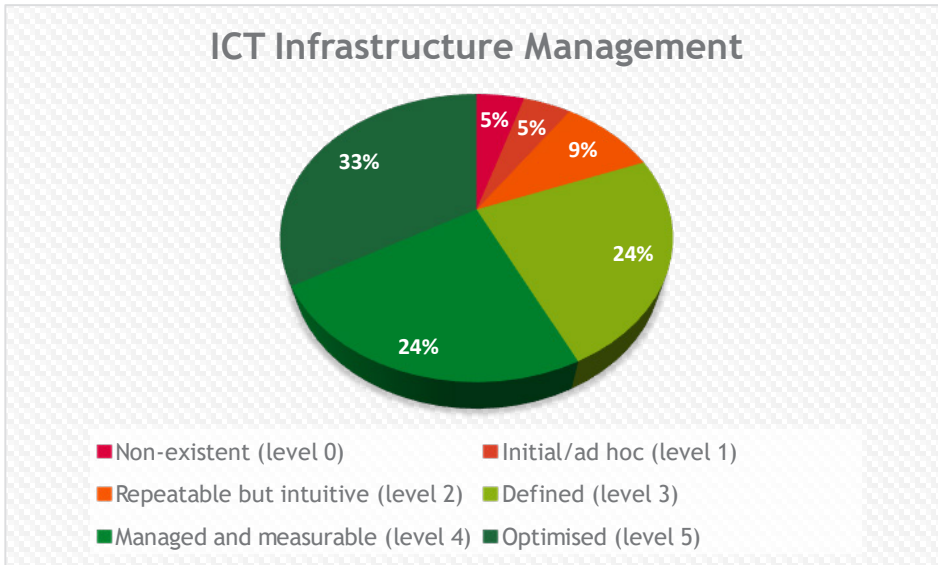
3.3 ICT Infrastructure Management

ICT infrastructure management is the process of managing an organization's technology infrastructure to ensure that it is operating efficiently and effectively. This includes planning, designing, deploying, operating, and maintaining technology systems and services. The infrastructure may include hardware, software, network, and data storage systems.

The audit assessed the compliance of 21 public entities with e-government standards and guidelines for ICT infrastructure management. The overall level of compliance is shown in **Figure 6** and the details of its results is summarized in **Appendix I**.



Figure 6: ICT infrastructure management compliance review



My further assessment of ICT infrastructure Management revealed inadequate infrastructure monitoring. At GPSA, TBA, EWURA, TCU, and MSD I noted that configured network and server monitoring tools were not adequately utilized whereby reports from these tools were not regularly reviewed or analysed, leading to untimely identification and resolution of infrastructure performance issues that could cause business disruption and data loss.

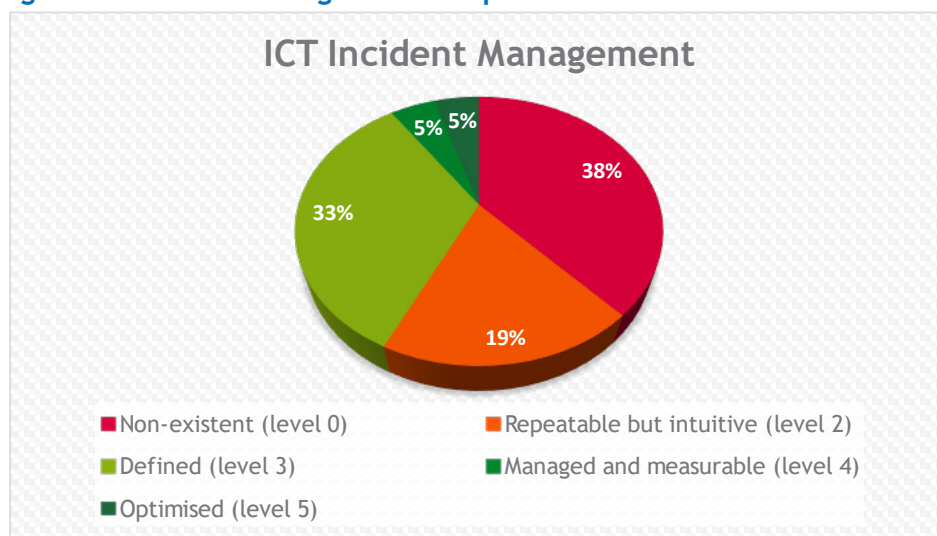
I recommend that MSD, TBA, EWURA, and TCU ensure monthly reports from infrastructure monitoring tools are reviewed, analysed, and reported to resolve noted exceptions.

3.4 ICT Incident Management

Incident Management is the efficient handling and resolution of incidents that affect service delivery. Proper incident management leads to improved customer satisfaction, increased efficiency, reduced downtime, better resource utilization, and an enhanced reputation for the organization. It also helps to identify and resolve underlying issues, leading to continuous improvement and increased efficiency in ICT operations.

The audit assessed the compliance of 21 public entities with e-government standards and guidelines for ICT Incident Management. The overall level of compliance is shown in **Figure 7** and the details of its results is summarized in **Appendix I**.

Figure 7: Incident management compliance review



In addition to assessing the level of compliance with ICT incident Management in audited public entities, my audit also evaluated the implementation of ICT incident Management in other entities without ranking. The audit identified several anomalies and weaknesses as summarized in the **Table 11**.

Table 11: Anomalies in ICT incident Management

Anomalies	Entities	Impact
Lack of Operational Level Agreements (OLA)	TANROADS, NIMR, JOT, TRC, TCU, MORUWASA, NECTA, TBA, PMO-LYED, MIIT, MLF-Livestock sector, EWURA, PO-RALG, WCF, TCAA, OTR, MOI, MNH, RITA, MoCLA, GPSA, MC, and MSD	lack of accountability in service delivery and the failure to measure key performance indicators
Lack of Documented Incident Management Procedures	TANROADS, NIMR, MORUWASA, TRC, TBA, JOT, MoCLA, MIIT, WCF, MNH, MOI, RITA, TCAA, and PO-RALG	delays in response to information system incidents and result in disruption of operations

Anomalies	Entities	Impact
Ineffective Reporting and Tracking of Incidents	NECTA, TCU, NIMR, GPSA, TCAA, MNH, MOI, RITA, TRC, JOT, PMO-LYED, TBA, MoCLA, MC, MIIT, MLF-Livestock sector, and MSD	Difficulties in recording and keeping incidents for later analysis to identify recurring issues for identification of root causes and finding permanent solutions

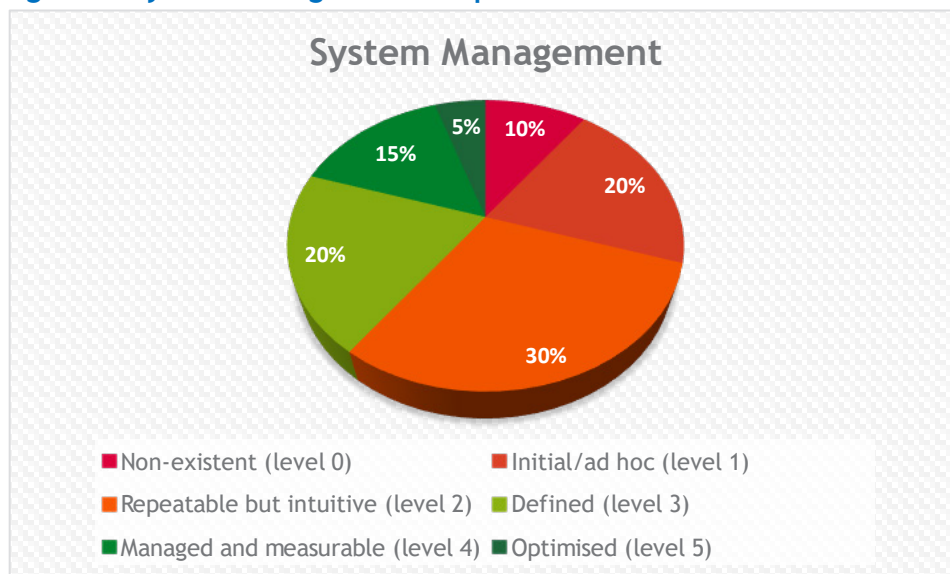
I recommend that management of the identified entities; (a) establish and operationalise OLA between the ICT department and other user departments for ICT service delivery performance measurement; (b) establish and operationalise formal documented procedures for handling incidents; and (c) ensure the availability of a tool through which incidents are reported.

3.5 System Management

An audit of application system management is a comprehensive evaluation of the processes, procedures, and controls in place for managing applications within an organization. The purpose of this audit is to assess the efficiency, effectiveness, and security of the application management system, identify potential risks, and provide recommendations for improvement.

The audit assessed the compliance of audited public entities with e-government standards and guidelines for System Management. The overall level of compliance is shown in **Figure 8** and the details of its results is summarized in **Appendix I**.

Figure 8: System management compliance review



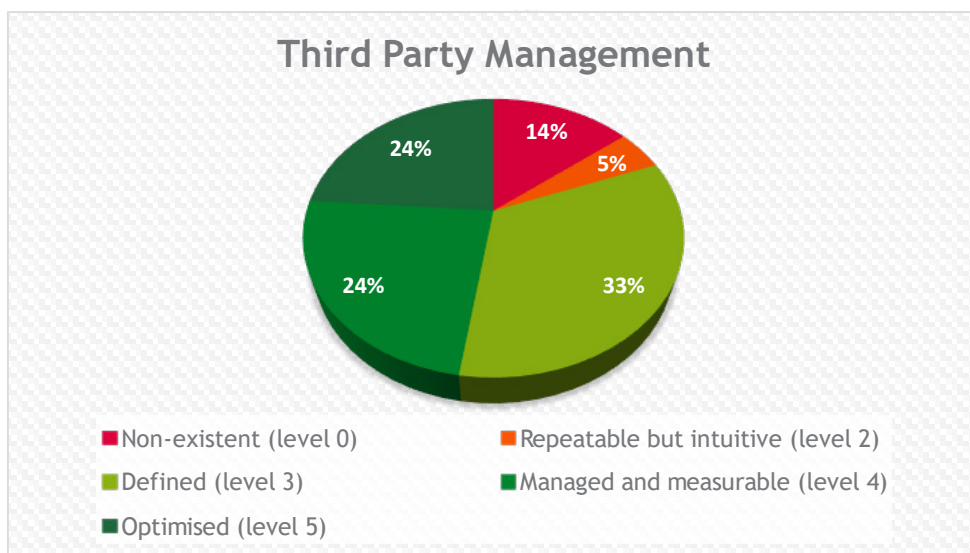
The audit of application system management has revealed key issues, including lack of review of privileged accounts, absence of adequate audit logs for databases and insufficient application logs details. The presence of default and generic accounts in databases and non-compliance with password security controls. The existence of active default database accounts, and the lack of recognition of internally developed application systems as intangible assets are also areas of concern. The audit has also noted anomalies in the acquisition and development of application systems, the usage of an operating systems and database management systems that are out of support.

I recommend that e-Government Authority to ensure public entities (a) conduct a review of all privileged accounts and implement regular monitoring to ensure that access is only granted to those who require it (b) Audit logs for databases and application systems should be enhanced to provide more detailed information on user activity, while password security controls should be strengthened (a) Eliminate default and generic accounts, upgrade outdated operating systems and database management systems (c) Recognize internally developed systems as assets, and address anomalies in the acquisition and development of application systems by implementing more rigorous project management and quality control processes.

3.6 Third Party Management

The management of ICT (Information and Communications Technology) vendors plays a critical role in ensuring the successful implementation and maintenance of technology solutions within an organization. My review of ICT third party management included assessment of key components such as contract management, vendor performance monitoring, and risk management. The objective of the audit was to determine the effectiveness and efficiency of the ICT vendor management process and to identify areas for improvement to ensure that the organization can effectively manage its ICT vendor relationships and minimize risks. Refer **Figure 9** which illustrates compliance level with third party management and the details of its results is summarized in **Appendix I**.

Figure 9: Third party management compliance review



It is essential for organizations to establish and maintain proper contracts and Service Level Agreements with their ICT service providers, review MoUs, monitor service provider performance, and have adequate ICT third-party management to ensure accountability and effective service delivery. My audit of ICT vendor management across various organizations noted the following issues:



3.6.1 Lack of Contract and Service Level Agreements with ICT Service Providers

The audit of ICT vendor management revealed government agencies that lack contracts and Service Level Agreements (SLA) with their respective ICT service providers, as shown in **Table 12**.

Table 12: Lack of Service Level Agreements with ICT Service Providers

Entity	Service provider	Service
GPSA	eGA	Hosting and internet services
TCAA	Indra	Aeronautical billing system (ABS)
NIMR Mwanza centre	TTCL	Internet service provision
	Prelink Medical Solutions	LIMS Application System
RITA	DIT	Consulting service on designing, developing, and implementing trustees' management system
	eGA	Marriage and Divorce System
	TTCL	Internet service
STAMICO	TTCL	Internet service provision
MNH	TTCL	Network services
	Vodacom	Network services
MoCLA	e-Government	Hosting and providing of internet service
	National Internet Data Center (NIDC)	Outdated Service Level Agreement (SLA) for hosting secondary sites
TBA	National Internet Data Centre (NIDC)	Internet service and application hosting
MLF	eGA	Application hosting service
	TTCL	Internet service

Lack of contracts and SLAs with ICT service providers could pose risks to these government agencies, including service disruption, data breaches, and vendor lock-in.

I recommended that these agencies establish formal agreements with their respective ICT service providers to mitigate these risks and ensure smooth service delivery.

3.6.2 Inadequate monitoring of service providers' performance

A review of ICT service provider performance monitoring at various government agencies; including EWURA, TANROADS, NECTA, TASAC and the



Ministry of Constitutional and Legal Affairs, revealed inadequate monitoring which leads to a hindrance in service improvement.

I recommend that these agencies establish a mechanism to monitor service provider performance and ensure that the monitoring is regularly conducted.

3.6.3 Uncontrolled Access of Vendors to Information Systems

During my audit of TTCL-PESA at TTCL and TASAC, I found out vendors were granted uncontrolled access to the information systems. Vendors had unrestricted access to the database servers and remote network access was granted indefinitely without regular review of vendor activities. This poses a risk to the security and sustainability of the system, as data may be inappropriately used and disseminated by the vendors or their employees.

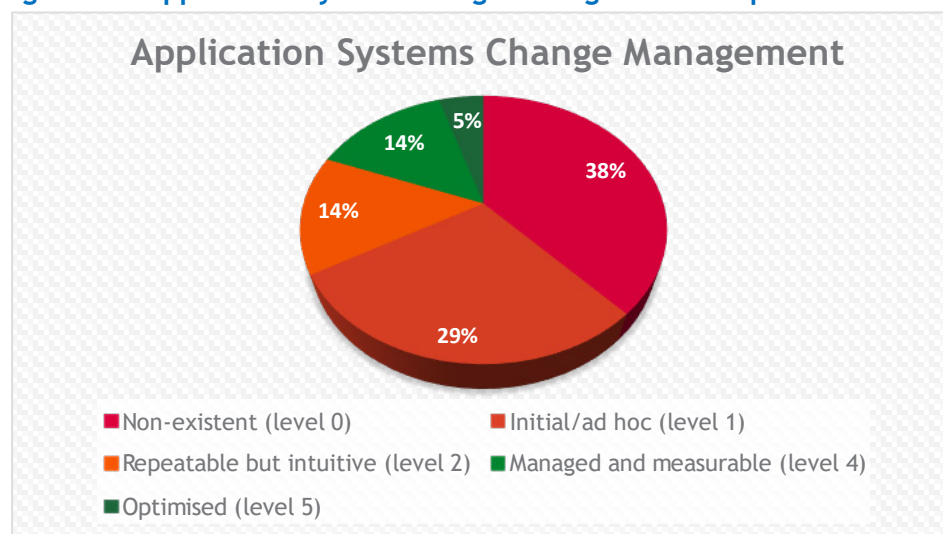
I recommend that TTCL and TASAC revoke vendor access and only grant access on a need basis to ensure the security and sustainability of their information systems.



3.7 Application systems Change Management

A change control framework is important to ensure consistent, reliable, and efficient changes. An evaluation of policies, procedures, and controls for managing changes to application systems is necessary to maintain the confidentiality, integrity, and availability of systems. All changes should be authorized, tested, implemented, and recorded with implementation and rollback plans in place to recover from adverse impacts.

The audit assessed the compliance of 21 public entities with e-government standards and guidelines for Application systems Change Management. The overall level of compliance is shown in **Figure 10** and the details of its results is summarized in **Appendix I**.

Figure 10: Application system change management compliance review

Alongside the assessment of compliance level for application systems change management in 21 audited public entities, my audit also evaluated the implementation of application systems change management in other entities without ranking and identified various anomalies and weaknesses as depicted in **Table 13**.

Table 13: Anomalies in application systems change management

Findings	Entities with Finding
Lack of documented change management procedures	NECTA, TCAA, TANROADS, NIMR, PMO-LYED, TBA, MIIT, Mining Commission, JOT
Unapproved change management procedure document	TCU, MLF (Livestock sector)
Lack of documented change rollback procedures	NECTA, TCU, TCAA, NIMR, TRC, RITA, PO-RALG, MIIT, MLF (Livestock sector), Mining Commission, TBS
Lack of documented change emergency handling procedures	NECTA, TCU, GPSA, TCAA, TANROADS, NIMR, TRC, PO-RALG, MIIT, Mining Commission, RITA
Lack of practice for identifying and updating systems documentation because of the changes implemented	NECTA, TCU, GPSA, TCAA, TANROADS, NIMR, TRC, PO-RALG, MIIT, MLF (Livestock sector), Mining Commission, TBS

Absence of these formalized change management procedures can lead to adverse effects on entities' operations, such as unplanned or excessive system downtime, ineffective and insufficient restoration of a system to its

original state, implementation delay of critical changes, and difficulty in support, maintenance, and modification of the application systems.

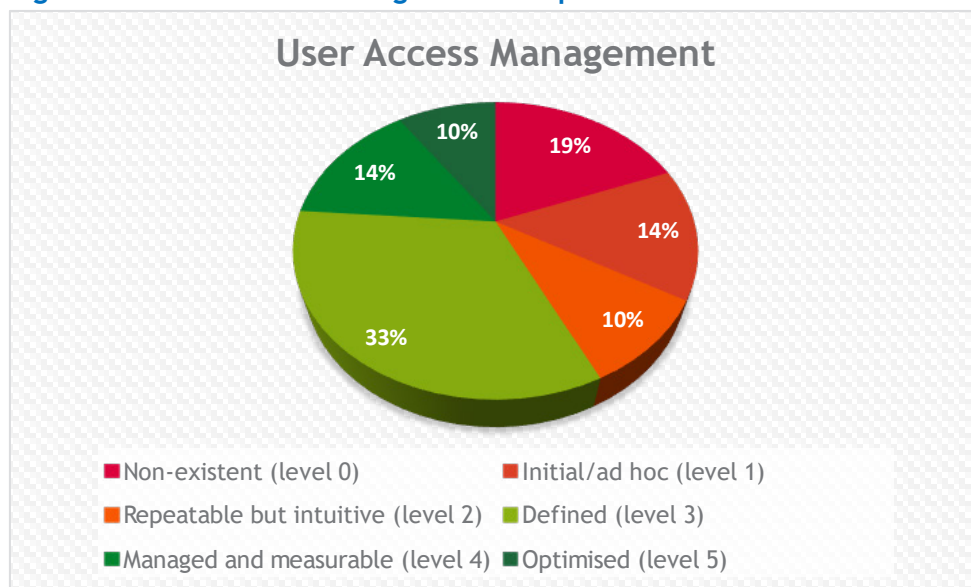
I recommend that NECTA, TCAA, TANROADS, NIMR, JOT, TCU, TBA, PMO-LYED, MIT, MC, MLF, TRC, RITA, GPSA, PO-RALG, and TBS develop, document, approve, and operationalize change management procedures, including documented change rollback and emergency change handling procedures, and practice for identifying and updating systems documentation because of the changes implemented.

3.8 User Access Management

Review of user access management intends to assess the effectiveness and efficiency of the User Access Management system within the organization. The objective was to identify any potential weaknesses in the user access management that could pose risks to the confidentiality, integrity, and availability of the organization's information and systems.

The audit assessed the compliance of 21 public entities with e-government standards and guidelines for user access management. The overall level of compliance is shown in **Figure 11** and the details of its results is summarized in **Appendix I**.

Figure 11: User access management compliance review



Alongside the assessment of compliance level for user access management in 21 audited public entities, my audit also evaluated the implementation of user access management in other entities without ranking and identified various anomalies and weaknesses as depicted in **Table 14**.

Table 14: Anomalies noted in user access management

Finding	Organizations Affected
Lack of regular reviews of user activities and access rights	TCU, GPSA, TANROADS, NIMR, NECTA, TRC, NIC, TPDC, TR, MORUWASA, Ministry of Constitutional and Legal Affairs, Mining Commission, PMO-LYED, TBA, PO-RALG, EWURA, Ministry of Livestock and Fisheries
Absence of formal procedures for granting and revoking user access to application systems and databases	PO-RALG, PMO-LYED

Lack of review can lead to unapproved and unauthorized users having access to applications or infrastructure.

I recommend that these organizations implement user access management controls, including regular reviews of user access rights and activities. Also, I recommend that the management of PO-RALG and PMO-LYED establish a procedure for granting and revoking access to application systems and databases to enhance their user access management process.

CHAPTER FOUR

ICT PROJECT MANAGEMENT

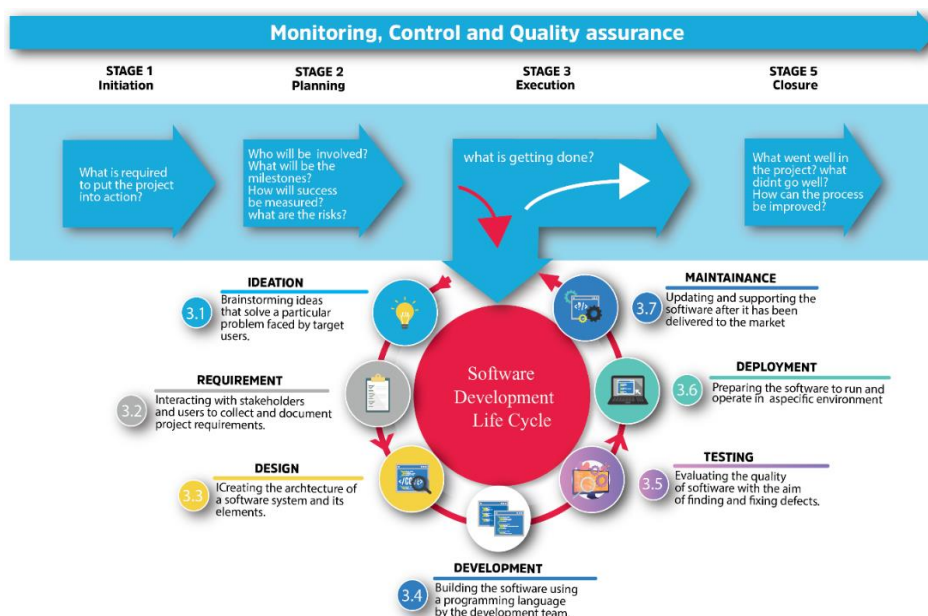


ICT PROJECT MANAGEMENT

4.0 Introduction

Sect. 24(1)-(2) of the e-Government Act, 2019 requires public institutions to implement ICT projects in a manner that ensures the anticipated benefits achieved and risks are optimized by complying with technical standards and guidelines as prescribed by the Authority.

This chapter presents assessment of effectiveness and efficiency of the ICT project management process within public institutions. The assessment provides an in-depth examination of the various stages of the ICT project management life cycle, including project initiation, planning, execution, monitoring and control, and closure.



The audit has been conducted to identify areas of improvement in the management of ICT projects and to ensure that organizations are maximizing the benefits of investments in technology. The findings and recommendations will serve as a valuable resource for decision-makers and stakeholders in the development and implementation of future ICT

projects. My audit of ICT projects implementation noted the following anomalies.

4.1 Delay in projects implementation

I have reviewed the implementation of several ICT projects in five entities and observed that these projects have experienced significant delays ranging from several months to over two years due to various reasons such as lack of funds and incomplete system requirements. Details of these projects and implementing entities are shown in **Table 15**.

Table 15: Delay in projects implementation

S/N	Name of the Entity	Project (Name of the system)	Delay	Project Cost (TZS)	Amount Spent (TZS)	Project Status
1	RITA	Civil Registrations	1 year and 11 months	170,000,000	68,000,000	Rollout
2	PO-RALG	TAUSI	1 year and 5 months	1,512,339,220	974,400,000	Rollout
3	MIIT	Data Warehouse	1 year	300,000,000	27,000,000	Development
4	TBA	Enhance of Government Real Estate Management	3 months	97,350,200.00	0	Development
5	MOCLAS	Justice Sector dashboard	2 years	413,660,000	413,660,000	Development

These delays can potentially result in project cost overrun and hinder the achievement of the intended goals.

I recommend that these government agencies ensure adequate funding and timely completion of their respective projects to avoid any further delays and maximize the potential benefits of the projects.

4.2 Lack of ICT Projects documentations

The e-Government ICT project review procedure requires public institutions to create an ICT Project Document (IPD) for projects, including project proposals, business cases, timelines, and financial considerations. However, the review of the ICT project management at TRC, MSD and TPA found out these entities have implemented various projects without proper

documentation, which can lead to unsustainable systems, missed objectives, delays, and cost overruns.

I recommend that these institutions should ensure they establish approved project documentation in line with e-Government guidelines.

4.3 Lack of mechanism to track application systems development costs

TRC, TANROADS, and NECTA, did not have a mechanism for tracking the costs associated with developing their application systems. This lack of a costing mechanism could lead to misstated values of reported intangible assets in the financial statements as required by Para 55 of IPSAS 31 Intangible Asset. This could potentially misleading management's decision-making process.

I recommend these establish a mechanism for tracking the costs associated with developing their application systems, report the value of internally developed application systems in their financial statements, and improve their record-keeping practices.

4.4 Nonperforming of Post-implementation review

Review of project management at TANROADS noted that post-implementation review for four projects implemented on developing Electronic Data Management, Software-Axle Weighers, Roads Maintenance Management, and Traffic Information Database System. Likewise, the same issue was noted at GPSA for Integrated Management Information System project. Lack of such review prevents public institutions from determining whether project objectives were met, how effectively the project was achieved, and learning lessons for the future.

I recommend that GPSA and TANROADS conduct post-implementation reviews to ensure project objectives are met.

4.5 Unproductive decisions in the establishment and implementation of ICT initiatives

During my review of ICT project implementation at TPA, I observed unproductive decision-making by the Authority in initiating and managing ICT projects. Specifically, the Authority began a project to improve the existing Terminal Operating System (TOS) for deep sea operations while

simultaneously initiating a project to develop the Port Operations System (POS) to replace TOS. Later, the Authority also commenced development of the Port Operations Application System (POAS) for Lighter Quay operations only but decided to include deep sea operations in the same project before its completion.

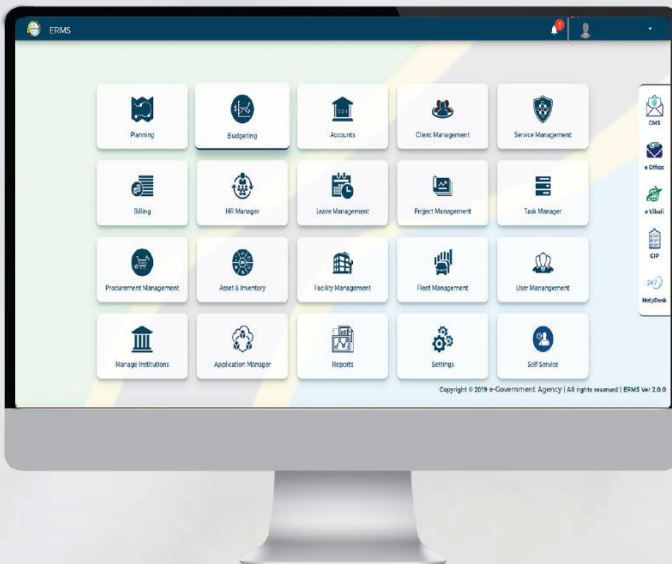
However, in year 2021/22 I found out management advertised a tender to get a vendor to resume the enhanced TOS project for both deep sea and lighter quay. These decisions have led to failed projects and increased project implementation costs.

I recommend that TPA conduct business process re-engineering and develop an Enterprise Architecture (EA) and technology roadmap before acquiring or enhancing any ICT systems.



CHAPTER FIVE

OPERATIONS EFFICIENCY OF THE E-GOVERNMENT AUTHORITY



OPERATIONAL EFFICIENCY OF THE E-GOVERNMENT AUTHORITY

5.0 Introduction

The e-Government Authority is responsible for enforcing compliance of public institutions with the e-Government related laws, regulations, standards, and guidelines for the planning, acquisition, implementation, delivery, support, and maintenance of ICT infrastructure and systems.

This chapter is based on an audit conducted to assess the performance of the Authority in fulfilling its responsibilities. The audit findings reveal several areas of concern, including inadequate compliance enforcement, inefficient ICT project review and approvals, and non-approval of software and hardware procured by public institutions.

5.1 Inadequate compliance enforcement

The e-Government Authority failed to complete all planned compliance assessments for public institutions in the 2021/22 year, as it only conducted 30% of them. Additional directives and unplanned assessment requests from public entities prevented the Authority from completing all assessments. This lack of enforcement of compliance by the e-Government Authority has significant implications for the effectiveness of e-Government initiatives and public services.

I recommend that e-Government Authority consider accommodating on-demand requests for compliance assessments in its annual action plan.

5.2 Inadequate verification of compliance recommendations

In the year 2021/22, the e-Government Authority conducted 61 compliance assessments. However, it only conducted one follow-up on the implementation of recommendations out of the 61 assessments, which constituted only 1.6% of the total assessments. This left 98.4% of the assessments not being followed upon, which is contrary to Reg. 36 (3) of e-Government General Regulations, 2020. The inadequate monitoring on the implementation of issued recommendations to public institutions resulted in noncompliance of public institutions with e-government guidelines and standards.

I recommend that the e-Government Authority improve its monitoring of compliance recommendations that are issued to public institutions by implementing a more effective system. Additionally, the e-Government Authority should include the status of the implementation of these recommendations in its biannual compliance assessment report.

5.3 Inefficient ICT projects review and approvals

My review of e-Government Authority's ICT project approval process revealed that 36 out of 53 projects were approved beyond the required 14 working days, and 20 projects have been waiting for approval for more than four months contrary to Reg. 28 of e-Government General Regulations, 2020. Inefficiency in review process can compromise the quality, relevance, sustainability, and value for money of the projects, as well as result in the duplication of application systems.

Furthermore, the audit revealed that 1 out of 5 ICT projects contracted to e-GA by public entities was reviewed and approved by Initiatives and Projects Management Section of the Authority.

I recommend that e-Government Authority monitor review process and approve projects within required timeframe, as per e-Government General Regulations and Government ICT Projects Review criteria and subject all ICT projects to the review process.

5.4 Inadequate customer service support

My review of e-Government Authority's (e-GA) Client Service Charter has identified two critical issues that require attention: inadequate customer service support and inadequate customer satisfaction tracking.

There were 216 incidents where e-GA took more than 30 days to attend to customers' complaints, which is in contravention of the Client Service Charter that mandates the Authority to resolve issues between 72 hours to 30 days. Such delays in attending to customer complaints could cascade to public institutions and ultimately delay service delivery to citizens.

Further, e-GA failed to conduct an annual customer satisfaction survey in the year under review, which hinders the Authority's ability to improve its services. To enhance its ICT support service delivery in public entities

I recommend that e-GA (a) regularly monitor and ensure timely resolution of reported incidents by public institutions; (b) conducts an annual customer satisfaction survey and follows up on its recommendations.



CHAPTER SIX

CONCLUSSION

06

CONCLUSION

The audit findings demonstrate the critical need for Tanzanian government to address significant weaknesses and deficiencies in their information and communication technology internal controls. These issues have the potential to result in revenue loss and potentially fraudulent activities.

To improve their operations, reduce revenue losses, and enhance their credibility and reputation, public entities must prioritize enhancing their system controls, reviewing their policies and procedures, and establishing appropriate controls to ensure compliance with e-Government act number 10 of 2019 and its regulations.

Similarly, it is essential to address the identified weaknesses in the government's ICT systems to enhance transparency, accountability, and effective service delivery. Taking these steps will help these entities overcome their weaknesses, improve service delivery, and enhance the effectiveness of ICT systems in public institutions.



Appendix I: Compliance Levels and Entities for Various ICT Management Domains

Domain	Compliance Level	No of Entities	Entities
Access Management	level-0	4	MIIT, PMO-LYED, NECTA, TRC
	level-1	3	MLF, MINING COMMISSION, RITA
	level-2	2	NIMR, JOT
	level-3	7	TBA, MoCLA, EWURA, WCF, UTT, TCU, MSD
	level-4	3	TANROADS, TCAA, PO-RALG
	level-5	2	PSSSF, GPSA
		21	
Application systems Change Management	level-0	8	MLF, MIIT, PMO-LYED, MINING COMMISSION, TANROADS, RITA, NIMR, TRC
	level-1	6	TBA, UTT, TCU, NECTA, MSD, JOT
	level-2	3	TCAA, GPSA, PO-RALG
	level-4	3	MoCLA, WCF, PSSSF
	level-5	1	EWURA
		21	
ICT Incident Management	level-0	8	TBA, MLF, MIIT, MoCLA, PMO-LYED, MINING COMMISSION, TCU, NIMR
	level-2	4	RITA, JOT, GPSA, TRC
	level-3	7	EWURA, WCF, UTT, TANROADS, TCAA, NECTA, MSD
	level-4	1	PO-RALG
	level-5	1	PSSSF
		21	
ICT Infrastructure Management	level-0	1	MIIT
	level-1	1	MINING COMMISSION
	level-2	2	MLF, TRC
	level-3	5	TBA, UTT, TCU, MSD, GPSA
	level-4	5	MoCLA, TANROADS, RITA, NIMR, NECTA
	level-5	7	PMO-LYED, EWURA, WCF, TCAA, PSSSF, JOT, PO-RALG
		21	
	level-0	6	MLF, MIIT, PMO-LYED, TANROADS, NIMR, TRC

Domain	Compliance Level	No of Entities	Entities
ICT Service Continuity Management	level-1	2	NECTA, JOT
	level-2	8	TBA, MoCLA, MINING COMMISSION, TCAA, RITA, MSD, GPSA, PO-RALG
	level-3	2	UTT, TCU
	level-4	2	EWURA, PSSSF
	level-5	1	WCF
		21	
Strategy Management for IT Services	level-0	1	MLF
	level-1	3	MIIT, TRC, PO-RALG
	level-2	5	TBA, PMO-LYED, MINING COMMISSION, TANROADS, RITA
	level-3	4	MoCLA, UTT, NIMR, GPSA
	level-4	7	EWURA, WCF, TCU, TCAA, PSSSF, NECTA, MSD
	level-5	1	JOT
		21	
System Management	level-0	2	MLF, NECTA
	level-1	4	PMO-LYED, RITA, NIMR, TRC
	level-2	6	MoCLA, MINING COMMISSION, UTT, TCU, MSD, JOT
	level-3	4	TBA, EWURA, TANROADS, GPSA
	level-4	3	WCF, TCAA, PO-RALG
	level-5	1	PSSSF
	level-N/A	1	MIIT
		21	
Third Party Management	level-0	3	TBA, PMO-LYED, GPSA
	level-2	1	RITA
	level-3	7	MIIT, MoCLA, MINING COMMISSION, UTT, TANROADS, NIMR, MSD
	level-4	5	MLF, EWURA, TCAA, NECTA, TRC
	level-5	5	WCF, TCU, PSSSF, JOT, PO-RALG
		21	

Appendix II: List of Audited Public entities.

Sn	Name of Entity
1	Public Service Social Security Fund (PSSSF)
2	National Examinations Council of Tanzania (NECTA)
3	National Institute for Medical Research (NIMR)
4	Tanzania Railways Corporation (TRC)
5	Registration Insolvency and Trusteeship Agency (RITA)
6	Government Procurement Services Agency (GPSA)
7	Unit Trust of Tanzania (UTT)
8	Medical Stores Department (MSD)
9	Tanzania National Roads Agency (TANROADS)
10	Tanzania Civil Aviation Authority (TCAA)
11	Workers Compensation Fund (WCF)
12	Judiciary of Tanzania
13	Tanzania Buildings Agency (TBA)
14	Tanzania Commission for Universities (TCU)
15	Energy and Water Utilities Regulatory Authority (EWURA)
16	Mining Commission
17	President's Office Regional Administration and Local Government (PO-RALG)
18	Ministry of Investment, Industry and Trade (MIIT)
19	Ministry of Livestock and Fisheries (Livestock section)
20	Ministry of Constitutional and Legal Affairs (MoCLA)
21	Prime Minister's Office - Labour, Youth, Employment and Persons with Disabilities (PMO-LYED)