THE UNITED REPUBLIC OF TANZANIA
NATIONAL AUDIT OFFICE (NAOT)

ISO 9001:2015 Certified

ANNUAL GENERAL REPORT ON INFORMATION SYSTEMS AUDITS

Controller and Auditor General
March 2026

THE UNITED REPUBLIC OF TANZANIA

NATIONAL AUDIT OFFICE

ISO 9001:2015 Certified

Controller and Auditor General, National Audit Office, Ukaguzi House, Mahakama Road, P.O. Box 950, 41104
Tambukareli, Dodoma. Telephone: 255(026)2161200-9,
E-mail: ocag@nao.go.tz, Website: www.nao.go.tz

Ref. No. CGA.23/421/2 **30 March 2026**

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

RE: ANNUAL REPORT OF THE CONTROLLER AND AUDITOR GENERAL ON THE AUDIT OF THE INFORMATION SYSTEMS FOR THE FINANCIAL YEAR 2024/25

I am pleased to submit my Annual General Report on the audit of the Information Systems for the financial year 2024/25 in accordance with Article 143(4) of the Constitution of the United Republic of Tanzania of 1977, and Sect. 34 of the Public Audit Act, Cap. 418.

This report presents audit findings and the recommended measures of redress that aim to foster accountability in the management and use of public resources, particularly those embedded within information systems and information technology infrastructure.

I humbly submit,

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

ABOUT THE NATIONAL AUDIT OFFICE

MANDATE

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

Vision, Mission & Motto

Vision 01

OUR VISION

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

Mission 02

OUR MISSION

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

Motto 03

OUR MOTTO

Modernizing External Audit for Stronger Public Confidence.

Core Values

Independence & Objectivity An impartial institution independently offering high-quality audit services in an unbiased manner.	**Professional Competence** Delivering audit services based on professional knowledge, skills, and best practices.
Integrity Observing high ethical standards and rules of law in the delivery of audit services.	**Creativity & Innovation** Encouraging value-adding ideas for continuous improvement of audit services.
Results-Oriented Focusing on reliable, timely, accurate, and clear performance targets.	**Teamwork Spirit** Valuing and working together with internal and external stakeholders.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviation	Description
Afya eHMS	Afya – electronic Health Management System
AMCOS	Agricultural Marketing Cooperative Societies
BiDMIS	Billing and Debt Management Information System
BPRA	Business and Property Registration Agency
BTI	Beekeeping Training Institute
CIMS	Conservation Information Management System
CRB	Contractors Registration Board
DART	Dar Rapid Transit Agency
DFCTS	The Digital Food Commodity Tracking System
DROMAS	District Roads Management System
DSFA	Deep Sea Fishing Authority
DUCE	Dar es Salaam University College of Education
EMS	Event Management System
ERMS	Enterprise Resources Management Suite
FFARS	Facility Financial Accounting and Reporting System
FIS	Fertiliser Information System
GBT	Gaming Board of Tanzania
GCLA	Government Chemist Laboratory Authority
GePG	Government electronic Payment Gateway
GoTHOMIS	Government of Tanzania Health Operations Management Information System
GPSA	Government Procurement Services Agency
HCMIS	Human Capital Management Information System
IAA	Institute of Accountancy Arusha
ICT	Information Communication Technology
IFMIS	Integrated Financial Management Information System
iHMIS	Integrated Hospital Management Information System
INTOSAI	International Organization of Supreme Audit Institutions
IPRS	ICT Professional Registration System
ISMS	Integrated Student Management System
ISSAIs	International Standards of Supreme Audit Institutions
ITGCs	Information Technology General Controls
JOT	Judiciary of Tanzania
KADCO	Kilimanjaro Airports Development Company Limited
LGTI	Local Government Training Institute
LIMS	Library Information Management System
MWAUWASA	Mwanza Urban Water Supply and Sanitation Authority
MoCLA	Ministry of Constitutional and Legal Affairs
MoW	Ministry of Water
NFRA	National Food Reserve Agency
NIDA	National Identification Authority
NIRC	National Irrigation Commission
OAG	Office of the Attorney General
OAGMIS	Office of Attorney General Management Information System

Abbreviation	Description
OAS	Online Application System
ORS	Online Registration System
OSG	Office of the Solicitor General
OWAIS	Online Work Permit Application and Issuance System
PAMIS	Postgraduate admission management information system
PCT	Pharmacy Council's of Tanzania
PMIS	Professional Management Information System
PMO-LYED	Prime Minister's Office – Labour, Youth, Employment and Disabilities
RITA	Registration Insolvency and Trusteeship Agency
RMMS	Road Maintenance Management System
SDD	System Design Document
SGR	Standard Gauge Railway
SOC	Service Organization Controls
SRS	System Requirement Specification
STAMICO	State Mining Corporation
TAA	Tanzania Airports Authority,
TALIRI	Tanzania Livestock Research Institute
TANCIS	Tanzania Customs Integrated System
TARI	Tanzania Agricultural Research Institute
TASAC	Tanzania Shipping Agencies Corporation
TAWA	Tanzania Wildlife Management Authority
TBC	Tanzania Broadcasting Corporation
TBS	Tanzania Bureau of Standards
TCB	Tanzania Coffee Board
TFB	Tanzania Film Board
TIRA	Tanzania Insurance Regulatory Authority
TMX	Tanzania Mercantile Exchange
TPA	Tanzania Ports Authority
TPRB	Town Planners Registration Board
TRC	Tanzania Railways Corporation
TTCL	Tanzania Telecommunications Company Limited
UCMS	The Unified Coffee Management System
VRB	Valuers Registration Board
WCF	Workers Compensation Fund
WMA	Weights and Measures Agency
WMA-MIS	Weights and Measures Agency - Management Information System
WRBWB	Wami/Ruvu Basin Water Board

STATEMENT
OF THE CONTROLLER AND AUDITOR GENERAL

It is my honour to submit the Annual General Report on Information Systems Audit for the Financial Year ended 30 June 2025. The report presents the results of audits conducted in 133 public institutions, focusing on ICT governance, cybersecurity, IT General Controls, system integration, and compliance with the e-Government Act, 2019 and related national ICT frameworks.

I commend the Government, under the leadership of Her Excellency Dr. Samia Suluhu Hassan, President of the United Republic of Tanzania, for its continued efforts to advance digital transformation in the public sector. As Government operations increasingly depend on digital systems, effective governance and strong ICT control environments are essential to ensure secure, reliable, and efficient service delivery and to sustain public trust.

Despite progress in ICT adoption, the overall ICT governance and control environment across public institutions remains inadequate to support secure and integrated digital Government operations. Weak governance oversight, gaps in compliance and IT General Controls, fragmented systems, and continued reliance on manual processes limit the benefits of ICT investments and increase exposure to cybersecurity, data integrity, and service delivery risks. Furthermore, although the SOC Type 2 audit confirmed the existence of control frameworks in centrally managed Government systems, identified deficiencies may heighten the risk of unauthorised access, uncontrolled system changes, and delayed response to ICT incidents.

In view of these challenges, public institutions are required to strengthen ICT governance structures, enhance compliance with established standards, improve system integration, and reinforce internal control frameworks to ensure that ICT investments effectively support accountable and efficient public service delivery. Accounting Officers, Governing Boards, and oversight authorities are therefore urged to take timely action in implementing the recommendations contained in this report.

The National Audit Office remains committed to executing its mandate with professionalism, independence, and integrity. Strong and secure information systems are fundamental to safeguarding public resources and sustaining citizens' confidence in Government digital services.

Finally, I extend my sincere appreciation to the staff of the National Audit Office and partner audit firms for their dedication and professionalism in supporting the fulfilment of our constitutional responsibilities.

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

EXECUTIVE SUMMARY

Introduction

1. This report presents the Audit findings on Information Systems conducted for the Financial Year 2024/25, encompassing 133 public institutions. The primary objective was to evaluate the adequacy and effectiveness of Information Communication Technology (ICT) governance frameworks, the implementation of IT General Controls (ITGCs), Service Organisation Controls (SOC Type 2), compliance with the e-Government Act of 2019, system utilisation and integration, and project management practices. The audit employed a risk-based approach guided by international standards, including ISSAI, COBIT 5, and ISO/IEC 27001.

Government Service Organisation Controls (SOC Type 2)

2. A specialised SOC Type 2 review was conducted on four key government ministries that provide shared and centralised systems: the Ministry of Finance, the Ministry of Water, the Prime Minister's Office – Regional Administration and Local Government (PMO-RALG), and the President's Office – Public Service Management and Good Governance (PO-PSMGG). While the systems were generally designed to achieve service commitments, the review identified significant control exceptions. Across these ministries, major deficiencies included outdated Service Level Agreements (SLAs), lack of configuration baselines, unrevoked user access, inadequate patch management, changes deployed without adequate testing, and ineffective incident management and tracking.

Compliance with e-Government Laws and Standards

3. The audit assessed 133 public entities against 11 ICT compliance domains using a five-level maturity model. Positively, 75% (100 entities) achieved the required minimum Compliance Level 3 or higher, demonstrating defined and implemented ICT controls. However, 25% (33 entities) fell below the acceptable threshold. Entities performed best in IT Governance, Physical Controls, and Environmental Controls, but showed critical weaknesses in ICT Incident Management, Application Systems and Database Management, and Business Continuity and Disaster Recovery.

Information Technology General Controls (ITGCs)

4. An evaluation of ITGCs across 133 public entities revealed widespread weaknesses that threaten the confidentiality, integrity, and availability of government systems. Notable weaknesses include:

- **IT Governance:** 33 entities lacked approved ICT strategies, and 37 entities did not conduct formal IT risk assessments.
- **Network and Database Security:** 82 entities failed to apply security patches to network devices consistently, and 82 entities had inadequate database audit logging.
- **Information Security and Access Controls:** 99 entities failed to review security logs regularly, 92 entities did not promptly revoke access for exited staff, and 31 entities granted excessive administrator privileges.
- **Business Continuity & Third-Party Management:** 98 entities did not regularly test their BCP/DRP, and 44 entities engaged ICT vendors without formal contractual agreements.

5. **System Development, Functionality, and Process Automation**
The audit identified significant inefficiencies in how digital systems are utilised and managed:

- **Integration and Fragmentation:** Several critical systems are not integrated, necessitating manual data entry and reconciliations. Furthermore, multiple entities operate duplicated or

fragmented systems—such as BRELA's four independent systems or the Ministry of Health's varied hospital systems—which escalates costs and undermines interoperability.

- **Process Automation:** 32 entities continue to rely on manual procedures for core business functions like billing, revenue collection, and HR processes, increasing the risk of revenue leakage and human error.
- **ICT Project Management:** The audit found severe delays and poor documentation across multiple ICT projects. For instance, BRELA's Online Registration System redesign was delayed by five years, and TAWA's Conservation Information Management System by six years. Several critical projects also lacked foundational documents like System Requirements Specifications (SRS) and Risk Registers.

Conclusion and General Recommendations

6. The audit concludes that the existing ICT governance and control environment across the audited public institutions is not adequate to fully support secure, integrated, and efficient digital Government operations. While progress has been made, persistent fragmentation, manual interventions, and weak IT controls limit the value of ICT investments.

7. The report strongly recommends that management across all entities enforce e-Government compliance, fully integrate systems using approved interoperability standards, eliminate duplicate applications, and strengthen ITGCs particularly regarding access controls, network security, and business continuity. Specific recommendations were also directed to the e-Government Authority (eGA) to enhance its oversight of integration and system utilisation, and to the Ministry of Health to deploy a unified, interoperable hospital management system.

CHAPTER ONE

01

Introduction

1.1 Introduction

8. Information and Communication Technology (ICT) continue to play a critical role in strengthening public service delivery by enhancing efficiency, transparency, accountability, and operational effectiveness across government institutions. As reliance on automated systems increases in financial management, revenue administration, and service delivery, the role of ICT governance, security controls, and the effective utilisation of digital systems has become essential.

9. The enactment of the e-Government Act, 2019, together with its supporting Regulations and Standards, provides a comprehensive framework for managing, securing, and standardising public sector ICT resources. Effective implementation of these frameworks ensures system reliability, data integrity, interoperability, and the protection of public resources.

10. This report presents the findings of the Information Systems Audit conducted for the Financial Year 2024/25. The audit was designed to assess the adequacy and effectiveness of ICT governance frameworks, compliance with the e-Government Act, 2019, the implementation of IT General Controls (ITGCs), Service Organisation Controls (SOC Type 2), system duplication, underutilization, and the integration and automation of systems, and ICT project management practices.

1.2 Audit Objective

11. The main objective of this audit was to assess how well public institutions govern and manage ICT systems, implement effective controls, and comply with the e-Government legal and regulatory framework. Specifically, the audit aimed to:

- Assess whether IT General Controls (ITGCs) are adequately designed and effectively implemented to safeguard government systems and data.
- Evaluate the effectiveness of Service Organisation Controls (SOC Type 2) in selected institutions.
- Determine the level of compliance with the e-Government Act, 2019 and its supporting Regulations and Standards using a defined compliance assessment model.
- Examine the effectiveness of the integration and utilisation of application systems, as well as the automation of key business processes.
- Review the governance and management of ICT projects.

1.3 Audit Scope

12. The audit covered 133 public institutions utilising ICT systems in their operations during the Financial Year 2024/25. The primary focus was on assessing IT General Controls across selected Ministries, Departments, Agencies, and other public entities. In addition, a Service Organisation Controls (SOC Type 2) review was conducted for four institutions providing government shared and centralised systems and services, namely:

- The Ministry of Finance (MoF).
- The President's Office – Public Service Management and Good Governance (PO-PSMGG).
- The Ministry of Water.
- The Prime Minister's Office - Regional Administration and Local Government (PMO-RALG).

13. Furthermore, the scope included an evaluation of:

- Compliance against the e-Government Act, 2019 and related standards.
- System integration, optimisation, and utilisation.
- The automation of business processes to eliminate manual interventions.
- ICT project management practices.

1.4 Audit Methodology

14. The Information Systems Audit was conducted in accordance with the International Standards of Supreme Audit Institutions (ISSAIs) issued by the International Organisation of Supreme Audit Institutions (INTOSAI). The audit was also guided by relevant national laws and regulations, including the e-Government Act, 2019, and aligned with established ICT governance and security frameworks such as COBIT 5, ISO/IEC 27001, AFROSAI-E IT Audit Guidelines, and SOC 2 principles.

15. The audit approach was risk-based. It involved reviewing policies and procedures, conducting interviews with management and ICT personnel, inspecting system configurations and documentation, testing controls, and evaluating compliance using a structured assessment framework. The audit assessed the adequacy, effectiveness, and reliability of ICT systems and controls in supporting government operations and enhancing service delivery.

CHAPTER TWO

02

Government Service Organization Controls

2.1 Introduction

16. Service Organisation Controls (SOC) Type 2 is an internationally recognised assurance framework designed to evaluate the design and operating effectiveness of controls at service organisations that provide services impacting their users' information systems and data. A SOC Type 2 report assures whether controls related to security, availability, processing integrity, confidentiality, and privacy are suitably designed and have operated effectively over a defined period. Unlike point-in-time assessments, SOC Type 2 focuses on the continuous operation of controls throughout the year, thereby providing a higher level of assurance to system users and other stakeholders.

17. In the Government of Tanzania ICT landscape, several Ministries operate as government service organisations by hosting, managing, and operating centralised application systems that are relied upon by multiple public entities for critical financial, administrative, and service delivery functions. These Ministries provide shared ICT services similar in nature to commercial service organisations, as their systems directly support financial transactions, revenue collection, human resource management, billing, and reporting processes across the public sector. Consequently, weaknesses in controls at these service organisations may have a widespread impact on multiple user entities.

18. The audit of Service Organisation Controls (SOC) Type 2 was conducted across four government Ministries to provide independent assurance on the effectiveness of controls governing centrally hosted and managed application systems. The audited service organisations included:

- The Ministry of Finance, which manages the MUSE system, the Budget Management System, the Government Asset Management Information System (GAMIS), and the Government Electronic Payment Gateway (GePG);
- The Ministry of Water, which manages the Maji-IS billing system used by Water Supply and Sanitation Authorities;
- The Prime Minister's Office – Regional Administration and Local Government Authorities (PMO-RALG), which manages the TAUSI revenue system, Facility Financial Accounting and Reporting System (FFARS), and Government of Tanzania Health Operations Management Information System (GoTHOMIS); and
- The President's Office – Public Service Management and Good Governance (PO-PSMGG), which manages the Human Capital Management Information System (HCMIS) for payroll and human resource management.

19. The purpose of conducting SOC Type 2 audits in these Ministries was to ensure that user public entities relying on these centrally managed systems have relevant controls suitably designed and operated effectively throughout the audit period. In addition, the SOC reports assure regulators, oversight bodies, auditors, and the general public that government service organisations have established and maintained effective control environments to safeguard public resources, ensure the reliability of system outputs, and support the continuity of critical government services.

20. In line with this objective, an examination was performed on the systems of the Ministry of Finance, the Prime Minister's Office – Regional Administration and Local Government, the President's Office, Public Service Management and Good Governance and the Ministry of Water for the period 1 July 2024 to 30 June 2025. Internal controls were examined based on the applicable Trust Services Criteria.

2.2 Opinion/Conclusion

21. In my opinion, except for the effects of the matters described in the exceptions section, in all material aspects, based on the applicable trust services criteria and criteria identified in the statements of the Ministry of Finance, Prime Minister's Office – Regional Administration and Local Government, President's Office Public Service Management and Good Governance and the Ministry of Water:

(a) The description fairly presents the Ministries' systems as designed and implemented throughout the period from 1 July 2024 to 30 June 2025, in accordance with the description criteria;
(b) The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the Ministries' service commitments and system requirements would be achieved if the controls operated effectively throughout the period 1 July 2024 to 30 June 2025 and if user entities applied the complementary controls; and
(c) The controls stated in the description operated effectively throughout the period to provide reasonable assurance that Ministries' service commitments and system requirements were achieved based on the applicable trust services criteria, and if complementary subservice organisation controls and complementary user entity controls assumed in the design of Ministries' controls operated effectively throughout that period.

2.3 Exceptions

22. **Ministry of Finance**

(i). Log retention and archival processes were not governed by formally approved policies, and requirements for retention periods, archiving, and monitoring were not documented. This reduces assurance that system logs are properly maintained, protected, and available for monitoring or investigation.
(ii). The Service Level Agreement (SLA) between the Ministry of Finance and the e-Government Authority for hosting and support of critical systems expired in July 2024 and had not been renewed, weakening vendor oversight and accountability.
(iii). Periodic reviews of user access rights and activities were not performed for MUSE, GAMIS, CBMS, and GePG during the period under review to ensure continued appropriateness and alignment with job responsibilities.
(iv). Role-based access controls (RBAC) were not consistently enforced in MUSE, allowing non-finance staff to perform financial transactions beyond their assigned responsibilities.
(v). Segregation of duties controls in MUSE were not enforced, enabling the same users to initiate, examine, and approve critical transactions, including fund allocations, distribution withdrawals, fund transfers, vendor creation, goods receipt notes, and imprest creation and retirement.

(vi). The Disaster Recovery Plan (DRP) was neither formally approved nor tested, reducing assurance over the system's ability to recover in the event of disruption.

(vii). Configuration baselines for IT infrastructure, systems, and applications were not established or documented, reducing assurance that secure and consistent system settings are maintained.

(viii). Exception handling procedures were not formally defined, and system-generated exceptions, although logged, were not consistently reviewed, analyzed, or escalated, limiting effective monitoring.

(ix). Formal change management procedures were not approved or operationalized.

(x). Security assessments, including vulnerability testing, were not performed prior to implementing system changes

(xi). Post-implementation reviews were not conducted to validate the completeness, accuracy, and stability of deployed changes.

23. **President's Office Public Service Management and Good Governance**

(i). Privileged account activity is not monitored, increasing the risk that unauthorised administrative activity may go undetected, leading to unauthorised changes, data manipulation, or misuse of access.

(ii). Database encryption is not enabled, increasing the risk that sensitive data may be exposed if storage is compromised, potentially resulting in a confidentiality breach.

(iii). Changes did not follow established procedures (eight instances), increasing the risk that unapproved or incomplete changes may be implemented, which may result in system outages or data integrity issues.

(iv). Changes were deployed without adequate testing, increasing the risk that defects or vulnerabilities may be introduced, which may result in processing integrity failures.

(v). Patch maintenance was not conducted, leaving known vulnerabilities unaddressed, which may result in a security incident.

(vi). Root cause analysis is not formally conducted, increasing the risk of recurring service disruptions.

(vii). No formal configuration baseline documentation, increases the risk of unauthorised system changes, which may lead to security issues and make it difficult to detect changes.

(viii). Incident management procedures not followed, increases the risk of delayed or ineffective incident response, which may result in an escalation of the incident's impact.

24. **Prime Minister's Office, Regional Administration and Local Government**

(i). Users were granted system access; however, their respective access authorisation forms did not specify the assigned roles or detailed access rights.

(ii). Access was granted to application users without formally approved access authorisation.

(iii). Access to the FFARS system was not revoked in a timely manner following their termination or retirement.

(iv). Periodic user access review reports did not evidence verification of user status, completeness of the user population, or assessment of the appropriateness of assigned access rights.

(v). There is an absence of a formal log retention policy governing the retention period and management of system and security logs.

(vi). Configuration baseline documentation for production systems is not established.

(vii). There was insufficient documentation evidencing formal change testing and management authorisation for system changes implemented during the period under review.

25. **Ministry of Water**

(i). There is an incomplete definition of roles and responsibilities in agreements with service providers, as certain SLAs (e.g., MoW with eGA) do not clearly define responsibilities and obligations.

(ii). Incident management procedures are not followed in practice, as incidents are reported via informal channels (WhatsApp/phone) instead of being logged in the designated incident management tool.

(iii). Risk assessments are not performed or updated annually, including the absence of updated risk registers incorporating security, fraud, and strategic risks.

(iv). Periodic user access reviews are not effectively designed or performed, limiting assurance that user access remains appropriate and aligned with job responsibilities.

(v). Incident logging and resolution tracking are ineffective due to the absence of a centralised help desk or incident management system.

(vi). Timeliness of incident resolution cannot be determined, as incidents are not consistently logged and tracked against defined service-level expectations.

(vii). Changes are implemented without adherence to formal approval, testing, and documentation requirements.

(viii). Post-implementation reviews are not consistently performed for the implemented changes, increasing the risk of undetected errors and system instability.

(ix). Risk mitigation activities are not consistently implemented, as annual risk assessments and mitigation actions are not regularly performed in line with the documented risk management program.

(x). Absence of a formal log retention policy governing the retention period and management of system and security logs.

CHAPTER THREE

03

Compliance with e-Government Laws and Standards

3.1 Introduction

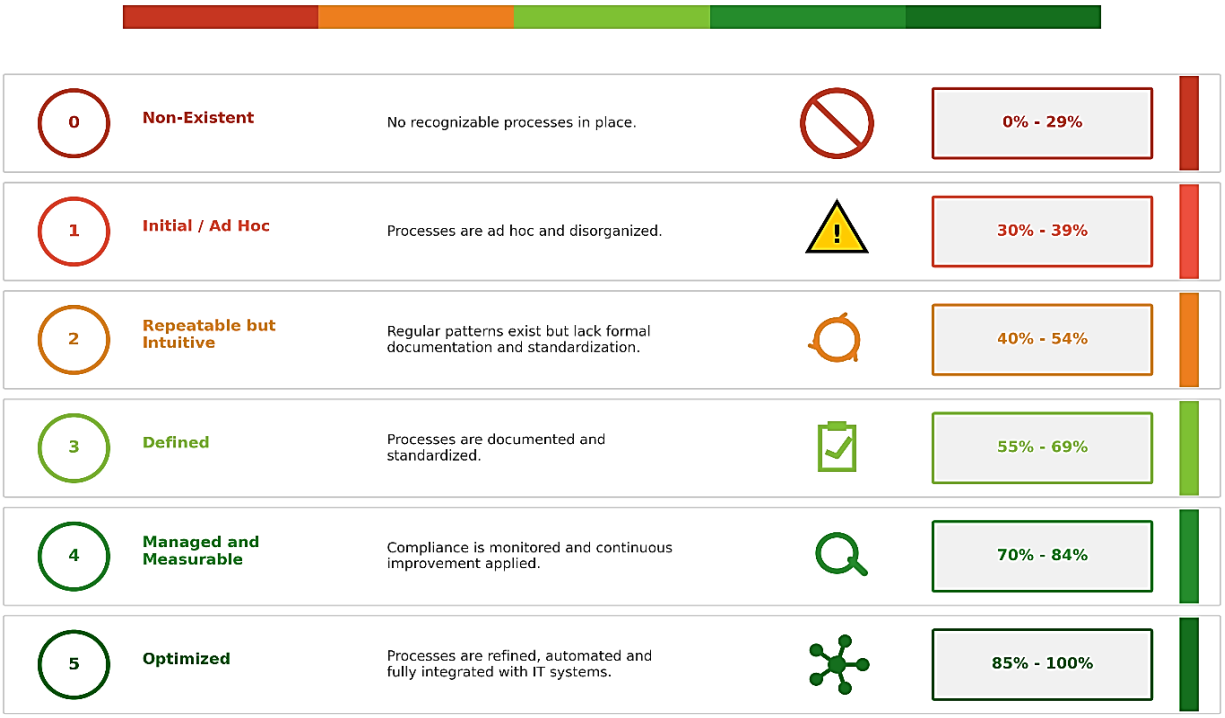
26. Compliance with e-Government laws, regulations, and standards is essential to ensure that public entities effectively leverage ICT to enhance service delivery, interoperability, security, and transparency. These requirements provide a structured framework for governing the use of ICT in the public sector and aim to promote standardisation, system integration, information protection, and the efficient utilisation of government ICT infrastructure and shared services.

27. The audit conducted a compliance assessment of 133 public entities to evaluate the extent to which they comply with applicable e-Government laws, regulations, and standards. The assessment covered 11 compliance domains, addressing critical aspects of ICT governance, information security, service continuity, and database management.

3.2 Assessment methodology and Rating Criteria

28. To determine the level of compliance, a standardised compliance maturity model was applied, comprising five compliance levels ranging from Level 0 (Non-existent) to Level 5 (Optimised). Under this model, public entities are expected to attain at least Level 3 (Defined) or higher across all domains and in their overall compliance posture, as this level indicates that processes are documented, standardised, and formally implemented. The Rating Scale and Criteria are presented in Figure 1.

Figure 1: Rating Scale and Criteria



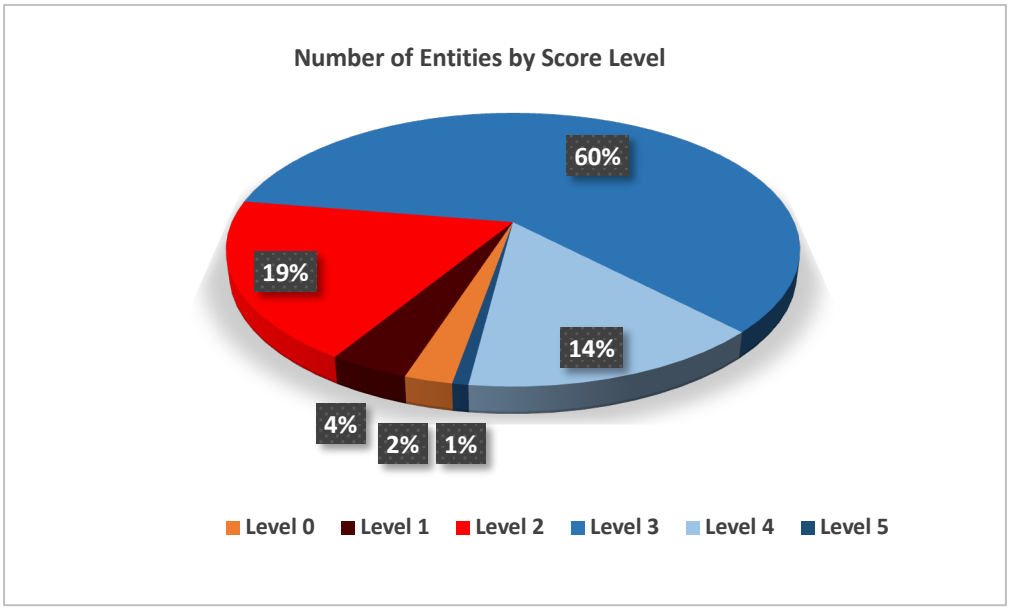
3.3 ICT Compliance Assessment Results

29. The ICT compliance assessment across the 11 domains provides an overview of the entities' adherence to established ICT control requirements. This section summarises overall compliance levels, indicating the proportion of entities that met or fell below the minimum compliance benchmark, and presents domain-level performance to highlight areas of relative strength and areas requiring improvement.

3.3.1 Overall ICT Compliance Level by Entities

30. The ICT compliance assessment showed that 100 entities (75%) attained Compliance Level 3 or higher, reflecting the presence of defined and consistently implemented ICT controls. In contrast, 33 entities (25%) fell below the minimum compliance threshold, indicating weaknesses in the formalisation, documentation, and enforcement of ICT control processes. Figure 2 illustrates the distribution of entities by compliance level.

Figure 2: Distribution of Entities Across ICT Compliance Level

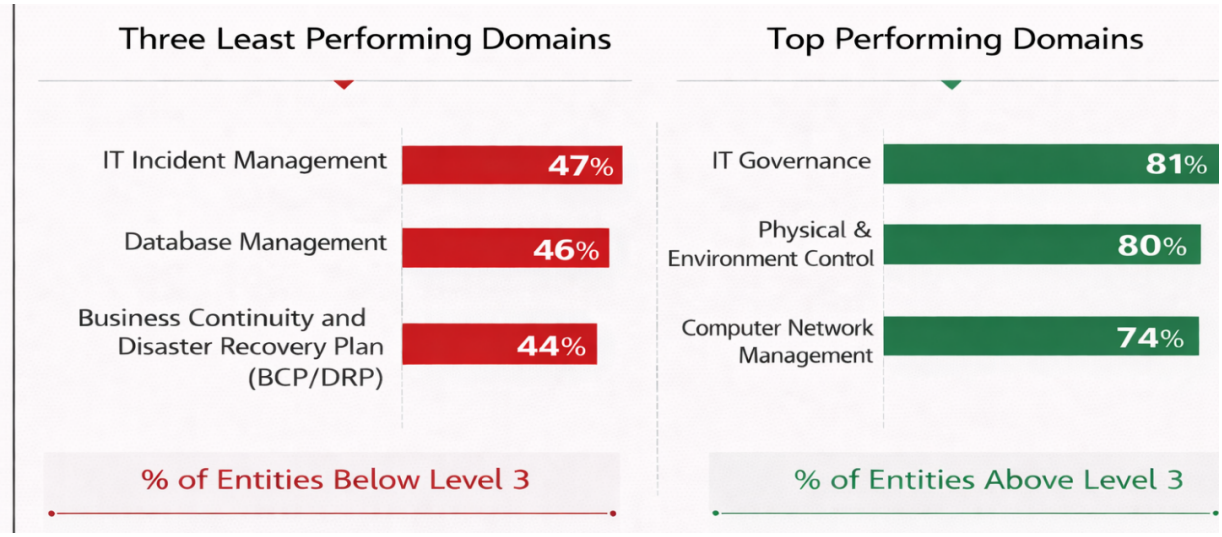


3.3.2 Performance of Entities Across ICT Domains

31. The ICT compliance assessment shows a variation in performance among the assessed entities. The three top-performing domains were IT Governance (81%), Physical and Environmental Controls (80%) and Computer Network Management (74%). These represent the highest proportion of entities that met or exceeded the minimum compliance benchmark, as illustrated in Figure 3.

In contrast, the three lowest-performing domains were IT Incident Management (47%), Database Management (46%), and Business Continuity and Disaster Recovery (44%). In these areas, fewer than half of the entities achieved the required compliance threshold, indicating notable weaknesses in these critical functions.

Figure 3: Performance of ICT Domains Across Assessed Entities



32. The failure of public entities to achieve the minimum compliance level (Level 3) highlights weaknesses in the implementation of ICT controls. This increases the risk of security incidents, operational disruptions, and sustained non-compliance with e-Government standards.

33. **I recommend that:**

(a) Entities rated below Level 3 should implement corrective measures to strengthen ICT controls and governance frameworks. Furthermore, the e-Government Authority (eGA) should enhance its monitoring and supervisory mechanisms to ensure these entities achieve the required level of compliance.

(b) Entities should prioritise strengthening controls in IT Incident Management, Application Systems and Database Management, and Business Continuity and Disaster Recovery by defining standards, standardising procedures, and ensuring effective implementation in practice.

CHAPTER FOUR

04

Information Technology General Controls (ITGCs)

4.1 Introduction

34. Information Technology General Controls (ITGCs) constitute the overarching controls that govern the planning, development, operation, security, and continuity of information systems within public institutions. These controls provide the foundation for application systems and are essential for ensuring that ICT environments support the confidentiality, integrity, and availability of information. Effective ITGCs enable public entities to safeguard ICT assets, manage risks associated with system operations, ensure reliable service delivery, and comply with applicable e-Government laws, regulations, and standards.

35. The audit of IT General Controls was conducted in 133 public entities to assess whether the overall ICT control environment was adequately designed and effectively implemented to support secure and reliable operation of information systems. The audit focused on key control areas, including IT governance, Computer network management, database management, user access management, information security, IT incident management, application systems change management, business continuity and disaster recovery management, and ICT third-party management.

36. The sections that follow present detailed audit results for each ITGC domain assessed. Each domain section highlights specific control weaknesses identified during the audit across the audited entities, together with their implications on the reliability, security, and resilience of information systems. Collectively, these domain-level findings provide a comprehensive view of the state of IT General Controls in public entities.

4.2 IT Governance

37. IT Governance provides the framework through which ICT is directed, controlled, and aligned with the organisational strategic objectives. It encompasses the establishment of ICT strategies, policies, governance structures, and risk management processes to ensure ICT resources are utilised effectively, risks are managed, and accountability is clearly defined. Accordingly, the audit assessed whether the existing IT governance arrangements were adequate to support strategic alignment, effective oversight, and proactive management of ICT-related risks.

38. The audit was expected to find a structured and well-defined IT governance framework supporting ICT planning, oversight, and risk management. However, the assessment identified gaps in key governance components, as detailed in the findings below.

4.2.1 Absence of an Approved ICT Strategy

39. The audit established that 33 entities operated without an approved ICT strategy to guide ICT investments and initiatives. The lack of a strategic framework increases the risk of fragmented ICT development, inefficient resource allocation, and limited contribution of ICT systems to achieving organisational objectives.

4.2.2 Misalignment Between ICT Strategy and Corporate Objectives

40. A review of strategic documents showed that 37 entities had ICT strategies that were not adequately aligned with their corporate objectives. This misalignment reduces the effectiveness of ICT as a strategic enabler and may result in systems that do not adequately support core business processes.

4.2.3 Weak ICT Governance Due to Absence of an ICT Steering Committee

41. The audit noted that 19 entities did not have a functional ICT Steering Committee to provide oversight and strategic direction. The absence of such governance structures weakens decision-making, prioritisation of ICT initiatives, and monitoring of ICT risks and performance.

4.2.4 Lack of an Approved ICT Policy

42. Assessment of policy frameworks revealed that 20 entities lacked an approved overarching ICT Policy. Without a guiding policy framework, ICT practices may be applied inconsistently, increasing exposure to operational inefficiencies, security weaknesses, and regulatory noncompliance.

4.2.5 Absence of Formal IT Risk Assessment Processes

43. The audit further identified that 37 entities did not conduct formal IT risk assessments regularly. Failure to systematically identify and manage ICT risks increases the likelihood of unanticipated system failures, security incidents, and service disruptions.

4.3 Computer Network Management

4.3.1 Introduction

44. Network Management controls are critical to ensuring the availability, reliability, and security of the information and communication technology (ICT) infrastructure that supports organisational operations. Effective network management includes proper access controls, continuous monitoring, timely patching, secure remote access, and sound configuration management of network devices. The audit assessed the adequacy and effectiveness of network management controls to determine whether the network infrastructure is protected against unauthorised access, cyber threats, and service disruptions.

45. The audit assessment revealed that several key network management controls were either inadequately designed or not operating effectively. The detailed findings arising from this assessment are presented below.

4.3.2 Weaknesses in Network Access Control

46. The audit found that 55 entities had weak network access control mechanisms that did not adequately restrict access to network resources. Such weaknesses increase the risk of unauthorised access to internal networks, potentially leading to data breaches and compromise of critical systems.

4.3.3 Inadequate Network Monitoring and Threat Detection Controls

47. Examination of network monitoring practices indicated that 48 entities lacked effective tools or processes to detect abnormal or malicious network activities. Inadequate monitoring reduces the ability to promptly detect cyber-attacks, increasing the potential impact of security incidents.

4.3.4 Absence of Effective Patch Management for Network Infrastructure

48. The audit established that 82 entities did not consistently apply security patches to network devices in accordance with vendor recommendations. Unpatched infrastructure remains vulnerable to known exploits, increasing the risk of network compromise and service outages.

4.3.5 Inadequate Controls Over Remote Network Access

49. Review of remote access arrangements showed that 35 entities had insufficient controls governing remote connectivity to their networks. Weak remote access controls increase exposure to unauthorised external access and associated security breaches.

4.3.6 Deficiencies in Network Device Configuration Management

50. Across 70 entities, configurations of critical network devices were not adequately documented, reviewed, or controlled. Poor configuration management increases the risk of misconfigurations that may weaken security controls or cause network disruptions.

4.4 Database Security and Management

4.4.1 Introduction

51. Database Security and Management controls are essential for protecting the confidentiality, integrity, and availability of data processed and stored within application systems. These controls encompass database patch management, access authorisation, activity logging and monitoring, backup and recovery arrangements, and encryption of sensitive data. The audit, therefore, examined whether the controls governing database environments were sufficient to safeguard critical data assets and support reliable system operations.

52. While the control framework requires database environments to be managed with strong security, monitoring, and recovery mechanisms, the audit identified instances where these controls were not operating as intended. The specific weaknesses identified are outlined in the findings below.

4.4.2 Inadequate Patch Management for Database Management Systems

53. The audit observed that 32 entities did not consistently patch database management systems to supported versions. This exposes databases to known vulnerabilities that may be exploited to gain unauthorised access or disrupt database services.

4.4.3 Weak Controls Over Database Access Authorisation

54. Assessment of database access controls revealed that 39 entities lacked effective authorisation and approval mechanisms. Weak access controls increase the risk of unauthorised data access, manipulation, or extraction of sensitive information.

4.4.4 Inadequate Database Audit Logging and Monitoring

55. The audit found that 82 entities did not consistently enable or review database audit logs for critical activities. Insufficient logging and monitoring reduce accountability and hinder timely detection of suspicious or unauthorised actions.

4.4.5 Weak Database Backup and Recovery Controls

56. Evaluation of backup arrangements showed that 44 entities had weak database backup and recovery practices. Such weaknesses increase the risk of data loss and prolonged system downtime following system failures or cyber incidents.

4.4.6 Lack of Encryption Controls for Sensitive Database Data

57. The audit identified that 43 entities did not consistently encrypt sensitive database data at rest or in transit. Lack of encryption exposes sensitive information to unauthorised disclosure and increases regulatory and reputational risks.

4.5 Information Security

4.5.1 Introduction

58. Information Security controls are designed to protect information assets against unauthorised access, disclosure, alteration, and loss while ensuring compliance with applicable legal, regulatory, and national ICT security requirements. These controls include security governance, incident detection and response, monitoring of security events, user awareness and training, and protection of sensitive information based on classification. The audit assessed whether the information security framework in place was adequate to safeguard information assets and support secure ICT operations.

59. Effective information security requires a combination of strong governance, technical controls, and informed users. The audit identified weaknesses across these dimensions, indicating that information security controls were not consistently applied or operating effectively. The detailed findings are presented below.

4.5.2 Absence of an Approved and Up-to-Date ICT Security Policy

60. The audit found that 22 entities operated without an approved and up-to-date ICT Security Policy. This gap results in inconsistent application of security controls and increased exposure to cyber threats.

4.5.3 Inadequate Security Incident Monitoring and Response Mechanisms

61. Assessment of incident detection capabilities showed that 63 entities lacked effective security incident monitoring and response mechanisms. Weak detection and response increase the likelihood of prolonged and impactful security incidents.

4.5.4 Weak Security Log Review and Monitoring Controls

62. The audit observed that 99 entities did not regularly review and act upon security logs. Insufficient log monitoring allows malicious activities to remain undetected within ICT environments.

4.5.5 Inadequate ICT Security Awareness and Training Program

63. The audit identified that 63 entities did not implement regular ICT security awareness training for staff. Lack of training increases susceptibility to phishing, malware, and social engineering attacks.

4.5.6 Inadequate Protection of Sensitive Information Based on Data Classification

64. Review of data protection practices showed that 65 entities did not consistently apply controls based on data classification. This exposes sensitive information to unauthorised access and disclosure.

4.6 ICT Incident Management

4.6.1 Introduction

65. ICT Incident Management controls are essential for ensuring that ICT and information security incidents are promptly identified, reported, escalated, resolved, and reviewed in order to minimise their impact on operations and information assets. Effective incident management supports service continuity, accountability, and continuous improvement of ICT controls. The audit assessed whether incident management arrangements were adequately designed and effectively implemented to support a timely and coordinated response to ICT incidents.

66. The audit expected incident management processes to be structured, clearly defined, and consistently applied across the organisation. However, the assessment identified weaknesses in key aspects of incident management that undermine the effectiveness of incident response. The detailed findings are presented below.

4.6.2 Absence of a Formal ICT Incident Management Procedure

67. The audit established that 57 entities did not have documented and approved ICT incident management procedures. Without formal procedures, incidents may be handled inconsistently and resolved inefficiently.

4.6.3 Unclear Roles and Responsibilities in ICT Incident Management

68. Assessment of ICT incident response arrangements revealed that 56 entities had unclear roles and responsibilities. This lack of clarity may delay incident reporting, escalation, and resolution.

4.6.4 Inadequate Monitoring of Incident Resolution Timelines

69. The audit noted that 82 entities did not monitor incident resolution timelines against defined service targets. Inadequate monitoring increases the risk of prolonged service disruptions.

4.6.5 Lack of Effective Escalation Procedures for Critical Incidents

70. The audit found that 66 entities lacked effective escalation mechanisms for high-impact incidents. Without escalation, critical incidents may not receive timely management attention.

4.6.6 Absence of Post-Incident Review and Continuous Improvement Processes

71. Review of incident records showed that 92 entities did not conduct post-incident reviews. Failure to capture lessons learned increases the likelihood of recurring incidents.

4.7 Application / System User Access Controls

4.7.1 Introduction

72. Application and System User Access Controls are fundamental to ensuring that only authorised users can access ICT systems and that such access is commensurate with assigned job responsibilities. Effective access controls support accountability, segregation of duties, and protection of information assets from unauthorised use or manipulation. The audit, therefore, examined the adequacy and effectiveness of user access control mechanisms implemented across application systems.

73. Strong access control practices require clearly defined procedures, timely updates of access rights, controlled assignment of privileged access, and continuous monitoring. The audit identified weaknesses in these key control areas, which are detailed in the findings below.

4.7.2 Absence of Formal User Account Management Procedures

74. The audit established that 41 entities lacked formal procedures for user account creation, modification, and revocation. This increases the likelihood that unauthorised or obsolete user accounts will remain active within systems.

4.7.3 Delayed Revocation and Update of User Access Rights

75. Audit evidence indicated that 92 entities did not promptly revoke or update access rights following staff exit or role changes. Delayed access revocation increases the risk of unauthorised system use and potential data misuse.

4.7.4 Excessive Privileges Assigned to Administrator Accounts

76. The audit noted that 31 entities granted administrator account privileges beyond what was necessary. Excessive privileges heighten the risk of unauthorised system changes and override of critical application controls.

4.7.5 Inadequate Periodic Review of User Access Rights

77. Review of access management practices showed that 80 entities did not conduct regular access rights reviews. Without periodic reviews, inappropriate access may persist undetected, weakening segregation of duties.

4.7.6 Weak Authentication Controls Over Privileged User Accounts

78. The audit further revealed that 52 entities did not enforce strong authentication mechanisms for privileged accounts. Weak authentication increases the likelihood of credential compromise and unauthorised access to critical systems.

4.8 Application Systems Change Management

4.8.1 Introduction

79. Application Systems Change Management controls are essential to ensure that changes to ICT systems are properly authorised, tested, and implemented in a controlled manner to maintain system integrity, availability, and security. These controls cover formal change procedures, approval mechanisms, environment segregation, user acceptance testing, and emergency change management. The audit assessed whether system changes were managed in a structured and controlled manner to minimise the risk of system failures and unauthorised modifications.

80. Change management practices should provide assurance that system modifications are predictable, traceable, and aligned with business requirements. The audit review, however, identified weaknesses in key change management practices that may undermine system stability and control effectiveness, as outlined in the findings below:

4.8.2 Absence of a Formal and Approved Change Management Procedure

81. The audit established that 53 entities did not have a formal and approved change management procedure to govern the initiation, approval, testing, implementation, and rollback of system changes. The absence of a structured change management framework increases the likelihood that changes are implemented inconsistently, potentially leading to system instability, service disruptions, and security vulnerabilities.

4.8.3 Implementation of System Changes Without Proper Authorisation

82. Audit evidence indicated that system changes within 41 entities were implemented without documented approval from authorised stakeholders. Such unauthorised changes weaken accountability over system modifications and heighten the risk of inappropriate or malicious changes that may compromise system functionality, data integrity, and security controls.

4.8.4 Inadequate Segregation Between Development, Test, and Production Environments

83. Across 32 entities, development, test, and production environments were not adequately segregated. Inadequate segregation increases the risk that untested or unauthorised changes are migrated directly into the production environment, potentially resulting in system errors, data loss, and increased exposure to security threats.

4.8.5 Absence of Formal User Acceptance Testing (UAT) Sign-Off for System Changes

84. The audit further revealed that 61 entities deployed system changes without obtaining formal User Acceptance Testing (UAT) sign-off from user departments. Deploying changes without UAT confirmation increases the risk that systems are placed into operation without assurance that business, functional, and security requirements have been met, which may adversely affect service delivery and user satisfaction.

4.8.6 Weak Controls Over Emergency System Changes

85. Review of emergency change practices showed that 51 entities had weak controls over emergency system changes, including inadequate documentation, limited post-implementation review, and a lack of management approval. Weak emergency change controls increase the risk that critical control procedures are bypassed, leading to system instability, security vulnerabilities, and reduced accountability for changes made under emergency conditions.

4.9 Business Continuity and Disaster Recovery

4.9.1 Introduction

86. Business Continuity and Disaster Recovery (BCP/DRP) controls are designed to ensure that critical business operations and ICT services can continue or be restored within acceptable timeframes following disruptions or disasters. These controls include management approval of continuity plans, identification and prioritisation of critical business functions, regular testing of continuity arrangements, reliable backup and recovery processes, and resilient disaster recovery infrastructure. The audit assessed whether BCP and DRP arrangements were adequate to support organisational resilience and continuity of critical services.

87. An effective BCP/DRP framework should be formally approved, risk-informed, regularly tested, and capable of supporting timely recovery of critical operations. However, the assessment identified gaps in key components of continuity and recovery planning that may limit the organisation’s ability to respond effectively to disruptive events. The detailed findings are presented below.

4.9.2 Lack of Management Approval for the Business Continuity Plan

88. The audit established that 35 entities had not obtained formal management approval for their Business Continuity Plans. Lack of approval weakens the ownership and enforceability of continuity arrangements.

4.9.3 Inadequate Identification of Critical Business Functions and Dependencies

89. The audit observed that 35 entities had not comprehensively identified critical business functions and dependencies. This limits effective prioritisation during recovery efforts.

4.9.4 Insufficient Testing and Drilling of Business Continuity and Disaster Recovery Plans

90. Assessment of testing activities showed that 98 entities did not regularly test their BCP and DRP. Insufficient testing reduces assurance that plans will function during actual disruptions.

4.9.5 Non-Compliance with Defined Data Backup and Recovery Objectives

91. The audit found that 64 entities did not consistently meet defined backup and recovery objectives during testing of their BCP and DRP. Non-compliance increases the risk of data loss and extended downtime.

4.9.6 Inadequate Disaster Recovery Site Separation and Resilience

92. The audit identified that 28 entities lacked adequate separation and resilience of disaster recovery sites. This increases the likelihood that a single event could impact both production and recovery environments.

4.10 ICT Third-Party Management

4.10.1 Introduction

93. ICT Third-Party Management controls are critical in ensuring that ICT services provided by external vendors are secure, reliable, cost-effective, and compliant with contractual and regulatory requirements. These controls include governance policies for vendor engagement, formal contractual arrangements, definition and monitoring of service levels, and enforcement of legal, security, and compliance obligations. The audit assessed whether third-party ICT services were managed in a manner that safeguards the organisation's interests and supports continuity of ICT services.

94. Given the organisation's reliance on external ICT service providers, effective third-party management should provide clear accountability, enforceable service expectations, and ongoing oversight of vendor performance. The audit review identified weaknesses in these areas, as outlined below

4.10.2 ICT Services Obtained Without Formal Contractual Agreements

95. Audit review revealed that 44 entities obtained ICT services from third parties without formal contractual agreements. Engaging vendors without contracts limits clarity over roles, responsibilities, and service obligations, thereby increasing exposure to service delivery failures, disputes, and the inability to enforce security or performance requirements.

4.10.3 Inadequate Definition of Service Levels in ICT Vendor Contracts

96. Examination of vendor contracts showed that 42 entities did not clearly define measurable Service Level Agreements (SLAs) covering availability, response times, and resolution targets. Poorly defined service levels reduce management's ability to hold vendors accountable and increase the likelihood of prolonged service interruptions and substandard service delivery.

4.10.4 Weak Monitoring and Oversight of ICT Vendor Performance

97. The audit found that 80 entities did not regularly monitor or evaluate vendor performance against agreed contractual terms and SLAs. Weak oversight of vendor performance allows persistent service deficiencies, security gaps, and non-compliance to remain unaddressed, negatively affecting the reliability of ICT services.

4.10.5 Contracts Lack Critical Legal, Security, and Compliance Clauses

98. Assessment of contractual provisions indicated that 47 entities had vendor contracts that lacked critical clauses related to information security obligations, audit rights, penalties, and compliance with legal and regulatory requirements. The absence of such clauses exposes the organisation to legal, security, and regulatory risks. It limits its ability to seek redress in the event of vendor non-compliance or security incidents.

CHAPTER FIVE

05

System Development, Functionality and Process Automation

5.1 Introduction

99. This chapter assesses system optimisation, process automation, and ICT project management across public institutions, identifying gaps in utilization of government centralizad systems, system integration, duplicated applications, reliance on manual processes, delayed ICT projects, and incomplete ICT project documentation. The findings emphasize the need to strengthen effective utilization of centralized system integration, automation, project planning, and oversight to enhance efficiency, accountability, and value for ICT investments.

5.2 Limited Adoption and Ineffective Utilisation of Government Centralised Systems

100. The Government of Tanzania has made significant investments in Information and Communication Technology (ICT) systems to modernize public financial management, procurement, asset management, and human resource administration. These systems are supported by relevant laws, regulations, and directives that mandate their adoption and use across public sector entities. However, despite these efforts, some public entities have not yet adopted these systems, while others that have implemented them are not utilizing them effectively. Details of these observations are presented below.

5.2.1 Non-Utilisation of Government Centralised Systems

101. Section 73(1) of the Public Procurement Act, 2023 requires procuring entities to ensure that procurement, supply and disposal of assets functions are implemented and reported through the electronic public procurement system. Further On 17 October 2016, the Ministry responsible for Regional Administration and Local Government issued directive ref. No. CEB.151/297/02/N/61 requires all LGAs to install the Government of Tanzania Health Operational Management Information System (GoT-HoMIS) in health facilities, to enhance revenue monitoring and control. Furthermore, Treasury Circular No. 1 of 2025 (Ref. No. MG.4/261/01) and Treasury Circular No. 5 of 2019 require all public entities to use approved financial management systems, including the MUSE application system. Where a public entity adopts a different system, it must seek prior approval from the Ministry of Finance. Despite the above requirements, my audit noted that some entities have not yet adopted or implemented these systems, as detailed below.

102. **MUSE:** 80 public authorities and other bodies processed financial transactions using accounting systems other than the mandatory MUSE system without obtaining prior ministerial approval, contrary to Government directives. Further details are provided in Appendix I.

103. This practice undermines the Government's unified financial management framework, weakens centralised oversight, and introduces significant risks of data manipulation, human error, and inaccurate reporting through reliance on non-integrated tools such as Microsoft Excel.

104. **I recommend that the respective authorities and other bodies, in collaboration with the Ministry of Finance, develop and implement a clear roadmap for full MUSE adoption in compliance with Treasury Circular No. 1 of 2025.**

105. National **e-Procurement System of Tanzania (NeST)**: 59 entities procured goods and services worth TZS 9.90 billion outside the NeST system, as shown in Table 1. This matter was similarly reported in the financial year 2023/24, where 88 entities procured goods and services worth TZS 31.81 billion outside the NeST system.

Table 1: Procurements made out of the e-procurement system

S/N	Name of LGA	Amount (TZS)	S/N	Name of LGA	Amount (TZS)
1	Meatu DC	1,398,310,832	31	Handeni DC	95,996,670
2	Kigamboni MC	616,452,429	32	Chunya DC	92,763,860
3	Songwe DC	469,082,628	33	Kondoa TC	82,860,000
4	Dar es Salaam CC	406,751,356	34	Ifakara TC	79,223,421
5	Serengeti DC	403,176,490	35	Shinyanga DC	78,835,898
6	Kondoa DC	375,740,021	36	Bahi DC	78,519,528
7	Kyela DC	342,096,965	37	Maswa DC	77,809,997
8	Kigoma DC	317,173,465	38	Mufindi DC	77,429,483
9	Songea MC	255,299,068	39	Nyasa DC	71,800,506
10	Tarime DC	252,958,432	40	Ngara DC	71,412,560
11	Kilindi DC	237,432,676	41	Singida DC	66,541,631
12	Kibondo DC	235,414,560	42	Ileje DC	56,638,538
13	Nachingwea DC	230,619,461	43	Mpimbwe DC	56,485,048
14	Sengerema DC	220,402,032	44	Mlele DC	56,483,013
15	Buhigwe DC	215,376,516	45	Kahama MC	53,843,692
16	Liwale DC	212,062,599	46	Chemba DC	53,192,000
17	Tanga CC	203,234,056	47	Misungwi DC	51,792,040
18	Bukoba MC	195,712,416	48	Singida MC	51,651,340
19	Nanyumbu DC	186,547,949	49	Nsimbo DC	51,079,100
20	Uvinza DC	184,788,142	50	Ushetu DC	50,635,811
21	Urambo DC	164,559,336	51	Madaba DC	48,992,900
22	Tunduru DC	163,578,330	52	Mpanda MC	47,116,434
23	Manyoni DC	139,857,769	53	Itilima DC	44,488,000
24	Musoma MC	138,398,834	54	Kilolo DC	33,107,260
25	Mpwapwa DC	122,744,986	55	Shinyanga MC	33,034,065
26	Kiteto DC	119,670,000	56	Bumbuli DC	29,254,646
27	Korogwe TC	115,027,896	57	Kilwa DC	24,700,000
28	Mkinga DC	114,127,500	58	Busega DC	12,489,720
29	Geita DC	113,896,500	59	Momba DC	9,210,522
30	Mbinga DC	112,298,200		Total	9,900,179,127

Source: NeST and payment vouchers.

106. Procurement outside the system undermines the Government's efforts to enhance efficiency, transparency, and accountability in public procurement.

107. **I recommend that management of LGAs continue capacity building and periodic compliance reviews to sustain the improved trend and ensure full adherence to the electronic procurement requirements.**

108. GoT-**HoMIS:** 23 Local Government Authorities (LGAs) collected non-tax revenue amounting to TZS 6.65 billion from health facilities without using the GoT-HoMIS system. This is a marked increase compared to the previous year, when 12 LGAs collected TZS 3.74 billion outside the system, indicating that the Government through PMO-RALG and LGA management did not take adequate corrective measures. The respective Councils are shown in Table 2

Table 2: LGAs Collected Revenue Outside the Approved System

S/N	Name of LGA	Amount (TZS)	S/N	Name of LGA	Amount (TZS)
1	Lushoto DC	25,286,750	12	Moshi MC	198,153,054
2	Malinyi DC	39,011,480	13	Kondoa DC	203,236,565
3	Ngorongoro DC	114,667,104	14	Sikonge DC	224,401,657
4	Ubungo MC	118,941,000	15	Moshi DC	229,114,768
5	Itilima DC	151,812,446	16	Singida DC	229,576,530
6	Kigoma Ujiji MC	152,557,170	17	Kasulu TC	234,464,591
7	Mbulu DC	160,548,939	18	Kilolo DC	334,793,354
8	Ulanga DC	165,731,508	19	Mufindi DC	471,329,662
9	Madaba DC	166,858,855	20	Mwanza CC	483,139,638
10	Uvinza DC	184,116,898	21	Manyoni DC	590,960,491
11	Mbinga DC	184,262,855	22	Iringa MC	751,757,699
			23	Tanga CC	1,241,661,378
				Total	6,656,384,392

Source: Collection reports from standalone GOTHOMIS

109. The non-compliance is primarily attributed to inadequate enforcement of government directives and insufficient supervisory follow-up to ensure full operationalisation of GoT-HoMIS in health facilities. Consequently, collecting revenue outside the approved electronic system undermines transparency, accountability, and operational efficiency. It increases the risk of revenue leakage, mismanagement, and loss of public funds, and limits the ability of LGAs to monitor and reconcile collections in real time.

110. **I recommend that: (a) the Government, through PMO-RALG and management of LGAs, enforce compliance with the use of GoT-HoMIS in all health facilities; and (b) LGAs strengthen supervisory mechanisms to prevent revenue collection outside the approved electronic system.**

5.2.2 Ineffective Utilisation of Government Centralised Systems

111. Regulation 4(1) of the Public Finance (Management of Public Property) Regulations, 2024 requires the Paymaster General to establish an electronic public asset register, and every Accounting Officer to record public property under their authority in the GAMIS system. Further, Public Service Circular No. 1 of 2021 requires all Government entities to utilise the Human Capital Management Information System (HCMIS) for staff management, payroll, and personnel actions. Additionally, the Public Employee Performance Management Information System (PEPMIS) is mandated by the President's Office for staff performance evaluations.

112. Government **Asset Management Information System (GAMIS):** A review of GAMIS and manual asset registers in 34 entities (down from 41 in 2023/24) revealed ineffective utilisation of the system. The audit identified discrepancies between assets recorded in GAMIS and the corresponding physical asset registers. Inconsistencies arose from incomplete, inaccurate, or untimely updates of asset information. The list of entities that underutilised the GAMIS system is shown in **Table 3**.

Table 3: The list of entities with ineffective utilisation of GAMIS

S/N	Name of the Entity	S/N	Name of the Entity	S/N	Name of the Entity
1	Bahi DC	13	Kasulu TC	25	Mwanza CC
2	Bariadi DC	14	Longido DC	26	Nanyamba TC
3	Bariadi TC	15	Magu DC	27	Njombe TC
4	Biharamulo DC	16	Manyoni DC	28	Nsimbo DC
5	Bukoba MC	17	Masai DC	29	Pangani DC
6	Bukombe DC	18	Mbarali DC	30	Arusha RS
7	Chato DC	19	Mbogwe DC	31	Njombe RS
8	DART	20	Meatu DC	32	Sengerema DC
9	Geita DC	21	Mlimba DC	33	Temeke MC
10	Itigi DC	22	Mpwapwa DC	34	Ubungo MC
11	Itilima DC	23	Mtwara DC		
12	Karatu DC	24	Mtwara MC		

Source: *Asset Registers, GAMIS reports and financial statements*

113. Incomplete recording of assets in GAMIS, combined with continued manual management of major asset classes, significantly undermines the reliability of financial statements. These practices weaken institutional accountability, limit transparency in asset tracking, and heighten the risk of misappropriation, loss, or unauthorised use of public assets.

114. I **recommend that ensure all relevant entities comprehensively register their assets in GAMIS and fully utilise the system for the preparation of accurate, complete, and reliable financial records. This will enhance transparency, strengthen accountability, and promote effective oversight in the management of public assets.**

115. HCMIS **(e-watumishi):** My audit noted that 15 Public Authorities and Other Bodies did not fully utilize HCMIS and PEPMIS for managing human resource information and related processes. This indicates that some entities are not effectively using the government's centralized human resource management systems to support proper record keeping, employee data management, and monitoring of human resource activities. Details of the identified entities are presented in **Table 4**.

Table 4*: List of Entities with Inadequate Utilization of Government Human Resources Systems*

S/n	Name of Public Entity	System(s) Affected	Identified Anomaly 2024/25
1	Tanzania Electric Supply Company Ltd	HCMIS	The company does not maintain personnel and payroll records for all public servants in the Human Capital Management Information System (HCMIS) as required by the Budget and Public Service Management guidelines
2	Electrical transmission and distribution company	HCMIS/ PEPMIS	ETDCO is not utilizing PEPMIS for staff performance management nor HCMIS for payroll administration; instead, payroll amounting to TZS 2.14 billion for 2024/25 was processed through the ERMS system.
3	Dar es Salaam Water Supply and Sanitation Authority	HCMIS	Audit review of DAWASA payroll administration revealed that the Authority has not fully utilised the HCMIS to process staff salaries. Examination of the June 2025 payroll indicated that, out of 2,085 staff, only 1,375 employees had been assigned cheque numbers generated through HCMIS
4	Universal Communication Service Access fund	HCMIS	Under-Utilisation of the HCMIS System and Inaccurate Employee Records
5	Tanzania Geothermal Development Company limited	HCMIS	TGDC has not used the HCMIS system to generate Personal Emolument budgets and continues to rely on the ERMS system
6	Cereal and other produce board	PEPMIS	Six employees had obtained performance scores below the required 60 marks in the implementation of PEPMIS contrary to the establishment circular issued by the Chief Secretary

S/n	Name of Public Entity	System(s) Affected	Identified Anomaly 2024/25
7	Mbeya water supply and sanitation authority	HCMIS	I found that the Authority had not been using the Human Capital Management Information System (HCMIS); instead, they had been using ERMS for payroll generation
8	Tanga Water Supply and Sanitation Authority	HCMIS	27 employees lacked HCMIS-generated cheque numbers. ERMS master data is missing birthdates and employment types.
9	Tanzania concrete pole manufacturing company	HCMIS	noted that TCPM has not used the HCMIS system to generate Personal Emolument budgets and continues to rely on the ERMS system
10	Tanzania Civil Aviation Authority	HCMIS	57 percent of staff (285 employees) remained unregistered at year-end.
11	Tanzania Posts Corporation	HCMIS / PEPMIS	Planned implementation for both systems were not realised during the financial year.
12	Watumishi housing investments	PEPMIS	Active users identified in the system who do not appear on the official HR staff list.
13	Morogoro Water Supply and Sanitation Authority	HCMIS	Implementation remains at the initial stage 49 months after system commencement.
14	Arusha water supply and sanitation authority	HCMIS	AUWSA is using the Enterprises Resources Management System (ERMS) for payroll, recruitment, promotions and staff management instead of HCMIS
15	Institute of Rural development planning	HCMIS	HCMIS reports 468 employees, the Staff Assessment system reflects only 99 employees, despite HCMIS being dependent on e-msawazo

***Source**: Entity system records*

116. This anomaly is attributed to delays in system implementation, incomplete data cleaning exercises, and technical issues in organisational-level mapping. Non-utilisation of these systems results in manual data handling, increased risk of inaccurate payroll records (including ghost employees), and lack of transparency in performance monitoring.

117. **I recommend that the respective public authorities and other bodies expedite data cleaning and staff registration to enable full system integration and ensure that all personnel and performance actions are processed through the government-approved electronic platforms.**

5.3 Integration of Application Systems

118. The audit identified significant integration anomalies across public entities. Failure to integrate systems leads to revenue leakage and operational inefficiencies. Key findings include:

119. **Dar Rapid Transit Agency (DART):** The NPK Parking Management System is not integrated with the Billing and Debt Management Information System (BiDMIS) to automatically capture parking transactions, generate control numbers, and reconcile parking revenues in real time. This increases the risk of revenue leakage and inadequate monitoring of transactions.

120. **Deep Sea Fishing Authority (DSFA):** The e-Billing system is not integrated with BRELA and Zanzibar Business and Property Registration Agency (BPRA) registration systems to validate the legal registration status of agents before billing and licensing. This may result in licensing unregistered entities.

121. **Judiciary of Tanzania (JoT):** The e-Wakili system is not integrated with the National Identification Authority (NIDA), the National Examinations Council of Tanzania (NECTA), and the Law School of Tanzania systems to support automated verification of petitioners' identity, academic qualifications, and professional eligibility during the processing of petitions for admission. This weakness increases the risk of approving unqualified applicants and causes delays in the processing of petitions for admission.

122. **Ministry of Constitutional and Legal Affairs (MoCLA):** The Legal Services System is not integrated with the Immigration system, NIDA, and Judiciary systems for verification of citizenship, identity, and court case status during service delivery. Manual verification may lead to unauthorised approvals of legal aid providers and operational inefficiencies.

123. **National Food Reserve Agency (NFRA):** The Digital Food Commodity Tracking System (DFCTS) is not integrated with GePG for billing and ERMS for revenue recognition. Manual processes increase the risk of revenue leakage.

124. **Office of the Attorney General (OAG):** The Office of Attorney General Management Information System (OAGMIS) is not integrated with e-Watumishi (HCMIS) for the automatic synchronisation of legal officers' human resource details. Reliance on manual data entry may result in inconsistencies and discrepancies in legal officers' information between the two systems.

125. **Prime Minister's Office - Labour, Youth, Employment and Disabilities (PMO-LYED):** The integration between the Online Work Permit Application and Issuance System (OWAIS) and the TRA and BRELA for automatic verification of TIN and Company registration status is not functional, resulting in manual verification, which increases the risk of inaccurate approvals of work permits.

126. **Tanzania Broadcasting Corporation (TBC):** SAP is not integrated with GePG and MUSE for automated billing, control number generation, and receivables recording. This may lead to inaccurate financial records and errors arising from manual reconciliations.

127. **Tanzania Bureau of Standards (TBS):** The Online Application System (OAS) is not integrated with the Tanzania Customs Integrated System (TANCIS) to access vessel manifests and validate imported goods. This may lead to duplication of efforts and reduce oversight efficiency

128. **Town Planners Registration Board (TPRB):** The TPRB billing system is not integrated with the e-Ardhi system to automatically capture approved town plans for billing purposes. This increases the risk of under/over-statement of revenue.

129. **Air Tanzania Company Limited:** The Enterprise Resource Management Suite (ERMS) used by Air Tanzania Company Limited for financial management is not integrated with several key systems that support core operations. It does not connect with the Bank of Tanzania or the International Air Transport Association platforms, requiring exchange rates to be manually sourced and updated, which increases the risk of errors and delays in foreign currency transactions. The system is also not linked to the AD aircraft maintenance inventory software, limiting accurate accounting of maintenance costs and stock levels, nor to the Crane Pax ticketing system, resulting in manual reconciliations and delayed revenue recognition. Overall, these integration gaps increase reliance on manual processes, leading to inefficiencies, higher error risk, and potential data inconsistencies.

130. **Tanzania Coffee Board:** The audit found that the Unified Coffee Management System (UCMS) is not integrated with key systems such as commercial banks, e-Kilimo, the Government e-Payment Gateway, Tanzania Revenue Authority, and the Tanzania Mercantile Exchange. As a result, payment verification, licence validation, export approval checks, trading data sharing, and automated revenue capture are not fully supported, weakening monitoring, transparency, and efficiency in coffee marketing and revenue management.

131. **Cashewnut Board of Tanzania:** The Cashew Industry Management Information System is not integrated with the TRA's Tanzania Customs Integrated System (TANCIS) to facilitate automated exchange and validation of export and regulatory information.

132. **Dodoma Water Supply and Sanitation Authority:** The ERMS is not integrated with GAMIS, resulting in manual transfer of asset information between the two systems.

133. **Kilimanjaro Airports Development Company Limited:** The KADCO billing system is not integrated with the GePG, requiring manual intervention to generate control numbers before payments are processed.

134. **Mkulazi Holding Company Limited:** The ERP system is not integrated with commercial banks, preventing the automated preparation of bank reconciliations.

135. **Tanzania National Parks:** The ARUTI system is not integrated with the Microsoft Dynamics NAV system. As a result, payroll expenditures processed in the ARUTI system are not automatically posted to Microsoft Dynamics NAV, requiring manual entries to update financial records.

136. **Tanzania Telecommunications Corporation:** The T-Pesa platform is not integrated with commercial banking systems and the NCARD platform, limiting automated transaction processing and reconciliation.

137. This increases the risk of inaccurate or incomplete data and operational delays.

138. **I recommend that management of these entities must prioritise full system-to-system integration of the identified systems using approved Government interoperability frameworks to enable automated data exchange, reduce manual processes, and improve accuracy and efficiency.**

5.4 Duplication and Fragmentation of Application Systems

139. Section 25(a) of the e-Government Act, 2019 requires public institutions to adopt sustainable and reliable digital systems by avoiding unnecessary duplication and, where feasible, implementing centralised solutions. This provision is intended to promote efficiency, interoperability, cost-effectiveness, and optimal utilisation of ICT resources across the public sector.

5.4.1 Public Entities with Duplicate Systems

140. Duplication of systems refers to the presence of multiple ICT systems within an organisation that perform the same or similar functions, leading to redundant processes, repeated data capture, and parallel operations. In this regard, the audit identified instances where public institutions operate multiple systems performing similar functions, as outlined below

(i) Ardhi University utilises both the Admission System and the Online Postgraduate Admission Management Information System (PAMIS) for student applications.

(ii) The Tanzania Fertiliser Regulatory Authority (TFRA) uses the Fertiliser Information System (FIS) alongside the Self-Bill Service Portal for billing functions.

(iii) The Institute of Accountancy Arusha (IAA) operates the Online Admission System (OAS) together with the Integrated Student Management System (ISMS) for student registration.

(iv) The Tanzania Airports Authority (TAA) utilises both the PMS Chip Coin System and the PMS Card System for car-parking billing management.

(v) The National Bureau of Statistics (NBS) uses two accounting systems, MUSE and Epicor, to manage bilateral agreement projects.

(vi) Arusha International Conference Centre operates parallel financial systems ERMS and Advanced Accounting Software (ADV) which are not intergrated, requiring manual transfer of revenue data between the two systems.

141. Duplication of the system increases operational costs, data inconsistencies, and weakened overall ICT governance and controls.

142. **I recommend that:**

(a) Public institutions currently operating multiple accounting systems comply with the directive issued by the Permanent Secretary-Treasury by migrating fully to MUSE and decommissioning all unapproved accounting systems within a specified timeframe.

(c) The Government, through the e-Government Authority, enforce the use of centralised and shared ICT systems for non-accounting functions and restrict institutions from developing or operating duplicate systems performing similar functions.

5.4.2 Public Entities with Fragmented Systems

143. A fragmented system refers to an ICT environment in which multiple independent systems support different components of the same business process but are inadequately integrated or not integrated at all, resulting in broken data flows that require manual interventions, interfaces, or reconciliations to complete end-to-end processes. In this regard, the audit noted cases where systems performing related functions operate independently without integration, thereby leading to fragmentation, as detailed below.

(i) **The ICT Commission (ICTC)** operates two separate systems: the Professional Management Information System (PMIS) and the Event Management System (EMS), both supporting the management of ICT professionals, including registration and professional events. Data between the two systems is shared manually. EMS is a limited system whose functions could be incorporated into PMIS, which already manages core institutional operations. Keeping EMS as a separate system increases operational complexity and raises maintenance and administration costs.

(ii) Additionally, the **Ministry of Health** operates multiple hospital information systems across different levels of public health facilities; however, these systems function independently and lack interoperability for seamless data exchange. GoTHOMIS is used in primary healthcare facilities and district hospitals, Jeeva at Muhimbili National Hospital, Afya eHMS at Regional Referral Hospitals, while zonal hospitals deploy their own facility-specific systems, such as iHMIS at Benjamin Mkapa Hospital. The fragmentation of these systems results in patient records not being synchronised across health facilities, limiting data sharing, increasing record duplication, undermining continuity of care, and reducing the overall effectiveness of healthcare service delivery.

(iii) Furthermore, **BRELA** operates four systems to support its core functions. The Online Registration System facilitates the registration of companies and business names; the Beneficial Ownership Portal manages the disclosure and reporting of beneficial ownership information; the BRELA Assessment and Billing System calculates fees, generates control numbers, and manages payments; and the Tanzania National Business Portal supports online business-related services, including registration and coordination of licenses and permits with other institutions. However, these systems operate independently, despite relying on each other for data sharing due to the interconnected nature of their processes. The fragmentation

of these systems hinders seamless data sharing, escalates operational and maintenance costs, and ultimately undermines overall organisational efficiency and effectiveness.

144. The duplication and fragmentation of systems may lead to increased operational and maintenance costs, data inconsistencies, service delivery inefficiencies, and difficulties in ensuring effective oversight.

145. **I recommend that:**

(a) Management of the respective entities undertake a comprehensive review of their ICT application landscape to identify fragmented systems and develop a time-bound plan to integrate, consolidate, or replace systems performing related functions, in order to ensure seamless end-to-end business processes.

(b) The Government, through the e-Government Authority, should enforce system interoperability standards and enterprise architecture compliance to ensure that all systems supporting similar or linked functions are integrated and capable of real-time data exchange.

(c) Public institutions should ensure that all ICT systems supporting interconnected business processes are fully integrated and interoperable, thereby eliminating manual data transfers, reducing data inconsistencies, and improving service delivery efficiency.

5.5 Non-Automation of Business Processes

146. An assessment of automation levels across 133 public entities revealed anomalies in the implementation of key business processes. In 30 entities, core business functions remain manual, limiting operational efficiency and effectiveness.

Table 5: Non-automated Business Processes by Entities

Entity	Non-Automated Processes	Implication
STAMICO	Revenue collection	Increases the risk of errors, omissions, and misstatements of revenue, while limiting timely recording and reconciliation of transactions
MWAUWASA	HR and Payroll Processes for contract employees	This can result in incorrect salary payments and unauthorised payments.
VRB	Revenue collection	Increases the risk of errors, omissions, and misstatements of revenue, while limiting timely recording and reconciliation of transactions.
TIRA	Statutory Penalties	Inaccurate billing resulting from manual calculations and inconsistent application of statutory penalty amounts
RITA	Marriage and divorce management, including verification Services, Adoption Services, Foreign Marriage Registration, and Certificate Error Correction.	This may result in a higher risk of human error, inefficiency and reduced customer satisfaction.
Deep-Sea Fishing Authority (DSFA)	Accounting process	Increases the risk of errors, omissions, and misstatements in the financial statement

Entity	Non-Automated Processes	Implication
	Application and issuance of the Deep-Sea Fishing certificate and certificate of authorisation to fish beyond the exclusive economic zone	May result in delays, human errors, potential loss of revenue and reduced efficiency.
TALIRI	Inventory management of various livestock research technologies and products	Increases the risk of data errors, stock discrepancies, weak inventory control, and delayed decision-making, thereby reducing operational efficiency.
	Billing of Research Consultancy Fees and Overhead Costs of Projects	The occurrence of errors, omissions, or inconsistencies in applying consultancy and overhead charge rates could result in a loss of revenue.
CRB	Promotions and demotions, salary increments, Personnel Emolument (PE) Budget management	This can result in incorrect salary payments, unauthorised payments and over-expenditure of PE budget.
PCT	Billing Process for the issuance of professional certificates to pharmaceutical practitioners, Inspection Fees, and Registration of Pharmaceutical Premises.	Increases the risk of errors, omissions, and misstatements of revenue, while limiting timely recording.
TAA	Tenants' management and bill management	Increase the risk of errors in charge computation and of inefficient results, affecting revenue accuracy and completeness.
DUCE	Student admission, billing, and payment tracking.	Increases the risk of errors and data inconsistencies, limits accurate tracking of receivables and payables, and reduces operational efficiency.
IAA	Application for Research Consultation and Short Courses, Billing Processes for Training, Facility Rental, Accommodation Services, and Verification of Diploma Examination Certificates.	This increases the risk of incorrect admission decisions and delays, resulting in operational inefficiencies and potential revenue loss.
GPSA	Fund Transfer Process	increases the risk of errors, incomplete postings, and unauthorised transfers, compromising the accuracy and completeness of wallet transactions.
NIRC	Irrigation service fees, annual fees, registration fees, application fees, and charges for hiring heavy equipment and machinery,	Increase risks, errors, delays, revenue leakage, transparency, and accountability
TASAC	Vessel Inspection, Certification, and Licensing Process for Small Vessels at Upcountry Stations.	increases the risk of incorrect revenue collection, which undermines the reliability and completeness of billing records
TBC	Marketing and Advertisement Processing Workflow	increase the risk of inaccurate client information, delays in issuing control numbers, inefficiencies in handling advertisement requests, and reduced traceability of programs submitted for editing or scheduling.

Entity	Non-Automated Processes	Implication
WMA	Electricity meter verification processes	Increase the risk of approving the use of substandard meters, revenue loss, and operational inefficiencies
BTI	Student Application and Admission Process	May lead to delays in processing applications, operational inefficiencies, and potential revenue loss from missed enrolments.
CRB	Monitoring Statutory Retirement Age	Financial loss due to continued salary payments to employees who have reached the statutory retirement age but remain active in the system;
GBT	Gaming License and Sticker Verification	Increase risk of revenue loss
Government Chemist Laboratory Authority (GCLA)	Computation of Chemical Import and Export Consignment Permit Fee/Registrations	Increases the risk of permit fee calculation errors, delays in processing permits, and potential revenue loss.
KADCO	• Aeronautical revenues, such as fire truck fees, VIP lounge service fees, and security fees, • Non-aeronautical revenues, including rents, sales of concessions, and utilities	Limited real-time monitoring and reporting affecting the efficiency and effectiveness of revenue management
LGTI	Student accommodation allocations management	increases the risk of data inaccuracies, duplicate allocation, and limits management's ability to generate reliable, real-time reports on hostel occupancy and revenue
Mining Commission	Penalty management	This may result in unintentional non-payment, leading to potential revenue loss.
Ministry Of Health	Revenue collection at health education programs, border health services, and health colleges	May lead to incorrect revenue collection and result in revenue misstatements.
TPA	Licensing and Pilotage Exemption Processes	Increases the risk of revenue leakage due to errors or potential deliberate manipulation of exemptions and license issuance
WRBWB	Data collection and sales, river restoration activities, and penalties and fines	Increases the risk of revenue leakage and reduces operational efficiency.
TAWA	Processing and billing of trophy dealer licenses and Special Wildlife Investment Concession Areas (SWICA) services	May result in unrecorded or under-collected payments, leading to potential revenue leakages.
TFB	Issuing of Film permits, licenses, and practitioner IDs The film review process	May result in unrecorded or under-collected payments, leading to potential revenue leakage and unauthorised film approvals.
TARI	Agricultural research management	• Reduced operational efficiency and delays in service delivery. • Limited scalability and responsiveness in addressing stakeholder needs.

Entity	Non-Automated Processes	Implication
		• Inadequate data for performance monitoring, decision-making, and reporting.
ATCL	Ticket and reservation system	• Reconciliation of ticket sales transactions between the ticket reservation system and payments made through the mobile money portal. • Computation of agents' commissions. • Approval of refunds is performed outside the system. • Computation of cost of excess baggage
Dodoma Water Supply and Sanitation Authority	Transfer of asset	• increases the risk of data inaccuracies, delays in reporting, and potential financial misstatement.
Tanzania National Parks	Payroll expenditures	• Delayed payroll expense recording leading to financial misstatement
Same-Mwanga Water Supply and Sanitation Authority	budget monitoring	• Inaccurate or delayed budget monitoring, leading to potential misallocation of funds and unreliable financial reporting
Tanzania Meat Board	Stakeholder registration and retention, processing of import and export certificates, stakeholder management and revenue collection, modification or cancellation of issued certificates, and recording, monitoring, and analysis of returned export consignments	• Inadequate enhancement of MIMIS limits operational flexibility and effective monitoring of export activities, leading to service delays, poor decision-making, and inability to track returned consignments
National Sports Council	annual renewals	Limited system functionality and reliance on manual processes weaken revenue tracking, data completeness, and operational efficiency. • This increases the risk of revenue leakage, human errors, and unauthorized system access, resulting in unreliable financial and operational information.
Tanzania Ports Authority	Issuance licensing of shipping service providers upon vessel arrival.	Lack of automation in these processes increases the risk of potential deliberate manipulation of exemptions and license issuance, as well as potential revenue leakage due to errors
Mikwambe English Medium	Billing process for school fee	Reliance on manual student fee collection and lack of a proper monitoring system increase the risk of fraud, corrupt practices, revenue loss, under-banking, and inaccurate reporting
Arusha School		
Kisimani Pre Primary School		
Maasai Pre and Primary		
Mzizima Primary School		
Mikongeni Primary School		
Majani ya Chai Primary School		

Entity	Non-Automated Processes	Implication
Zanaki Primary School		
Gogo Primary School		

147. **I recommend that:**

(a) Public institutions develop and implement a time-bound plan to automate key business processes, prioritising high-risk areas such as revenue collection, billing, payroll, and licensing to enhance efficiency, accuracy, and service delivery.

(b) The Government, through the e-Government Authority, provide oversight and enforce standards to ensure that automation initiatives are aligned with national ICT frameworks, integrated with existing systems, and do not result in further duplication or fragmentation.

5.6 Under-utilisation of Application Systems

148. The evaluation of information system utilisation across public institutions revealed that entities have deployed information systems that were customised or acquired to address specific operational and user requirements, despite the investments made in the development and acquisition of these systems, a notable underutilisation of key functionalities and system modules was identified, as summarised in **Table 6**.

Table 6 : Under-utilisation of Application Systems

Sn	Entity Name	System	Under-utilised Module
1.	Office of Attorney General	OAGMIS system	Contract Management Module
2.	TTCL	VFD system	VFD postpaid Module
3.	Weights and Measures Agency	Weights and Measures Agency - Management Information System (WMA-MIS)	Metrological Supervision Module
4.	Mzumbe University	Library Information Management System (LIMS)	Library Books Module
5.	WCF	Enterprise Resource Management Suite (ERMS)	Payroll Module
6.	Mining Commission	Land Folio System	Offence Module
7.	LGTI	Student Information System (SIS)	Student status change module
8.	Tanzania Film Board	MUSE	Inventory Module
9.	Tanzania Mercantile Exchange	Online Trading System	Entire System

149. This underutilisation has limited the systems' ability to support core business processes, achieve their intended objectives, and deliver value for money, thereby undermining the expected return on investment.

150. **I recommend that management implement deliberate measures to ensure full and effective utilisation of information systems by enforcing system usage, enhancing user capacity, and aligning system functionalities with institutional business processes, thereby achieving intended objectives and maximising return on investment.**

5.7 Anomalies in ICT project management

151. A review of ICT project management in public entities revealed weaknesses in project planning, governance, monitoring, documentation, and data migration controls. Projects were not completed

within approved timelines, lacked essential documentation, and exhibited deficiencies in data migration processes.

5.7.1 Delays in ICT Project Implementation

152. The delayed projects include the following:

- The redesign of the Online Registration System (ORS) at **BRELA**, initiated in March 2020 and initially scheduled for completion within three months, experienced a delay of five years, with project costs exceeding the original budget.

- The Professional Management Information System (PMIS), implemented by the **ICT Commission (ICTC)**, commenced in January 2025 with a planned six-month implementation period but remained under implementation as of November 2025, indicating a delay of five months.

- The Artisanal and Small-Scale Mining (ASM) Portal project implemented by the **State Mining Corporation (STAMICO)**, which was scheduled for deployment by March 2025, remained under development as of November 2025, indicating a delay of eight months.

- The **Tanzania Airports Authority (TAA)** implemented the Integrated Financial Management Information System (IFMIS) project, which commenced in March 2024 and was scheduled for completion in September 2024. However, as of September 2025, the project had not been completed, indicating a one-year delay despite the Defects Liability Period (DLP) having elapsed.

- The **Tanzania Coffee Board (TCB)** launched the Unified Coffee Management System (UCMS) project in 2022 with an 18-month implementation timeline. However, as of December 2025, the project remained incomplete, indicating a delay of about one year.

- The District Roads Management System (DROMAS) upgrade project by **Tanzania Rural and Urban Roads Agency (TARURA)**, scheduled for implementation between November 2022 and April 2023, remained in the planning phase as of September 2025, indicating a delay of two years.

- The Conservation Information Management System (CIMS) project by **TAWA**, initiated in 2018 with an original completion target of January 2019, remained incomplete as of August,2025, reflecting a delay of six years.

- The National Energy Information Management System (NEIMS) and Nishati Dashboard projects, implemented by the **Ministry of Energy** and originally scheduled for completion by December 2023, remained in the system development phase as of September 2025, indicating a delay of two years.

- The Afya eHMS project, implemented by the **Ministry of Health**, was not completed within the extended contractual deadline of 30 June 2025 and remained incomplete as of October 2025, indicating a delay of four months.

- The Maji-IS Enhancement project, implemented by the **Ministry of Water**, with 37 planned system functions for the 2024/25 financial year, remained incomplete as of September 2025. Indicating a delay of three months.

153. These delays hindered timely service-delivery improvements and exposed ICT investments to the risk of inefficiency and cost overruns.

154. **I recommend that Management:**

(a)Strengthen project planning, governance, and monitoring to prevent ICT project delays; and

(b)Develop and implement strategies and action plans to address ongoing delays and restore projects to the approved implementation timelines.

5.7.2 Inadequate Project Documentation

155. The review revealed that eight projects had insufficient documentation, details of which are summarised in **Table 7.**

Table 7: Missing ICT Project Documentation

S/N	Entity	Missing Project Documents
1.	Tanzania Rural and Urban Roads Agency (TARURA)	(i) Project Implementation Plan (ii) Project Risk Register
2.	Ministry of Lands, Housing and Human Settlements Development	(i) Quality Assurance Plan (ii) Performance Monitoring Reports (iii) Change Management Plans
3.	Valuers Registration Board	(i) System Requirements Specification (SRS) (ii) Formal Sign-off / Verification
4.	ICT Commission (ICTC)	(i) Quality Assurance Plan (ii) Performance Monitoring Reports (iii) Data Migration Plan
5.	Vocational Education and Training Authority (VETA)	Project Implementation Plan
6.	Medical Store Department (MSD)	(i) Project Proposal / Charter (ii) Terms of Reference (ToR) (iii) System Requirements Specification (SRS) (iv) System Design Document (SDD) (v) User Acceptance Testing (UAT) Reports
7.	Tanzania Coffee Board	(i) Project Implementation Plan (ii) Project Risk Register (iii) Cost Breakdown (iv) System Requirements Specification (SRS) (v) System Design Document (SDD) (vi) Monitoring Reports (vii) Change Management Plans
8.	Ministry Of Information, Culture, Arts and Sports (MICAS)	(i) Project Charter (ii) System Requirements Specifications (SRS) (iii) Progress & Completion Reports

156. The absence of adequate project documentation undermines the effective management and execution of ICT projects. It impedes proper system development, testing, and risk mitigation, increasing the likelihood of errors, delays, and cost overruns, while reducing accountability and stakeholder confidence.

157. **I recommend that the management of TARURA, MLHHSD, VRB, ICTC, VETA, MSD, Tanzania Coffee Board and MICAS:**

(a) Establish formal governance processes to ensure timely review, approval, and updates of all project documents, and

(b) Develop and approve critical project documentation, including project plans, risk registers, SRS, SDD and user acceptance procedures.

5.7.3 Data migration planning

158. Data migration planning is a critical element of ICT project management, as it ensures that historical and current data are accurately transferred, validated, and reconciled when new systems replace existing processes, thereby safeguarding data integrity, completeness, and reliability.

159. However, the audit discovered weaknesses in data migration planning and execution at the Town Planner Registration Board (TPRB) and the ICT Commission (ICTC). At TPRB, historical registration and payment records for town planners were not migrated to the Billing System, leaving them outside the automated environment. At ICTC, data migration from IPRS to PIMS was inadequately planned and validated, resulting in incomplete ICT professionals' records after migration. At TASAC, receivable data previously managed under the Epicor system had not been migrated to the Tanzania Revenue Gateway (TRG) system, resulting in fragmented receivables management and reliance on manual tracking mechanisms.

160. **I recommend that the management of TPRB, ICTC and TASAC:**

(a) Develop and implement formal data migration plans that include clear scope definition, source-to-target mapping, reconciliation procedures, and validation controls; and

(b) Ensure the complete and accurate migration of historical and current records into automated systems to maintain data integrity, reliability, and completeness.

CHAPTER SIX

06

Conclusion And General Recommendations

6.1 Overall Conclusion

161. Based on the audit procedures performed across 133 public institutions, it is concluded that the existing ICT governance and control environment is not adequate to fully support secure, integrated, and efficient digital Government operations.

162. While progress in the implementation of ICT across Government entities is evident, gaps remain in compliance with e-Government requirements, IT General Controls, system integrations, and ICT project management. Weaknesses in governance oversight, security controls, access management, business continuity, and documentation indicate inconsistent application of established standards.

163. Additionally, the persistence of fragmented systems, duplicated applications, manual processes, and underutilization of ICT systems limits the value derived from ICT investments. These factors increase the government's exposure to risks related to cybersecurity, data integrity, and the reliability of service delivery.

164. Overall, strengthened governance, enhanced compliance enforcement, improved system integration and control frameworks are necessary to ensure that ICT investments effectively support accountable, secure, and efficient public service delivery.

165. The SOC Type 2 audit of the Ministry of Finance, the Ministry of Water, the Prime Minister's Office – Regional Administration and Local Government (PMO-RALG), and the President's Office – Public Service Management and Good Governance (PO-PSMGG) found that the systems' descriptions fairly represent their design and implementation, and that the Ministries have established control frameworks to support the security, availability, processing integrity, confidentiality, and privacy of centrally managed government systems. However, several control deficiencies were identified which may increase the risk of unauthorized access, undetected system changes, and delayed response to system incidents across government systems relied upon by multiple public entities. Strengthening these control areas is therefore necessary to enhance the reliability, security, and continuity of critical government digital services.

6.2 General recommendations

166. To enhance the performance, security, and reliability of government ICT systems, the following measures are recommended:

i) Compliance With E-Government Laws and Standards

- Public entities must implement approved ICT strategies, establish functional ICT Steering Committees, conduct regular IT risk assessments, and maintain effective ICT policy frameworks.
- The relevant authorities should strictly enforce compliance with the e-Government Act, 2019 and related standards to promote consistent ICT practices, accountability, and efficient utilisation of ICT resources.

ii) Information Technology General Controls

- Strengthen controls over network security, database management, and user access, including timely patch management, strong authentication, and periodic access reviews.
- Establish effective incident detection and response mechanisms and ensure implementation and regular testing of Business Continuity and Disaster Recovery Plans (BCP/DRP).
- Improve third-party ICT management by ensuring all services are governed by formal contracts and active Service Level Agreement (SLA) monitoring.

iii) Process automation and system utilisation

- Integrate application systems using approved government interoperability standards to eliminate data silos.
- Eliminate the duplication and fragmentation of ICT systems to reduce operational costs.
- Automate key business processes to improve efficiency and transparency while ensuring the full utilisation of existing system functionalities.
- Strengthen ICT project planning, monitoring, documentation, and data migration controls to avoid delays and cost overruns.

167. The following are specific recommendations issued to individual government entities and directed toward Ministries and Institutions responsible for coordinating and overseeing ICT at national and sector levels, to strengthen security, efficiency, and effectiveness in support of economic growth.

6.3 Recommendations to Key Ministries and Authority

6.3.1 e-Government Authority

168. I recommend that the management of eGA:

(a) Enhance support to public institutions in implementing established standards, policies, procedures, and regulations, and strengthen monitoring of ICT controls to ensure consistent compliance with these requirements.

(b) Enhance oversight of integration among government systems to enable secure and efficient data sharing, promote interoperability, and increase the effectiveness of public service delivery.

(c) Strengthen oversight mechanisms to ensure optimal use of existing application systems and prevent unnecessary duplication of ICT systems across public entities.

(d) Prioritise the automation of business processes in public institutions to improve efficiency in service delivery, reduce bureaucracy, increase transparency, accountability, and facilitate secure information sharing among government entities.

(e) Strengthen monitoring and oversight of ICT system development projects in public institutions to ensure timely completion in compliance with established policies, standards, guidelines, regulations, and procedures.

6.3.2 Ministry of Finance, Ministry of Water, President's Office – Public Service Management and Good Governance, Prime Minister's Office – Regional Administration and Local Government

169. In order to strengthen the effectiveness of controls over centrally managed government systems, I recommend that the Ministries take the following measures:

(i) Management should ensure that system access is granted based on formally approved access requests, supported by clearly defined user roles and responsibilities. Periodic user access reviews should be conducted regularly to confirm that access rights remain appropriate, and access for terminated or transferred personnel should be revoked promptly.

(ii) Privileged accounts should be subject to continuous monitoring to detect unauthorised or inappropriate administrative activities. Audit logging mechanisms should be supported by formal log retention policies to ensure that system logs are preserved and available for investigation and monitoring purposes.

(iii) Management should ensure that all system changes follow established change management procedures, including documented approval, testing in non-production environments, and post-implementation review. This will reduce the risk of introducing system errors, vulnerabilities, or processing disruptions.

(iv) Government service organisations should establish and enforce formal incident management processes supported by a centralised incident logging and tracking mechanism. All incidents should be formally recorded, monitored, and resolved within defined service-level expectations, and root-cause analysis should be performed for significant incidents to prevent recurrence.

(v) Ministries should ensure that enterprise risk assessments are conducted and updated regularly, including the identification and evaluation of information security, fraud, operational, and strategic risks. Risk registers should be maintained and reviewed periodically to support timely mitigation of emerging risks.

(vi) Formal configuration baselines should be established and documented for system infrastructure, applications, and databases to ensure consistent and secure system settings. Patch management procedures should also be implemented and monitored to ensure timely remediation of known vulnerabilities.

(vii) Service Level Agreements with external service providers, including the e-Government Authority and other ICT vendors, should clearly define roles, responsibilities, service expectations, and accountability mechanisms. Ministries should ensure that such

agreements remain valid, reviewed periodically, and aligned with operational requirements.

(viii) Disaster recovery plans and business continuity procedures should be formally approved, periodically tested, and updated to ensure the continued availability of critical government systems during disruptions.

6.3.3 Ministry of Health

170. I recommend that the management of the Ministry of Health:

i) Ensure the implementation of a standardised system across all zonal hospitals and a single unified system across all national hospitals.

ii) Ensure these systems are fully integrated with GoTHOMIS (used at primary health facilities) and Afya eHMS (used at regional referral hospitals). This will enhance interoperability, ensure data consistency, and provide a seamless “continuum of care” for patients across all levels of the healthcare system.

Appendices

Appendix I: Overall Compliance Level for Each Entity

Entity	Overall Compliance Level
Centre for Agricultural Mechanisation and Rural Technology	Level 0
Deep Sea Fishing Authority	Level 0
Valuers Registration Board	Level 0
Tanzania Film Board	Level 1
Institute of Judicial Administration	Level 1
Personal Data Protection Commission	Level 2
Town Planners Registration Board	Level 1
Local Government Training Institute	Level 1
University of Dodoma	Level 2
Ministry of Information, Culture, Arts and Sports	Level 2
Drug Control and Enforcement Authority	Level 2
Nzega Urban Water Supply and Sanitary Authority	Level 2
Wami Ruvu	Level 2
National College of Tourism	Level 2
Beekeeping Training Institute-Tabora	Level 2
Ministry of industry and trade	Level 2
Ministry of Community Development, Gender, Women and Special Groups	Level 2
National Prosecution Service	Level 2
Agriculture Seeds Agency	Level 2
National Food Reserve Agency	Level 2
National Irrigation Commission	Level 2
The Benjamin Mkapa Hospital	Level 2
Pharmacy Council	Level 2
Legal Training Institute for Practical Studies in Tanzania (LST)	Level 2
Ardhi University	Level 2
Prime Minister's Office-Labour Youth Employment and Disability	Level 2
Rural Energy Agency	Level 2
Ministry of Energy	Level 2
ICT Commission	Level 2
Ministry of Livestock and Fisheries (Livestock Sector)	Level 2
Tanzania Livestock Research Institute	Level 2
Tanzania Electrical, Mechanical and Electronics Services Agency	Level 2
Air Tanzania Company Limited	Level 3
Medical Store Department	Level 3
Tanzania Institute of Education	Level 3
Tanga Urban Water Supply and Sanitation Authority	Level 3
Tanzania Coffee Board	Level 3
Tanzania Forest Services Agency	Level 3
National Water Fund	Level 3
Rural Water Supply and Sanitation Agency	Level 3

Entity	Overall Compliance Level
Mbeya University of Science and Technology	Level 3
Mkulazi Holding Company	Level 3
Dar Rapid Transit Agency	Level 3
Tanzania Rural and Urban Roads Agency	Level 3
Judiciary of Tanzania	Level 3
Tanzania Buildings Agency	Level 3
Tanzania National Roads Agency	Level 3
The Mining Commission	Level 3
Ministry of Minerals	Level 3
Ministry of Agriculture	Level 3
Tanzania Agricultural Research Institute	Level 3
Tanzania Fertilizer Regulatory Authority	Level 3
Tanzania Official Seed Certification Institute	Level 3
Government Chemist Laboratory Authority	Level 3
Ministry of Health	Level 3
National Identification Authority	Level 3
Ministry of Water	Level 3
Ministry of Natural Resources and Tourism	Level 3
Tanzania Wildlife Management Authority	Level 3
Ministry of Education, Science and Technology	Level 3
Ministry of Constitutional and Legal Affairs	Level 3
Office of the Attorney General	Level 3
Office of Solicitor General	Level 3
Registration Insolvency Trust Agency	Level 3
Immigration Department	Level 3
Tanzania Social Action Fund	Level 3
Tanzania Revenue Authority	Level 3
Government Procurement Service Agency	Level 3
Tanzania Institute of Accountancy	Level 3
Dar es Salaam University College of Education	Level 3
Higher Education Students Loans Board	Level 3
Muhimbili University of Health and Allied Sciences	Level 3
Tanzania Investment Centre	Level 3
University of Dar es Salaam	Level 3
Vocational Education and Training Authority	Level 3
Tanzania Standard Newspapers	Level 3
Universal Communications Service Access Fund	Level 3
Institute of Accountancy Arusha	Level 3
Morogoro Water Supply and Sanitation Authority	Level 3
Sokoine University of Agriculture	Level 3
Tanzania Education Authority	Level 3
Tanzania Engineering and Manufacturing Design Organisation	Level 3
Kilimanjaro Airports Development Company	Level 3
Tanzania Electric Supply Company	Level 3
National Insurance Corporation	Level 3

Entity	Overall Compliance Level
Dar es Salaam Water Supply and Sanitation Authority	Level 3
Mwanza Urban Water Supply and Sanitation Authority	Level 3
National Bureau of Statistics	Level 3
Tanzania Petroleum Development Corporation	Level 3
TTCL - PESA	Level 3
Muhimbili University of Health and Allied Sciences	Level 3
Energy and Water Utilities Regulatory Authority	Level 3
Land Transport Regulatory Authority of Tanzania	Level 3
Ngorongoro Conservation Area Authority	Level 3
Tanzania Insurance Regulatory Authority	Level 3
Tanzania Broadcasting Corporation	Level 3
Tanzania Ports Authority	Level 3
Tanzania Railway Corporation	Level 3
State Mining Corporation	Level 3
STAMIGOLD Company Limited	Level 3
Cereals And Other Produce Board	Level 3
Contractors Registration Board	Level 3
Fair Competition Commission	Level 3
National Council for Technical and Vocational Education and Training	Level 3
Tanzania Shipping Agencies Corporation	Level 3
Tanzania Bureau of Standards	Level 3
Tanzania Airport Authorities	Level 3
Occupational Safety and Health Authority	Level 3
Tanzania Meteorological Agency	Level 3
Ministry of Lands, Housing and Human Settlements Development	Level 3
PO-Public Service Management and Good Governance	Level 3
Nelson Mandela-African Institution of Science and Technology	Level 3
Ministry of Works	Level 3
Ministry of Transport	Level 3
Ministry of Finance	Level 4
Mzumbe University	Level 4
National Housing Corporation	Level 4
Workers Compensation Fund	Level 4
Tanzania Telecommunications Company Limited	Level 4
Muhimbili National Hospital	Level 4
Tanzania Cotton Board	Level 4
Tanzania National Parks Authority	Level 4
Gaming Board of Tanzania	Level 4
Public Procurement Regulatory Authority	Level 4
Police Force Department	Level 4
Petroleum Bulk Procurement Agency	Level 4
Public Service Recruitment Secretariat	Level 4
Business Registration and Licensing Agency	Level 4
Weights and Measures Agency	Level 4
The Office of the National Assembly	Level 4

Entity	Overall Compliance Level
Prime Minister's Office, Regional Administration and Local Government	Level 4
Roads Fund Board	Level 4
e-Government Authority	Level 5

Appendix II: Entities using an alternative accounting system other than MUSE

S/n	Name of entity	Accounting system in use
1.	DIT Consulting Bureau	Quick Book
2.	DIT company	Quick Book
3.	Kilimanjaro International Leather Industries Company Limited	Relies on Microsoft Excel to record and manage accounting transactions
4.	Tanzania Ports Authority	Uses SAP ERP system as its core financial-management and accounting platform
5.	Ocean Road Cancer Institute (ORCI)	ERMS
6.	National Examination Council of Tanzania (NECTA)	ERMS
7.	Tanzania Coffee Board (TCB)	Sage Evolution
8.	Gaming Board of Tanzania	ERMS
9.	Tanzania Sisal Board (TSB)	ERMS
10.	Tanzania Tea Board(TTeaB)	
11.	Cereals and Other Produce Board (COPB)	ERMS
12.	Procur.& Suppl Profes.(PSPTB)	ERMS
13.	National Housing Corporation (NHC)	ERP - Integrated System
14.	National Sugar Institute	Quick book
15.	Air Tanzania Company Ltd (ATCL)	For FY 2024/25, they used Pastel. However, starting in April 2025, they began migrating to ERMS therefore, the FY 2025/26 financial statements will be generated from ERMS.
16.	Muhimbili National Hospital	JEEVA system
17.	Muhimbili National Hospital-MLOGANZILA	JEEVA system
18.	Tanzania Agricultural Development Bank Limited	Integrated Core Banking System
19.	Small Enterprises Loan Fund	iCBS (Core Banking System), Data Center - CBS
20.	Tanzania Electric Supply Co. Ltd.	Using I-SCALA
21.	Tanzania Fertilizer Company	Using ERMS
22.	Tanzania Commercial Bank	Rubikon ERP
23.	Keko Pharmaceutical Industries (1997) Ltd	Uses Tally accounting system and Microsoft Excel to record and manage accounting transactions.
24.	Usafiri Dar-Es-Salaam (UDA)/UDART	UDA uses Vision 8 System but is in the process of getting TR Number before migrating to MUSE while UDART the subsidiary uses Vision 8 System
25.	Azania Bank Limited	Flexcube (Core Banking System)
26.	National Insurance Corporation	ERMS
27.	Workers Compensation Fund	ERMS
28.	Mkulazi Holding Company Limited	ERP
29.	Tanzania Biotech Product Limited	SAGE (ERMS under discussion)
30.	Sisalana Tanzania Company	SAGE
31.	Kilimanjaro Machine Tools Company	Manual
32.	Makambako Water Supply and Sanitation Authority	ERMS
33.	National Social Security Fund	Oracle E-Business Suite (ERP)
34.	National Development Corporation	MUSE
35.	UTT AMIS	SAGE
36.	Tanzania Posts Corporation	SAGE AND MUSE (From 01 July 2025; ERMS)
37.	TIB Development Bank Limited	T-24 CORE BANKING SYSTEM
38.	TIB Rasilimali Company	T-24 CORE BANKING SYSTEM
39.	Housing and Pension Company	SAGE
40.	Tanzania Concrete Poles Manufacturing Co.	Using ERMS
41.	Electrical Transmission and Distribution Co.	Using ERMS
42.	Tanzania Geothermal Development Company	Using ERMS
43.	Ubungo Plaza Ltd	Using Myob
44.	National Health Insurance Fund	Using ERMS
45.	Dar es Salaam Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
46.	Kahama-Shinyanga Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
47.	Mwanza Water Supply and Sanitation Authority	using ERMS, currently in the transition phase

S/n	Name of entity	Accounting system in use
48.	Arusha Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
49.	Tanga Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
50.	Mbeya Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
51.	Dodoma Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
52.	Tabora Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
53.	Moshi Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
54.	Iringa Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
55.	Shinyanga Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
56.	Morogoro Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
57.	Kahama Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
58.	Musoma Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
59.	Mtwara Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
60.	Kigoma Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
61.	Songea Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
62.	Bukoba Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
63.	Lindi Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
64.	Singida Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
65.	Bariadi Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
66.	Mpanda Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
67.	Sumbawanga Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
68.	Masasi-Nachingwea Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
69.	Babati Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
70.	Same-Mwanga Water Supply and Sanitation Authority	2024/25 used Excel - Currently in the transition phase for using ERMS
71.	Nzega Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
72.	Tukuyu Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
73.	Njombe Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
74.	Karatu Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
75.	Geita Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
76.	Kyela Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
77.	Namtumbo Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
78.	Ngara Water Supply and Sanitation Authority	using ERMS, currently in the transition phase
79.	National Insurance Corporation	that the Corporation has been utilizing the Enterprise Resource Management Suite (ERMS) system for accounting and financial operations.
80.	Makambako Water Supply and Sanitation Authority	using ERMS, currently in the transition phase

ANNUAL GENERAL REPORT ON INFORMATION SYSTEMS AUDITS

National Audit Office (NAOT)
4 Mahakama Road, Tambukareli
P. O. BOX 950, 41104 Dodoma
TEL: +255 (026) 2161200
Fax: +255 (026) 2321245
Email: ocag@nao.go.tz

ISO 9001:2015 Certified