ISO 9001:2015 Certified

THE UNITED REPUBLIC OF TANZANIA
NATIONAL AUDIT OFFICE

PERFORMANCE AUDIT REPORT ON THE UTILISATION OF ICT SYSTEMS IN REGULATORY AUTHORITIES IN THE DELIVERY OF THE REGULATORY SERVICES

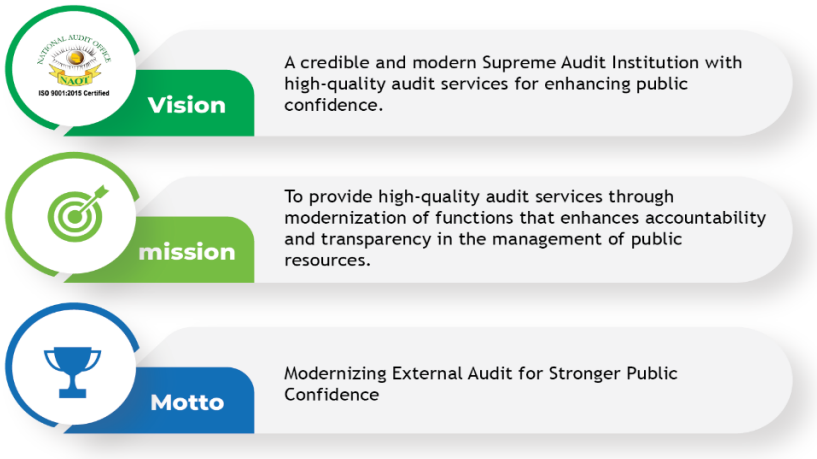
CONTROLLER AND AUDITOR GENERAL
MARCH 2025

About the National Audit Office

Mandate

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

NAOT Vision, Mission & Motto



Core Values

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

Professional competence: We deliver high quality audit services based on appropriate professional knowledge, skills, and best practices.

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

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

Results-Oriented: We focus on achievements of reliable, timely, accurate, useful, and clear performance targets.

Team Work Spirit: We value and work together with internal and external stakeholders.

PREFACE

Section 28 of the Public Audit Act, CAP 418 [R.E. 2021] gives mandate to the Controller and Auditor General to carry out Performance Audit (Value-for-Money Audit) to establish the economy, efficiency and effectiveness of any expenditure or use of resources in the Ministries, Departments and Agencies (MDAs), Local Government Authorities (LGAs) and Public Authorities and Other Bodies, which involves enquiring, examining, investigating and reporting, as deemed necessary under the circumstances.

I have the honour to submit to H.E. Hon. Dr. Samia Suluhu Hassan, President of the United Republic of Tanzania, and through her to the National Assembly, the Performance Audit Report on the Utilisation of ICT Systems in Regulatory Authorities in the Delivery of Regulatory Services.

The report contains findings, conclusions and recommendations that are directed to the e-Government Authority (e-GA). The e-Government Authority had the opportunity to scrutinize and comment on the factual contents of the report. I wish to acknowledge that discussions with e-GA have been useful and constructive.

My Office intends to conduct a follow-up at an appropriate time regarding actions taken by the audited entity concerning the recommendations given in this report.

I would like to thank my staff for their commitment to preparing this report. I also acknowledge the audited entity for cooperating with my office, which has facilitated the timely completion of the audit.

Charles E. Kichere
Controller and Auditor General
Dodoma, United Republic of Tanzania
March 2025

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

BP	:	Business Process
BRELA	:	Business Registration and Licensing Agency
e-GA	:	The e-Government Authority
FYDP III	:	The Third Five-Year Development Plan Phase
G2B	:	Government to Business
G2G	:	Government to Government
GePG	:	Government Electronic Payment Gateway
ICT	:	Information and Communication Technology
ICTC	:	Information and Communication Technology Commission
KPIs	:	Key Performance Indicators
LATRA	:	Land Transport Regulatory Authority
M&E	:	Monitoring and Evaluation
MC	:	Mining Commission
MICIT	:	Ministry of Information, Communications and Information Technology
NACTVET	:	National Council for Technical and Vocational Education and Training
NIDA	:	National Identification Authority
PIs	:	Public Institutions
PO-PSMGG	:	President's Office – Public Service Management and Good Governance
PPRA	:	Public Procurement Regulatory Authority
PURA	:	Petroleum Upstream Regulatory Authority
RA	:	Regulatory Authorities
SAIs	:	Supreme Audit Institutions
SDGs	:	Sustainable Development Goals
TCRA	:	Tanzania Communication Regulatory Authority
TDV- 2025	:	Tanzania Development Vision 2025
TMDA	:	Tanzania Medicines and Medical Devices Authority
URT	:	United Republic of Tanzania

EXECUTIVE SUMMARY

The e-Government Act of 2019 requires the e-Government Authority to coordinate, oversee and promote e-Government initiatives and enforce e-Government-related policies, laws, regulations, standards and guidelines in public institutions[1]. Also, the Regulatory Authorities oversee sectors such as telecommunications, energy, finance, and health, among others, to ensure compliance with national laws and standards.

To achieve their regulatory roles and objectives, Section 28 (a) of the e-Government Act, 2019 requires the Regulatory Authorities to use and utilise ICT systems to deliver government services and improve the efficiency, transparency, and accessibility of regulatory services.

The main objective of the audit was to assess whether e-GA has adequately managed and overseen the implementation of the e-government initiatives to ensure the effective utilisation of ICT systems in the delivery of regulatory services. The audit focused on the assessment of the extent of utilisation of ICT systems, interventions and plans to enhance utilisation of ICT systems, management of business continuity, and monitoring and coordination with other stakeholders on the oversight function for effective utilization of ICT systems. The audit covered four financial years, from 2020/21 to 2023/24.

Main Audit Findings

Inadequate Development and Utilisation of ICT Systems in the Delivery of Regulatory Services

The audit noted inadequate automation of the business process to enhance the effective delivery of regulatory services, with 43% of assessed business processes not automated for delivering services. This poses a risk to effective e-government service delivery in public institutions.

Inadequate Establishment and Implementation of Interventions to Enhance the Management and Utilisation of ICT Systems

The audit noted inadequate establishment and implementation of strategies and plans for the management and utilisation of ICT of the government

[1] Section 5 (1) of the e-Government Act, 2019

services, including percentage and level of preparedness for cyber-attacks. Also, the audit noted the absence of sub-tasks of the main activates planned.

Additionally, the audit noted that e-GA did not adequately evaluate the ICT Maturity status of public institutions, which is four years per the requirements of the e-Government General Regulations, 2020. This was attributed to the fact that e-GA did not ensure that public institutions adequately conduct the self-evaluation of ICT maturity status as required. This contributes to drawbacks in interventions by public institutions regarding ICT maturity growth.

Inadequate Management of the Business Continuity in the Delivery of e-Services

The audit noted interoperability among the developed ICT systems within the regulatory authorities. It was observed that LATRA, MC, NACTVET, and TMDA were not adequately integrated with external ICT systems such as BRELA, NIDA (for MC, NACTVET and TMDA), TRA (for MC and TBS) and Tanzania Police Force (for LATRA) in their daily operations. Inadequate interoperability for data exchange results in the ineffectiveness of data validation, accessibility and integrity, ultimately affecting the effective delivery of e-government services, especially when verifying the submitted data.

Additionally, e-GA did not effectively ensure adequate preparation and management of Disaster Recovery Plans (DRPs) for ICT systems in Public Institutions, specifically in regulatory authorities. The audit noted that one out of the eight (12%) selected Regulatory Authorities did not have the DRPs, and none of the visited Regulatory Authorities had tested for these plans to assess the entities' readiness to respond to the disaster. Inadequate testing of the DRP affects the confidence in the public institutions in disaster preparedness.

Inadequate Monitoring and Control of the Implementation of the e-Government Interventions in Public Institutions

The audit noted that there was inadequate performance assessment of the ICT Project and ICT systems. e-GA did not adequately conduct the ICT projects and systems performance audit to determine whether they delivered the intended services efficiently. Although effectiveness and

efficiency were considered in the ICT systems review, they were not thoroughly assessed, which contributes to inadequate measurement of the impact of ICT systems on service delivery.

Also, there was inadequate security risk identification and assessment of new and existing infrastructure. e-GA lacked the ICT security incidents database to support investigations on the ICT Systems, nor did it conduct an analysis of ICT security events and incidents, which contributes to the vulnerability of the security in ICT systems.

Furthermore, e-GA did not have a plan in place to conduct a follow-up on the issued recommendation on inspections and assessment of ICT systems and projects. In this regard, no audits were conducted to assess the governance of data quality, data integrity or performance of service delivery. Over the course of four financial years, e-GA has not conducted a follow-up audit on the issued recommendations, which may hinder the effective implementation of corrective actions.

Audit Conclusion

The audit recognizes the efforts made by e-GA and the regulatory authorities to automate business processes through the use of ICT systems aimed at enhancing the delivery of regulatory services. Also, e-GA made efforts to develop templates for compliance with standards, guidelines, laws and regulations and worked to build the capacity of internal auditors on ICT assessments within their respective public institutions. However, there was inadequate management and oversight on the implementation of e-government initiatives to ensure the effective utilisation of ICT systems in the delivery of regulatory services. This has been noted in several assessment areas, including interventions to manage and oversee e-service business continuity, monitoring and control of the ICT systems, and coordination among key stakeholders.

Audit Recommendations

The e-Government Authority (e-GA) is urged to:

a) Enhance the promotion and compliance enforcement of e-government services so as to improve ICT system utilization,

automate business processes, conduct regular maturity assessments, and monitor ICT performance in achieving institutional objectives;

b) Enhance its enforcement of the management and use of standardized ICT management tools in public institutions to ensure effective use of key documents such as Disaster Recovery Plans (DRP), Service Level Agreements (SLA), Operational Level Agreements (OLA), and Change Management Strategies;

c) Develop and implement a comprehensive strategy and detailed plans that outline clear coverage for inspection and review of ICT systems and compliance assessment in public institutions, which details the frequency of inspections, targets and performance indicators to enable the e-GA to effectively monitor, evaluate, and improve its enforcement efforts;

d) Enhance monitoring and evaluation of all the e-government initiatives and interventions and use the results to take corrective actions for improvement. This should include conducting regular analysis of monitoring data for informed decision-making, engaging relevant institutional steering committees, and ensuring follow-up on the implementation of recommendations provided to public institutions.

CHAPTER ONE

INTRODUCTION

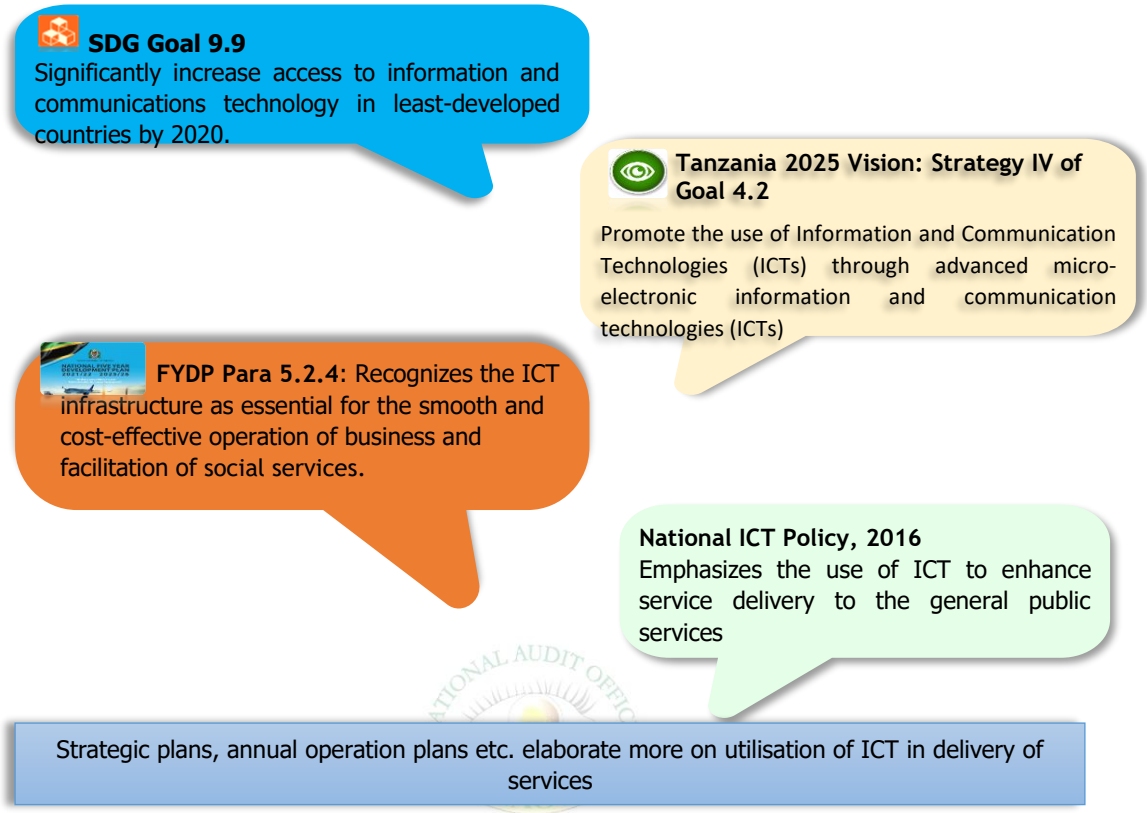
1.1 Background Information

The regulatory authorities oversee various sectors, such as telecommunications, energy, finance, and health, to ensure compliance with national laws and standards.

To perform their regulatory roles and objectives, it is required by Section 28 (a) of the e-Government Act, 2019 that the Regulatory Authorities should use and utilise ICT systems to deliver government services and improve the efficiency, transparency, and accessibility of regulatory services.

In Tanzania, the e-Government Authority (e-GA), which was established after the enactment of the e-Government Act in 2019, is responsible for coordinating, overseeing and promoting e-Government initiatives and enforcing e-Government related policies, laws, regulations, standards and guidelines in a public institution, and serves esteemed beneficiaries who utilise fully e-GA products and services. The beneficiaries are categorised into two groups: public institutions and citizens. Thus, e-GA offers government-to-government (G2G) services to increase public institutions' capacity to offer services to citizens (G2C), businesses (G2B), and government employees (G2E).

Different international and national plans and goals have emphasized the need for the management and utilisation of ICT in public services, as presented in the following illustration:



Given the above, enhancing the management and utilisation of the ICT system in regulatory authorities is key for effectively delivering regulatory services in the country.

1.2 Motivation for the Audit

The audit was motivated by ICT's significance in supporting the achievement of National and Sustainable Development Goals (SDGs). The specific factors that motivated the audit are detailed below.

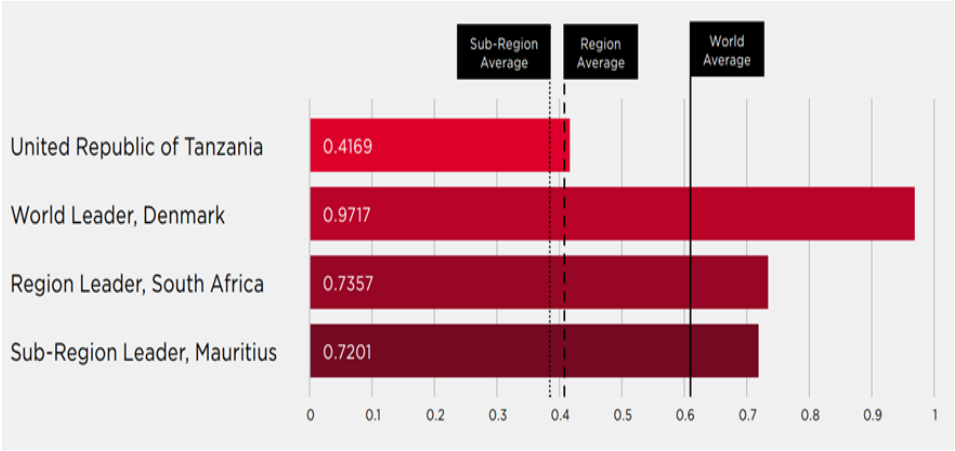
(a) Tanzania was Ranked Low in the UN e-Government Development Index (EGDI) Survey in the Use of ICT

A report on Advancing e-government: Lessons from Tanzania (Part 2), by Sone Osakwe, published in the UN Global System for Mobile Communications (GSMA), 2023 and the UN E-Government Survey, 2022 revealed that, according to the Global Innovation Index Study conducted in 2022, the country scored 55.3 out of 100 in the sub-indicator of government online

services. In addition, Tanzania was ranked low (153rd out of 193 UN member countries globally) in the United Nations e-government survey of 2022.

Also, according to the UN e-government survey, 2022 on digital government patterns, Tanzania scored 0.4169, below the world average of 0.6[2]. The evaluation examined the range and quality of online services, the state of telecommunication infrastructure, and the existing human capacity to use these services, as depicted in **Figure 1.1**.

Figure 1.1: Tanzania's Global Rank in ICT Innovation in e-Government Services



Source: Auditors' Analysis of Global Index Statistics, 2024

Figure 1.1 shows that although Tanzania has put in significant efforts, the global innovation index in ICT use is still insufficient to meet the global average Innovation Index. This indicates the need for public sector entities, including the regulatory authorities, to enhance the management and utilisation of ICT.

(b) Uncoordinated Business Processes in the Use of ICT Systems

Para 2.5.2 of the Tanzania e-Government Strategy, 2022, states that one of the problems in the provision of e-government services is that traditionally, many public services are delivered in person, within certain working hours,

[2] Global Development Index is a composite measure of three important dimensions of e-government, namely: provision of online services, telecommunication connectivity and human capacity.

and with a heavy reliance on paper forms. Lack of service delivery harmonisation due to unintegrated business processes means public institutions are working in silos. These unintegrated service provision procedures lead to discontinuities in the service provision from one institution to another, making the entire process highly inefficient.

Also, the strategy highlights a notable lack of collaboration among public institutions at the business processes level. Thus, there is a need to re-engineer the business process to eliminate unnecessary exchange of manual paper documents. This inefficiency complicates service delivery and contributes to increased operational costs and delays in public service responsiveness.

Further, the strategy indicated uneven maturity in applying e-government initiatives to enhance governmental functions and service delivery among public institutions. Most e-government systems are developed and implemented separately, according to the jurisdictional boundaries of an individual institution, rather than being integrated cooperatively according to function or discipline.

In addition, the implementation report on the working group of the Internet Government 2019 held by the e-Government Authority (e-GA) identified some of the challenges public institutions face in implementing e-government efforts, including the non-observance of guidelines and principles of e-government management.

(c) Limited and Unintegrated e-Services

Para 2.5.6 of the Tanzania e-Government Strategy, 2022, states that one of the problems in the provision of e-government services is the implementation of the e-Government Strategy 2013, which had uneven success in using e-government solutions to deliver e-services. It was reported that some of the systems developed are not used to deliver e-service; they were rarely used to process information within institutions.

In addition, most e-services were developed and delivered in isolation by individual public institutions rather than being integrated according to function. Furthermore, e-government services involving inter-institutional cooperation are especially difficult to develop and promote, partly because

of a lack of collaboration mechanisms to support such inter-institutional cooperation.

The Implementation Report from the Working Group on the Internet Government 2019 held by the e-Government Authority (e-GA) noted that despite the success of the e-GA, there are still several implementation challenges. One of these challenges is the presence of systems that do not communicate or exchange information (within and between institutions). The existence of these challenges hinders the planning for the development of the ICT systems.

(d) National Visions, including Tanzania Development Vision 2025 and the Third National Five-Year Development Plan

Objective 4.2 (IV) of the Tanzania Development Vision 2025 highlights the need to promote Information and Communication Technologies as they are central to competitive social and economic transformation. According to this objective, ICT is a major driving force for the realisation of the Vision, and it should be harnessed persistently in all sectors of the economy and service provision. The objective has also been put to the benefit of government entities to enable the provision of services to meet the basic needs of the people, increase quality and productivity, and promote competitiveness.

Also, this audit is motivated by the need to promote innovation and application of ICT in service delivery to ensure a competitive economy as included in the National Five-Year Development Plan III from 2021/22 to 2025/26. Objective 5.2.1 of the Third National Five-Year Development Plan states that one of the seven key interventions is to promote innovation and application of Information and Communication Technology (ICT) in service delivery.

Harnessing Information and Communication Technologies and their management requires appropriate skills, capabilities, and adequate investment for proper management, utilisation, and improvement. In this regard, this audit will align with the vision's objective. It will provide means for attaining its targets upon implementation of the audit recommendation issued to the audited entities.

1.3 Design of the Audit

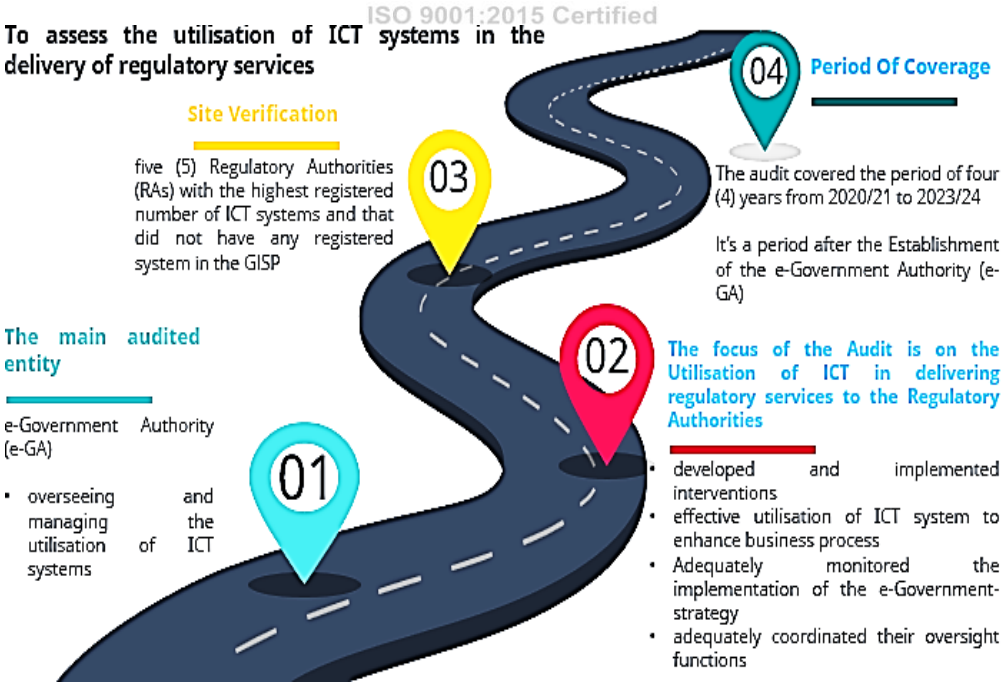
1.3.1 Audit Objective

The main objective of the audit was to assess whether e-GA has adequately managed and overseen the implementation of e-government initiatives to ensure the effective utilisation of ICT systems in the delivery of regulatory services.

Specifically, the audit focused on assessing whether:

(a) ICT systems are developed and utilized in delivering regulatory services to the regulatory authorities;
(b) e-GA has developed and implemented interventions to enhance the utilisation of the ICT systems in delivering regulatory services;
(c) e-GA and regulatory authorities ensure effective utilisation of ICT systems to enhance e-service business continuity;
(d) e-GA adequately monitored the implementation of the e-government initiatives in delivering regulatory services; and
(e) e-GA adequately coordinated oversight functions to ensure the effective utilisation of ICT systems in delivering regulatory services.

1.3.2 Scope of the Audit



1.4 Assessment Criteria

The audit criteria were drawn from policies, legislation, standards, good practices, and strategic plans. The audit criteria were based on the roles played by e-GA and the selected regulatory authorities. The following are the broader assessment criteria for each of the specific audit objectives:

(a) Availability and Utilisation of ICT Systems in Delivering Regulatory Services

Pillar 3 of Tanzania's e-Government Strategy, 2022 requires public institutions, including regulatory authorities, to deliver e-services to the beneficiaries through the use of ICT systems and ensure the availability, accessibility and high-quality e-services across multiple delivery channels.

Furthermore, regulation 50 (1) of the e-Government Regulations, 2020 requires the e-Government Authority to conduct an annual evaluation of public institutions' ICT maturity level. It also requires Public Institutions to self-evaluate, submit the report to the e-GA, verify the evaluation results, and publish the results in the public institutions' ICT maturity report.

(b) Development and Implementation of Interventions to Enhance Management and Utilisation of ICT in Delivering Regulatory Services

Clause 3.10.4 of e-Government Strategy, 2022 states that the e-Government management framework should be strengthened to enhance the e-Government policy and framework, strengthen its legislative environment, and improve its institutional framework.

Further, Section 5(2l) of the e-Government Act, 2019 requires e-GA to monitor and evaluate the implementation of e-Government strategy in public institutions. Also, Section 2.3 of e-GA's Procedures for Government ICT Project Clearance, Monitoring, and Closures, 2020 requires the Authority to monitor and evaluate the Government ICT project in compliance with the ICT Project Monitoring and Evaluation Framework.

Also, paragraph 1.1.5 of the National ICT Policy, 2016 states that the e-Government Authority (e-GA) should promote the use of ICT in the Public Service.

(c) Effective Utilisation of ICT Systems to Enhance e-Service Business Continuity

Section 42 (b) of the e-Government Act, 2019 states that a public institution shall develop and implement a Disaster Recovery Plan (DRP) for information system continuity management.

Furthermore, Regulation 39 (a) of e-Government Regulations, 2020 requires a public institution to ensure that the e-Government services rendered are reliable and citizen-centric to implement business continuity management. This is supposed to include operationalizing a Disaster Recovery Plan submitted to the authority covering such systems that facilitate the rendering of such e-Government services.

Regulation 42 of the e-Government Regulations, 2020 requires a public institution to ensure that (a) e-government services delivered have adequate support systems to the end users, (b) establish an e-service support desk that is easily accessible to enhance delivering of e-service to end users; (c) endeavour to ensure the support desk provides services throughout, and that the services are responsive to the problems of their respective users; and (d) communicate to e- Government services users whenever the service support desk will not be accessible.

In reference to paragraph 2.1.3.2 (xii) of the National ICT Policy, 2016, one of the specific objectives is to strengthen the regulatory environment that facilitates the acquisition, utilisation and development of ICT in Tanzania.

(d) Monitoring of the Implementation of e-Government Initiatives in the Regulatory Authorities

Section 5(2)(l) of the e-Government Act, 2019 requires the Authority (e-GA) to monitor and evaluate the implementation of e-Government initiatives in public institutions.

Section 6 (c) of the e-Government Act, 2019 mandates the Authority to inspect any ICT project, systems, and infrastructure to ensure compliance with e-Government standards and guidelines by any public institution.

Section 5 (f) of the e-Government Act, 2019 requires e-GA to ensure end-to-end visibility of Government ICT systems and other systems offering services to the Government, including undertaking periodic audits of them.

(e) Coordination and Decision-making Platform for Overseeing the Management of ICT in the Delivery of Regulatory Services

Clause 5.2 of the National ICT policy, 2016 states that the Ministry Responsible for e-government will be responsible for developing e-government policy and facilitating its implementation in Government institutions. It further requires the e-government Agency (Authority) to coordinate, oversee, promote, and enforce e-government in public institutions.

Section 5 (1) of the e-Government Act, 2019 requires the e-Government Authority to coordinate, oversee, and promote e-government initiatives and enforce the implementation of e-government-related policies, laws, regulations, standards and guidelines in public institutions.

1.5 Sampling Techniques, Methods for Data Collection and Analysis

The audit gathered information to address the audit objectives and questions. The audit evidence was triangulated with different sources of information. Data were gathered from MICIT, e-GA, and the regulatory authorities that were visited. Below are detailed explanations for each method used for sampling, data collection and analysis.

1.5.1 Sampling Techniques

A multistage sampling technique was used to select the regulatory authorities for verification and data collection, and the sample size was established as summarised below:

Stage 1: Identification of Regulatory Authorities and ICT Systems

Using the available number of Regulatory Authorities in the country and a list of ICT systems extracted from the Government ICT Services Portal (GISP) database for the respective Regulatory Authorities, the Regulatory Authorities were first arranged in order of the number of ICT systems they are using.

Stage 2: Determination of the Number of Regulatory Authorities to be Covered

A systematic sampling approach was used in the available 20 regulatory authorities. These regulatory authorities are allocated to different ministries and perform different functions. This sampling process was designed to ensure that all categories of Regulatory Authorities and their respective business processes were included. Considering the available human resources, time, and budget for this audit, a sample size of eight regulatory authorities was selected.

From the sampled eight regulatory authorities and the provided number of ICT assets in public institutions provided by e-GA, the audit selected the regulatory authorities based on the number of ICT systems registered in the Government ICT Services Portal (GISP). The numbers that were found in GISP were conclusive for the selection, as detailed in **Table 1.1**.

Table 1.1: Sampled Regulatory Authorities with a High Number of ICT Systems in each Sector Ministry

Ministry	Name of the Regulatory Authority	No. of ICT Systems Registered in GISP
Ministry of Transport	Land Transport Regulatory Authority (LATRA)	27
Ministry of Minerals	Petroleum Upstream Regulatory Authority (PURA)	14
Ministry of Health	Tanzania Medicines and Medical Devices Authority (TMDA)	2
Ministry of Industry and Trade	Tanzania Bureau of Standards (TBS)	17
Ministry of Finance	Tanzania Revenue Authority (TRA)	46

Ministry	Name of the Regulatory Authority	No. of ICT Systems Registered in GISP
Ministry of Education, Science and Technology	National Council for Technical and Vocational Education and Training	2
Ministry of Minerals	Mining Commission (MC)	1

Source: Auditors' Analysis on the List of Regulatory Authorities in GISP, 2024

Stage 3: Selection of the Regulatory Authorities with ICT Systems Used in Cross-cutting Public Institutions

Purposive sampling was used to select the Public Procurement Regulatory Authority (PPRA), which has the ICT system (NeST) that is crosscutting in all public institutions.

Following the sampling techniques used, the audit visited eight regulatory authorities, namely LATRA, PURA, TMDA, TBS, TRA Mining Commission, NACTVET and PPRA.

Also, the audit purposively selected 21 ICT systems from the selected regulatory authorities, as elaborated in **Table 1.3.** These are all the ICT systems used by the selected regulatory authorities except for TRA, where the selection was based on the randomly limited number of ICT systems.

Table 1.2: Selected ICT Systems in the Respective Regulatory Authorities

Regulatory Authority	The Available ICT Systems that were Assessed
LATRA	• LATRA VTS Management Console • RRIMS - (Railway & Road Information Management System)
PPRA	• NeST
NACTVET	• Teachers' registration • Admission system • Examination system • Foreign award evaluation system • Transcript system
MC	• Mining Market Management Information System (MMMIS) • Mining Information Management System (MIMS) • Trimble Land folio

Regulatory Authority	The Available ICT Systems that were Assessed
TMDA	• Regulatory Information Management System (RIMS) • Laboratory Management Information System (LMIS)
PURA	• ProSource • Pretel ***NB:*** *They are Internal ICT Systems*
TRA	• Taxpayer Portal (TRA Online Services) • Online Auction • Electronic Tax Stamps Management System – Purchased • CMVRS – Online services
TBS	• i-SQMT (Product certification on products inside the country) • OAS (Online Application System)

Source: Auditors' Analysis of the List of ICT Systems in GISP, 2024

1.4.1 Data Collection Methods

The audit gathered reliable and sufficient audit evidence to address the audit questions and achieve the objective of the audit. Different methods such as document reviews, interviews, and observations/physical verifications/systems walk-throughs were used, as detailed below:

(a) Documents Review

Different documents were reviewed to obtain information about the management of Regulatory Authorities in the implementation of the e-government strategy. National ICT Policy, 2016, strategic plans, annual plans, annual reports and inspection reports were reviewed, and the reasons for reviewing them are listed in **Appendix 2**.

(b) Interviews

Interviews were conducted to obtain more information and clarification on the information obtained through document review and observation. The participants who were interviewed were directors, managers, and officials responsible for the management of ICT in e-GA, as well as regulatory authorities. Also, officials from user departments with respective business processes were interviewed, as indicated in **Appendix 3.**

(c) Observations and System Walkthrough

The audit observed the ICT systems operations in regulatory authorities in the delivery of regulatory services. The selection of ICT systems for system walkthrough depended on the outcome of the reviewed documents and interviews with the sampled officials in respective entities.

Furthermore, various ICT systems such as NeST, Trimble Land folio, i-SQMT (product certification on products inside the country) and OAS (Online Application System) were reviewed to identify the challenges facing the management of e-governance in the delivery of regulatory services.

The ICT systems in the selected regulatory authorities were observed and reviewed to understand their functionality, linkage with the regulatory functions, and the existing performance problems encountered while delivering regulatory services.

1.4.2 Data Analysis

The collected data was analysed using both qualitative and quantitative methods to obtain facts and sufficient information regarding the management of e-Governance in regulatory authorities in the delivery of regulatory services.

a) Analysis of Qualitative Data

Content analysis techniques on the strategies, plans and implementation reports were used to analyse qualitative data by identifying different concepts and facts originating from interviews or document reviews and categorizing them based on their assertions. These data included the management of maturity assessment, availability and updates on the disaster recovery interventions, coordination, monitoring and evaluation and availability of ICT systems in the Government ICT System Portal (GISP).

b) Analysis of Quantitative Data

Quantitative data regarding the number of ICT systems inspections, security and compliance assessments, ICT system reviews and follow-up of the issued recommendation with multiple occurrences was tabulated in spreadsheets

to develop point data or time series data and relevant facts extracted from the obtained figures.

The tabulated data was summed, averaged, or proportioned to extract relevant information and relationships from the figures. The sums, averages, or percentages were presented using different types of charts depending on the nature of the data to explain facts for point data or establish the trends for time series data, and other quantitative information/data with single occurrence was presented as they are in the reports by explaining the facts they assert.

1.6 Standards Used for the Audit

The audit was conducted in accordance with the International Standards of Supreme Audit Institutions (ISSAIs) issued by the International Organization of Supreme Audit Institutions (INTOSAI). These standards require that the audit is planned and performed to obtain sufficient and appropriate evidence to provide a reasonable basis for findings and conclusions based on the audit objective.

1.7 Structure of the Report

CHAPTER TWO

SYSTEM FOR MANAGING UTILISATION OF ICT SYSTEMS IN REGULATORY AUTHORITIES

2.1 Introduction

This chapter highlights the legal framework governing the process, funding, roles, responsibilities, and human resources for managing and utilizing the ICT systems in Regulatory Authorities in the delivery of regulatory services.

2.2 Policy and Legal Framework Governing the Utilisation of ICT Systems

The following policies, acts, guidelines, and strategies guide the management and utilization of ICT systems.

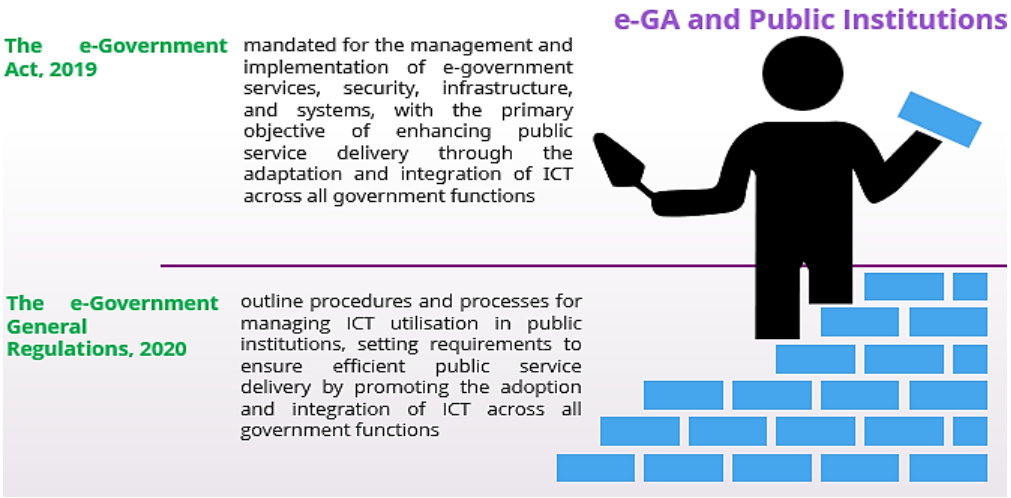
2.2.1 National Information and Communication Policy, 2016

The National ICT Policy of 2016 aims to accelerate socio-economic development to transform the country into a middle-income economy and an ICT-enabled knowledge society. One of the key focuses of the policy is to enhance service delivery to the general public by utilising ICT in public institutions through operationalising, enforcement, monitoring, and evaluation of ICT systems. By aligning with this policy, Regulatory Authorities can leverage ICT to improve efficiency, transparency, and accessibility in public service delivery.

2.2.2 Legislation

Different acts, guidelines, and strategies guide Regulatory Authorities in the utilisation of ICT systems to deliver regulatory services as explained hereunder:

Figure 2.1: Legislation Guiding the Utilisation of ICT Systems

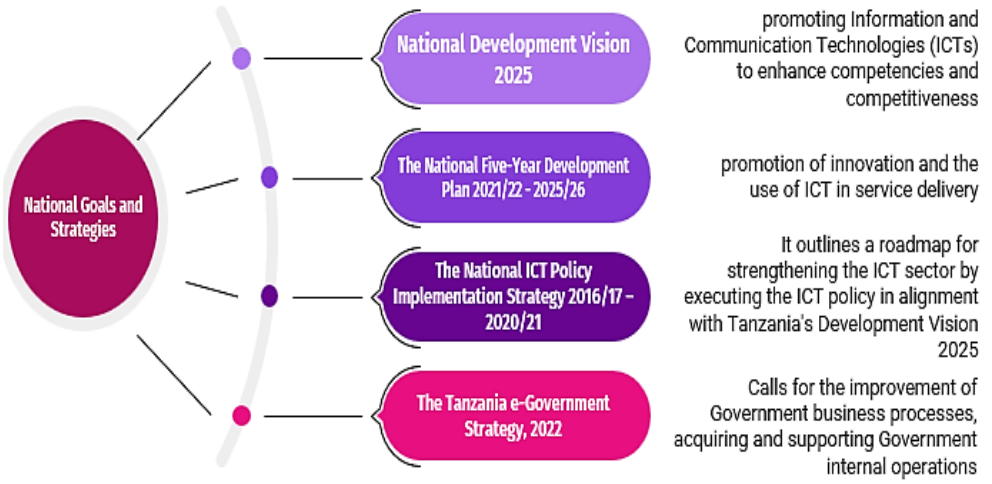


Source: Auditors' Analysis on the e-GA Approved Functions and Organisation Structures, 2024

2.3 National Goals and Strategies

The following are the National goals and strategies that govern the management and utilisation of ICT systems in the country.

Figure 2.2: National Goals and Strategies for Managing Utilisation of ICT Systems

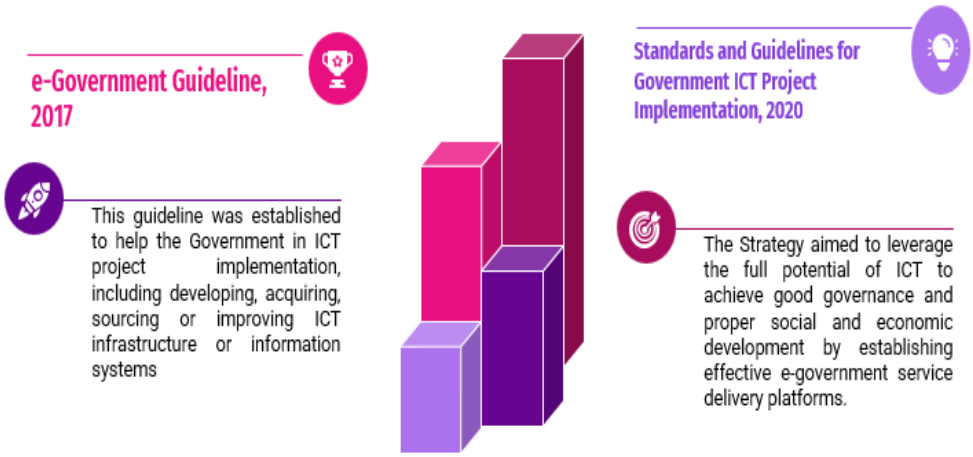


Source: Auditors' Analysis of the National Goals, National ICT Policy and e-Government Strategies, 2024

2.4 The e-Government Guidelines

The guidelines for the management and utilisation of ICT in the country, including the Regulatory Authorities, are as detailed below:

Figure 2.3: Guidelines on Utilisation of ICT Systems



Source: Auditors' Analysis of the e-Government and ICT Project Implementation Guidelines (2020), 2024

2.5 Roles and Responsibilities of Key Actors and Stakeholders

2.5.1 Roles of Key Actors

(a) e-Government Authority (e-GA)

Sections 5 (1) and (2) of the e-government Act of 2019 give a mandate to the e-Government Authority and stipulate the following functions.

Figure 2.4: Mandates of e-GA to Ensure Utilisation of ICT Systems in Regulatory Authorities

Source: Auditors' Analysis of the e-Government Act (2019), 2024

According to the approved function and organisation structure of 2020, the e-Government Authority operates under the following directorates to facilitate the management and utilisation of ICT in public institutions, including Regulatory Authorities in the delivery of regulatory services.

i. Directorate of Compliance and Security Management

The different management sections and their respective roles in relation to the audit focus are described below.

Figure 2.5: Approved Functions for Security and Standards and Compliance Sections

Security Management Section

- Develop, test and implement security plans, products and controls;
- Investigate and take appropriate corrective actions for ICT security incidents across public institutions;
- Co-ordinate development of ICT Business continuity plans

Standards and Compliance Management Section

- Undertake monitoring and compliance with government Standards and Guidelines and
- Monitor e-government compliance and prepare compliance reports;

Source: Auditors' Analysis of the e-GA Approved Functions and Organisation Structure, 2024

ii. Directorate of Service Management

This directorate is responsible for supporting public institutions in applying e-Government standards and guidelines. The following sections presented in **Figure 2.6** details the utilisation of ICT in public institutions.

Figure 2.6: Approved Functions for Research, Innovation and Training, and Customer Service Support and Statistics Sections

Research, Innovation and Training Section

- Develop and implement training plans for public institutions on e-government initiatives; and
- Plan and manage e-government-related training for public institutions' employees;

Customer Service Support and Statistics Section

- Provide solutions to client complaints received;
- Provide call centre services for users across the public services; and
- Co-ordinate collection, analysis, interpretation and presentation of authority's data and statistics;

Source: Auditors' Analysis of the e-GA Approved Functions and Organisation Structure, 2024

(b) Regulatory Authorities

The Regulatory Authorities have different roles to play in the management and utilisation of ICT in the delivery of regulatory services. Section 21 of the e-Government Act of 2019 requires public institutions to have an ICT Management Unit in the form of a Directorate, Department or Unit responsible for ICT matters and with staff as may be required to efficiently perform functions.

Moreover, Section 18 of the e-Government Act of 2019 necessitates the establishment of an Institutional ICT Steering Committee to provide technical guidance on the implementation of ICT initiatives in all public institutions. The roles of the Institutional Steering Committees include reviewing and approving the ICT policy and strategy of the respective public institutions, ensuring e-government guidelines and standards are implemented by the institutions, continuously monitoring and evaluating institutional ICT projects and advising on ICT investments and priorities.

(c) National e-Government Steering Committee

Section 16 of the e-Government Act, 2019 states that the National e-Government steering committee shall perform various functions, including providing strategic and policy direction required to drive the transformation of the public service delivery and administration in the digital age and approving crosscutting ICT policies, strategies, masterplan and directives in the government.

(d) e-Government Technical Committee

Section 17 of the e-Government Act, 2019 states that the e-Government Technical Committee shall perform various functions, including reviewing and recommending e-government policies, strategies, and master plans for adoption by all public institutions and approving e-government standards and practices to facilitate data sharing across public institutions.

2.5.2 Roles of Other Stakeholders

(a) Ministry of Information, Communication and Information Technology (MICIT)

According to Para 5.1 of the National Information and Communication Technology Policy of 2016, the Ministry of Information, Communication and Information Technology is responsible for the overall coordination of ICT policy implementation, monitoring, evaluation, periodic review of the policy, and formulation of strategies. It also initiates legislation for policy implementation. Other responsibilities include providing awareness guidelines and mainstreaming the ICT policy to all sectors. In implementing this policy, the Ministry, through the ICT Commission, is required to facilitate, promote and coordinate the implementation of national ICT development projects.

(b) Information and Communication Technology Commission (ICTC)

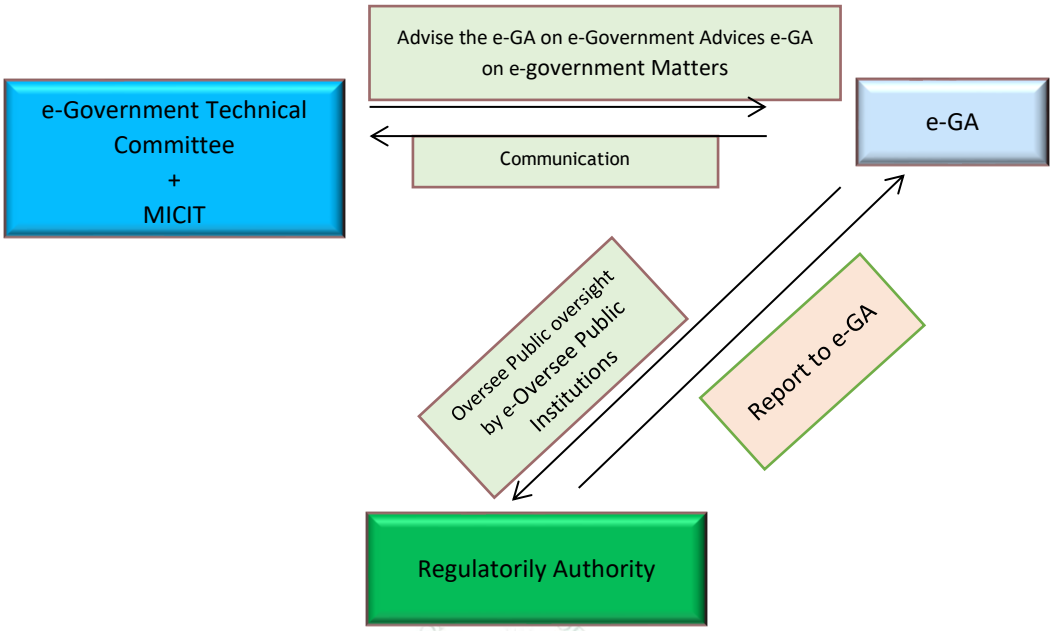
The commission provides advice, strategic planning, implementation, and investment in ICT; monitors and coordinates National ICT initiatives; and provides foresight on trends and opportunities for ICT uptake for the nation's socio-economic development[3]. The ICT Commission also promotes and fosters investment and development of the ICT industry.

2.6 Relationship between Key Actors and Stakeholders

The relationship between the actors and stakeholders is illustrated in **Figure 2.7.**

[3] The Information and Communication Technologies Commission (ICTC) was established by the Presidential Decree Government Notice (GN) No.532 published in the Government Gazette No. 4 Vol. 96 dated 20 November 2015.

Figure 2.7: Summary of Interrelationship and Accountability of Key Actors in the Management and Utilisation of ICT

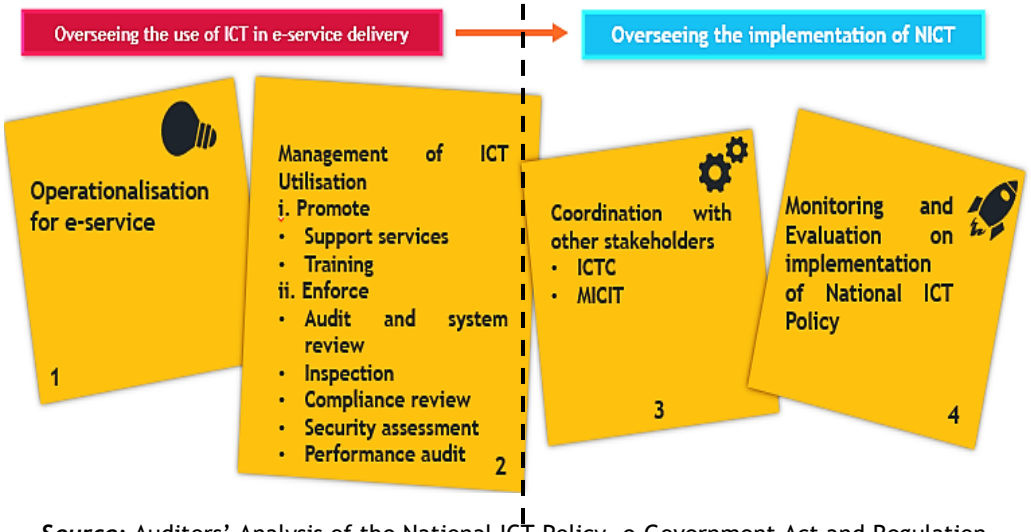


Source: Auditors' Analysis of the National ICT Policy, e-Government Act and Regulation, 2024

2.7 Processes for Managing Utilisation of ICT Systems in Regulatory Authorities

The process for managing ICT systems in the delivery of regulatory services by Regulatory Authorities is derived from different tools, including National ICT Policy 2016, the e-Government Authority Act, 2019, and the e-Government Authority Regulations, 2020. These tools define the series of activities to ensure that ICT systems are effectively managed and utilised within the governance structure to achieve the set vision. The overall process is illustrated in **Figure 2.8.**

Figure 2.8: Overall Processes for Management and Utilisation of ICT



Source: Auditors' Analysis of the National ICT Policy, e-Government Act and Regulation, 2024

Moreover, the responsibilities and roles pertaining to the management and utilisation of ICT are depicted in **Figure 2.9.**

Figure 2.9: Summary of the Output of Process Description on the Management and Utilisation of ICT in Regulatory Authorities

Oversee	Operationalization	Support Services	Training	Audit and system review
E-GA: Ensure effective governance	E-GA and Regulatory Authority-To implement	E-GA: to provide assistance to trouble shoot	e-GA and Regulatory Authority: to enhance skills	e-GA and Regulatory Authority to assess efficiency of ICT systems
Monitoring and Evaluation	Coordination	Performance audit	Security assessment	Compliance review
E-GA to assess the result of the monitoring	e-GA to bring stakeholders together	e-GA and Regulatory Authority to assess performance of service delivery using ICT	e-GA and Regulatory Authority: to assess security of data	e-GA and Regulatory Authority: to assess adherence to regulations

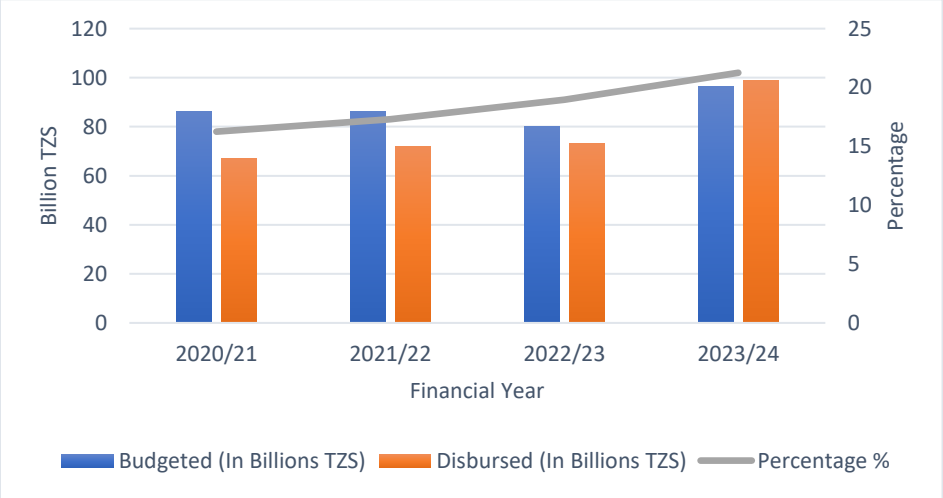
Source: Auditors' Analysis of the National ICT Policy, e-Government Act and Regulations, 2024

2.8 Resources for Managing the Effective Utilisation of ICT Systems in Regulatory Authorities

2.8.1 Financial Resources at e-GA

The associated budget allocated and costs incurred by e-GA to ensure the effective utilisation of ICT systems in public institutions were distributed across four years, as shown in **Figure 2.10.** It has been noted that there has been an increasing trend in the past four years in terms of budgeting and also disbursement. In the financial year 2023/24, the disbursement amount exceeded the budgeted amount.

Figure 2.10: Budget and Funds Disbursement for Management and Utilisation of ICT Systems in Regulatory Authorities at e-GA

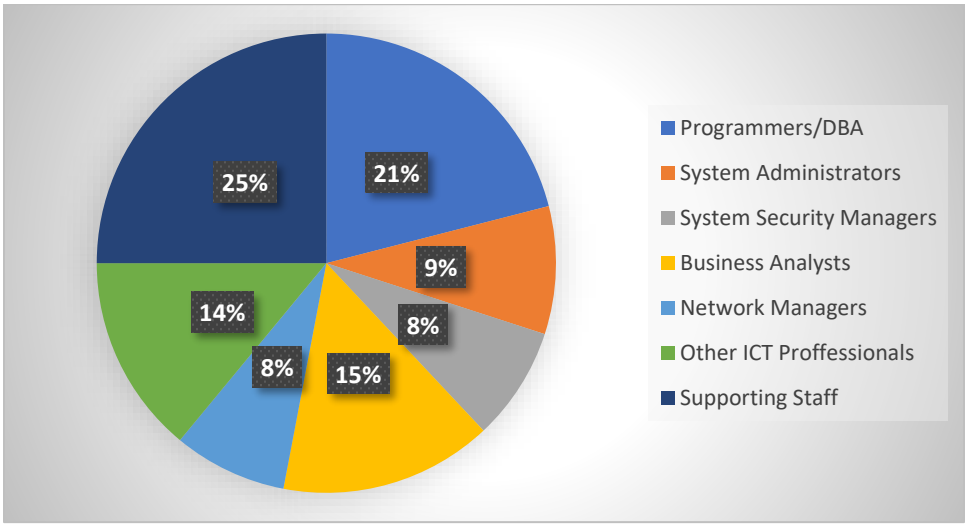


Source: Auditors' Analysis of e-GAs MTEF and Annual Financial Reports, 2024

2.8.2 Human Resources at e-GA

The human resources at e-GA constitute various professions relevant to overseeing the utilisation of ICT in public Institutions. The total number of staff at e-GA is 221, and the percentage for the major categories of professions as per requirements is provided in **Figure 2.11.**

Figure 2.11: Staff Category by Profession at e-GA



Source: Auditors' Analysis of e-GA Staff Establishment, 2024

CHAPTER THREE

AUDIT FINDINGS

3.1 Introduction

This chapter presents audit findings on the performance of the e-Government Authority (e-GA) in managing and utilisation of ICT through overseeing the implementation of the e-government initiatives to ensure the effective utilisation of ICT systems in the delivery of regulatory services.

The findings address the five specific audit objectives described in Section 1.3.1 of this report. The audit noted several efforts made to utilise ICT systems. However, there were some gaps in the management and utilisation of ICT systems in the delivery of regulatory services.

The audit noted inadequate performance on the utilisation of ICT systems by the regulatory authorities due to insufficient automation of business processes. Also, the audit noted that e-GA and Regulatory Authorities did not adequately assess the efficiency of service delivery.

Furthermore, the audit noted that there was inadequate assessment of data analysis and data governance during the processing and publishing of the data, which was supposed to be conducted by the public institutions before sending them online as per regulation 53 of the e-Government General Regulations, 2020 which states that a public institution shall manage and govern electronic data throughout the whole life cycle of the data. Moreover, the audit noted inadequate management of ICT systems security assessments. These findings are further analysed in the following sections.

3.2 Inadequate Development and Utilisation of ICT Systems by Regulatory Authorities

The analysis of the extent of development and utilisation of ICT systems by the Regulatory Authorities revealed that 14% of Regulatory Authorities did not register their ICT systems in the Government ICT Services Portal (GISP), which was intended to track their utilisation and performance. This is contrary to Section 26(1)(d) of the e-Government Act 2019, which requires public institutions to maintain a register of all Government ICT resources

owned through a central system managed by the Authority to properly utilise and manage Government-owned ICT resources.

This limited e-GA to effectively perform its mandate as specified in Section 5 (1) of the e-Government Act, 2019, which is to coordinate, oversee and promote e-government initiatives and enforce e-government-related policies, laws, regulations, standards and guidelines in public institutions.

Furthermore, it was observed that 31% of the business processes in the visited Regulatory Authorities were not included in ICT systems, leading to inadequate contributions to the achievement of their objectives. The details of these anomalies are outlined below:

3.2.1 14% of Regulatory Authorities have not Registered the ICT Systems in GISP

An analysis of information from the Government ICT Service Portal (GISP) revealed that three out of 21 Regulatory Authorities (14%) have not yet registered the ICT system in the GISP as per the requirement of Section 26(1)(d) of e-Government Act, 2019. This indicates that they developed the ICT systems, but they did not register them in the GISP. **Table 3.1** presents the extent to which regulatory authorities, categorised by sectors, have registered their ICT systems in the GISP.

Table 3.1: Extent of Registration of ICT Systems in RAs

Sectors	Total Number of Regulatory Authorities	No. of RAs that have Registered ICT Systems in GISP
Agriculture	3	2
Communication	1	1
Education	2	1
Mining	4	3
Finance	5	5
Health	1	1
Industry	2	2
Transportation	3	3
Total	**21**	**18**

Source: Auditors' Analysis of Information Extracted from GISP, 2024

Based on **Table 3.1**, the three regulatory authorities that have unregistered ICT systems fall under the agriculture, education, and mining sectors. These

include the Mining Commission, NACTVET, and Tanzania Plant Health and Pesticides Authority, as shown in **Appendix 4.**

Furthermore, in the eight regulatory authorities visited, the audit found that 56 out of 68 ICT systems were not registered in GISP but were operating and utilising ICT in delivering their business process, as further elaborated in **Table 3.2.**

Table 3.2: Unregistered ICT systems in GISP from the Visited Regulatory Authorities

Name of the Regulatory Authority	Number of ICT Systems Utilised by RA	Number of ICT Systems not Registered in the GISP
Mining Commission (MC)	4	3
National Council for Technical and Vocational Education and Training (NACTVET)	5	3
Tanzania Medicines and Medical Devices Authority (TMDA)	2	0
Public Procurement Regulatory Authority (PPRA)	1	0
Land Transport Regulatory Authority (LATRA)	2	1
Petroleum Upstream Regulatory Authority (PURA)	2	1
Tanzania Bureau of Standards (TBS)	2	2
Tanzania Revenue Authority (TRA)	50	46
Total	**68**	**56**

Source: Auditors' Analysis of the Data Extracted from the GISP, 2024

Table 3.2 shows that the Tanzania Medicines and Medical Devices Authority (TMDA) and Public Procurement Regulatory Authority (PPRA) did not register all their ICT systems in GISP. Apart from these registered ICT systems, three out of eight sampled regulatory authorities partially registered their ICT systems despite being informed by e-GA that they were required to register the ICT systems in the GISP[4]. Moreover, the audit noted that only TBS had registered all its ICT systems.

[4] Audit report on ICT Project, Compliance and Security Assessment, 15 August 2024

The interviewed ICT officials of the visited regulatory authorities indicated that there is an absence of prioritisation on registration of the ICT systems in GISP.

The audit revealed that compliance has not been achieved despite various efforts by the Authority to remind public institutions, including regulatory authorities, to submit complete and accurate ICT initiatives. Key reminders were issued through letters with reference numbers BD.140/257/01/1 (7 June 2024), AC.155/287/013/150 (31 March 2020), and AC.155/287/01M/41 (9 September 2021), sent to all public institutions. Additionally, the Authority reminded NACTVET and the Mining Commission to update their information in GISP via letters (Ref. BC.141/211/01/104 and BC.141/211/01/118, both dated 27 September 2024).

However, these authority's efforts have proven to be inadequate in ensuring compliance with the requirements. Additionally, there has been inadequate enforcement by e-GA to regulatory authorities to ensure all ICT systems are registered into GISP during the development of the ICT systems. This has partly contributed to the failure to ensure all ICT systems are registered in the GISP.

The presence of unregistered ICT systems in the GISP has hindered e-GA from obtaining sufficient information on the status of the ICT operations across the government. It has also prevented e-GA from evaluating how these systems attain their intended objectives. Consequently, this has also impacted e-GA's ability to perform its oversight function of assessing how regulatory authorities utilise these ICT systems to deliver regulatory services.

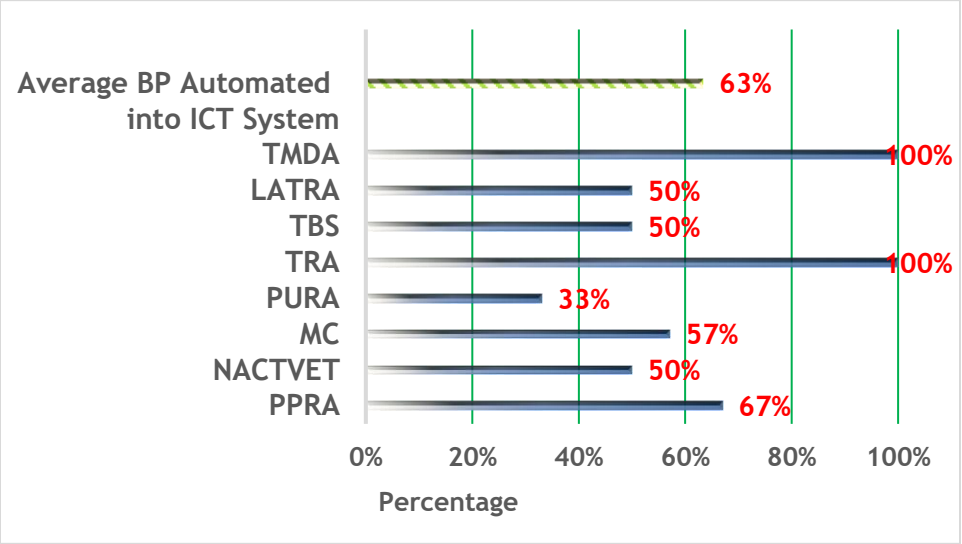
3.2.2 Inadequate Automation of the Business Processes into the ICT Systems in the Visited Regulatory Authorities

A review of the ICT systems and the respective regulatory authorities' establishment acts revealed that six of the eight regulatory authorities have not fully automated their business processes. This is contrary to Section 29 of the e-Government Act, 2019, which requires public institutions to reduce paper documents that they acquire, prepare, circulate, and preserve by innovating and digitalizing work processes and sharing administrative information amongst public institutions.

The audit further found that 13 out of the 30 business processes in the eight regulatory authorities visited, equivalent to 43%, had not yet been automated. This shows inadequate adherence to Section 3 of the e-Government Guideline, 2017, which requires public institutions to develop and implement their Enterprise Architecture (EA) for identifying all the main components of an Institution: its business processes, information systems and infrastructure, the ways the components work together to achieve defined business objectives and the way the information systems support the business processes of the institution.

The percentage of business processes automated for the respective regulatory authorities visited is presented in **Figure 3.1,** and detailed information is presented in **Appendix 6** of this report.

Figure 3.1: Percentage of Business Processes that were Automated into ICT Systems in the Regulatory Authorities Visited



Source: Auditors' Analysis of Business Process in the Visited Regulatory Authorities, 2024

Figure 3.1 shows that six of the eight regulatory authorities have their business processes partially included in the ICT systems. The percentage of business processes automated ranged from 33% to 67%. The figure also shows that an average of 37% of the business processes in the visited regulatory authorities were not automated/included in ICT systems.

The audit noted that in its ICT system review assessment conducted in December 2023, e-GA reminded the Mining Commission (among other

selected regulatory authorities) to automate their business processes. However, by December 2024, the time of this audit, 57% of the Commission's business processes remained unautomated, indicating that the approach used by e-GA was not adequate.

Inadequate inclusion of the business process in the ICT systems denied the regulatory authorities the opportunity to improve the efficiency and effectiveness in the delivery of their regulatory functions through the utilisation of ICT systems.

Further, the audit found that inadequate inclusion of business processes in the ICT system of the regulatory authorities visited was also contributed by the following factors:

Inadequate Guidance and Assistance on Automation of Business Process

Based on the review of e-GA's Annual Operation Plans and Performance Reports for the financial years 2020/21 to 2023/24, it was noted that the e-Government Authority did not adequately provide guidance and assistance that aimed at ensuring that the regulatory authorities automate their business processes.

Furthermore, the audit revealed that, while e-GA planned and conducted awareness programs on assessing the ICT systems' security and compliance with laws, regulations, and guidelines, these programs covered only the regulatory authorities with the ICT systems, while those without the ICT systems were not covered to encourage them to automate their business process into ICT systems.

Inadequate automation of the business process leads to reliance on human interventions in unautomated business processes, heightening the risk of human error.

3.2.3 Regulatory Authorities had not Tracked the Contribution of ICT Systems in Achieving their Objective

The audit noted that after the development of the ICT systems by the ICT departments of the regulatory authorities, the systems were deployed to users. However, during their utilisation period, the ICT Department did not

assess the systems to determine the extent to which the developed ICT systems contributed to achieving the intended objectives to enhance the delivery of services.

Besides, the ICT Departments of the respective regulatory authorities had not taken the initiative to measure the impact of automation and non-automation of their business process in relation to their established institutional strategic objectives.

For PPRA, there is a risk of inadequate measurement of the number of legal advice provided to PEs and bidders on PPA. Similarly, for NACTVET, there is a risk of not attaining adequate management of foreign awards, enhanced training at all levels and adequate curriculum development, review, delivery and assessment. These areas represent missing integration in business processes.

Also, the Mining Commission faces risks related to unautomated business processes related to the anti-smuggling of minerals. This led to inadequate implementation of anti-smuggling of minerals and reduced contribution to GDP due to inadequately managed quality and quantity of the minerals extracted. For LATRA, it may lead to inadequate evaluation of land transport safety initiatives against offences.

The inadequacy of public institutions in tracking the contribution of ICT systems to the achievement of their objective is contrary to Section 28(a) of the e-Government Act of 2019, which requires the use of ICT to deliver government services. This inadequacy has adversely affected the goals and achievements of the respective institutions. e-GA clarified that the public institutions were regularly reminded through letters to abide by the laws, regulations, and standards, but these efforts were not effective, and there was no assessment done by the public institutions.

Through the review of the letters with Reference No. BD.140/257/01/1 dated 7 June 2024, AC.155/287/013/150 dated 31 March 2020, and AC.155/287/01M/41 dated 9 September 2021, it was found that e-GA has been encouraging the Public Institutions to comply with e- Government Act, 2029 and its regulations, standards and guidelines. Nevertheless, the instructions were not specific in enforcing tracking of the contribution of ICT systems in achieving their objectives.

This resulted from the failure of the Regulatory Authorities to seek advice from the e-Government Authority in the development of ICT systems and from e-GA's interventions to capacitate the public institutions to improve the automation of the business processes.

3.2.4 Inadequate ICT Systems' Accessibility to Web-based Platform

The audit reviewed the web-based interface of the selected ICT systems in each visited Regulatory Authority and noted that the developed ICT systems could not be easily accessed to accommodate multi-language support. They were also not easily accessible to persons with disabilities, which was contrary to Regulations 40 and 41 of the e-Government Regulations, 2020, which required their inclusion in public institutions during the development of ICT systems. The regulations require consideration of accessibility for persons with disabilities as far as practicable. More details are shown in **Table 3.3.**

Table 3.3: Inadequate ICT System's Accessibility to a Web-based Platform

Regulatory Authority	ICT system	Mobile compatibility	Multi-language support	Accessibility for persons with disabilities
MC	Mining Cadastre	Compatible	Cannot change to Swahili	Not covered
TMDA	Regulatory Information	Compatible	Cannot change to Swahili	Not covered
TRA	Taxpayer Portal	Compatible	Cannot change to Swahili	Not covered
NACTVET	Technical Teachers' Registration	Compatible	Cannot change to Swahili	Not covered
LATRA	RRIMS	Compatible	The RRIMS user manual is only in Swahili	Not covered
TBS	I-SQMT	Compatible	Cannot change to Swahili	Not covered
PPRA	NesT	Compatible	NesT does not fully switch to Swahili in the user interface	Not covered

Source: Walkthrough of ICT Systems from the Visited Regulatory Authorities, 2024

Table 3.3 shows that all the assessed ICT systems did not have accessibility for persons with disabilities. It also shows that there were ICT systems with challenges in completing the use of at least two languages, Swahili and English. Further clarification from e-GA on how they ensured the Software Requirement Specifications (SRS) included these items, but it was clarified that e-GA considered the requirement of the project based on the stakeholder needs. However, the information provided does not relieve the development of the ICT system from adhering to the regulations.

Furthermore, the audit team noted that during the assessments of the ICT systems and projects, e-GA reviewed the websites only to check whether they complied with the accessibility requirement.

This has been contributed by inadequate management during the ICT systems development, especially in the preparation of Software Requirement Specifications, which hinders the intended objective of all the developed ICT systems from being user-friendly and improving e-service delivery.

3.3 Inadequate Development and Implementation of Interventions to Enhance the Management and Utilisation of ICT Systems

The audits noted the inadequate strategies, plans, and implementation of plans and strategies and, maturity assessments regarding the utilisation of ICT systems, which is contrary to Section 5 (1) of the e-Government Act, 2019, which requires e-GA to monitor, oversee, and coordinate and promote the utilisation of ICT in public institutions. The detailed information on these identified issues is provided hereunder:

3.3.1 Inadequate Strategies and Plans to Facilitate Utilisation of ICT Systems in Cyber Security

The analysis of the interventions, targets and strategic objectives of the e-Government Strategy, 2022 in comparison with the e-Government Authority Strategic Plan, showed anomalies regarding the interventions on cyber security as detailed in **Table 3.4**

Table 3.4: Anomalies Noted on Interventions Related to the e-Government Strategy

Objective	Targets	Outcome Indicators	Remark on the e-GA Strategic Plan[5] (SP) (2021-2026)	Remarks on Established Plans
e-Government cyber-security ecosystem improved	Strengthen e-Government cyber-security infrastructure	% change of e-Government cyber-attacks cases Level of preparedness of cyber attacks	Objective C elaborated on the coverage of the security measures, but it does not establish the extent of outcomes of the e-government strategy. The set thresholds are not shown in the strategic plan.	Did not elaborate on the actual target to ensure the change of cyber-attack cases
e-Government Management Frameworks Strengthened Strategy	Enhance e-government policy framework	Enhance Cyber-security technical capabilities and awareness		Did not elaborate on how to ensure enhanced cybersecurity technical capabilities and awareness
	Improve e-Government Institutional framework.			
	e-Government Policy developed by June 2024			

Source: Auditors' Analysis of the e-Government Strategy, 2024

Table 3.4 shows that the following strategic plans and annual plans established by e-GA did not elaborate on how they are going to cover the extent as shown in objectives and outcomes regarding the change and level of preparedness in cyber-attacks.

Furthermore, the outcome indicators and targets established were missing actual measurable thresholds to be met. This has been contributed by the inadequate preparation of strategies and detailed sub-tasks for each

[5] e-Government Authority Strategic Plan 2021/2022 – 2025/2026

objective by e-GA. Consequently, e-GA has failed to ensure that the objectives are met and well monitored. Furthermore, the audit noted the following issues:

e-GA did not Adequately Prepare its Plans to Meet the Prepared Strategic Objectives

Para 1.1 of the Ministry of Finance Guidelines for Preparation Plans and Budget, 2020/21 requires the accounting officers to establish strategies to address obligations and core functions. To fulfil its duties and responsibilities in ensuring that there is improved utilisation of ICT systems in public institutions, e-GA is required to establish strategies and interventions and incorporate these strategies in its annual operation plan for effective implementation.

The assessment of the adequacy of e-strategy in the e-GA's Annual Operation Plans (from 2020/21 to 2023/24) revealed that the established strategic interventions were not adequately prepared for proper implementation, as shown in **Table 3.5.**

Table 3.5: Anomalies in the e-GA Annual Operation Plans

Financial Year	Activity Code	Annual Plan intervention	Auditors' Remarks
2020/21 to 2023/24	F09S01	To coordinate, monitor and evaluate the e-Government initiatives	Lacked the detailed sub-tasks to conduct monitoring and evaluation of e-government initiatives
	C12S01	To provide ICT security technical support and advisory services to Public Institutions	Well addressed through eGSOC[6].
	D01S01	To conduct e-government systems, application and services compliance and quality assurance	Did not cover the detailed sub-tasks to be covered during these activities

[6] e-Government Security Operations Centre

Financial Year	Activity Code	Annual Plan intervention	Auditors' Remarks
		assessments to Public Institutions	
	D06S01	To develop, review and enforce e-Government Standards and Guidelines for Public Institutions	Did not describe detailed sub-tasks for the enforcement of e-government standards and guidelines.
	D02S01	To operationalize the e-service sustainability framework	Lacked detailed sub-tasks for the e-services sustainability frameworks
	D05S01	To develop and operationalize e-service monitoring and evaluation framework	M&E plans are available
	D05S03	e-Government initiatives monitoring and evaluation framework developed and operationalized	M&E plans are available

Source: Auditors' Analysis of e-GA's Annual Operations Plans (2020/21 to 2023/24), 2024

Table 3.5 shows that the annual plans for inspection, compliance, and security assessment of the ICT systems were not adequately prepared. This was contributed by the following factors:

i) Established Reporting Tools for Specific Targets of Public Institutions to e-GA did not have the Provision to Assess the Gaps

The audit noted that the tool established by e-GA to capture the implementation of the e-government strategy across the public institutions, including Regulatory Authorities, did not include a provision for collecting information on the number of business processes that have been automated and those that have not been included into ICT systems. This hinders e-GA from monitoring and evaluating the implementation of e-government strategy in public institutions as specified in Section 5(2l) of the e-Government Act, 2019.

This gap in the reporting templates also affects the availability of information on the extent of utilisation of ICT systems in the delivery of regulatory services by Regulatory Authorities. Also, the lack of this information denied e-GA to take the appropriate interventions for improving the digitalization of government services. Furthermore, the inability to track and measure ICT adoption hinders the assessment of progress toward the achievement of the 2026 goal for full e-government service delivery, making it difficult to evaluate annual milestones and ensure that the target is met.

ii) e-GA did not Adequately Prepare Institutional Plans

The audit noted that plans that were developed by e-GA in their annual operation plans from the financial year 2020/21 to 2023/24 were vague. This was evidenced by the absence of detailed subtasks to elaborate on how the main activity will be conducted and attained. This vagueness of the plans is contrary to the Ministry of Finance Guidelines for Preparation of Plans and Budget, 2020/21. Specifically, Form No. 14B and 14 C on the preparation of annual action plans require the preparation of details on objective code and description, target code and description, activity code and description, main tasks (activity phases) and sub-tasks (milestones).

The audit noted the presence of undetailed sub-tasks in the separate annual operation plans. This has been contributed by the absence of internal control to ensure that plans are adequately prepared to aid the conducting of the planned main task. This, in turn, caused a lot of challenges in the performance implementation of the planned tasks in the aspect of security and compliance assessment and security assessment of ICT systems, especially in the regulatory authorities.

3.3.2 Inadequate Implementation of Strategies and Plans for the Management and Utilisation of ICT Systems

Assessment of the implementation of the established interventions for ensuring effective utilisation of ICT systems revealed the following anomalies:

- ***e-GA did not Adequately Implement the KPIs Set in the e-Government Strategy***

One of the e-government strategies was to strengthen the e-government management framework by ensuring that public institutions comply with e-government standards. The audit noted that for the past four years, starting from the financial year 2020/21 to 2023/24, three objectives of the e-government strategy were not adequately implemented.

The audit further noted that e-GA has been implementing this objective by conducting security assessments and inspections and assessing public institutions' compliance with e-government standards and guidelines. However, the analysis of the implemented interventions revealed several gaps**.** The gaps included the absence of statistics and planned targets hindering the actual measurable values on the implementation of the set objectives, as presented in **Table 3.6**.

Table 3.6: Anomalies in the Implementation of e-Government Strategy

Objective	Outcome Indicators	Implementation Status
e-Government cyber-security ecosystem improved	Percentage change in e-Government cyber-attacks cases	Lack of reported changes in e-Government cyber-attacks cases. Also, there is no defined method to assess the per cent of change in e-government cyber-attack cases.
	Level of preparedness for cyber attacks	Data on the tested level of preparedness for cyber-attacks is absent.
e-Government management frameworks strengthened	Percentage of Public Institutions that comply with e-Government standards and guidelines	Security assessment, inspection, and compliance assessment conducted. However, an analysis of the public institutions' compliance with e-government standards and guidelines was conducted.

Source: Auditors' Analysis of Annual Implementation Reports (2020/21 to 2023/24), 2024

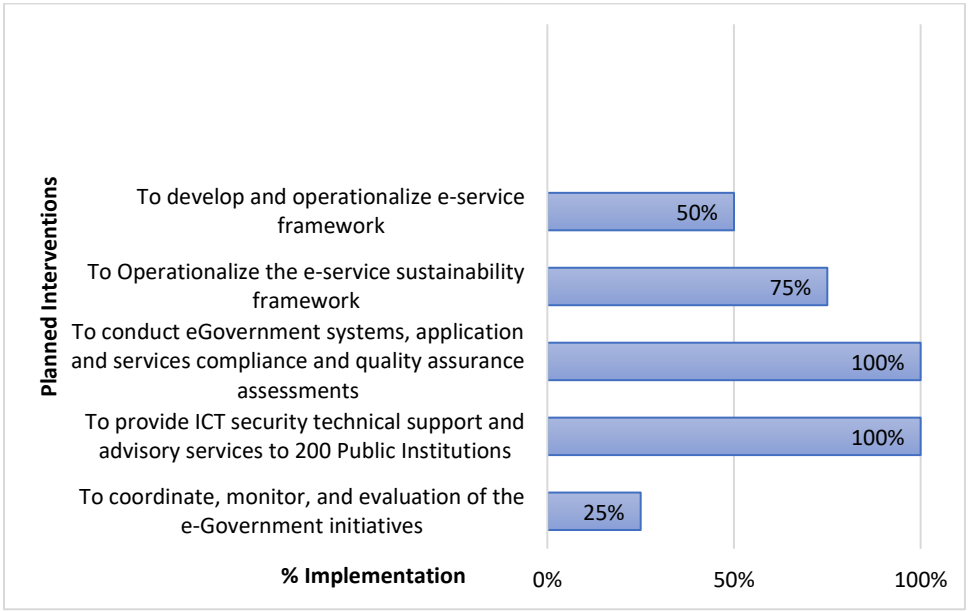
Table 3.6 shows that e-GA did not adequately implement the established objectives linked with the utilisation of ICT in the delivery of government services. However, several efforts have been made to address the

intervention stated in the strategic plans. Furthermore, strategic objectives were not adequately attained as the objectives did not have performance indicators.

- ***e-GA did not Adequately Implement its Plans to Ensure the Effective Utilisation of ICT Systems***

The reviewed e-GA annual plans and implementation reports revealed that e-GA did not adequately implement its plans, which focused on ensuring the effective utilisation of ICT systems. The analysis of Annual Implementation Reports from the financial year 2020/21 to 2023/24 indicated that all implemented plans were generic and that e-GA did not categorize them according to the maturity and risk-based assessment of public institutions. **Figure 3.2** presents the extent of the implementation of plans.

Figure 3.2: Inadequate Implementation of Plans to Manage Utilisation of ICT Systems from 2020/21 to 2023/24



Source: Auditors' Analysis of e-GA Annual Implementation Reports, 2024

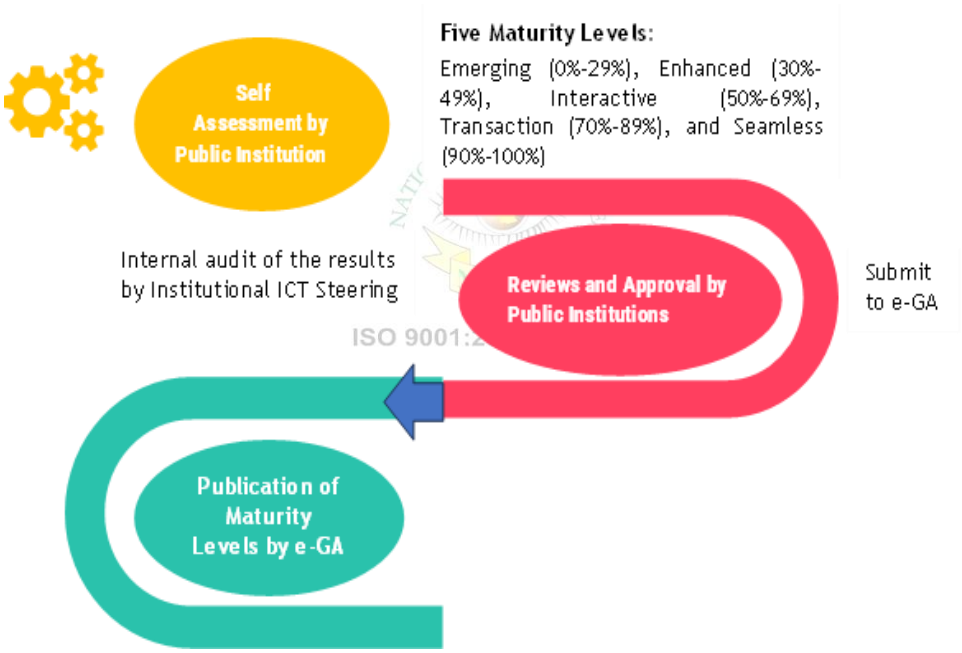
Figure 3.2 shows that two out of five annually planned interventions were fully implemented successfully, while three of the interventions were partially implemented. More details are elaborated on in **Appendix 10**.

This leaves the regulatory authorities stranded, but there is an ineffective and standardized framework to ensure e-government services are provided.

3.3.3 Inadequate Evaluation of ICT Maturity Status of the Regulatory Authorities

e-GA was supposed to perform an annual evaluation of the maturity status of the public institutions in the utilisation of ICT systems as required by Regulation 50 (1) of the e-Government General Regulations, 2020, as illustrated in **Figure 3.3**[7].

Figure 3.3: e-Government Capability Maturity Framework



Source: e-GA Capability Maturity Framework (2023), 2024

The audit found that, from 2020/21 to 2022/23, the eight visited regulatory authorities did not conduct the annual ICT maturity assessment as required by Regulation 50 (1) (a). Also, the e-Government Authority (e-GA) did not adequately evaluate the maturity status of public institutions over the past four years despite the establishment of this regulation.

[7] e-Government Capability Maturity Framework (https://ega.go.tz/uploads/standarddocuments/sw-1692042035-e-GOVERNMENT%20CAPABILITY%20MATURITY%20FRAMEWORK%20(1).pdf)

Further, it was found that e-GA developed a maturity status assessment guideline in 2023, three years after the regulation was established. Similarly, as of October 2024, at the time of this audit, no self-evaluation reports had been submitted by the visited eight Regulatory Authorities to the e-GA for verification and publication. This is contrary to Regulation 50 (1) (a) of the e-Government Regulations, 2020, which requires public institutions to self-evaluate, submit the report to the e-GA for verification and publish the results in the public institutions' ICT maturity report.

This has been attributed to inadequate enforcement by e-GA to ensure that self-evaluation of ICT maturity status is conducted as required by the regulatory authorities. The inadequate enforcement was primarily due to delays in developing the guiding tool for the collection of this information (maturity level framework) that was developed in 2023, three years after the establishment of the e-Government General Regulations, 2020.

Furthermore, through the inspection report submitted to PBPA[8] (apart from the visited public institutions), the audit has noted that efforts made by e-GA during the inspection of the ICT system recommended conducting the ICT maturity assessment, but there were neither reports to recommend on this aspect nor reminder letters sent to other public institutions, especially regulatory authorities.

Inadequate evaluation of ICT Maturity level resulted in the following:

(i) Inadequate Operationalisation of ICT Systems in the Delivery of e-Services in Regulatory Authorities

According to the World Bank's Report, 2023, on the GovTech Maturity Index (GTMI[9]), it was reported that Tanzania scored 0.552 out of the average of 0.860 in the utilisation of ICT systems (e-services digitalisation) in the delivery of the services of all countries in the world. This data included all public institutions. However, to date, it has been noted that the government has not measured a maturity level index of its own to assess the transition of the government from paperwork to ICT systems.

[8] EGAESA072234 ICT System Project, Inspection, Security and Compliance assessment report to PBPA (16 May 2024)

[9] The GovTech Maturity Index (GTMI) was introduced to measure countries' maturity in digital government transformation in four GovTech focus areas: (i) core government systems and shared digital platforms, (ii) online service delivery, (iii) digital citizen engagement, and (iv) GovTech enablers

Because of this, Pillar 3 of the e-government strategy of 2022 has not been attained. According to this pillar, the level of maturity of e-services for the financial year 2023/24, one year after the baseline year (2022/23), was projected to be 25%, with a target of reaching 70% by the fifth year (2024/25) from the baseline year (2020/21).

(ii) Lack of Comprehensive Information on the Implementation of e-Government Strategy

As a result of the absence of an evaluation of maturity level assessment, there was a lack of comprehensive understanding of how public institutions, including regulatory authorities, have operationalized and implemented the e-government strategy to enhance the delivery of their regulatory services.

3.4 Inadequate Management of the Business Continuity in the Delivery of e-Services

The assessment of the adequacy of action by e-GA and Regulatory Authorities in supporting e-service business continuity revealed several anomalies. These included inadequate disaster recovery planning and management, inadequate use of ICT systems for e-service delivery, and insufficient engagement of key stakeholders to ensure system harmonization, interoperability and integration. Additionally, weaknesses in change management and inadequate capacity building for ICT users in public institutions, including regulatory authorities, were noted. These anomalies are further explained below:

3.4.1 e-GA did not Adequately Facilitate the Regulatory Authorities in the Preparation and Management of Disaster Recovery for ICT Systems

A review of the e-GA Government ICT Services Portal (GISP) and interviews with the officials from e-GA noted that public institutions were required to report institutional progress in a timely manner by submitting key documents for managing the ICT systems, including disaster recovery plans.

However, it was noted that there were no disaster recovery plans in the portal to enable e-GA monitoring. This was contrary to Regulation 39 (a) of the e-Government General Regulations, 2020, which requires public institutions to implement business continuity management to ensure the

reliability and citizen-centric nature of the e-government services rendered, including operationalising a disaster recovery plan covering the systems that facilitate the delivery of such e-government services.
As a result, e-GA lacked a clear overview of how disaster recovery management was implemented, which is key to ensuring effective disaster preparedness.

Furthermore, inadequate intervention to ensure business continuity in the provision of e-government services is exemplified by the following anomalies noted in the eight visited regulatory authorities:

One out of Eight Visited Regulatory Authorities did not have a Disaster Recovery Plan

Officials from the visited Regulatory Authorities pointed out that one out of the eight Regulatory Authorities did not have DRP, as shown in **Table 3.7,** which is contrary to Section 42 (b) of the e-Government Act, 2019, which requires public institutions to develop and implement a disaster recovery plan (DRP) for information system continuity management. This happened despite the fact that e-GA developed guidelines and templates for public institutions to use in preparing the DRPs.

Table 3.7*:* Status of Availability and Operationalisation of Disaster Recovery Plan in the Visited RAs

Regulatory Authority	Availability of DRP	Submission to e-GA
LATRA	Available	Not submitted
PPRA	Not available	Not submitted
NACTVET	Available	Not submitted
Mining Commission	Available	Not submitted
TMDA	Available	Not submitted
PURA	Available	Not submitted
TBS	Available	Not submitted
TRA	Available	Not submitted

Source: Auditors' Analysis of the DRP from the Sampled Regulatory Authorities, 2024

Table 3.7 shows that one out of the eight selected Regulatory Authorities lacked disaster recovery plans. It also shows that the seven Regulatory Authorities with disaster recovery plans did not submit them to GISP,

although e-GA kept reminding them through letters[10] to submit information to the portal. Hence, the efforts have not been effective, as anomalies were still noted in the visited public institutions. Officials from e-GA indicated that during the e-GA site visits and inspection of the regulatory authorities, the authorities reminded the public institutions to prepare the plans, but these efforts were inadequate.

On the other hand, officials from the visited Regulatory Authorities mentioned various reasons for not having DRPs in their areas. The officials from PPRA stated that it was due to the prolonged internal reviews and that they still had DRP in draft form at the date of the audit[11].

Also, the audit noted that this was attributed to a lack of prioritization by the public institutions to ensure that the plan was in place as required by the e-Government Act and its regulations. Officials indicated that PPRA had the Institutional Business Continuity Plan (BCP), which shows the procedures for the management of services in the institution, but it did not specifically cover disaster preparedness with respect to ICT. It was also noted that e-GA did not provide training on the preparation and the importance of such a plan.

Lack of a DRP is likely to result in unpreparedness and failure to recover the systems and information in case of disaster. This eventually undermines the certainty of business continuity in regulatory services.

(i) Use of an Outdated Disaster Recovery Plan (DRP)

The audit noted that one of the six regulatory authorities had an outdated Disaster Recovery Plan (DRP), contrary to para 3 of the Disaster Recovery Plans (DRP) template, which requires public institutions to review the DRP at least once in every three years, as shown in **Table 3.8.** However, the audit noted that there were no efforts to review the document to assess its adequacy and update it.

[10] **AC.155/287/013/150** dated 31 March 2020, and **AC.155/287/01M/41** dated 9 September, 2021
[11] October 2024

Table 3.8: Status of the Validity of the Available DRPs in the Visited Regulatory Authorities

Name of Regulatory Authority	Status of DRP (Outdated/ Updated)	Expiry Date
NACTVET	Updated	May 2025
Mining Commission	Outdated	June, 2024
TMDA	Updated	June, 2027
TRA	Updated	August 2027
PURA	Updated	September 2027
TBS	Updated	January 2027
LATRA	Updated	October 2024

Source: Auditors' Analysis of the DRPs in Regulatory Authorities, 2024

The unavailability and the use of outdated DRPs were attributed to inadequate efforts by e-GA despite submitting letters[12] reminding the public institutions to submit the information through GISP. These efforts were not effective, as some anomalies were still identified in the visited public institutions.

As a result, there was insufficient assurance in disaster preparedness to safeguard effective business continuity management in the delivery of e-services.

(ii) Inadequate Testing of Disaster Recovery Plan

The audit noted that there was no testing of DRPs by the respective Regulatory Authorities for the purpose of information system continuity management as required by Section 42 (c) of the e-Government Act, 2019 and Section 3.2.1 of the e-GA approved Functions and Organisation Structure, 2020. This absence of testing was attributed to the following factors:

(a) Absence of the Disaster Recovery Testing Schedule

The audit noted that there was inadequate management of the disaster recovery plan which was contributed by the fact that the business continuity plans did not adequately cover the procedures for managing the test of the disaster recovery plan.

[12] AC.155/287/013/150 and AC.155/287/01M/41

For the information system continuity management, a test of disaster recovery preparedness at such intervals needs to be conducted, and the report needs to be submitted to the e-GA.

(b) Inadequate Enforcement by e-GA to ensure Testing of the DRPs

The audit acknowledges that e-GA developed the template for public institutions to follow and, through its inspections, issued the recommendation to public institutions to adequately manage the DRP[13]. However, the audit noted that there was inadequate enforcement to ensure that all public institutions comply with the requirements of the Act to have and test the DRPs.

The inadequate testing of the disaster recovery plan will lead to the following consequences:

(a) Risk of Unpreparedness in Case of Disaster Occurrence

There is a risk that Regulatory Authorities may experience e-service unpreparedness for disaster, which may lead to the absence of service and loss of data.

(b) Risk in Increased Services Vulnerability

The lack of a disaster recovery plan puts entities at risk of data loss due to hardware failures, cyber-attacks, failure of storage system infrastructure as a result of the inability to backup critical data, or other disasters like network attacks, website attacks, loss of internet services denial of services and other cybercrimes. Also, the absence of DRP means no predefined processes to restore systems quickly, leading to extended downtimes, which implies significant financial losses, reputational damage, operational disruptions, and difficulty maintaining customer service.

3.4.2 Inadequate ICT Service Management in Utilising ICT Systems

ICT systems service management plays a crucial role in automating institutional business processes to improve accountability and enhance the

[13] PBPA- ICT Project Inspection, Security and Compliance Assessment (16 May 2024); e-GAESA072234

delivery of services within regulatory authorities. However, the audit observed inadequate management and utilisation of the ICT systems through notable gaps in the service and operation level agreements, as well as the helpdesk support platform, as detailed below:

(i) Inadequate Management of the Service and Operational Level Agreements

The audit noted inadequate availability of the service level and operational service agreement documents in the eight visited Regulatory Authorities, contrary to Regulation 39 (c) of the e-Government Regulations, 2020. This regulation requires public institutions to ensure that the e-government services rendered maintain the service level agreements with their respective service providers who facilitate the accessibility of e-government services to guarantee the reliability of e-Government services.

It was noted that LATRA and PPRA did not have service-level agreements. It was further revealed that the Mining Commission did not have both serviceand operational level agreements to ensure the effective utilisation of ICT in the delivery of regulatory services. Only TMDA was noted to have both of the documents. NACTVET did not have the operational level agreement, and the service level agreement was not applicable because it did not host her systems at e-GA. Despite the availability of the SLAs at TMDA, there was no established performance metric to assess the attainment of the established agreements.

So far, the efforts made by e-GA have been to develop a template to guide public institutions in the development of SLAs and OLAs. However, several anomalies were still noted regarding the SLAs and OLAs in the visited public institutions. It was noted that the available interventions were not effective enough to ensure that there is adequate management of SLAs and OLAs in public institutions.

The lack of these documents was attributed to inadequate enforcement and collaboration by e-GA with these regulatory authorities to ensure their availability and the delivery of citizen-centric services. Consequently, service providers are likely to fail to ensure quality and effective services. Also, the lack of documents hinders measuring the performance metrics of services provided.

(ii) Inadequately Prepared Operation Level Agreements to Ensure Service Level

The audit reviewed the operational level agreement at TMDA and noted that the document was approved on November 2023 by the Director General and the Head of the ICT Unit. However, the interview with an official from a user department in one of the regulatory authorities revealed that they still did not know anything about it.

Table 3.9: Discrepancies Noted in the Operational Level Agreement

Name of the Visited Regulatory Authority	Noted Discrepancies
TMDA	• The user department officials were not aware of the document. • The parties (user departments) did not sign this document to have an agreement.
PPRA	• The parties (user departments) did not sign this document to agree.
LATRA	• The parties (user departments) did not sign this document to agree.

Source: Operational Level Agreement for the visited Regulatory Authority, 2024

Furthermore, the audit noted that the Director Generals previously signed the agreement, but it was not signed by the heads of the user departments as an agreement between both parties during the operations. This raises some doubts about the management of this document as to whether the institution utilises the ICT platform effectively in the delivery of government services.

This was caused by the inadequate oversight of the development of these documents by the respective public institutions and e-Government Authority (e-GA) before they became operational. Also, during the interview with the officials from user departments in the visited Regulatory Authorities, it was noted that they lacked awareness of the importance of this document in their daily operations in the delivery of e-government services.

(iii) Absence of Helpdesk Support Platform for Tracking the Status of the Reported Incidents

The assessment of the adequacy of the helpdesk platform at e-GA, which is meant to address issues reported by the regulatory authorities, revealed that the help desk was present. However, the platform has not been adequately utilised by Regulatory Authorities.

This was evidenced by the inaccessibility of the helpdesk platform to the Regulatory Authorities, as the ICT service requests and incidents were only reported and communicated through telephone calls and e-mails. This is contrary to Para 5.1 of the e-GA's e-government helpdesk and ICT support processes guideline 2016, which strongly advises that service requests from public institutions are made directly via the helpdesk system.

The audit noted that, out of the seven regulatory authorities that hosted their ICT systems at e-GA, only one, namely TMDA, had access to the helpdesk. The interviews with the ICT officials noted that inadequate utilisation of the ICT helpdesk for reporting incidences and cases was contributed by a lack of service level agreements between e-GA and these Regulatory Authorities.

The rest of the regulatory authorities received and registered the incidents through telephone and email. This jeopardizes the assurance to collect all the incidents that need to be addressed.

Furthermore, the audit assessed the availability of the helpdesk system in the visited regulatory authorities and checked whether they were used to attend to the reported cases from the users and citizens. The audit also reviewed the feedback methods of the reported incidents. In this regard, the audit noted that the Regulatory Authorities did not have a helpdesk system to serve as an incident communication platform, which further led to inadequate channels for feedback to clients in response to incidents, as shown in **Table 3.10.**

Table 3.10: Availability of Helpdesk Systems and Communication Channel in Visited Regulatory Authorities

Name of the Visited Regulatory Authority	Availability to Helpdesk	Communication Channels
TMDA	Available	Help desk system
NACTVET		
PURA		
TRA		
PPRA		
TBS	Not Available	Telephone and email addresses, which are human-driven intervention
LATRA		
MC		

Source: Site Verification from the Visited Regulatory Authorities, 2024

Table 3.10 shows that three out of the eight (37.7%) Regulatory Authorities visited did not have a helpdesk system to attend to the reported cases regarding the challenges in the services provided. This was caused by the inadequacy of enforcement by e-GA to ensure that all the respective regulatory authorities and e-GA track all their challenging issues properly and work on them together.

The audit further shows that only TMDA, NACTVET, PURA, PPRA and TRA used the proper feedback mechanism that allows clients to register their complaints and track the implementation of their cases, making monitoring reported incidents easier. The rest of the authorities used telephones and emails for reporting, which required manual registration and compilation of feedback even though e-GA had established a helpdesk to report the incidents. One of the authorities that used this system is the Mining Commission (among other selected regulatory authorities). This was noted during the ICT system review assessment, which determined whether the authorities ensured effective helpdesk operations.

Inadequate use of appropriate feedback mechanisms is contrary to Para 3.9 of a guide on the preparation and implementation of client service charters for public service and the client's feedback on service delivery. The charter encourages clients to provide feedback in the form of compliments, suggestions, and complaints as a means of improving service delivery.

3.4.3 Fragmented and Non-interoperable ICT Systems to Link with other Key ICT Systems

(i) Non-interoperable ICT Systems

The interviewed officials from the user departments of seven out of eight visited Regulatory Authorities indicated low interoperability of the ICT systems, as they were unable to exchange data with other related stakeholders.

This is contrary to Regulation 25 of the e-Government General Regulations, 2020, which requires the e-GA and public institutions to collaborate in the development and deployment of ICT systems. It also requires the e-GA and public institutions to consider interoperability during business process re-engineering. This collaboration is essential for information exchange in delivering e-government services.

Similarly, a systems walkthrough of 13 ICT systems on the end user interface of eight respective Regulatory Authorities confirmed the same finding. **Table 3.11** shows the extent of interoperability of the assessed ICT systems.

Table 3.11: Inadequate Interoperability with Visited Regulatory Authorities for Verification of Information

Regulatory Authority	ICT System Available and Assessed	Anomalies in Interoperability with other Systems	Reason to Integrate
LATRA	• LATRA VTS Management Console	Does not link with the Tanzania Police Force ICT systems	Information on registered business traffic management cases
NACTVET	• Teachers' registration • Examination system • Foreign award evaluation system • Transcript system • Student admission system	They are not interoperating with all key[14] ICT systems	To clearly verify data and documents shared by the applicants

[14] Nida, BRELA and GePG

Regulatory Authority	ICT System Available and Assessed	Anomalies in Interoperability with other Systems	Reason to Integrate
MC	• Mining market management information system (MMMIS) • Mining information management system (MIMS) • Trimble land folio	They are not linked to other needed ICT systems, including NIDA, TRA, and BRELA ICT Systems.	To clearly verify data and documents shared by the applicants.
TMDA	• Regulatory Information Management System (RIMS) • Laboratory Management Information System (LMIS)	They are not linked to BRELA, NIDA	To clearly verify data and documents shared by the applicants
TBS	• i-SQMT (Product certification on products inside the country) • OAS (Online Application System)	Requires physical Verification on the submitted attachments for BRELA, Business License, NIDA, and TRA (Not Integrated)	To clearly verify data and documents shared by the applicants

Source: Auditors' Analysis of ICT Systems in the Visited Regulatory Authorities, 2024

Table 3.11 shows that ICT systems in PPRA and NACTVET can exchange data with other key ICT systems[15] when the verification of information submitted by clients, including certificates, permits, and licenses, is needed. Also, the audit noted that TBS, LATRA, the Mining Commission and TMDA, in their daily business processes based on the end user interface, could not provide access to fetch information from ICT systems outside their entities. However, it was noted that e-GA recommended to the Mining Commission during the ICT system review assessment[16] that they should ensure that the systems are integrated with other ICT systems.

Non-interoperability among ICT systems in the visited Regulatory Authorities was caused by inadequate advisory and guidance by e-GA on the

[15] BRELA, Nida, TRA, GePG
[16] Mining Commission, 27 December 2023 ICT system review report

ICT development process that should include identifying key stakeholders to be linked for data exchange. Further interviews noted that the lack of interoperation was caused by cost-associated data exchange among the parts.

This results in prolonged processes because some processes are being done manually, and validation of information from the clients takes a long time. Also, failure to link with BRELA leads to over-reliance on submitted papers for verification and may not guarantee the validity of the certificates. Also, failure to link to NIDA triggers the failure to validate the citizenship of the applicants.

Inadequate interoperability causes inefficient communication among stakeholders and inadequate coordination of Regulatory Authorities with their stakeholders.

(ii) Presence of Fragmented ICT Systems in the Regulatory Authorities

It was noted that, among the eight visited regulatory authorities, only NACTVET and the Mining Commission (MC) had ICT systems that were fragmented in executing their business processes. The audit further noted that the identified ICT systems were designed to perform their functions independently, and each department had its own ICT system. Since the isolated systems worked independently, they were characterized by a lack of integration and interoperability because they were made of different technology platforms and applications.

Further, the audit noted that three out of the eight visited regulatory authorities had fragmented ICT systems, which required separate maintenance and ICT system costs of operations. These regulatory authorities included LATRA, the Mining Commission and NACTVET, as listed in **Appendix 5**.

The interviews with the ICT officials in the visited Regulatory Authorities noted that these isolated ICT systems arose from inadequate advice by e-GA on how to link with the existing ICT systems. Another cause of isolated systems, as identified through interviews with officials from the visited Regulatory Authorities, was reliance on outdated ICT systems implemented

many years ago, which are associated with high operational and maintenance costs.

3.4.4 Inadequate Change Management to Ensure Business Continuity

The audit noted that five of the eight visited regulatory authorities did not have ICT change management strategies to keep their technologies updated, which is essential for ensuring effective e-government services delivery. This is contrary to para 2.2.2.3 (i) of the e-GA's Guideline for Development, Acquisition, Operation and Maintenance of e-Government Application, 2020, which requires any changes such as bugs and error fixing, patches and upgrades to be undertaken in accordance with the change management process and to be properly documented.

The interview with the ICT officials and the review of the annual plans and annual maintenance reports in the Regulatory Authorities noted that the focus was only on the general repair of the ICT hardware devices in place, such as laptops and not on responding to technological changes.

Because of this, it is challenging to ensure that changes in ICT systems are carried out with a systematic approach. This is due to the following reasons:

(i) Inadequate Change Management Frameworks/Processes in Regulatory Authorities

The audit noted that among the visited regulatory authorities, only TMDA had the established document for procedures of change management for ICT systems. The absence of structured procedure/guidance results in fragmented efforts, making it difficult for public institutions to track. The required changes in the developed ICT systems are based on emerging technologies and needs.

(ii) Inadequate Advice and Supervision from e-GA

The audit reviewed the plans and strategies by e-GA to facilitate the development of the change management strategies and noted that there was no plan and intervention to ensure their development and implementation. It was also noted that e-GA, through its compliance review, did not cover this aspect.

The role of e-GA is crucial in guiding public institutions through digital transformations and organizational changes. However, the inadequate advice and support from e-GA regarding the formulation of formal change management strategies was a significant roadblock to public institutions. This gap may lead to difficulties adapting to new processes, technologies, and organisational structures, which hampers effective service delivery.

3.4.5 Ineffective Promotion of Personnel Capacity Building among Key Actors in the Delivery of Regulatory Services

The audit noted that there was inadequate implementation of the planned targets to ensure that they fulfil the established e-Government Pillar No. 6 of the e-Government Strategy, 2022 and Section 5 (2) (h) of the e-Government Act, 2019, which requires to enhance capacity of public institutions to implement e-government initiatives as shown in **Table 3.12.**

Table 3.12: Coverage of Capacity Building Interventions of the e-Government Strategies from Base Year 2022/23

Planned Targets	Year of Completion	Current Status
Five e-Government professional fora conducted	Annually	Fully implemented
e-Government training needs assessment conducted	June 2024	Not started for implementation
ICT staff needs assessment conducted by June 2024	June 2024	Not started for implementation
To facilitate the transfer of digital skill-set and capacity Building of ICT staff by June 2025	June 2025	Ongoing implementation
e-Government policy makers training program developed and implemented	June 2026	Not started for implementation
e-Government for the end-user training program for 25,000 public servants conducted	June 2026	Not started for implementation

Source: Auditors' Analysis of the Implementation of Targets on Capacity Building in e-Governance, 2024

Table 3.12 shows that four out of six planned targets were not implemented, and only one for e-government professional forums was fully implemented. Furthermore, for the transfer of digital skill sets and capacity

building of ICT staff, the activity has been noted to be under implementation.

The audit reviewed the e-Government Authority's Annual Performance Reports from 2020/21 to 2023/24 for the purpose of assessing the enhancement of the capacity of public institutions and implementing e-government initiatives as required by Section 5(2) (h) of the e-Government Act, 2019 and Regulation 48 (c) of the e-Government General Regulations, 2020. To implement this, e-GA was required to create awareness and build the capacity of public institutions regarding the risks in cyberspace.

The e-Government Authority (e-GA) conducted training to 234 public institutions, but there was no report showing the number of trainees and their respective cadres. Still, among all the covered public institutions, e-GA did not state the distributions according to the categories that could openly state how many Regulatory Authorities were covered, as shown in **Table 3.13.**

Table 3.13: Status of the Coverage of Capacity Building Training to Regulatory Authorities

Financial Year	Category	Topic to be Covered in Training	
		ICT System Security[17]	e-Services Delivery
2020/21	Public Institutions	220	0
	Regulatory Authorities	0	0
2021/22	Public Institutions	13	14
	Regulatory Authorities	0	0
2022/23	Public Institutions	0	0
	Regulatory Authorities	0	0
2023/24	Public Institutions	31	0
	Regulatory Authorities	0	0

Source: Auditors' Analysis of the e-GA Annual Plans, 2024

The audit team noted that e-GA had entered the Memorandum of Understanding (MoU) with higher learning institutions from 2020/21 to 2022/23, which was outdated during the time of the audit.

In Section 3.5 of the MoU with these learning institutions, e-GA was required to evaluate the training provided, but there is no report showing that the

[17] Regulation 48 (c), (k) of the e-government regulations, 2020

evaluation was conducted. Also, Section 3.6 of the MoU showed that e-GA was required to track all the training conducted, but the audit noted the absence of a report to show how e-GA tracks the training conducted, and thus, the audit is questioning whether they are effectively conducted or conducted at all.

Furthermore, interviews with officials from the visited Regulatory Authorities revealed that there was inadequate collaboration with e-GA to facilitate the development of the training needs assessment due to a lack of communication and advice on how to attain the training objective. Moreover, there were inadequate efforts by the respective Regulatory Authorities to facilitate the capacity building of their ICT staff and user departments.

This was caused by the following factors:

(i) Lack of Plans and Budget for Capacity Building Programs in the Regulatory Authorities

A review of e-GA's MTEF noted a lack of capacity-building plans and budget to ensure that all public institutions have ICT management and implementation capabilities to enhance the effective implementation of the e-government strategy.

(ii) Lack of Training Needs Assessment

The audit noted that e-GA did not prepare any training needs assessment to identify the aspects that may need to be covered in the training. Furthermore, the audit pointed out that the e-Government Authority did not prepare a training needs assessment database to identify the risks to institutions and areas to be covered. Furthermore, the audit noted that e-GA did not collaborate with the stakeholders, especially the regulatory authorities, in collecting these training needs for developing the training programs.

The inadequate training and capacity building lead to the risk of inefficient e-services providers in terms of skills to utilise ICT systems in the delivery of government services. Moreover, the issues arising from inadequate capacity building cause inefficiency in attaining the e-government vision of ensuring the high quality of the e-services provided to users.

3.4.6 Inadequate Implementation of the Capacity-building Initiatives to Personnel to Enhance e-Services Delivery

A review of the training reports from the visited Regulatory Authorities noted that capacity-building programs for user departments and technical personnel responsible for the ICT systems were not adequately conducted. This is contrary to Regulation 37(e) of the e-Government General Regulations, 2020, which requires public institutions to provide public awareness of all available e-government services through available channels of communication with wider outreach and continuously improve the e-Government services to cope with emerging changes in the environment, including changes in technology.

It was also noted that for the past four financial years, LATRA, PPRA, and the Mining Commission have not conducted training for ICT system users and technical staff. On the other hand, NACTVET and TMDA conducted the training for the ICT system users and technical staff.

This was partly caused by inadequate oversight under e-GA and Regulatory Authorities' steering committee on the implementation of the planned activities. This is because e-GA, in their monitoring plan activities, did not check the implementation of training provided to staff of the Regulatory Authorities regarding ICT issues as it was absent in the annual plans.

In this regard, failing to conduct capacity building for user departments and ICT technical staff significantly hampers the effectiveness of ICT systems. Without proper training, users are likely to be less informed on the ways to utilise systems efficiently, leading to operational errors, reduced productivity, and frustration.

Furthermore, the audit noted that technical staff lack up-to-date skills and knowledge in areas of ICT systems development, repair and maintenance, and cyber-security preparedness, which prevents them from properly managing, maintaining, and optimising ICT infrastructure, resulting in system vulnerabilities.

Ultimately, this is likely to diminish the overall return on ICT investments and impede the organisation's ability to adapt to technological advancements.

3.5 Inadequate Monitoring and Control of the Implementation of the e-Government Interventions

The audit noted that e-GA did not adequately monitor the implementation of the e-Government strategy. This is against the requirement of para 3.10.3 of the e-Government Strategy, 2022, which mandates that MICIT and e-GA provide oversight in the implementation of the e-government strategy.

This is indicated by various anomalies in monitoring and control of the development of ICT projects. These included measuring the performance of the developed ICT systems, inspecting e-government systems, and following up on recommendations issued during ICT system inspection. More details on the noted anomalies are elaborated below:

3.5.1 Inadequate Measuring of the Performance of the Developed ICT Systems in the Regulatory Authorities

A review of user acceptance tests and the ICT systems review reports noted that there were deployed ICT systems with incomplete user acceptance assessments. Also, there were inadequate ICT system reviews to assess the effectiveness of the ICT systems in public institutions. These are further highlighted below:

(a) Inadequate Management of the User Acceptance Tests of the Developed ICT Systems

The e-Government authority (e-GA) was required to ensure that Regulatory Authorities adequately and comprehensively carry out the user acceptance tests of all developed ICT systems before they are deployed to users. The audit reviewed the submitted User Acceptance Tests (UAT) results, which were stated to be a final document in the visited Regulatory Authorities and noted that the selected six ICT systems failed the test, and some of the items were not tested while the two remaining regulatory authorities had vendor based ICT systems. **Table 3.14** presents the details.

Table 3.14: Status of the UAT Items Assessed Before Being Deployed to Users

Regulatory Authority	ICT system	Number of Items in the ICT System	Number of Items Not Tested	Percentage (%) of Items Not Tested	Number of Items Tested and Failed	Percentage (%) of Failed Items
Mining Commission	Mining Cadastral Information Management System (MCIMS)	222	91	41	1	0.5
PPRA	National e-Procurement System of Tanzania (NeST)	334	1	0.3	38	11.4
TBS	Integrated standardisation, Quality Assurance, Metrology, and Testing System (i-SQMT)	133	11	8	46	35
LATRA	RRIMS	226	6	3	20	9
NACTVET	Students' admission	No UAT Reports				
TRA	CMRS-Online services	35	0	0	5	15

Source: Auditors' Analysis on the User Acceptance Tests, 2024

Table 3.14 shows that the percentage of items that were not tested ranged from 0.3% to 41%. It further shows that, among the tested items, 0.5% to 35% failed the User Acceptance Test. This means that the testing is not effective, and therefore, these ICT systems were going live with a number of items that have not been tested and others that have failed the test. Furthermore, the MCIMS developed at the Mining Commission did not meet the requirement in one item; NeST, which PPRA developed, fell short in 38

items of the UAT and i-SQMT, developed by TBS, did not meet the requirement in 46 items. However, TMDA and PURA purchased the ICT systems for their business processes.

Regulatory Authorities were supposed to seek advice from the mandated authority (e-GA) on ICT, and, as part of the development of the process on consultancy service, e-GA was supposed to provide guidance on discrepancies noted on the ICT systems to be cleared before they are deployed. However, the audit found that there were no documents and reports that show that improvements were made or any communications from e-GA regarding the UAT conducted. This gap limits the understanding that the stated ICT systems are still under development or completed despite the fact that they have already been deployed.

According to the review of the Government ICT Service Portal (GISP), these ICT systems were eventually registered by e-GA. However, inquiries made at e-GA showed that e-GA did not check the three systems' UAT results to ascertain their appropriateness. This results in uncertainty in the quality of the ICT systems developed and deployed, which puts into question the controls that are used during the development of the ICT systems.

The deployment of ICT systems with unsolved anomalies puts at risk the inefficiency of delivering the government services that entail their respective business process.

(b) Inadequate Measuring of the Performance of the Developed ICT Systems

To monitor and control ICT system development, the e-Government Authority is required to measure the performance of the developed ICT systems and infrastructure as per Section 6(b) of the e-Government Act, 2019, which mandates e-GA to undertake performance audits on any ICT project, systems, and infrastructure in public institutions.

However, through the reviews of the e-GA Strategic Plan 2021/22- 2025/26 for all four financial years under review and interviews held with e-GA officials, the audit noted that e-GA did not regularly conduct ICT systems performance audits. This was evidenced by the lack of performance audit reports on the ICT systems developed by the Regulatory Authorities. The

audit noted that at the time of the audit, a total of 172 ICT systems were developed and utilised across various public institutions. This was also confirmed during visits to the Regulatory Authorities, where the audit noted that the performance of all 68 ICT systems in the visited Regulatory Authorities had never been assessed by e-GA.

Through interviews conducted with officials from the visited Regulatory Authorities, the audit noted that e-GA only conducted inspections of ICT systems on aspects of ICT standards and guidelines compliance assessment and ICT system security assessment.

Furthermore, the review of e-GA annual plans for the financial years 2020/21 to 2023/24 noted that there was no planned activity for conducting performance audits on the ICT projects and systems in public institutions, including the Regulatory Authorities. Instead, e-GA focuses on measuring the number of public institutions receiving protective security services, the number of institutions using shared e-government resources, the number of new shared e-government systems developed, and the smooth exchange of information between ICT systems.

The audit reviewed the engagement plans for inspection, compliance and security assessments that were submitted to public institutions, including regulatory authorities by e-GA and noted that in Section 1.2.2 on the specific objective, e-GA intended to cover performance assessment on the aspect of effectiveness and efficiency of ICT systems to meet the business objectives of a particular public institution but this was not covered in all the engagement plans that were sent to public institutions. Furthermore, the review of the inspection, compliance and security assessment reports shows that e-GA did not cover those aspects.

Officials of the e-Government Authority indicated that the performance audit on the developed ICT systems was conducted simultaneously with ICT system inspections, compliance assessment, and security assessment. However, In the review of the inspection and assessment reports, no performance issue on the developed ICT systems was reported. Furthermore, the lack of plans and strategies for conducting performance audits of the ICT projects and systems was attributed to the non-prioritization to conduct performance audits.

Consequently, non-conducting performance audits on ICT systems directly hinder the enhancement of the ICT system's performance and efficiency. This poses the risk of inadequate e-service delivery and attainment of e-governance.

3.5.2 e-GA did not effectively Inspect, Review, and Assess the ICT Systems to Enhance Compliance and Effective Delivery of Services

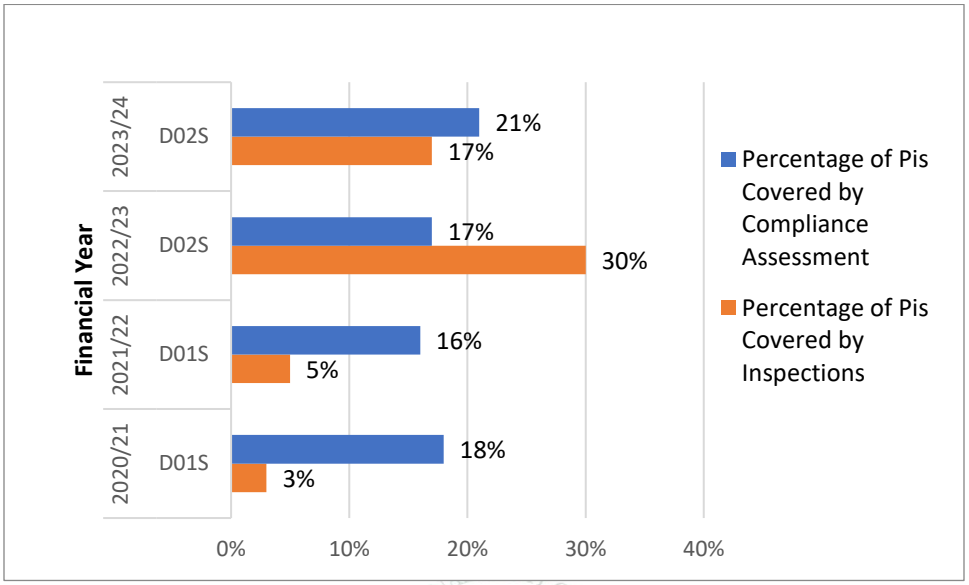
To meet the requirements of Sections 5(2)(j) and 6 (c) of the e-Government Act, 2019 and Regulation 34 (2) of the e-government General Regulations, 2020, e-GA was expected to inspect, assess, and review ICT systems to enforce security, ensure compliance, and facilitate the effective delivery of regulatory services through undertaking ICT systems audits and ICT security assessments on Government ICT systems.

However, a review of the inspection and assessment plans and their corresponding reports from the financial years 2020/21 to 2023/24 revealed several anomalies that indicate e-GA's ineffectiveness in enhancing compliance, ICT system security and system quality. These shortcomings are outlined below:

Ineffective Inspections and Compliance Assessment of the ICT Systems in Public Institutions

A review of e-GA's implementation reports from the financial years 2020/21 to 2023/24 noted that e-GA made an effort to inspect public institutions, including Regulatory Authorities. There was an increasing trend of inspection and compliance assessment of ICT systems in public institutions; however, not all public institutions were reached, as shown in **Figure 3.4**.

Figure 3.4: Conducted Inspections and Compliance Assessment of ICT Systems in Public Institutions



Source: Auditors' Analysis of e-GA's Annual Performance Report, 2024

Figure 3.4 shows that e-GA conducted inspections and compliance assessments to a maximum of 30% and 21%, respectively, out of all the 326[18] public institutions. **Table 3.15** shows critical anomalies that were found from the inspections and compliance assessments that were conducted.

The review of the inspection and compliance assessment reports noted that e-GA provided the recommendations to be addressed to ensure that there is improvement in the ICT systems. It also requested that the implementation status be submitted. Even though there were few implementation statuses submitted by public institutions, there was the absence of enforcement on acquiring the implementation status by the respective public institutions. Also, e-GA was supposed to conduct a follow-up on the issued recommendations but did not adequately conduct it, as detailed in **Section 3.5.3.**

[18] https://www.tanzania.go.tz/directories/mdas

Table 3.15: Observations from ICT Project Inspections and Compliance Assessments Conducted by e-GA

SN	Issue	Recommendation
1	Implementation of ICT Initiatives without obtaining approval from the e-Government Authority	Ensuring that ICT initiatives and projects obtain necessary approval from the authority prior to starting their implementation.
2	Inadequate Operationalization of the ICT Steering Committee	a) Develop an ICT Steering Committee Charter that stipulates roles and responsibilities, composition, and meeting affairs according to which the Committee shall operate; and b) Ensure that the ICT Steering Committee meets at least once a quarter in a financial year and retains the minutes of the meeting.
3	Inadequate ICT Service Continuity Management	a) Test the disaster recovery plan at such intervals to ensure its effectiveness; b) Document the data backup management procedures; and c) Implement a mechanism to transfer backup data to an offsite location once the backup operation is completed for a specific day to avoid data loss.
4	Inadequate automation of business processes	a) Ensure that all processes that were not automated in the existing systems are effectively automated in the new system; and b) Ensure that applicants are able to submit their applications in different activities online without visiting offices; this will improve the efficiency of service delivery.
5	Ineffectiveness of the helpdesk operations	a) Establish a mechanism to keep records of customers' complaints, assigned staff, status, time until closure; and b) Analyse helpdesk reports, identify frequently reported issues or complaints from clients and develop a solution to help clients.

Source: e-GA's Report for ICT Project Inspection, Compliance Assessment and System Review, 2024

The causes of the insufficient inspections and compliance assessment included the following:

(a) e-GA did not Adequately Plan for Inspection of ICT Systems

The review of e-GA's Annual Operational Plans for the financial years 2020/21-2023/24 revealed that the plans did not specify the number of inspections to be conducted and the number of ICT systems to be assessed in a particular financial year. This indicates non-adherence to regulation 33 (1) of the e-Government Regulations, 2020, which requires an e-government inspector to conduct an inspection based on a detailed inspection plan, as shown in **Table 3.16.**

Table 3.16: Planned ICT Systems Inspection in Public Institutions (PIs)

Financial Year	Target/ Activity Code	Description	Auditors Comment
2020/21	D05S03	e-Government initiatives on monitoring and evaluation framework developed and operationalized by June 2021	Monitoring activity did not mention the extent of inspections to be conducted, including the number of Public Institutions and inspection areas.
	D01S01	To conduct e-government systems, application and services compliance and quality assurance assessments to 50 public Institutions	The 50 Public Institutions mentioned to be covered in the inspection were not specified in terms of the areas and categories.
2021/22	D05S03	e-Government initiatives on monitoring and evaluation framework developed and operationalized by Jue 2022	Monitoring activity did not mention the extent of inspection to be covered, so to include the number of Public Institutions and inspection areas.
	D01S	Government Information Systems and Infrastructure Compliance Assessment	The compliance assessment plan did not indicate the number and category of the public institution to be covered.

Financial Year	Target/ Activity Code	Description	Auditors Comment
2022/23	D01S	Government Information Systems and Infrastructure Compliance Assessment	The compliance assessment plan did not indicate the number and category of the public institution to be covered.
2023/24	D0201S	Government information systems and infrastructure compliance assessment plan annually implemented by June 2024	The compliance assessment plan did not indicate the number and category of the public institution to be covered.

Source: Auditors' Analysis on e-GA Annual Plans, 2024

Table 3.16 shows that e-GA did not clearly state the number of inspections to assess compliance and system security. It also shows that e-GA's plans for inspection and compliance assessments were not specific on the number of public institutions and categories to be covered.

Therefore, an unspecified number of ICT systems inspections planned and categories or nature of public institutions to inspect directly hinder the measurement of the performance of e-GA on these activities.

(b) e-GA Conducted Compliance Assessment to 10% of the Regulatory Authorities

The audit reviewed e-GA's compliance assessment reports from the financial year 2020/21 to 2023/24 and revealed that in four financial years, the Authority managed to conduct general system compliance assessment to only 10% of all the Regulatory Authorities, as shown in **Table 3.17.**

Table 3.17: Compliance Assessment Conducted in Regulatory Authorities

Financial Year	Total Number of Compliance Assessments Conducted in RA	Total Number of RA	Assessments Conducted in RA (%)
2020/21	02	20	10
2021/22	Not conducted	20	0
2022/23	Not conducted	20	0
2023/24	Not conducted	20	0

Source: Auditors' Analysis of the Annual Performance Report, 2024

Table 3.17 shows that in all four financial years, e-GA managed to conduct compliance Assessments on the ICT system in the Regulatory Authorities only in the financial year 2020/21. Out of the 20 regulatory authorities, e-GA managed to conduct compliance assessments for only two regulatory authorities (LATRA in June 2022 and TMDA in September 2021), which make up 10% of the regulatory authorities.

The audit noted that there is a lack of detailed planning of activities in e-GA, which indicates the number of assessments that are going to be conducted. The available plans just provide general statements on the aspect of coverage. Due to this lack of detailed planning, from 2021/22 to 2023/24, the Regulatory Authorities were not assessed. Moreover, the coverage of 10% in the financial year 2020/21 was caused by the same challenge highlighted above. Thus, there is a lack of subtasks and categories of public institutions based on the level of maturity and risks regarding ICT systems.

Furthermore, the audit, through site verification on the remaining selected Regulatory Authorities (other than LATRA and TMDA), noted that e-GA did not conduct an ICT system compliance assessment. This was evidenced by a lack of compliance assessment reports from all the visited regulatory authorities. In the review of the e-GA annual plans, the audit noted the absence of categorization of public instructions for coverage on compliance assessment. This poses the risk that the ICT systems used by Regulatory Authorities may have undetected issues.

(i) Inadequate Implementation of ICT Systems Review by e-GA

Through the review of the e-GA's Annual Performance Report from the Financial Year 2020/21 to 2023/24, the audit noted that e-GA did not adequately conduct ICT systems review of public institutions, as illustrated in **Table 3.18.**

Table 3.18: Number of ICT System Reviews by e-GA

Regulatory Authority	Target code	Number of Public Institutions Planned for ICT System Reviews	Number of Public Institutions conducted for ICT System Reviews	Percentage Implemented (%)
2020/21	C02S	100	26	26
2021/22	C02S	500	3	0.6
2022/23	C05S	500	5	1
2023/24	C04S	160	10[19]	6.3

Source: Auditor Analysis on e-GA Annual Performance Report, 2024

Table 3.18 shows that e-GA conducted only 26% of the planned number of ICT system reviews in 2020/21, and it sharply declined in the subsequent years to less than 10%. This was caused by the absence of detailed strategies and sub-tasks to reach out to all the planned public institutions.

This implies that e-GA changed to use a reactive approach in conducting those system reviews as opposed to doing system reviews based on their assessment of the risks, which goes against the fourth schedule of the e-government General Regulations of 2020, which requires e-GA to conduct regular systems reviews as one of the services rendered.

(ii) Inadequate Implementation of ICT System Security Assessment

Through the review of the e-GA Annual Plans from the financial year 2020/21 to 2023/24, the audit noted that e-GA included security assessments stating clearly the intended number of assessments during the financial years 2020/21, 2022/23 and 2023/24. However, in 2021/22, security assessments were excluded from the plan, contrary to Section 5(2)(j) of the e-Government Act 2019, which requires e-GA to conduct ICT system security assessment on the e-government ICT systems offering services to the government. It further was noted that e-GA never achieved the planned numbers of security assessments in any of the three financial years, as shown in **Table 3.19.**

[19] System Reviews were conducted by e-GA upon the demand from Public Institutions

Table 3.19: Planned and Actual ICT System Security Assessments Conducted

Financial Year	Target Code	Number of public Institutions for Security Assessments Planned	Number of Public Institutions for Security Assessments Conducted	Percentage Implemented (%)
2020/21	C12S	Not clearly stated	90	45
2021/22	C12S	Not clearly stated	52	Not measurable
2022/23	C16S	Not clearly stated	621	Not measurable
2023/24	C16S	Not clearly stated	565	Not measurable

Source: Auditors' Analysis of e-GA Annual Plans and Performance Report, 2024

Based on **Table 3.19,** e-GA conducted between 45% and 77% of the planned security assessment, the lowest level being in 2020/21. During the four financial years, e-GA did not have a defined plan for the security assessment even though it had been conducting the assessments during the implementation. In addition, it was noted that e-GA conducted an ICT system security assessment for some regulatory authorities, including LATRA and TMDA, from 2020/21 to 2023/24.

Inadequate meetings of the planned ICT systems security assessments in public institutions have been caused by the absence of detailed strategies and sub-tasks to reach out to all the planned public institutions.

Also, e-GA did not conduct a specified ICT systems security assessment known as a full assessment to identify the possible security risks before they occur, as stated in the fourth schedule of the e-government regulations, 2020. This was caused by the following reasons:

(a) Inadequate Security Risk Identification and Assessment for New and Existing Infrastructure

A review of the ICT systems security assessment reports revealed that e-GA did not adequately identify and assess security risks on the new and existing infrastructures before they embarked on security assessments of the ICT systems as required by objective 3.5.4 of the Government Cyber Security

Strategy, 2022 to ensure the management and enhancement of cyber security in public institutions through security risk identification.

This was because e-GA lacked the ICT security incidents database for conducted investigations on the ICT systems. This is contrary to Section 3.2.1(v) of the e-GA's approved functions and organisation structure, 2020, which requires the e-GA through the security Management Section to investigate and take appropriate corrective actions for ICT security incidents.

The audit requested the registration of events and incidents that were reported to e-GA concerning the ICT security issues from e-GA, but this was never issued. The register was important for monitoring and evaluating the nature and severity of the ICT security issues that occurred.

The lack of ICT security incidents and events register leads to the risk of inadequate analysis of ICT security events and incidents. The audit noted that e-GA lacked evaluation reports of the ICT security events, which shows the number of events received and the number of events escalated for ICT analysis.

(b) Non-Covering of ICT Systems Data Audit in Public Institutions

Section 49 of the e-Government Act, 2019 states that in the case of capturing, storing, processing, and sharing electronic data, public institutions shall comply with technical standards and guidelines issued by the Authority. Also, Section 5(f) of the e-government Act, 2019 states that e-GA ensures end-to-end visibility of Government ICT systems and other systems offering services to the Government, including undertaking periodic audits of them.

Through the review of the ICT system, security and compliance assessments conducted by e-GA on the visited Regulatory Authorities, the audit noted that e-GA did not cover the ICT systems data audit to evaluate the quality, consistency, accuracy and completeness of the used data to assess the effectiveness of data collection and processing as detailed in **Table 3.20**.

Table 3.20: Inspections Conducted in ICT Systems on the Visited Regulatory Authorities

Regulatory Authorities	ICT Systems Reviewed	Issues Covered During the Assessment	Remarks
TMDA	Regulatory Information Management Systems (RIMS)	• Administration and backup operations • Infrastructures that support the operationalization of the ICT systems • ICT security management practice • Compliance of ICT systems with the relevant policies, laws, regulations and standards	The assessment did not cover all the aspects of data auditing.
LATRA	Vehicle tracking systems (VTS)	• Supporting environment of the ICT system (operating systems and network devices) • ICT security management practice • Compliance of ICT systems with the relevant policies, laws, regulations and standards	The assessment did not cover the data audit aspect.

Source: ICT Systems Inspections, Compliance Assessment, Security Assessment and System Review, 2024

Inadequate coverage of the data audit in the inspections by e-GA was due to non-prioritization of the ICT system data audit. This poses the risk to public institutions using invalid data or issuing invalid information.

(c) Inadequate ICT Systems Self-assessment by Regulatory Authorities

In this regard, regulatory authorities were required to conduct annual self-assessments on ICT systems security assessment, compliance assessment, system review, and system audit and submit quarterly reports to the e-GA through respective institutional steering committees.

Despite sending a request to the visited Regulatory Authorities, the audit was not availed with the self-assessment reports from the financial year 2020/21 to 2023/24 to verify the adequacy of the assessment conducted by

the visited Regulatory Authorities. This shows non-adherence to Section 22 (1 to 3) of the e-Government Act, 2019, which requires public institutions to conduct a self-assessment on the implementation of e-Government initiatives and submit a copy to e-GA.

In addition, the audit noted that e-GA developed a guideline[20] for public institutions to conduct their self-assessment regarding ICT systems. Meanwhile, it was noted that these efforts were not adequate in ensuring this aspect is fulfilled.

By not conducting self-assessments on the ICT systems, the Regulatory Authorities and e-GA miss the opportunity to identify potential threats and challenges to the ICT systems, thereby jeopardizing the safety of information and business continuity.

3.5.3 Lack of Follow-up on Issued Recommendations During ICT System Assessment

Inquiries at e-GA and the visited regulatory authorities revealed that e-GA did not ensure the implementation of recommendations issued during the ICT system inspection through follow-up with the respective regulatory authorities. This was contrary to Regulation 36(3) of e-Government General Regulations, 2020, which requires an inspector to conduct a follow-up inspection to verify the implementation of corrective actions. The noted lack of follow-up was caused by the following factors:

Lack of Plan for Conducting a Follow-up Audit on the Issued Recommendations

Through the review of the e-GA annual plans from the financial year 2020/21 to 2023/24, the audit noted that e-GA did not have a plan to conduct a follow-up on recommendations issued to Regulatory Authorities based on inspections conducted. Furthermore, the audit reviewed the annual implementation reports and confirmed that in all four financial years, e-GA did not conduct a follow-up of the issued recommendations.

[20] https://www.ega.go.tz/uploads/standarddocuments/en-1703850905-e-GOVERNMENT%20SECURITY%20OPERATIONS%20GUIDELINE.pdf

However, in the review of the inspection reports, there was no assessment of the level of implementation of recommendations reported on the previous inspection conducted on the public institutions, including Regulatory Authorities.

This implies a lack of prioritization of follow-up on the issued recommendation as the tool for enhancing e-government strategy in the public institution. The lack of planning for follow-up causes the risk of a number of unresolved issues and loss of credibility, hence hindering the attainment of e-government strategy in public institutions, including Regulatory Authorities, in the delivery of e-government services.

3.6 Inadequate Monitoring and Evaluation of the e-Government Initiatives

The audit team noted that there was inadequate evaluation and implementation of the e-government interventions, as highlighted below:

3.6.1 Inadequate Evaluation of the e-Government Implementation by e-GA

Pursuant to Section 5(2) (l) of the e-Government Act, 2019, e-GA is required to monitor and evaluate the implementation of e-government interventions in public institutions. This means that after monitoring the e-government interventions in public institutions, an evaluation of the obtained information was required to assess the extent of the problem and propose a corrective measure.

The analysis of annual budgets, plans, and performance reports revealed that, from the financial year 2020/21 to 2023/24, e-GA planned to conduct monitoring and evaluation of public institutions. The plans and budget included the development and operationalisation of the e-Government initiatives monitoring and evaluation framework for the utilisation of ICT in the delivery of government services, as shown in **Table 3.22.**

Table 3.21: Planned Budget for Monitoring and Evaluation of e-Government Initiatives

Code	Total Budgeted Amount (TZS)				
	2020/21	2021/22	2022/23	2023/24	Sub-Total
D05S03	42,200,000	40,200,000	-	-	**82,400,000**
D05S01	-	-	392,880,000	-	**392,880,000**
C19S01	-	-	-	267,900,000	**267,900,000**
Total	**42,200,000**	**40,200,000**	**392,880,000**	**267,900,000**	**743,180,000**

Source: Auditors' Analysis of e-GA's Budget from Financial Year 2020/21 to 2023/24

Table 3.22 shows that from the financial year 2020/21 to 2023/24, e-GA budgeted a total of TZS 743,180,000 for conducting monitoring and evaluation activities for government ICT initiatives. Furthermore, the audit noted that the planned activities did not elaborate on what aspects would be monitored and evaluated.

The audit reviewed the implementation reports of the monitoring and evaluation activities conducted by e-GA and noted that e-GA performed activities as shown in **Table 3.23.**

Table 3.22: Implementation of Monitoring and Evaluation of e-Government Initiatives

Financial Year	Code	Implementation Output
2020/21	D05S03	a) 81 Public institutions provided with project review and advisory services; b) A total of 44 technical meetings have been conducted with public institutions to discuss the best ways or approaches for undertaking e-government projects; c) Provided technical guidance on the implementation of Government ICT projects and the use of the Government ICT Services Portal (GISP) to 89 public institutions; d) Conducted 33 technical meetings on e-government initiatives with 32 public institutions; e) Conducted Government ICT Project inspection in 11 public institutions; f) Improved Government ICT Services Portal (GISP) to allow integration with other internal systems like ERMS and e-office; and **g)** Improved GISP features such as the inclusion of project progress reports, technical advisories, and various reports.

Financial Year	Code	Implementation Output
2021/22	D05S03	a) Developed draft Government ICT projects M&E framework; b) 68 e-Government Projects were reviewed, and technical recommendations were provided through GISP; c) Raised awareness of e-service sustainability to 110 public institutions; d) Conducted a GISP review and prepared a comprehensive list of requirements for the improvement of GISP; and **e)** Conducted Government ICT Project inspections in 16 public institutions.
2022/23	D05S01	a) 99 ICT project inspections were conducted in 10 Public Institutions, namely the Tanzania Tourism Board - TTB, Tanzania Ports Authority - TPA, Ministry of Land, Housing and Human Settlement Development - MLHHSD, Higher Students' Education Loan Board - HESLB, MUHAS, MoEST, MoCLA, UDOM, IFM etc. **b)** One project performance audit was conducted in one Public Institution, namely the National Examinations Council of Tanzania (NECTA).
2023/24	C19S01	a) 54 Public Institutions were provided with project inspections; b) 119 ICT project inspections were conducted in Public Institutions; and **c)** 70 technical meetings with public institutions were conducted to discuss the best approaches to undertaking different e-government projects.

Source: e-GA's Annual Performance Reports from the Financial Year 2020/21 to 2023/24

Table 3.21 shows that e-GA conducted only monitoring activities for public institutions from the financial year 2020/21 to 2023/24. This suggests that e-GA did not evaluate the information obtained from monitoring regarding the implementation of e-government interventions. e-GA was supposed to use the collected information to evaluate the extent of implementation of e-government initiatives. However, there were no reports of evaluations conducted by e-GA.

The audit further noted an absence of defined metrics in planned activities to assess the progress of e-government initiatives, leading to unclear benchmarks for evaluation. This implies that the objectives were vague and

unclear in enabling one to understand the goal, and it became difficult to measure success or areas that need improvement.

This resulted in the following:

(i) Inadequate Measuring of National ICT Policy Outcomes

E-government initiatives are often linked to broader governance and policy goals, such as improved service delivery, citizen engagement, and administrative efficiency. Failure to evaluate the monitoring data can result in poor policy outcomes, as the government may not fully understand the impact of the initiatives taken on the goals that were set.

(ii) Security and Privacy Risks

Inadequate evaluation of monitoring data may result in undetected security vulnerabilities or data privacy issues within the e-government system. Regular assessments are critical for identifying and addressing potential risks to user data and the integrity of government systems.

3.6.2 Inadequate Utilisation of Monitoring and Evaluation Results on Implementation of e-Government Strategic Plan

e-GA was supposed to use the results of the conducted monitoring and evaluation to establish interventions towards improving all areas that were noted to have risks and challenges in the implementation of e-government initiatives as required by Section 5(2)(l) of the e-Government Act, 2019 that there should be monitoring and evaluation of the implementation of the e-government initiatives in public institutions.

The audit noted that due to inadequate monitoring and evaluation of the implementation of e-government initiatives in public institutions, e-GA did not have any results to be utilised to trigger suitable and appropriate interventions for improvement.

It was revealed that the prepared monitoring and evaluation documents were only for measuring the e-GA undertakings, but the same was used to measure the implementation of the e-government interventions in public institutions.

This was caused by a lack of evaluation results regarding the monitoring activities conducted as required by the monitoring and evaluation

framework specifically to assess the implementation of e-government initiatives that could provide guidance to collect information, analyse it, and report on the monitoring and evaluation results. This has resulted in the following anomalies.

(i) Inadequate Integration of M&E in Decision-Making by e-GA

It was noted that there are anomalies in decision-making interventions. Specifically, the absence of monitoring and evaluation findings hindered e-GA from being informed on the strategy adjustments or changes. Also, e-GA could not measure the performance of the efforts and interventions in promoting, overseeing, monitoring, and coordinating the utilisation of ICT in regulatory authorities.

(ii) Failure to Meet Strategic Objectives of Achieving a High Level of Utilisation of ICT

The overarching goal of the e-government strategy is to enhance ICT utilisation in regulatory services. If performance metrics from monitoring and evaluation are ignored, there is a high risk that the objectives related to service efficiency, accessibility, and transparency will not be met.

3.7 Coordination for Overseeing the Utilisation of ICT

The implementation of the ICT Policy involves various stakeholders heading towards the same direction of government services, which requires proper coordination. Thus, the institutional framework, as stipulated in the National ICT Policy of 2016, articulates the major roles of key institutions in enhancing the utilisation of ICT in public institutions.

The audit found several anomalies related to coordination among key actors and reporting procedures. Also, there were inadequate plans and implementation of M&E for the performance of public institutions, and the utilisation of M&E resulted in the implementation of an e-government strategy. More details have been elaborated below:

3.7.1 Inadequate Communication Procedures and Coordination Among Key Actors

The audit revealed that the reporting and communication procedures between e-GA and MICIT are not adequate, although they both share the

implementation of the ICT policy in the country. e-GA, which enforces the implementation of e-government standards and guidelines through the use of ICT systems, does not share information with MICIT, whose core business process in the country is ICT. MICIT also is responsible for the overall coordination of the implementation of ICT policy.

3.7.2 Unclear Roles to Implement the Efforts Stated in the National ICT Policy

The audit reviewed the developed roles and responsibilities according to ICT policy and the e-Government Act. It noted that MICIT is supposed to coordinate policy implementation, monitoring, evaluation, and periodic review of the policy. In contrast, e-GA is supposed to develop e-government policy and facilitate its implementation in Government institutions. That is in line with the e-GA's goal to coordinate, oversee, promote, and enforce e-government in public institutions.

All the stated issues are directly related to the implementation of ICT policy, but there is no common ground established between the two actors to ensure smooth communication.

This is contributed to by the inadequate development of the establishment of documents to generate clear roles and responsibilities, which led to the failure to execute ICT policy directions.

CHAPTER FOUR

AUDIT CONCLUSION

4.1 Introduction

This chapter draws the audit conclusion based on the findings described in Chapter Three. The basis for drawing the audit conclusions is the overall and specific objectives of the audit, as presented in Chapter One of this report.

4.2 Overall Audit Conclusion

The audit recognizes the efforts made by e-GA and the regulatory authorities to automate business processes through the use of ICT systems to enhance the delivery of regulatory services. Also, e-GA made efforts to develop templates that comply with standards, guidelines, laws, and regulations. This further included capacitating the internal auditors on all matters regarding the assessment of ICT in their respective public institutions. However, there was inadequate management and oversight on the implementation of an e-government strategy to ensure the effective utilisation of ICT systems in the delivery of regulatory services. This has been noted in the assessment of areas, including interventions to manage and oversee e-service business continuity, monitoring and control of the ICT systems, and coordination among key stakeholders.

4.3 Specific Audit Conclusions

4.3.1 Inadequate Intervention to Enhance the Management and Utilisation of ICT in the Delivery of Regulatory Services

The strategies and plans put in place by e-GA to facilitate the management and utilisation of ICT in the delivery of Regulatory services were inadequate. Also, the available strategies and plans for the management and utilisation of ICT in the delivery of regulatory services were inadequately implemented to ensure that they improve oversight on the utilisation of ICT in the delivery of government services.

e-GA did not effectively assess the status of ICT maturity level in the country by evaluating and publishing the results as per e-government regulations in 2020.

4.3.2 Inadequate Management of the Business Continuity to Enhance the Delivery of e-Services

e-GA did not effectively enforce regulatory authorities to prepare and manage disaster recovery for ICT systems in the delivery of regulatory services to ensure business continuity is maintained. Also, customer service management in utilising ICT systems does not adequately function to ensure the effective delivery of regulatory services.

It was noted that e-GA and Regulatory Authorities ineffectively manage ICT systems to ensure business continuity in the delivery of regulatory services. Moreover, there is a lack of control and oversight to ensure the implementation of changes in the management of ICT aspects. Also, there is ineffective management of personnel capacity building in the delivery of quality regulatory service. This is attributed to a lack of adequate plans to implement capacity-building interventions to enhance e-services delivery, although e-GA has been making capacity-building efforts to improve the inspection of ICT systems in its respective public institutions.

4.3.3 Inadequate Monitoring and Control of the Implementation of the e-Government Strategy

It is concluded that the performance of the developed ICT systems in the delivery of regulatory services is inadequately managed.

Furthermore, e-GA did not adequately inspect, assess, and enforce ICT system security, compliance, and system review to enhance the effective delivery of regulatory services, which are critical to ensuring the effective delivery of government services. Following that, e-GA did not ensure the implementation of recommendations issued during ICT system inspection and assessment. This would also ensure the effective delivery of regulatory services and manage follow-ups. Follow-up was not done due to a lack of prioritization of the matter.

4.3.4 Insufficient Coordination of Decision-Making Platform and M&E for Overseeing the Utilisation of ICT

The ambiguity in roles and insufficient coordination between e-GA and other stakeholders, including the Ministry of Information Communication and Information Technology (MICIT), further impedes and reduces the overall effectiveness of regulatory services.

There is inadequate monitoring and evaluation of the e-government strategic plans by e-GA; there are no reports on how they have ensured results for the government initiatives in the country as per the interventions made.

CHAPTER FIVE

AUDIT RECOMMENDATIONS

5.1 Introduction

This chapter presents recommendations directed to the e-Government Authority (e-GA) on the improvement of the utilisation of ICT in the delivery of regulatory services in the country.

5.2 Recommendations to the Audited Entity

The e-Government Authority (e-GA) is urged to:

a) Enhance the promotion and compliance enforcement of e-government services to improve ICT system utilization, automate business processes, conduct regular maturity assessments, and monitor ICT performance in achieving institutional objectives;

b) Enhance its enforcement of the management and use of standardized ICT management tools in public institutions to ensure effective use of key documents such as Disaster Recovery Plans (DRP), Service Level Agreements (SLA), Operational Level Agreements (OLA), and Change Management Strategies;

c) Develop and implement a comprehensive strategy and detailed plans that outline clear coverage for inspection and review of ICT systems and compliance assessment in public institutions, which detail the frequency of inspections, targets and performance indicators to enable the e-GA to effectively monitor, evaluate, and improve its enforcement efforts; and

d) Enhance monitoring and evaluation of all the e-government initiatives and interventions and use the results to take corrective actions for improvement. This should include regular analysis of monitoring data for informed decision-making, engaging relevant institutional steering committees, and ensuring follow-up on the implementation of recommendations provided to public institutions.

LIST OF REFERENCES

1. The United Republic of Tanzania (2000): *Tanzania Development Vision 2025,* Tanzania

2. The United Republic of Tanzania (2021); *National Five-Year Development Plan III from 2021/22 to 2025/26*, Tanzania

3. Ministry of Information, Communication and Information Technology (2016): *National Information and Communication Technology Policy*, Tanzania

4. Ministry of Information, Communication and Information Technology, (2015): *National ICT Policy Implementation Strategy 2016/17 – 2020/21*, Tanzania

5. President's Office - Public Service Management and Good Governance (2019): *e-Government Strategy 2021/2022 - 2025/2026,* Tanzania

6. The e-Government Authority (e-GA) (2017, 2022): *Annual Financial Performance Reports (2020/2021 – 2023/2024),* Tanzania

7. The e-Government Authority (e-GA). (2011): *e-Government Strategic Plan 2011/2017 - 2020/2021*, Tanzania

8. The e-Government Authority (e-GA). (2020): *e-Government Security Assessment Reports (2020/21-2023/24)*, Tanzania

9. The e-Government Authority (e-GA). (2014): *ICT Project Implementation Guideline*, Tanzania

10. The United Republic of Tanzania (2019): *The e-Government Act*, Tanzania

11. The United Republic of Tanzania (2017): *The e-Government Guideline*, Tanzania

12. The United Republic of Tanzania (2020): *The e-Government General Regulations*, Tanzania

APPENDICES

Appendix 1: Responses from e-Government Authority (e-GA)

This part provides responses from the e-Government Authority. The responses are divided into two parts: general and specific comments for each issued audit recommendation.

A: Overall Responses

e-Government will continue to perform its mandates in line with the e-Government Act, 2019, e-Government General Regulations, 2020 and the existing e-Government Standards and Guidelines.

B: Specific Responses

Specific Responses: e-GA is urged to:

No	Issued Recommendation	Comment(s) from e-GA	Action(s) to be Taken	Timeline
1	Enhance the promotion and compliance enforcement of e-government services to improve ICT system utilization, automate business processes, conduct regular maturity assessments, and monitor ICT performance in achieving institutional objectives;	e-GA Management has noted the auditor's recommendation for implementation. As part of the implementation of the e-GA Rolling Strategic Plan 2021/2022-2025/2026, the Authority has taken the following initiatives: i. Collaborated with the Internal Auditor General –	The Authority will continue with: - i. Provision of awareness and technical training to public institutions' internal auditors and security SPOCs to promote the development and utilization of ICT systems in line with the e-Government Act 2019, e-Government General Regulations	FY 2025/2026 – FY 2027/2028

		IAG to raise awareness and conduct training for Internal Auditors from Public Institutions on e-Government related policies, laws, regulations, standards, and guidelines so that compliance on the matter is closely enforced and achieved at the individual institution level; ii. Conducted security training for Single Point of Contact (SPOC) appointed in various public institutions to enhance the capacity of the institutions; iii. Conducted ICT project inspections, compliance, security, and system reviews of public institutions to promote automation of business processes and support the achievement of	2020, Standards and Guidelines. ii. Conducting ICT project inspections, compliance audits, and security assessments for public institutions and continuing to follow up on the implementation of the recommendations provided during assessments. iii. Conducting follow-ups with public institutions to perform self-evaluation and submit the report. The Authority will also perform verification and publish the results in line with the requirement of Regulation 50 of e-Government General Regulations.	

No	Issued Recommendation	Comment(s) from e-GA	Action(s) to be Taken	Timeline
		public institutions' objectives. iv. Established and operationalised the standards and guidelines for the development, acquisition, operation and maintenance of e-Government applications. This aims to assist public institutions in their initiatives to automate their business processes and foster the development and efficient utilization of ICT systems. v. Established and operationalized e-Government Capability Maturity Framework to provide means for public institutions to self-evaluate their ICT Maturity Status. Among other things, it includes automation of the self-evaluation process through		

No	Issued Recommendation	Comment(s) from e-GA	Action(s) to be Taken	Timeline
		the Government ICT Services Portal (GISP).		
2	Enhance its enforcement of the management and use of standardized ICT management tools in public institutions to ensure effective use of key documents such as Disaster Recovery Plans (DRP), Service Level Agreements (SLA), Operational Level Agreements (OLA), and Change Management Strategies;	e-GA Management has noted the auditor's recommendation for implementation. As part of the implementation of the e-GA Rolling Strategic Plan 2021/2022 - 2025/2026, the Authority has undertaken the following initiatives: - i. **Collaborated with the Internal Auditor General** - IAG to provide awareness and training to Internal Auditors from Public Institutions on e-government related policies, laws, regulations, standards, and guidelines so that compliance on the matter is closely enforced and achieved at	The Authority will continue with: - i. Provision of awareness and technical support to public institutions to ensure Disaster Recovery Plan (DRP), Service Level Agreement (SLA), Operational Level Agreement (OLA) and Change management Policies/Strategies among others. ii. Conducting ICT project inspections, compliance, security and system reviews of public institutions to enforce the management and the use of	FY 2025/2026 – FY 2027/2028

No	Issued Recommendation	Comment(s) from e-GA	Action(s) to be Taken	Timeline
		the individual institution level; ii. Established and operationalized guidelines for the development, acquisition, operations and maintenance of e-Government applications that guide public institutions on matters related to service level agreement (SLA), operational level agreement (OLA) and change management policies/strategies, among others iii. Developed and published templates for Disaster Recovery Plans (DRP), Service Level Agreements (SLA), and Operational Level Agreements (OLA) to assist public institutions in	standardised ICT tools.	

No	Issued Recommendation	Comment(s) from e-GA	Action(s) to be Taken	Timeline
		the establishment of the same. iv. Conducted ICT project inspections, compliance, security and system reviews of public institutions to enforce the management and the use of standardised ICT tools that include Disaster Recovery Plan (DRP), Service Level Agreement (SLA), Operational Level Agreement (OLA) and Change management Policies/Strategies among others.		
3	Develop and implement a comprehensive strategy and detailed plans that outline clear coverage for inspection and review of ICT systems and compliance	e-GA Management has noted the auditor's recommendation for implementation. In the course of implementation of the e-GA Rolling Strategic Plan 2021/2022 -	The Authority will continue developing and operationalizing the e-Government Authority Compliance Assessment Annual Operation Plan for each financial year to guide coverage for ICT project	FY 2025/2026 – FY 2027/2028

No	Issued Recommendation	Comment(s) from e-GA	Action(s) to be Taken	Timeline
	assessment in public institutions, which detail the frequency of inspections, targets and performance indicators to enable the e-GA to effectively monitor, evaluate, and improve its enforcement efforts	2025/2026, the Authority has developed and operationalized the e-Government Compliance Assessment Annual Operation Plan for each financial year to guide, among others, coverage for ICT project inspections, compliance, security and system reviews in line with the standing e-Government Authority Strategic Plan.	inspections, compliance, security and system reviews in line with the standing e-Government Authority Strategic Plan.	
4	d) Enhance monitoring and evaluation of all the e-government initiatives and interventions and use the results to take corrective actions for improvement. This should include regular analysis of monitoring data for informed decision-making, engaging	e-GA Management has noted the auditor's recommendation for implementation. As part of the implementation of the e-GA Rolling Strategic Plan 2021/2022-2025/2026, the Authority has taken the following initiatives: - Collaborated with the Internal Auditor General – IAG to provide awareness and training to Internal	The Authority will continue with the following; Collaboration with the Internal Auditor General –	FY 2025/2026 – FY 2027/2028

No	Issued Recommendation	Comment(s) from e-GA	Action(s) to be Taken	Timeline
	relevant institutional steering committees, and ensuring follow-up on the implementation of recommendations provided to public institutions.	Auditors from Public Institutions on e-Government related policies, laws, regulations, standards, and guidelines so that compliance on the matter is closely enforced and achieved at the individual institution level. This includes matters related to the engagement of the relevant Institutional Steering Committee. i. Conducted ICT project inspections and compliance, security, and system reviews of public institutions to monitor and evaluate e-government initiatives and interventions. ii. Performed follow-up on the implementation of recommendations provided to public institutions during	IAG to provide awareness and training to Internal Auditors from Public Institutions on e-Government related policies, laws, regulations, standards, and guidelines so that compliance on the matter is closely enforced and achieved at the individual institution level; This includes matters related to the engagement of the relevant Institutional Steering Committee; i. Conducting ICT project inspections, compliance, security and system reviews of public institutions to monitor and evaluate e-government initiatives and interventions.	

No	Issued Recommendation	Comment(s) from e-GA	Action(s) to be Taken	Timeline
		the conduct of ICT project inspections, compliance, security and system reviews	**ii.** Performing follow-up on the implementation of recommendations provided to public institutions during the conduct of ICT project inspections	

Appendix 2: Documents Reviewed

This part provides a list of documents reviewed and the reasons for reviewing them.

Category	Name of the Document	Reason
Policy and Legislation (Laws Acts, Policies and Regulations)	National ICT Policy, 2016 e-Government Act, 2019 e-Government Regulations, 2020	To assess: Policies, laws, regulations, guidelines and standards governing management of ICT systems in the country Actors and key stakeholders responsible for the management of ICT systems Mandate and responsibilities of the actors and key stakeholders The policy statement for the management of ICT systems in the country A specific policy statement that will form part of the assessment criteria during the main study The processes involved in the management of ICT systems in the country
Guidelines	Maturity status guideline, 2023 e-Government Guidelines, 2017	To assess the: Principles and standards that guide the management and utilisation of ICT systems in the country Processes involved in the management of ICT Systems A specific guide statement that will form part of the assessment criteria during the main study
Strategic Plans	Strategic Plans of:	To assess:

Category	Name of the Document	Reason
	e-GA Strategic plan for the period of 2013 to 2018 e-GA Strategic plan for the Period of 2022 to 2026	Strategies and interventions for the management of ICT in the country Objectives, Target, and Goals set for the management of ICT systems To assess strategies and objectives if they are in line with the regulatory function of the respective Regulatory Authorities
Annual Plans (2017/18-2022/23)	Annual Plans of: e-GA Annual plans from the selected RAs include LATRA, PURA, TMDA, TBS, Mining Commission, NACTVET, and PPRA. Concept Note User Acceptance Report Training Report	To assess: Annual goals and objectives; Key performance indicators for the ICT systems Governance structure/ Monitoring and evaluation strategies Allocation of resources Planned ICT systems and their Objectives Planned approach and milestone for the development of the targeted ICT systems To assess the plans from the selected Regulatory Authorities in place for the management of ICT systems

Category	Name of the Document	Reason
Annual Implementation Reports (2017/18-2022/23)	Annual implementation Reports and Performance Reports of the ICT systems from: eGA Selected Regulatory Authorities for Verification include LATRA, PURA, TMDA, TBS, Mining Commission, NACTVET, and PPRA.	To evaluate the progress of implementing the planned activities related to the management and utilisation of ICT in Regulatory Authorities To identify reported drawbacks and challenges in the management and implementation of ICT in regulatory services. To identify the achievement made in the utilisation of the ICT systems available in the respective regulatory authorities
Annual budgets and budget implementation reports	Medium-Term Expenditure Framework of the e-GA Selected Regulatory Authorities	To assess the allocation, distribution and trend of expenditure of the allocated funds for the management and utilisation of ICT in Regulatory Authorities. To assess the challenges in the allocation of financial resources To assess the expenditure status of the budget allocated
Monitoring and evaluation reports	Monitoring and evaluating reports from e-GA Selected RAs include LATRA, PURA, TMDA, TBS, Mining Commission, NACTVET, and PPRA.	To assess the performance trend of delivery of regulatory services through utilisation of the ICT systems To evaluate the measures made towards the promotion and utilisation of ICT systems in the delivery of regulatory services To assess the challenges and their associated causes regarding the management and utilisation of ICT in Regulatory Authorities.

Category	Name of the Document	Reason
		To assess the extent of the management and implementation of ICT in the delivery of regulatory services.

Source:Auditors' Analysis of List oif Reviewed Documents, 2024

Appendix 3: Officials Interviewed

This part gives details on the officials interviewed and reasons for interviewing the selected officials.

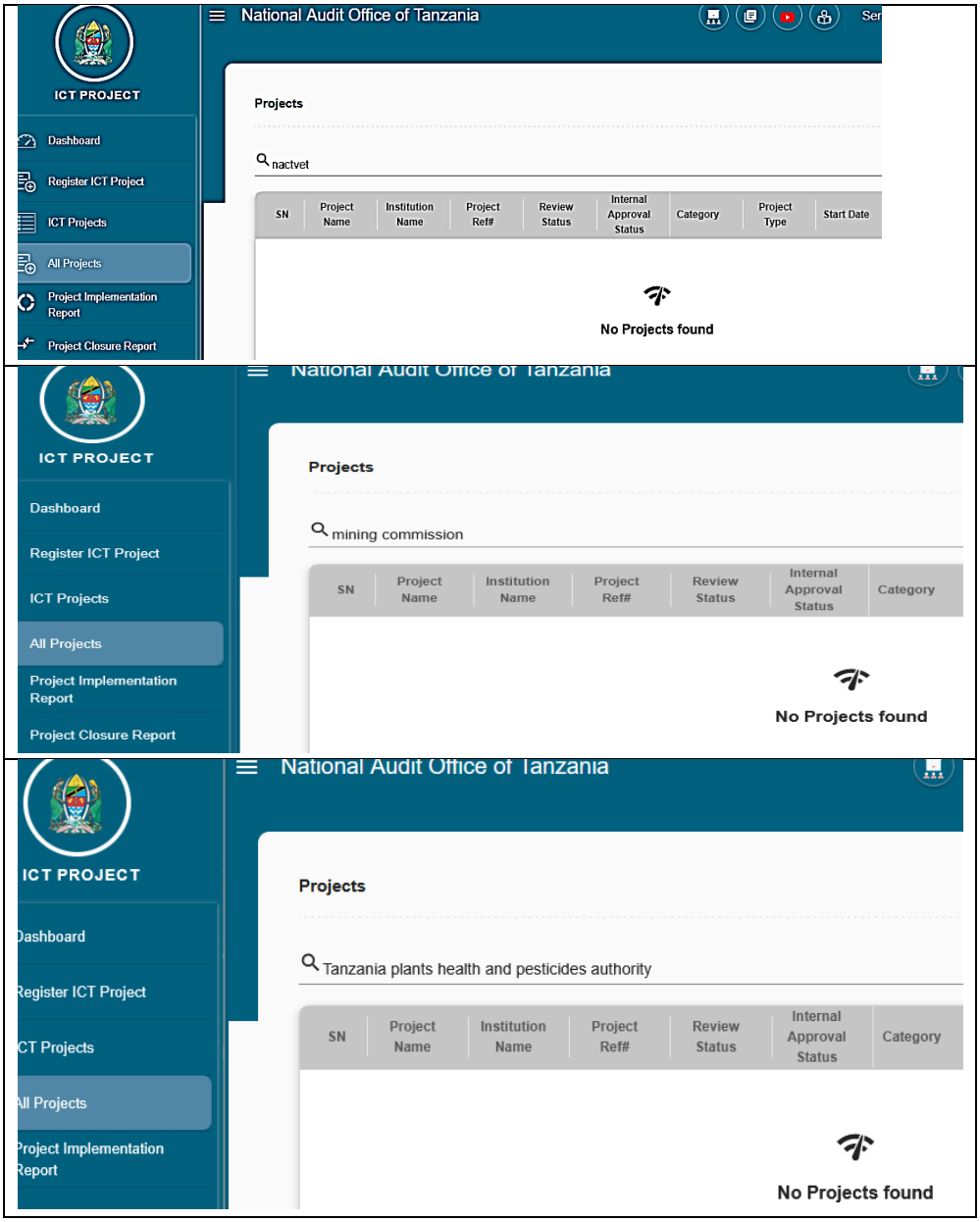
Institution	Official Interviewed	Reason(s) for Interviewing them
e-GA	• Director, Infrastructure and Operations Directorate • Director, Service Management Directorate • Managers and Officials from the Systems Development Section • Managers and Officials from the Data Centre Section • Managers and Officials from the Initiatives and Project Management Section	• To assess the management of ICT in Regulatory Authorities • To assess the policy and legislation governing the management of ICT in Regulatory Authorities • To evaluate the challenges facing adequate management of ICT in Regulatory Authorities. • To assess the management of resources in the management of ICT in the delivery of regulatory services
Selected Regulatory Authorities (LATRA, PURA, TMDA, TBS, Mining Commission, NACTVET and PPRA)	• Heads and Officials from respective Divisions and Sections regarding the management and utilisation of ICT in the delivery of regulatory services	To assess the following: • Exiting ICT systems in the respective Regulatory Authorities • Governing structures and processes for the management and utilisation of ICT in the Regulatory Authorities • Existing operational and technical manuals, concept notes for the ICT systems • Challenges facing the management and utilisation of ICT by the Regulatory Authorities

Institution	Official Interviewed	Reason(s) for Interviewing them
		• Performance of ICT systems in supporting the delivery of regulatory services • Benefits gained through the utilisation of the ICT systems

Source:Auditors' Analysis of the List of Interviewed Officials , 2024

Appendix 4: GISP Data on ICT Systems not Registered

This photo shows the display of the assessment done by the audit to verify the registration of ICT systems in the GISP.



Source: Auditors' Analysis of the ICT Systems in the GISP, 2024

Appendix 5: Sampled ICT Systems, their Status of Registration in GISP and Fragmented ICT systems

Regulatory Authority	ICT system Available in Public Institutions	Registered ICT systems
LATRA	• LATRA VTS Management Console • RRIMS - (Railway & Road Information Management System)	RRIMS - (Railway & Road Information Management System)
PPRA	• NeST	NeST (e-Procurement System)
NACTVET	• Teachers' registration • Examination system • Foreign award evaluation system • Transcript system • Student Admission System	• Teachers' registration • Examination system
MC	• Mining Market Management Information System (MMMIS) • Mining Information Management System (MIMS) • Trimble Land folio • Local Content	• Mining Market Management Information System (MMMIS) • Mining Information Management System (MIMS) • Local Content
TMDA	• Regulatory Information Management System (RIMS) • Laboratory Management Information System (LMIS)	NIL
PURA	• ProSource • Pretel ***NB:*** *They are Internal ICT Systems*	ProSource
TRA	• Taxpayer Portal (TRA Online Services) • Online Auction • Electronic Tax Stamps Management System – Purchased • CMVRS – Online services	NIL
TBS	• i-SQMT (Product certification on products inside the country) • OAS (Online Application System)	• i-SQMT (Product certification on products inside the country)

Regulatory Authority	ICT system Available in Public Institutions	Registered ICT systems
		• OAS (Online Application System)

Source: Auditors' Analysis of ICT systems Registered in GISP, 2024

Appendix 6: Extent of the Business Process Automated into ICT

This part shows the extent of the business process re-engineering by the regulatory authorities for ICT systems.

SN	Regulatory Authority	Number of Business Process (BP)	Number of BP Re-engineered	Number of BP not Re-engineered	Percentage (%)
1	TMDA	•Medicines •Medical devices and industry •Laboratory (3)	All Business processes (3)	0	100
2	PPRA	•Procurement services •Monitoring and compliance •Advisory services (3)	2	Advisory services on PPRA procedures are done through emails (1)	67
3	NACTVET	•Curriculum approval •Institution registration •Teachers' registration •Students' admission •Foreign award evaluation •Quality control and monitoring (6)	3	•Foreign award evaluation is done manually •Teachers' registration in a respective college is not traced •Curriculum approval is done manually (3)	50
4	MC	•Counteract minerals smuggling		•Counteract minerals smuggling	57

SN	Regulatory Authority	Number of Business Process (BP)	Number of BP Re-engineered	Number of BP not Re-engineered	Percentage (%)
		•Minerals royalty evasion in collaboration with relevant Government authorities •Provide, upon request, information to a mineral right holder or any other person who is engaged in mining operations. • Issue license • Carry out inspections or investigations • Monitor and audit the quality and quantity of minerals produced and exported. • Local content plan and corporate social responsibility (7)	4	•Provide, upon request, information to a mineral right holder or any other person who is engaged in mining operations. •Monitor and audit the quality and quantity of minerals produced and exported.	
5	LATRA	• Provides the licence	2	• Examination tests the applicants	50

SN	Regulatory Authority	Number of Business Process (BP)	Number of BP Re-engineered	Number of BP not Re-engineered	Percentage (%)
		• Registers and controls drivers • Manages offenses due to deviation of LATRA • Examination tests for the applicants (4)		• Manages Offenses due to deviation of LATRA (2)	
6	TBS	• To undertake measures for quality control of commodities, services and environment of all descriptions and to promote standardization in industry and trade. • To approve, register and control the use of standard marks • To undertake pre-shipment verification conformity (PVoC) to standards • To control the import	2	• To approve, register and control the use of standard marks • Importation control of commodities (2)	50

SN	Regulatory Authority	Number of Business Process (BP)	Number of BP Re-engineered	Number of BP not Re-engineered	Percentage (%)
		and exportation of commodities (4)			
7	PURA	• Reserve estimation and measurement of produced petroleum • Licensing round • Research and investigation (3)	1	• Reserve estimation is done in paper works by daily reports, and No link with machines at the site for the accuracy of the submitted data. • Licensing round is done manually and not linked with NeST (2)	33
		3030	177	1313	
Average of Engineered Business Processes					69%

Source:Auditors' Analysis of Business Process in the Visited Regulatory Authorities, 2024

Appendix 7: Inadequate Implementation of Plans to Manage Effective Utilisation of ICT in the Delivery of Regulatory Services

This part shows the analysis of the coverage of implementation of plans by e-Government Authority for the management of effective utilisation of ICT in the delivery of regulatory services.

Activity Code	Annual Plan intervention	2020/21	2021/22	2022/23	2023/24	Total Not done
F09S01	To coordinate, monitor, and evaluate the e-Government initiatives	X	v	x	X	3
C12S01	To provide ICT security technical support and advisory services to 200 Public Institutions	V	v	v	V	0
D01S01	To conduct e-government systems, application and services compliance, and quality assurance assessments	V	v	v	v	0
D06S01	To develop, review, and enforce e-government standards and guidelines	V	v	v	v	0
D02S01	To operationalize the e-service sustainability framework	V	v	x	x	2
D05S01	To develop and operationalize e-service monitoring and evaluation framework	V	v	x	x	2
D05S03	e-Government initiatives monitoring and evaluation	X	x	x	x	4

Activity Code	Annual Plan intervention	2020/21	2021/22	2022/23	2023/24	Total Not done
	framework developed and operationalized					

Source:Auditors' Analysis of the e-GA Annual Operational Plans, 2024

Appendix 8: Planned and Conducted ICT System Inspection in Public Institutions

This part shows the extent of planning and implementation of ICT systems inspection in public institutions and Regulatory Authorities.

Regulatory Authority	Target code	Aspect	Number of PI	Percentage in All number of PI
2020/21	D05S03	Inspection	11	3%
	D01S	Compliance Assessment	59	18%
2021/22	D05S03	Inspection	16	5%
	D01S	Compliance Assessment	53	16%
2022/23	C19S	Inspection	99	30%
	D02S	Compliance Assessment	57	17%
2023/24	C19S01	Inspection	54	17%
	D02S	Compliance Assessment	67	21%

Source:Auditors' Analysis of the e-GA Annual Inspection and Compliance Assesment, 2024

Appendix 9: Number of Public Institutions in the Country

This photo shows the display of the categories of public institutions in the country.

Source:Auditors' Analysis on the Main Government Website, 2024

Appendix 10: Extent of Implementation of Plans to Manage Utilisation of ICT Systems

This part shows the implementation of the planned activities on the aspects of coordination, monitoring and evaluation of the e-government activities.

Activity Code	Annual Plan intervention	2020/21	2021/22	2022/23	2023/24	Total Not done
F09S01	To coordinate, monitor, and evaluate the e-Government initiatives	Coordination and evaluation part is not covered	v	Coordination and evaluation part is not covered	Coordination and evaluation part is not covered	3
C12S01	To provide ICT security technical support and advisory services to 200 Public Institutions	v	v	v	v	0
D01S01	To conduct eGovernment systems, application and services compliance and quality assurance assessments	v	v	v	v	0
D02S01	To operationalize the e-service sustainability framework	v	v	Not found in the e-GA performance progress report	v	1

Activity Code	Annual Plan intervention	2020/21	2021/22	2022/23	2023/24	Total Not done
D05S01	To develop and operationalize the e-service framework	v	v	No evaluation report is available No document to show the e-services framework	No evaluation report is available No document to show the e-services framework	2
D05S03	e-Government initiatives monitoring and evaluation framework developed and operationalized	No evaluation report is available regarding the e-Government initiatives	No evaluation report is available regarding the e-Government initiatives	No performance audit report as an evaluation	No evaluation report is available regarding the e-Government initiatives	4

Source:Auditors' Analysis of the e-GA Annual Plans and Implementation Reports, 2024

National Audit Office of Tanzania (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