



THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE
e-GOVERNMENT AUTHORITY

ISO 9001:2015|ISO/IEC 27001:2022 CERTIFIED



e-Government **Emerging Technologies Governance Framework**



August 2026

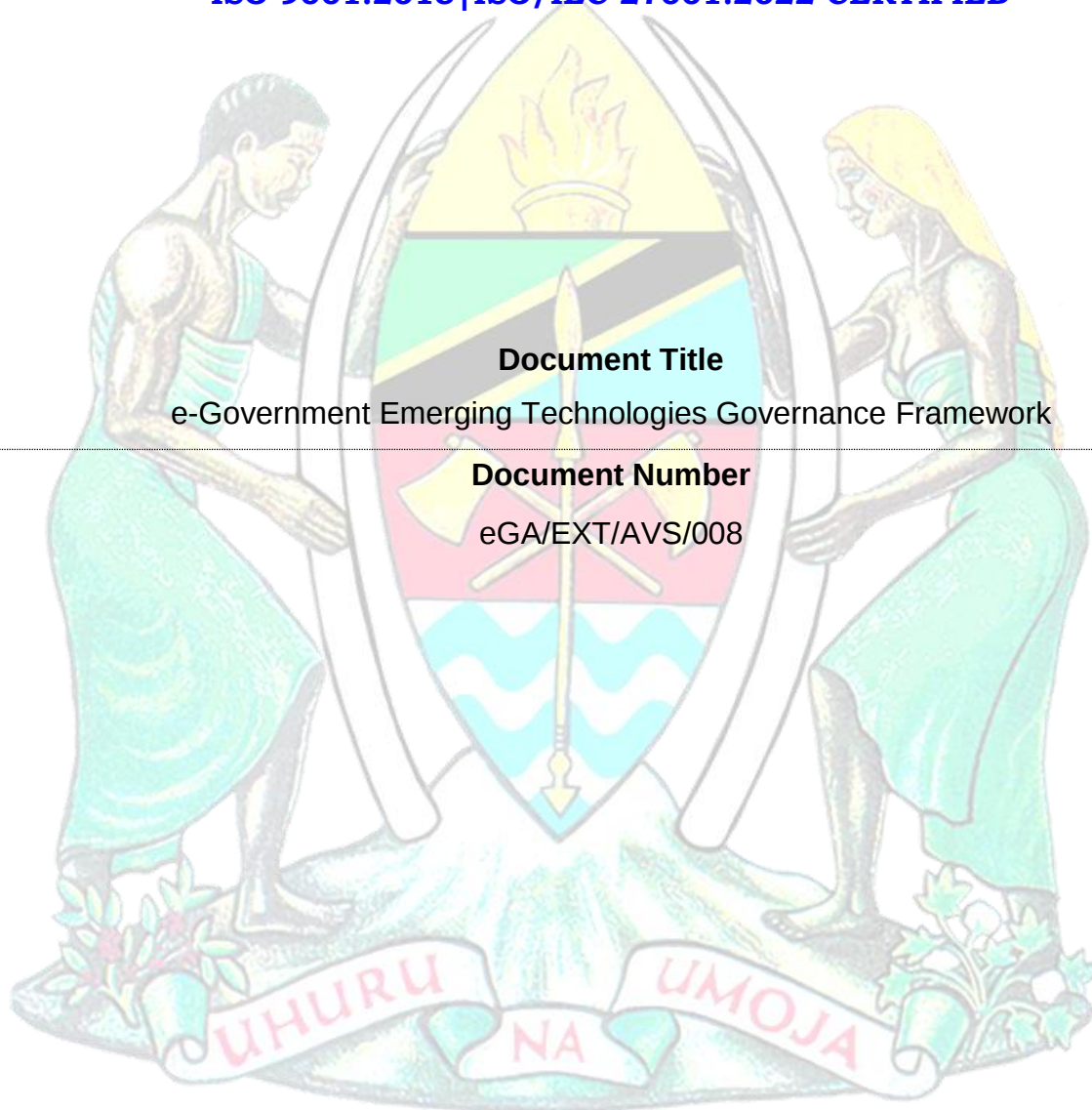


THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE

e-GOVERNMENT AUTHORITY

ISO 9001:2015|ISO/IEC 27001:2022 CERTIFIED



Document Title

e-Government Emerging Technologies Governance Framework

Document Number

eGA/EXT/AVS/008

APPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	Dr. Mussa M. Kissaka	Board Chairperson		31.08.2026

Version: 1.0 – August 2026

PREFACE

Public institutions operate in a rapidly evolving digital environment in which emerging technologies are increasingly transforming public service delivery. The emerging technologies present opportunities to enhance institutional performance, improve service delivery, foster innovation, strengthen the use of Government data, and improve responsiveness to public needs. However, if adopted without an appropriate governance framework, they may introduce risks relating to governance, legal, ethics, security, privacy, interoperability, accountability, sustainability, operations, and public trust.

Pursuant to sections 5(2)(c), 5(2)(i), 5(2)(q), and 22(3) of the e-Government Act, Cap.273, R.E.2023, the Authority is mandated to provide guidance to Public Institutions on e-Government initiatives, set ICT standards and procedures, promote e-Government research, development and innovation. Furthermore, Dira 2050 embraces the use of emerging technologies to accelerate digital transformation, enhance public sector efficiency, foster innovation, promote socio-economic progress, boost global competitiveness, and ensure ethical and accountable use, hence improving public service delivery. In fulfilment of these requirements, the Authority has developed the e-Government Emerging Technologies Governance Framework to provide a structured approach for the development, deployment, use, monitoring, and oversight of emerging technologies so that they are safe, trustworthy, ethical, and compliant with applicable laws and regulations.

The Authority urges all Public Institutions to apply this Framework when adopting, acquiring, developing, deploying, operating, monitoring, changing, or retiring emerging technology solutions. Proper application of this Framework will contribute to responsible innovation, strengthened public trust, protection of Government systems and data, and delivery of secure, inclusive, accountable, and sustainable digital public services.

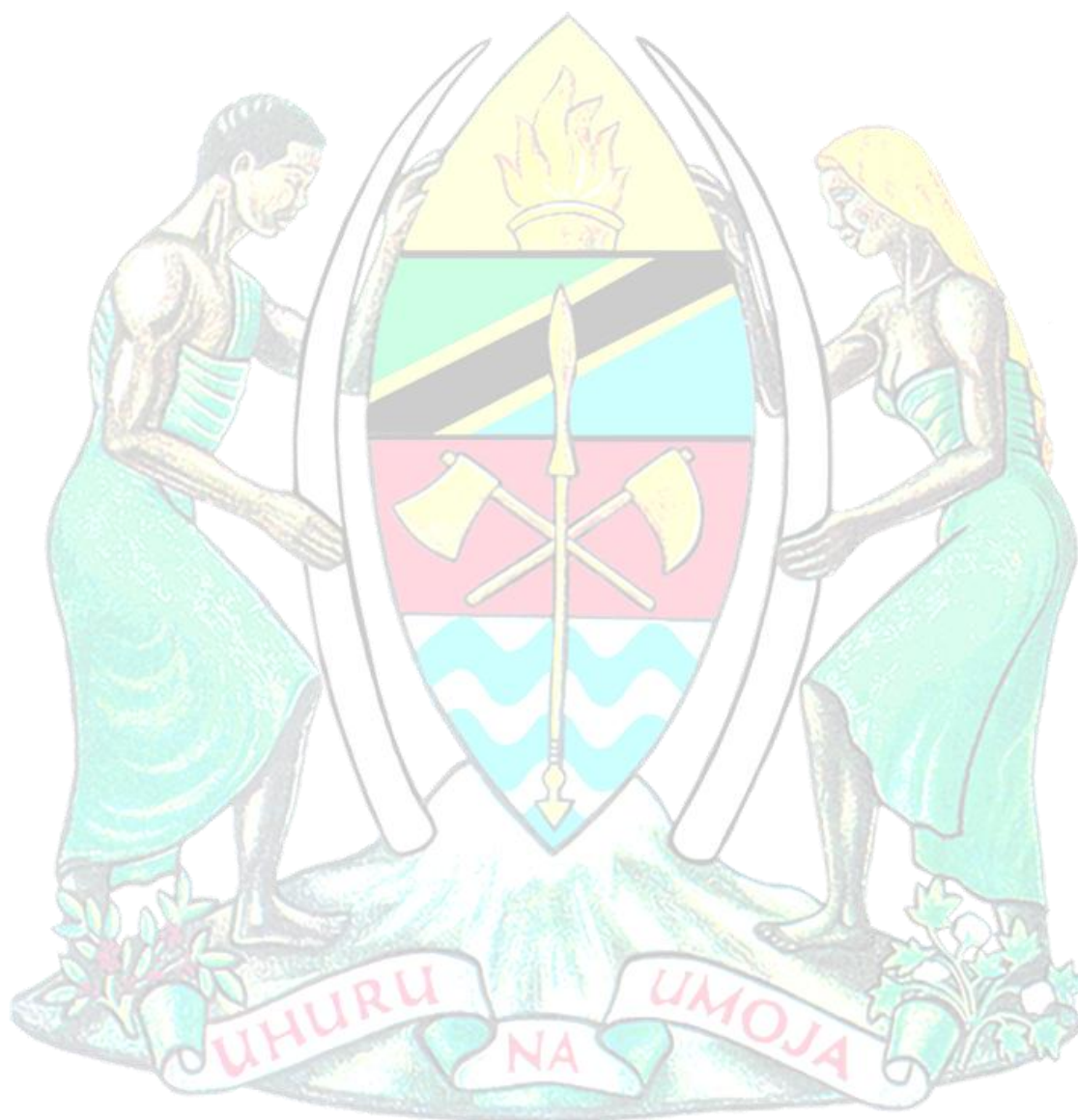


Dr. Mussa M. Kissaka
BOARD CHAIRPERSON

Table of Contents

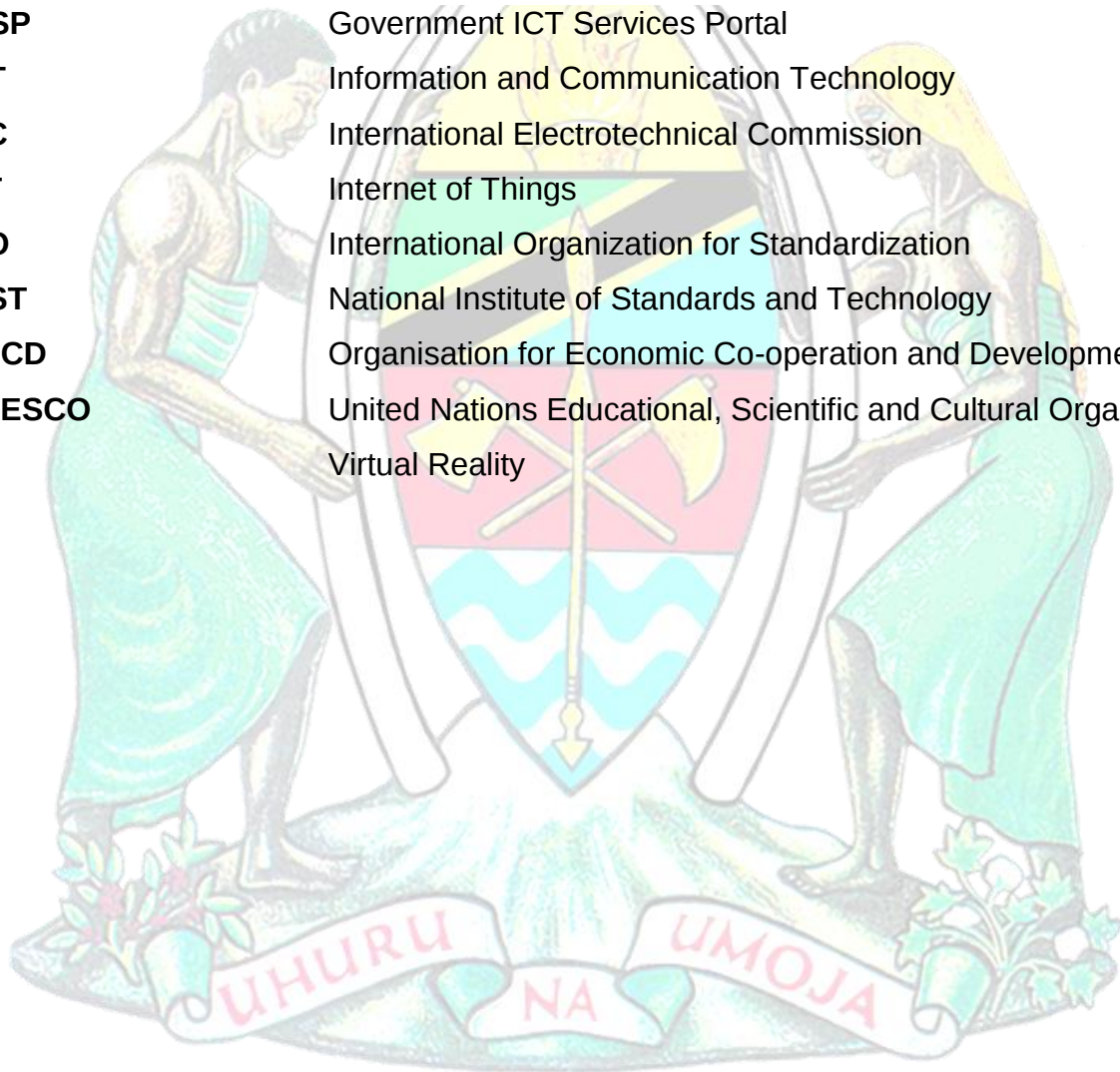
PREFACE	3
ACRONYMS	6
GLOSSARY	7
1 INTRODUCTION	12
1.1 Overview	12
1.2 Purpose	13
1.3 Rationale	13
1.4 Scope	14
2 E-GOVERNMENT EMERGING TECHNOLOGIES GOVERNANCE FRAMEWORK	15
2.1 Emerging Technologies Governance Principles	15
2.1.1 Public Value and Public Interest	16
2.1.2 Fairness, Non – Discrimination and Inclusion	17
2.1.3 Accountability and Responsible Ownership	18
2.1.4 Transparency, Explainability and Traceability	19
2.1.5 Security, Safety, and Resilience	20
2.1.6 Privacy and Data Protection	21
2.1.7 Interoperability and Integration	22
2.1.8 Human Oversight and Control	23
2.1.9 Sustainability	24
2.2 Emerging Technologies Governance Roles and Responsibilities	25
2.2.1 e-Government Authority	25
2.2.2 Institutional ICT Steering Committee	25
2.2.3 ICT Management Unit	25
2.2.4 Business Process Owner	26
2.3 e-Government Emerging Technology Lifecycle	26
2.3.1 Initiation	27
2.3.2 Design	28
2.3.3 Acquisition and Development	28
2.3.4 Testing and Validation	29
2.3.5 Deployment	29
2.3.6 Operation and Monitoring	29
2.3.7 Retirement	30
2.4 Emerging Technology Risk Management	30
2.5 Emerging Technology Impact Assessment	31
2.6 Compliance and Assurance	32

3	IMPLEMENTATION, REVIEW AND ENFORCEMENT	32
4	RELATED DOCUMENTS	32
5	DOCUMENT CONTROL	33
	APPENDIX I: EMERGING TECHNOLOGY USE CASE TEMPLATE	35



ACRONYMS

AI	Artificial Intelligence
AR	Augmented Reality
AU	African Union
Dira 2050	Tanzania Development Vision 2050
e-GA	e-Government Authority
GISP	Government ICT Services Portal
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
UNESCO	United Nations Educational, Scientific and Cultural Organization
VR	Virtual Reality



GLOSSARY



Accountability	The allocated responsibility of an individual, organisation, or emerging technology actor for the proper functioning, decisions, and outputs of an emerging technology or emerging-technology system, together with the obligation to answer for those decisions to another party according to defined criteria.
Algorithm	A defined set of rules or instructions followed by a computer system to perform a computation, solve a problem, or produce an output from given inputs.
Artificial Intelligence	is the capability of computer systems to perform tasks that normally require human intelligence, including learning, reasoning, prediction, content generation, decision support, and pattern recognition.
Assurance	An independent or objective evaluation providing confidence that an emerging technology solution and its governance arrangements remain suitable, adequate, and effective.
Augmented Reality	a view of the real physical environment supplemented or overlaid with computer-generated digital information (images, sound, video, text, or graphics) registered into that environment in real time.
Automated Decision-Making	A decision made solely on the basis of automated processing where that decision produces legal effects or otherwise significantly affects the person concerned.
Automation Bias	The tendency of humans to over-rely on, or uncritically accept, outputs or recommendations produced by an automated system, even where those outputs are incorrect.
Bias	A systematic difference in the treatment of certain individuals, groups, or objects compared to others, which may arise from data, design choices, or use context and may result in unfair or discriminatory outcomes.

Blockchain	A digital record system where information is stored in linked blocks and shared across a network, making records difficult to alter without detection.
Business Process Owner	The institution unit/section/department/directorate responsible for the business function where an emerging technology solution is implemented.
Data Governance	The framework of policies, roles, processes, and controls through which an institution ensures that data is managed lawfully, securely, and in a manner that preserves its quality, integrity, and appropriate use.
Due Diligence	A structured process of investigating and evaluating an emerging technology solution, vendor, or service provider before making decision.
Edge Computing	A distributed computing approach that enables data processing and analysis at or near the source of data generation, reducing dependence on centralized computing resources and supporting real-time operations.
Emerging Technology	A new or rapidly developing technology that may significantly change how services, systems, data, or institutional operations are managed or delivered. Example of these technologies include Artificial Intelligence (AI), Blockchain, Internet of Things (IoT), Robotics, Virtual Reality (VR)/Augmented Reality (AR), Quantum Computing and Edge Computing.
Emerging Technology lifecycle	The stages an emerging technology solution goes through from initiation, design, acquisition or development, testing and validation, deployment and operation, monitoring and change control, to retirement or decommissioning.
Emerging Technology Use Case	a specific, real-world application where an emerging technology(such as AI, blockchain, or AR/VR) solves a distinct problem.

Explainability		The property of an emerging technology system that allows the important factors influencing its results to be expressed in a way that humans can understand, addressing the question of why a particular output was produced.
Generative Intelligence	Artificial	A category of artificial intelligence systems capable of producing new content such as text, images, audio, video, or code based on patterns learned from data from a given input.
Human Oversight		The design measures and operational mechanisms that enable a natural person to effectively understand, monitor, intervene in, and where necessary halt the operation of an emerging-technology system during its period of use, in order to prevent or minimise risks.
Impact Assessment		A structured review used to understand how a proposed technology may affect services, people, data, security, operations, legal obligations, and public trust.
Internet of Things		An infrastructure of interconnected objects, people, systems and information resources, together with services that collect, exchange, process, and react to information through appropriate communication networks.
Interoperability		The ability of different information technology systems and software applications to communicate, exchange data and use of information that has been exchanged.
Machine Learning		A branch of artificial intelligence in which systems improve their performance on a task by learning patterns from data, rather than being explicitly programmed for every scenario.
Personal Data		Any information relating to an identified or identifiable natural person, as provided under the Personal Data Protection Act, Cap.44, R.E.2023 and related regulations.
Principle Implication		The specific obligations, requirements, responsibilities, or actions that public institutions are expected to implement in order to comply with a principle.

Principle Rationale

The explanation describing why a principle exists and the governance objective it is intended to achieve. It provides the reasoning behind the principle and the problem it seeks to address.

Profiling

Any form of automated processing of personal data to evaluate, analyse, or predict aspects of a natural person, such as behaviour, performance, preferences, reliability, or location.

Quantum Computing

An advanced computing technology that leverages quantum-mechanical phenomena to perform computations that may be infeasible or significantly less efficient using classical computing systems.

Residual Risk

The level of risk that remains after mitigation measures, controls, or safeguards have been applied.

Resilience

The ability of a system, service, or institution to withstand, adapt to, and recover from disruptions, failures, attacks, or adverse conditions while maintaining acceptable levels of service.

Risk Assessment

A structured process for identifying possible risks, analysing how serious they are, and deciding what controls or actions are needed to manage them.

Robotics

The application of programmable machines capable of sensing, processing information, and performing physical or digital tasks autonomously or under human supervision to achieve defined objectives.

Scalability

The capability of a technology solution to handle increased workload, users, or data volumes, or to be expanded to accommodate growth and future advancements, without loss of performance or the need for fundamental redesign.

Smart Contract

A self-executing computer program stored on a blockchain that automatically performs, controls, or documents agreed actions when predefined conditions are met.

Transparency

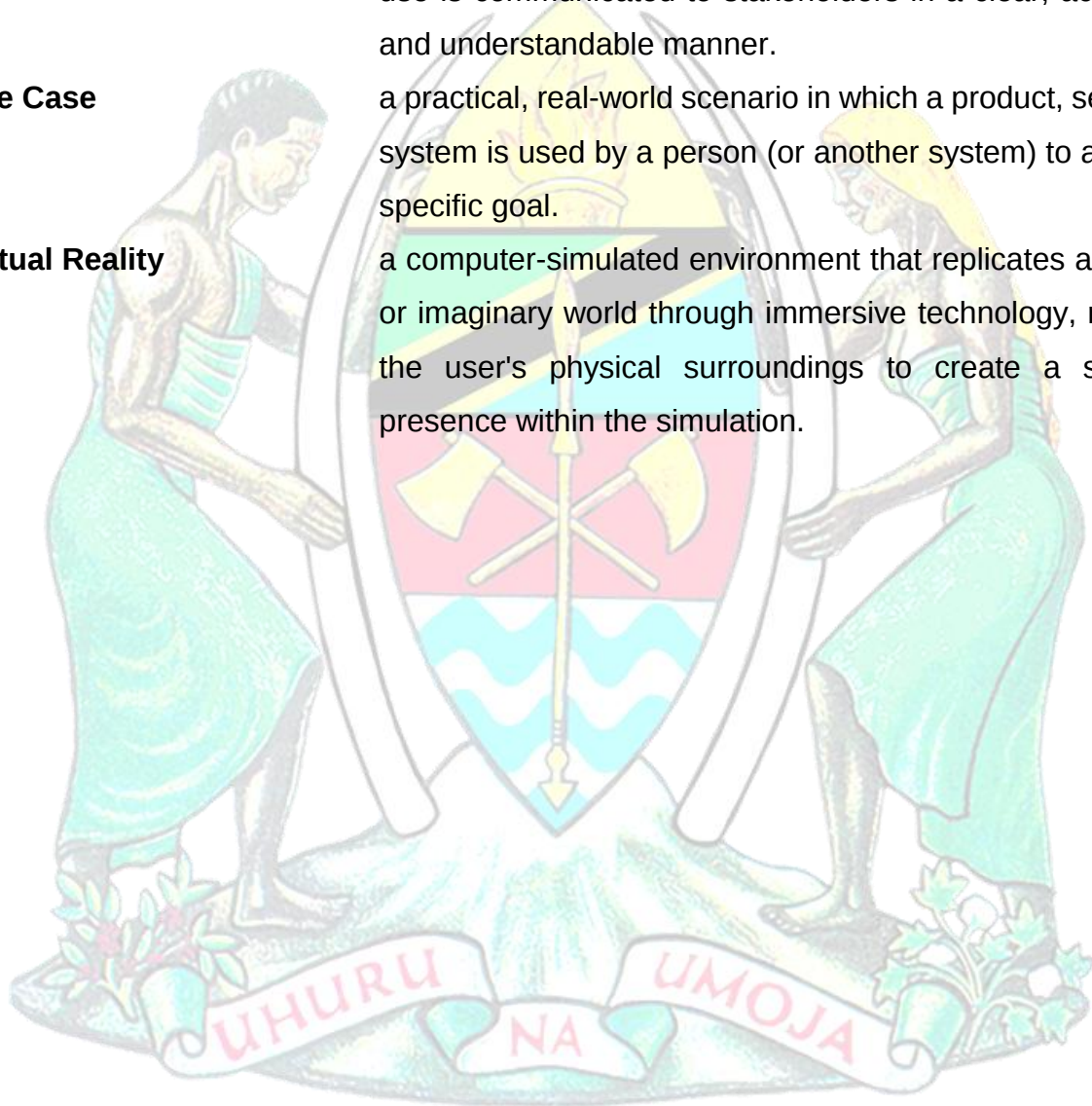
The property of an emerging technology whereby relevant information about its purpose, capabilities, limitations, and use is communicated to stakeholders in a clear, accessible, and understandable manner.

Use Case

a practical, real-world scenario in which a product, service, or system is used by a person (or another system) to achieve a specific goal.

Virtual Reality

a computer-simulated environment that replicates a physical or imaginary world through immersive technology, replacing the user's physical surroundings to create a sense of presence within the simulation.



1 INTRODUCTION

1.1 Overview

The e-Government Authority (e-GA), an ISO 9001:2015 and ISO/IEC 27001:2022 certified public institution established under the e-Government Act, Cap 273, R.E.2023 is mandated to coordinate, oversee, and promote e-Government initiatives, as well as enforce related policies, laws, regulations, standards, and guidelines across public institutions.

The rapid evolution and adoption of emerging technologies, including Artificial Intelligence (AI), Blockchain, Internet of Things (IoT), Virtual Reality (VR)/Augmented Reality (AR), Robotics, Quantum Computing, Edge Computing, and other emerging technologies, presents significant opportunities for transforming the delivery of public services. The Government through Dira 2050 recognizes the potential use of emerging technologies to accelerate digital transformation, enhance public sector efficiency, foster innovation, promote socio-economic progress, boost global competitiveness, and ensure ethical and accountable use, hence improving public service delivery. However, their adoption also introduces new and evolving challenges relating to governance, ethics, privacy, cybersecurity, data protection, accountability, interoperability, skills, sustainability, and responsible use.

In this context, e-GA has developed the e-Government Emerging Technologies Governance Framework to provide a structured and coordinated approach for the identification, assessment, adoption, implementation, monitoring, and responsible use of emerging technologies within public institutions. The Framework seeks to ensure that emerging technologies are adopted in a manner that is secure, ethical, inclusive, transparent, accountable, sustainable, cost effective and aligned with national development priorities and the Government's digital transformation agenda.

The Framework further establishes guiding principles, governance structures, roles and responsibilities, risk management and impact assessment requirements, compliance measures, and monitoring arrangements to support public institutions in effectively managing emerging technologies throughout their lifecycle.

1.2 Purpose

The purpose of this Framework is to provide comprehensive guidance for the governance, adoption, implementation, and management of emerging technologies within public institutions. The framework promotes innovation while safeguarding citizens' rights, government integrity, and national digital transformation objectives.

Specifically, the framework aims to:

- i. promote lawful, ethical and secure governance of emerging technologies;
- ii. achieve consistent and effective management of emerging technologies throughout their life cycle;
- iii. enable proactive identification, assessment and mitigation of risks associated with emerging technologies; and
- iv. establish a foundation for the development and implementation of the emerging technology specific standards, guidelines, procedures and tools.

1.3 Rationale

Public institutions are increasingly operating in a digital environment in which emerging technologies are becoming more visible, more accessible, and more relevant to the delivery of public services. While such technologies present opportunities for efficiency, innovation, service improvement, and improved public value, they also introduce governance, legal, ethical, security, privacy, interoperability, accountability, and public-trust concern that require a coordinated and consistent Government response.

In line with sections 5(2)(c), 5(2)(i), 5(2)(q), and 22(3) of the e-Government Act, Cap.273, R.E.2023, the e-Government Authority is mandated to guide Public Institutions on e-Government initiatives, promote e-Government research, development and innovation, and

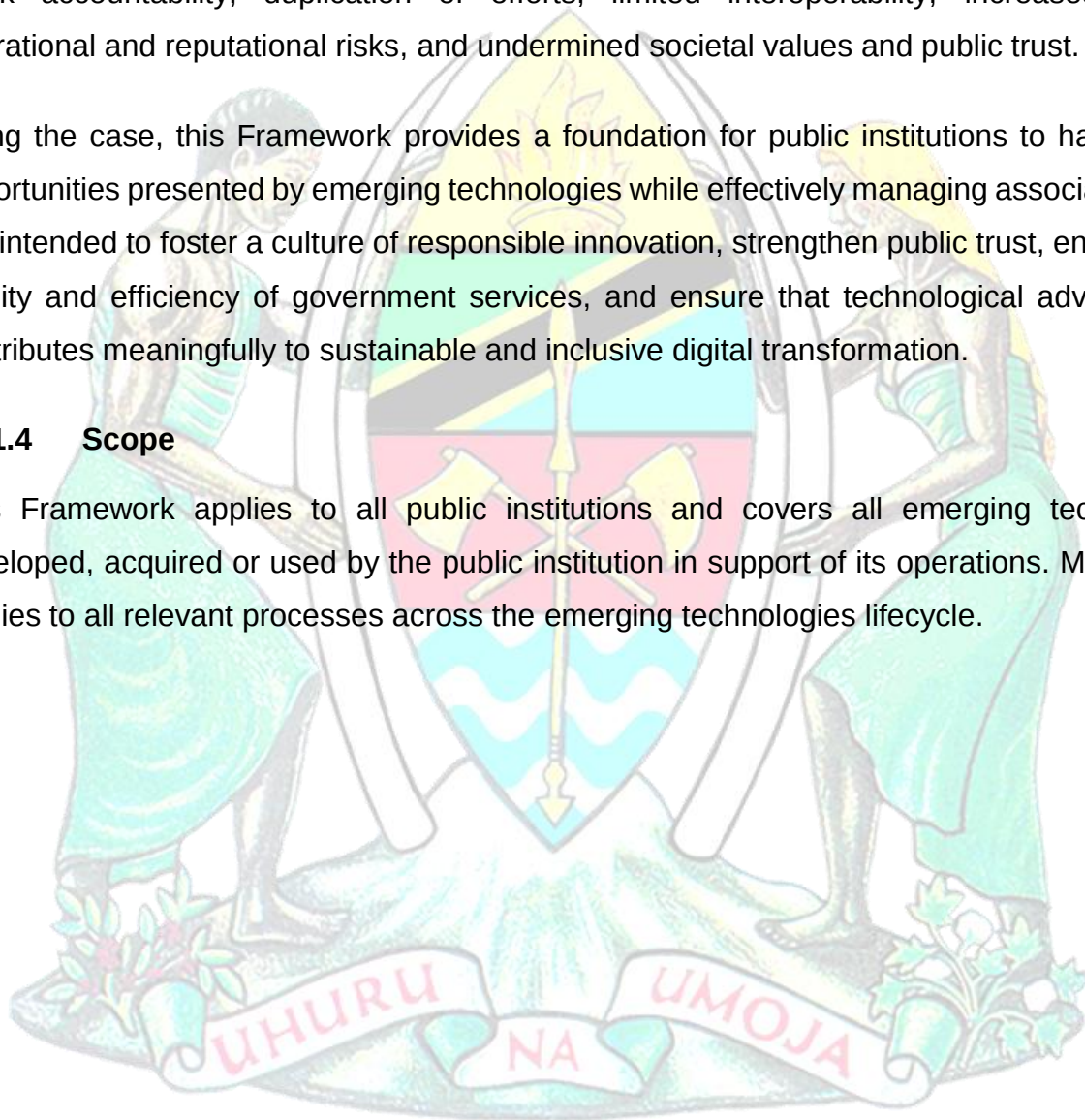
ensure that e-Government initiatives are managed in accordance with standards and guidelines issued by the Authority.

In the absence of a common governance framework, public institutions may adopt or use emerging technologies inconsistently, leading to unequal access, fragmented decision-making, weak accountability, duplication of efforts, limited interoperability, increased ethical, operational and reputational risks, and undermined societal values and public trust.

Being the case, this Framework provides a foundation for public institutions to harness the opportunities presented by emerging technologies while effectively managing associated risks. It is intended to foster a culture of responsible innovation, strengthen public trust, enhance the quality and efficiency of government services, and ensure that technological advancement contributes meaningfully to sustainable and inclusive digital transformation.

1.4 Scope

This Framework applies to all public institutions and covers all emerging technologies developed, acquired or used by the public institution in support of its operations. Moreover, it applies to all relevant processes across the emerging technologies lifecycle.



2 e-GOVERNMENT EMERGING TECHNOLOGIES GOVERNANCE FRAMEWORK

2.1 Emerging Technologies Governance Principles

The governance principles set out in this section provide an overview of the values and governance expectations that guide the responsible adoption, use, oversight, and management of emerging technologies. Public institutions shall demonstrate implementation of these governance principles throughout the emerging technology lifecycle. Figure1 depicts the Emerging Technologies Governance Principles.



Figure 1 – e-Government Emerging Technologies Governance Principles

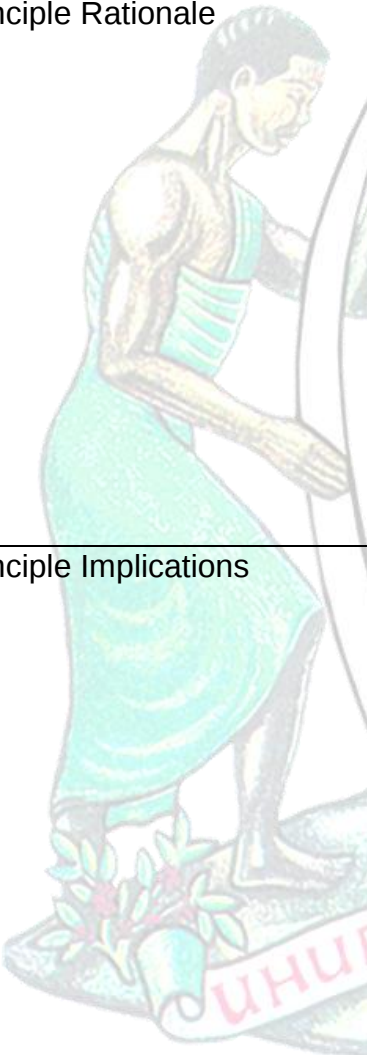
2.1.1 Public Value and Public Interest

Clear justification that emerging technologies serve public functions, service delivery needs, and the public interest.

Principle #1	Public Value and Public Interest
Principle Rationale	This principle emphasises that emerging technologies are adopted to support legitimate public functions, institutional needs, service delivery objectives, or public interest outcomes. It helps ensure that technology adoption is driven by clear public value rather than novelty, market pressure, or vendor influence.
Principle Implications	Public Institution shall: i. adopt, deploy, and use emerging technologies to support and improve public service delivery, strengthen administrative effectiveness, support evidence-based decision-making, or otherwise advances legitimate public interest objectives; ii. ensure that the adoption of emerging technologies is justified by a clear need and expected value not solely on the basis of novelty, market trends, or vendor influence; iii. ensure that the expected public value of an emerging technology use case is considered together with its governance, operational, legal, ethical, and security implications; and iv. consider local context and language needs when adopting and using emerging technologies.

2.1.2 Fairness, Non – Discrimination and Inclusion

Fair, lawful, inclusive, and non-discriminatory use of emerging technologies that avoids unjust exclusion or harm.

Principle #2	Fairness, Non – Discrimination and Inclusion
Principle Rationale 	This principle emphasises that emerging technologies are used in a manner consistent with applicable laws, regulations, public-sector ethics, and institutional mandates. It covers fairness, non-discrimination, avoidance of arbitrary or deceptive use, and prevention of technology uses that may be abusive, harmful, or incompatible with public-sector obligations. It supports accessible digital services and helps reduce the risk of unjust exclusion, inaccessible services, or disproportionate adverse effects on particular individuals, groups, or communities.
Principle Implications	Public Institution shall: - assess emerging technology use cases for potential unfair treatment, discriminatory effects, arbitrary outcomes, or disproportionate adverse effects; - ensure that emerging technologies are designed, acquired, configured, deployed, and used in a manner consistent with fairness and non-discrimination; - document and address unfairness and discrimination risks; - monitor emerging technology solution to timely detect unfair treatment, discriminatory effect, arbitrary outcomes or disproportionate adverse effects;

	v. suspend an emerging technology solution upon detection of unfairness and discriminatory incidents until adequate mitigations are applied; and vi. take reasonable measures to reduce the risk that emerging technology adoption results in unjust exclusion, inaccessible services, or disproportionate adverse effects on particular individuals, groups, or communities.
--	---

2.1.3 Accountability and Responsible Ownership

Clear institutional responsibility and ownership for each emerging technology use case.

Principle #3	Accountability and Responsible Ownership
Principle Rationale	This principle emphasises that responsibility for each emerging technology use case remains clearly identifiable within the institution. It recognises that technology solutions, vendors, automated processes, or technical teams do not replace institutional accountability for decisions, actions, outcomes, and consequences arising from the use of emerging technologies.
Principle Implications	Public Institution shall: i. clearly designate accountable owner for each emerging technology use case; ii. remain accountable and responsible for decisions, actions, outcomes, and consequences arising from their use of emerging technologies; and iii. establish clear roles and responsibilities for decision-making, oversight, risk management, monitoring, and

	compliance throughout the emerging technologies lifecycle.
--	--

2.1.4 Transparency, Explainability and Traceability

Clear visibility, explanation, tracking, and auditing of emerging technology use, decisions, and outcomes.

Principle #4	Transparency, Explainability and Traceability
Principle Rationale	This principle emphasises on ensuring that emerging technologies are operated in a manner that enables clear understanding of how they function, how decisions are made, and how outcomes are produced. They shall ensure that processes are open and understandable to stakeholders and all actions, data usage, and system changes can be tracked and audited throughout the lifecycle of the technology.
Principle Implications	Public Institution shall: i. ensure that the use of emerging technologies is sufficiently transparent to support accountability, lawful oversight, audit, and strengthen public trust; ii. be able to explain the scope, purpose, role, and outputs of an emerging technology solution used in support of institution's operations; and iii. maintain adequate records, and documentation regarding the origin, purpose, configuration, dependencies, changes, and governance status of emerging technology solutions used within the institution.

2.1.5 Security, Safety, and Resilience

Protection of Government systems, data, services, users, and operations from harm, misuse, disruption, and failure.

Principle #5	Security, Safety, and Resilience
Principle Rationale	This principle emphasises on protecting Government systems, data, services, users, and operations from compromise, misuse, malfunction, harmful effects, service disruption, and continuity failure. It emphasises secure design, safe operation, risk-based protection, incident response, recovery, and resilience throughout the technology lifecycle.
Principle Implications	Public Institution shall: i. address security, resilience, and safe operation considerations across the emerging technology lifecycle, including during initiation, design, acquisition/development, deployment, operation, monitoring, and retirement; ii. assess and manage emerging technologies in a manner proportionate to their security, operational, service delivery, and public trust implications; and iii. take reasonable measures to prevent, detect, respond to, and recover from misuse, malfunction, compromise, failure, or harmful effects associated with emerging technologies.

2.1.6 Privacy and Data Protection

Lawful, secure, purpose-bound, and accountable handling of data used in emerging technology solutions.

Principle #6	Privacy and Data Protection
Principle Rationale	This principle emphasises lawful, secure, purpose-bound, and accountable handling of data and information used in emerging technology solutions. It is particularly important where technologies use personal, sensitive, and confidential data to support public-service delivery.
Principle Implications	Public Institution shall: i. adopt and use emerging technologies in compliance with applicable legal and regulatory requirements concerning privacy and data protection; ii. govern data and information handled through emerging technology solutions in a lawful, purpose bound, risk-informed manner and appropriately safeguarded; and iii. consider privacy and data protection implications at the earliest stages of technology assessment, design, procurement, and development.

2.1.7 Interoperability and Integration

Effective connection and compatibility with existing Government systems, platforms, devices, workflows, and service channels.

Principle #7	Interoperability and Integration
Principle Rationale	This principle emphasises that emerging technology solutions work effectively with existing Government systems, data platforms, devices, workflows, and service delivery channels. It supports secure information exchange, coordinated service delivery, standardisation, compatibility, and long-term maintainability while reducing duplication and system fragmentation.
Principle Implications	Public Institution shall: - adopt emerging technology solutions in alignment with e-Government Standards and Guidelines regarding interoperability and integration; - avoid adopting technology solutions that unnecessarily fragment Government systems, impair interoperability, duplicate existing capabilities, or create barriers to system integration; and - adopt emerging technology that support compatibility, information exchange and long-term maintainability.

2.1.8 Human Oversight and Control

Qualified human oversight, review, intervention, and control over emerging technology operations and outcomes.

Principle #8	Human Oversight and Control
Principle Rationale	This principle emphasises on the involvement of qualified individuals in monitoring, supervising, and managing the operation and outcomes of emerging technologies to ensure that decisions, actions, and processes remain lawful, ethical, accurate, and aligned with institutional objectives.
Principle Implications	Public Institution shall: - subject emerging technologies to meaningful human oversight proportionate to the context, sensitivity and risk of the use case, the degree of automation, potential effect on rights and interests, effect on public service delivery and security implications; and - ensure that humans retain the ability to review, intervene, override, or stop automated processes where necessary, particularly in situations involving significant risks, errors, or impacts on individuals and society.

2.1.9 Sustainability

Long-term public value, efficiency, resilience, environmentally friendly and responsible use of resources in adopting emerging technology.

Principle #9	Sustainability
Principle Rationale	This principle emphasises on the responsible development and use of technologies in a manner that promotes continuous improvement, efficiency, and innovation while minimizing negative environmental, social, and economic impacts. It ensures that emerging technologies support long-term public value, resource efficiency, resilience, and sustainable national development goals.
Principle Implications	Public Institution shall: - take into account long-term operational sustainability, resource implications, maintainability, and broader impact in the adoption or continued use of an emerging technology; - adopt emerging technologies in an efficient and environment friendly manner in line with applicable laws and operational needs; - ensure continuous capacity building and professional development of their staff to develop and maintain the competencies required for the responsible adoption, use, and management of emerging technologies; and - encourage innovation in the use of emerging technologies in a manner that remains environment friendly, lawful, risk-informed, accountable, and aligned with the public interest.

2.2 Emerging Technologies Governance Roles and Responsibilities

Defining roles and responsibilities is critical for ensuring accountability throughout the Emerging Technology Lifecycle. The following roles and responsibilities are defined for proper governance of Emerging Technologies.

2.2.1 e-Government Authority

- i. Review, monitor, coordinate, and oversee emerging technology initiatives in public institutions; and
- ii. Promote research, development and innovation of emerging technologies.

2.2.2 Institutional ICT Steering Committee

- i. Ensure emerging technology initiatives align with institutional objectives and applicable governance, risk management, and compliance requirements;
- ii. Review and approve emerging technology use cases;
- iii. Oversee the management of risks associated with emerging technologies and ensure that appropriate mitigation measures are established and maintained;
- iv. Ensure the responsible, secure and ethical use of emerging technologies across the institution; and
- v. Perform continuous monitoring and evaluation of emerging technology initiatives.

2.2.3 ICT Management Unit

- i. Provide technical guidance, coordination, support and advisory services on the implementation of emerging technologies within the institution;
- ii. Ensure implementation of emerging technology initiatives are aligned with the provisions of the e-Government Act, regulations, standards, guidelines, and other applicable legal and regulatory requirements;

- iii. Ensure emerging technology risks such as security, privacy, interoperability, ethical and technical risks are mitigated to the institutional risk acceptable level;
- iv. Monitor the availability, performance, safety, integrity, reliability and capacity of deployed emerging technologies against defined service levels; and
- v. Conduct awareness and capacity building to support the responsible, secure, and effective adoption of emerging technologies across the institution.

2.2.4 Business Process Owner

- i. Define and confirm business objectives, needs and requirements that emerging technology is intending to address;
- ii. Participate in the evaluation, testing and acceptance of emerging technology solutions prior to deployment;
- iii. Monitor the performance of emerging technology solution to ensure business objectives are achieved; and
- iv. Own the respective emerging technology use case and solution.

2.3 e-Government Emerging Technology Lifecycle

The e-Government Emerging Technology Lifecycle guides how public institutions identify, evaluate, adopt, integrate, and retire emerging technology solutions. It ensures that technology adoption is systematic, risk-aware, and aligned with institutional goals. Figure 2 shows the e-Government Emerging Technology Lifecycle Stages.

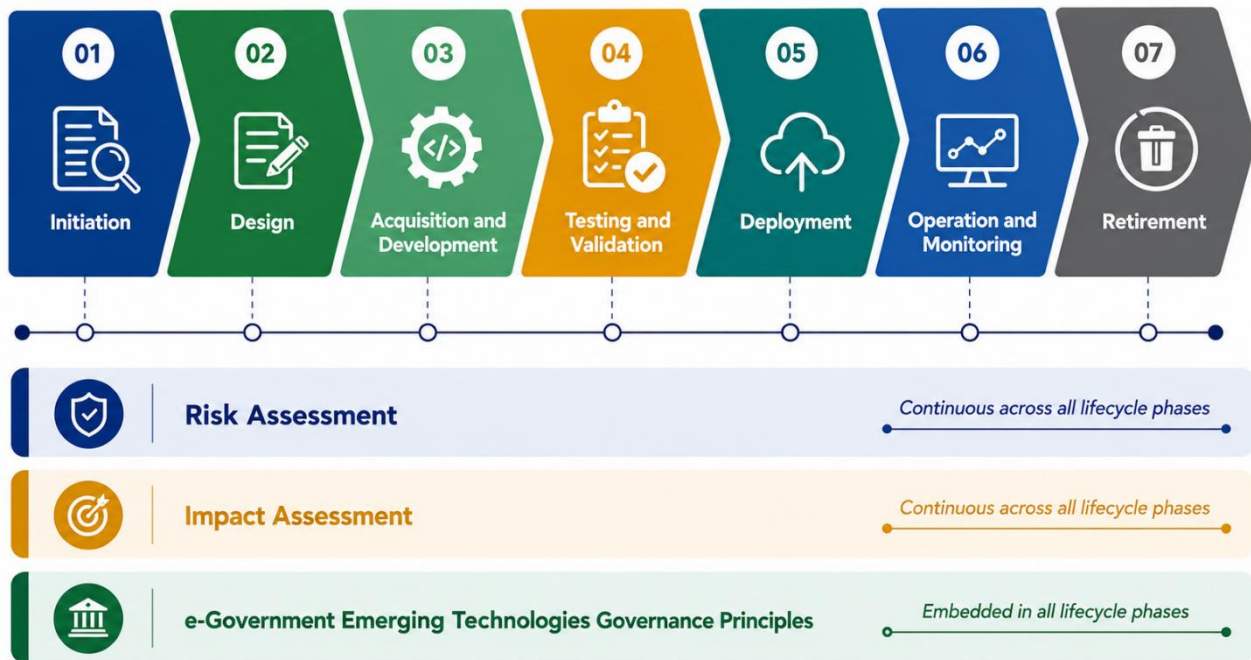


Figure 2: e-Government Emerging Technology Lifecycle Stages

2.3.1 Initiation

- Emerging technology use case shall be identified before its development, acquisition, or operational use;
- The emerging technology use case shall be documented using the template in **Appendix I – Emerging Technology Use Case Template**;
- The emerging technology use case shall be approved by the Institutional ICT Steering Committee;
- The emerging technology use case shall be implemented in alignment with the Standards and Guidelines for Government ICT Project Implementation; and
- Appropriate training shall be provided to personnel involved in the design, development, deployment, management, oversight, and use of emerging technologies.

2.3.2 Design

- i. The suitability of a proposed emerging technology solution shall be assessed before acquisition, development, or operational use;
- ii. The proposed design solution shall be appropriate to the intended function and shall not introduce unnecessary complexity, duplication, and unmanaged dependency;
- iii. A detailed solution design shall be developed and documented for the proposed emerging technology use case, based on its intended purpose, scope, data requirements, integration points, operational context, security requirements, human oversight arrangements and the nature of the solution;
- iv. any adopted emerging technology shall be scalable to accommodate future advancements and interoperable across diverse platforms and vendors.;
- v. Privacy, data protection, cybersecurity, resilience, integration, interoperability, safety, ethical, performance, operational, legal and regulatory requirements shall be considered and incorporated into the design;
- vi. The design shall specify the data required for the use case, including the source, type, sensitivity, volume, quality, lawful basis, access arrangements, retention requirements, and restrictions on further use or sharing; and
- vii. Where the use case involves automated recommendations, automated influence, or automated decision-making, the design shall define the required level of human oversight.

2.3.3 Acquisition and Development

- i. Emerging technology solutions shall be acquired or developed in adherence to e-Government Act, regulations, standards, guidelines and other applicable legal and regulatory requirements;
- ii. Emerging technologies shall be acquired or developed based on approved business requirements and use cases;
- iii. Documentations of acquisition or development activities shall be adequately maintained; and

- iv. Appropriate due diligence shall be conducted on emerging technology solutions, vendors, and service providers to assess their suitability, security, reliability, compliance, and associated risks prior to acquisition, adoption, or deployment.

2.3.4 Testing and Validation

- i. Each emerging technology solution shall be subjected to appropriate testing and validation before deployment into operational use;
- ii. The extent of testing and validation shall be proportionate to the nature, complexity, and risk level of the use case;
- iii. Testing and validation shall address functionality, reliability, security, interoperability, operational readiness, and any other material concern relevant to the intended use of the solution;
- iv. All test scenarios and results shall be properly documented; and
- v. All significant defects, unresolved risks, or material governance concerns identified during testing or validation shall be addressed before deployment or operational use.

2.3.5 Deployment

- i. Emerging technology solution shall be deployed into operational use after appropriate approval;
- ii. Deployment and operational approval shall be based on completion of the required governance, risk, legal, technical, and assurance steps applicable to the use case;
- iii. Deployment shall be phased, piloted, or introduced in a controlled manner, proportionate to the nature of the use case and the operational environment in which it will be used;

2.3.6 Operation and Monitoring

- i. Emerging technology solutions shall be monitored throughout their operational lifecycle;
- ii. Emerging technology solutions shall be monitoring the performance, reliability, governance compliance, security issues, operational incidents, emerging risks, and continued fitness for purpose;

- iii. The continued appropriateness of an emerging technology solution shall be reviewed where there is a material change in its purpose, design, context, data, users, dependencies, or risk profile;
- iv. The operation of emerging technology solutions shall remain subject to oversight and is not treated as self-sustaining once deployed;
- v. Significant incidents, failures, misuse, or breaches, relating to emerging technologies shall be identified and documented; and
- vi. Appropriate records of incidents, responses, lessons identified, and actions taken shall be recorded and maintained.

2.3.7 Retirement

- i. Emerging technology solutions shall be retired, exited, replaced, or decommissioned in a controlled and accountable manner;
- ii. Retirement shall consider data protection, records management, service continuity, contractual obligations, auditability, and any other applicable legal or operational requirement;
- iii. Exit, transition, handover, or disengagement shall be properly governed and documented where an external provider is involved;
- iv. The retirement of an emerging technology solution shall not result in avoidable disruption, unmanaged dependency, loss of records, loss of accountability, or compromise of Government data, information and systems; and
- v. Records of the retired or decommissioned solution shall be retained as may be required by law.

2.4 Emerging Technology Risk Management

Risk management is the foundational governance process that enables public institutions to make informed, responsible, and evidence-based decisions about the adoption and deployment of emerging technologies. For proper governance of emerging technologies:

- i. risk assessment is conducted proportionate to the nature, purpose, context, and possible impact before approving its development, acquisition, deployment or operational use;
- ii. risk assessments shall include technical, cybersecurity, data privacy, ethical, operational, environmental, legal, regulatory and other applicable risks;
- iii. identified risks shall be classified into risk levels as per the Institutional Risk Management Framework;
- iv. regular review of the identified risks shall be performed whenever there is a material change in the design, purpose, deployment context, data, users, operational environment, or dependencies of the use case with approval subject to review;
- v. identified risks shall be managed to an acceptable level to support the safe, effective, and successful implementation of emerging technology use cases; and
- vi. each material risk identified shall be mapped to the corresponding designed mitigation, control, safeguard, or fallback, and any residual risk shall be documented for consideration in subsequent approval and assurance steps.

2.5 Emerging Technology Impact Assessment

- i. Impact assessment shall be performed to assess how the emerging technology's deployment affects individuals, communities, institutions, and society at large across the dimensions such as fairness and non-discrimination, privacy, safety, security, accountability, transparency, explainability and reliability;
- ii. The Impact Assessment shall determine both the positive and negative impacts of the Emerging Technology;
- iii. Impact assessment shall be performed according to the planned intervals or when significant changes are proposed to occur; and
- iv. The result of the impact assessment shall be documented and retained.

2.6 Compliance and Assurance

Emerging Technology solutions shall undergo annual compliance assessment and quality review to verify effectiveness, legal compliance and alignment with institutional goals while driving continuous improvement and accountability.

3 IMPLEMENTATION, REVIEW AND ENFORCEMENT

This framework shall be:

- 3.1 Effective upon being reviewed and approved by the Authority Board of Directors.
- 3.2 Subjected to review at least once every three years or whenever necessary changes are needed.
- 3.3 Consistently complied with, any exceptions to its application must duly be authorized.

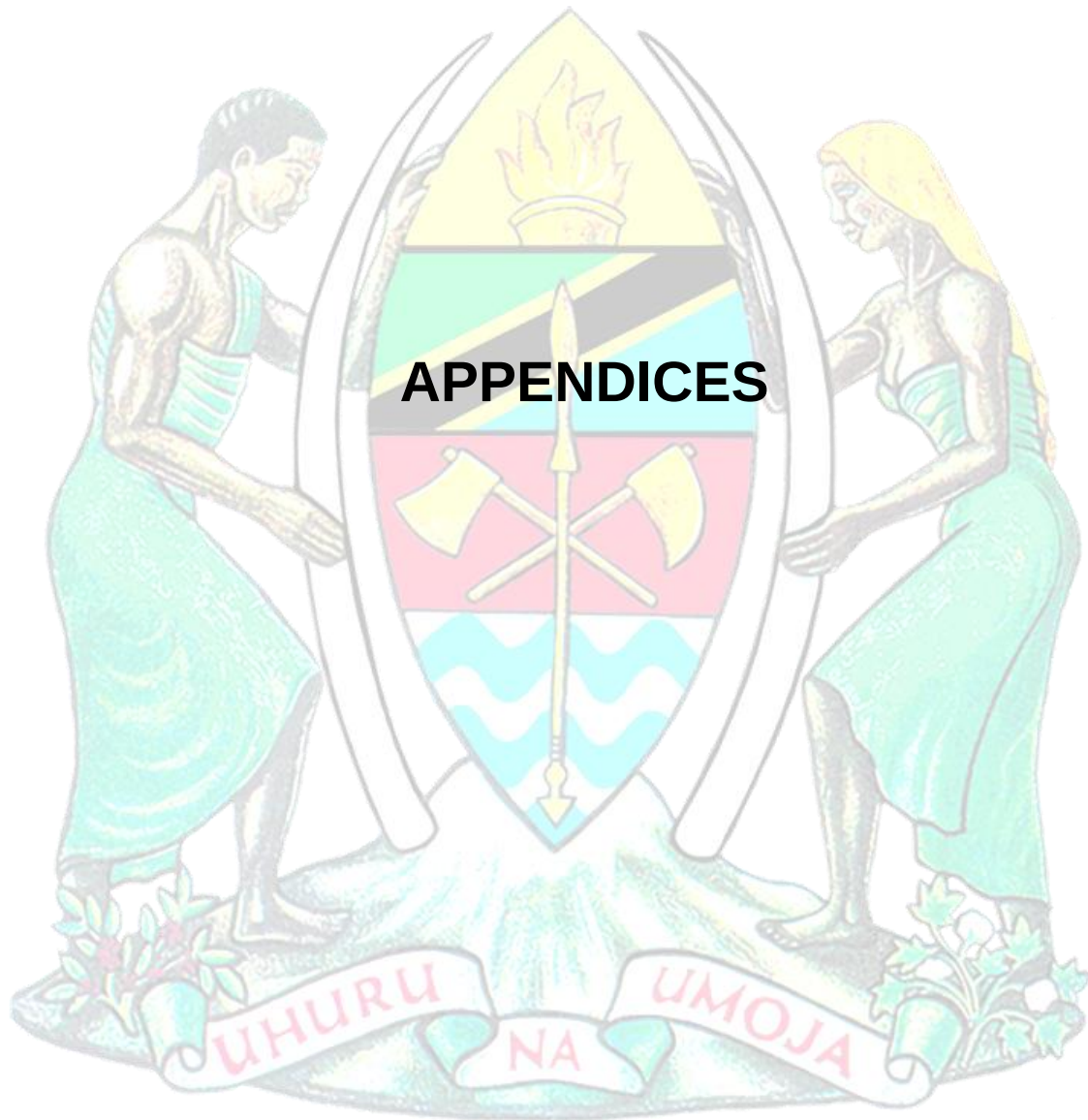
4 RELATED DOCUMENTS

- 1.1. The e-Government Act, Cap.273, R.E.2023;
- 1.2. The e-Government (General) Regulations, GN. No. 75 of 2020 as amended by GN. No. 375 of 2025;
- 1.3. National ICT Policy, 2016;
- 1.4. Tanzania e-Government Strategy, 2022;
- 1.5. e-Government Technology Roadmap, 2024;
- 1.6. UNESCO Tanzania AI Readiness Assessment Report, 2025;
- 1.7. The Personal Data Protection Act, Cap.44, R.E.2023;
- 1.8. Tanzania Development Vision 2050 (Dira 2050);
- 1.9. Tanzania Digital Economy Strategic Framework 2024 – 2034;
- 1.10. UNESCO Recommendation on the Ethics of Artificial Intelligence, 2021;
- 1.11. OECD AI Principles, 2024;
- 1.12. AU Continental AI Strategy, 2024;

- 1.13. e-Government Security Operations Guidelines (eGA/EXT/ISA/004);
- 1.14. e-Government Infrastructure Architecture Standards and Technical guidelines (eGA/EXT/IRA/001);
- 1.15. e-Government Integration Architecture Standards and Technical Guidelines (eGA/EXT/ITA/001);
- 1.16. e-Government Interoperability Framework Standards and Technical Guidelines (eGA/EXT/GIF/001);
- 1.17. e-Government Guidelines, 2017;
- 1.18. Standards and Guidelines for Development, Acquisition, Operation and Maintenance of e-Government Applications (eGA/EXT/APA/005);
- 1.19. Standards and Guidelines for Government ICT Project Management Implementation (eGA/EXT/BSA/008);
- 1.20. Procedures for Government ICT Project Clearance, Monitoring and Closure (eGA/EXT/BSA/009); and
- 1.21. NIST AI Risk Management Framework (AI RMF 1.0), 2023.

5 DOCUMENT CONTROL

Version	Name	Comment	Date
Ver. 1.0	e-GA	Creation of Document	August 2026



Appendix I: Emerging Technology Use Case Template

1. Use Case Basic Information

Item	Details
Public Institution Name	
Department / Unit	
Use Case Title	
Use Case Owner	
Type of Emerging Technology	<<Artificial intelligence / Blockchain/ Internet of Things / Robotics / Virtual or augmented reality / Quantum Computing / Advanced automation / Other>>
Brief Description	<<Briefly explain how you are intending to use the emerging technology. Use simple, clear language, avoiding technical jargon where possible.>>
Problem or Need Addressed	
Expected Benefit	<<State the expected benefit of the use case to the institution and relevant stakeholders>>
Intended Users	<<Expected users of the emerging technology solution>>
Internal Stakeholders	
External Stakeholders	
Services, functions or Processes to be Supported	
Linkage to the Strategic Goal	<< What strategic business goal that this Emerging Technology use case will support >>
Data to be Involved	<< Describe the data to be used and their data sources>>

2. Emerging Technology Profile

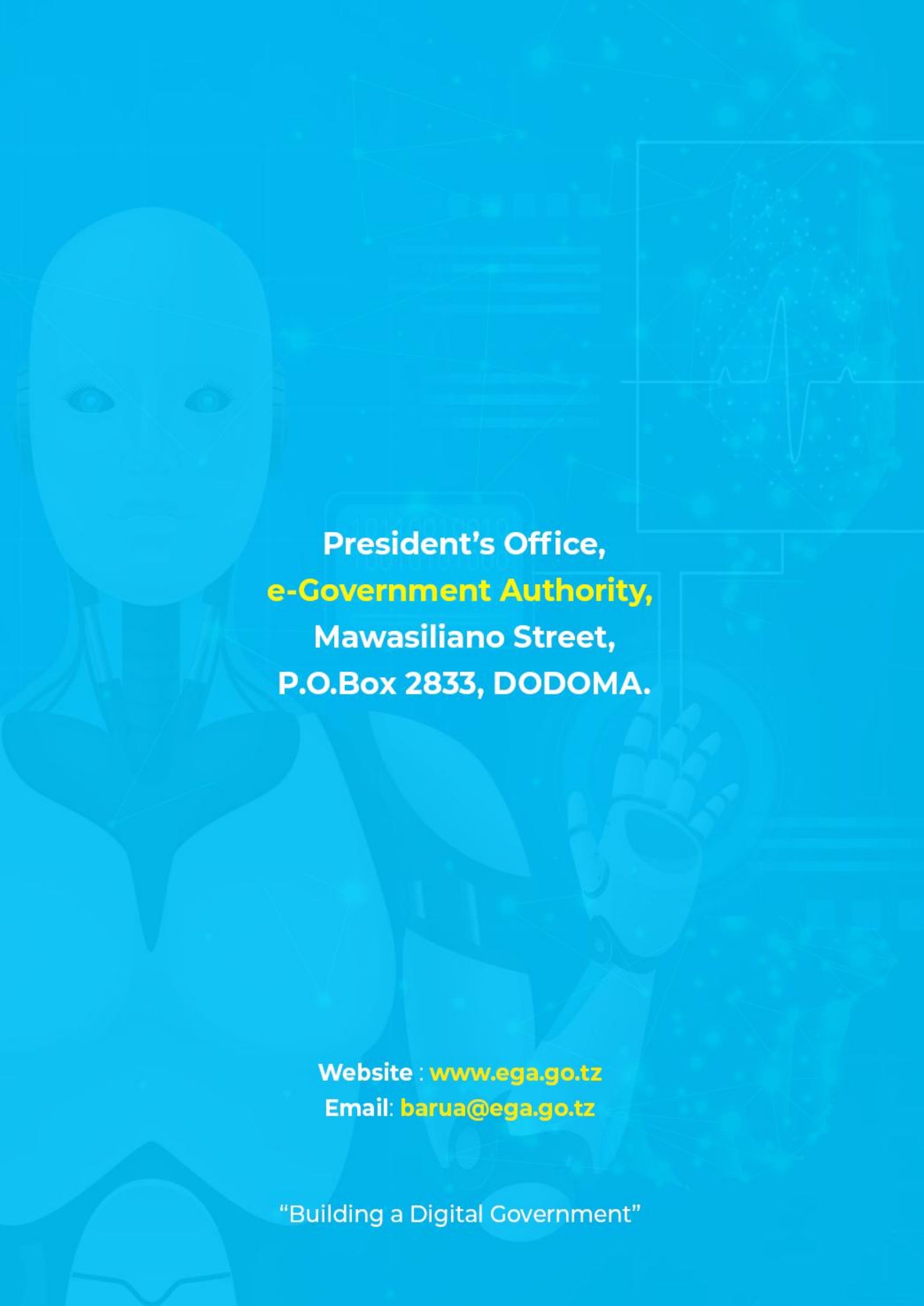
Item	Details
Core Capability	<<Describe the core capability of the emerging technology such as <i>Detection / Verification / Prediction / Automation / Monitoring / Simulation / Tracking / Transaction recording / Recommendation / Decision support / Content generation/ Physical actuation /Distributed Consensus/ Smart Contract/ Immutability/ Other</i> >>
Implementation Mode	<<Inhouse/Outsource Development or Acquired>>
Challenges and Requirements	<<Mention the challenges, limitation and requirements around technology, infrastructure, skills, capability and resources>>
Known Failure Modes	
Out-of-Scope Uses	
Dependencies and Integration Requirements	<<Describe the systems, platforms, infrastructures, data sources, integrations, third party services and technical capabilities required for the successful implementation and operation of the proposed emerging technology use case>>
Hosting / Operating Environment	Government Data Center/On-premise /Off-premise / Other
Justification	<< Briefly outline non emerging technology alternatives that could address the problem described and provide the reasons why the proposed emerging technology will be more appropriate compared to the non-emerging technology alternatives>>

3. Governance, Risk and Compliance Concerns

Area	Concerns	Mitigation Plan
Legal	<<Identify legal concerns with respect to the use case>>	
Ethical	<<Identify ethical concerns with respect to the use case such as biasness, discrimination and non-transparency>>	
Privacy	<<Identify privacy concerns with respect to the use case>>	
Security and Safety	<<Identify security and safety concerns with respect to the use case>>	
Operation	<<Identify operation concerns with respect to the use case>>	

4. Approval Details

Prepared By: Designation: Signature: Date:	Approved By: Designation: Signature: Date:	Approved By: Designation: Signature: Date:
---	---	---



**President's Office,
e-Government Authority,
Mawasiliano Street,
P.O.Box 2833, DODOMA.**

**Website : www.ega.go.tz
Email: barua@ega.go.tz**

"Building a Digital Government"