THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE

e-GOVERNMENT AUTHORITY

ISO 9001:2015 Certified

Document Title

Guidebook for Formulating and Governing Enterprise Architecture in Public Institutions

Document Number

eGA/EXT/AVS/004

Approval	Name	Job Title/ Role	Signature	Date
Approved by	Dr. Mussa M. Kisaka	Board Chairman		31/12/2024

Version: 1.0 – December 2024

PREFACE

Guidebook for Governing and Formulating Enterprise Architecture in Public Institutions is a resource designed to assist organizations in navigating the complex landscape of enterprise architecture (EA) to drive business success and innovation.

In today's rapidly evolving business environment, Public Institutions face increasing demands to align technology with business objectives, optimize operational efficiency, manage risks effectively, and foster innovation. Enterprise architecture serves as a strategic framework that enables public institutions to achieve these goals by providing a holistic view of the enterprise's structure, processes, systems, and technologies.

In that regard, it was apparent for enactment of the e-Government Act No. 10 of 2019 and its subsequent Regulations, 2020, which provide guidance on proper approach for implementing e-Government and establishment of e-Government Authority with mandate of coordinating, promoting and overseeing e-Government implementations as well as enforcing compliance with laws, regulations, standards and guidelines related to e-Government implementations in Public Institutions.

This guidebook is structured to provide a systematic approach to enterprise architecture, covering essential concepts, methodologies, best practices, and practical insights to support architecture practitioners at every phase of their journey. Whether you are establishing a new EA practice, refining existing processes, or seeking to leverage EA to drive digital transformation, this guidebook offers valuable guidance and actionable strategies.

Dr. Mussa M. Kisaka

BOARD CHAIRMAN

ACRONYMS

ADM	Architecture Development Method
ARM	Application Reference Model
BRM	Business Reference Model
BTRA	Business Transformation Readiness Assessment
CSF	Critical Success Factors
DBMS	Database Management System
DevOps	Development Operations
EA	Enterprise Architecture
e-GA	e-Government Authority
ICT	Information and Communication Technologies
ISO	International Organization for Standardization
IT	Information Technology
KPI	Key Performance Indicator
LAN	Local Area Network
MDA	Ministries, Departments and Agencies
PO-PSMGG	President Office – Public Service Management and Good Governance
RAD	Rapid Application Development
SAN	Storage Area Network
SLA	Service Level Agreement
TRM	Technology Reference Model
WAN	Wide Area Network

GLOSSARY

Assumption	A statement of probable fact that has not been fully validated at this stage, due to external constraints.
Business Transformation Readiness Assessment	A technique used for evaluating and quantifying an organization's readiness to undergo change.
Candidate Roadmap Components	An initial, high-level plan that outlines potential projects, initiatives, and activities required to achieve the desired future state of an enterprise's architecture.
Concerns	Are interests in a system relevant to one or more of its stakeholders. Concerns may pertain to any aspect of the system's functioning, development, or operation, including considerations such as performance, reliability, security, distribution, and evolvability and may determine the acceptability of the system.
Constraint	An external factor that prevents an organization from pursuing particular approaches to meet its goals.
Enterprise Architecture	is a strategic approach that organizations use to structure their IT infrastructure and business processes to meet specific goals. It involves the design and management of an organization's overall structure, processes, information technology (IT) systems, and technology infrastructure. Logical organization of a business and its supporting data, applications and IT infrastructure, with clearly defined goals and objectives for the future success of the business.

Data Entity	An encapsulation of data that is recognized by a business domain expert as a thing. Logical data entities can be tied to applications, repositories, and services and may be structured according to implementation considerations.
DevOps	A set of practices for automating the processes between software development and information technology operations teams so that they can build, test, and release software faster and more reliably.
e-Government	The use of information and communication technologies (ICT) by the Government to deliver public services
Principles	These are general rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which an organization sets about fulfilling its mission.
Value Stream	- Designed to create an end-to-end perspective of value from the customer' or stakeholder's perspective. - End to end collection of value-adding activities that create an overall result for a customer, stakeholder or end-user.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 Overview

The e-Government Authority also known as "e-GA" is a public institution established in September, 2019 under the e-Government Act No. 10 of 2019. The Authority is mandated to coordinate, oversee, promote e-Government initiatives and enforce e-Government related policies, laws, regulations, standards and guidelines to public institutions. The Act empowers e-GA to effectively formulate, manage and enforce Public Institutions compliance with e-Government standards and guidelines.

Pursuant to the provisions of Section 3.4.1 of e-Government Guidelines requires public institutions to develop and implement Enterprise Architecture to enable and accelerate development of effective Digital Government within the institution by complying with the e-Government Enterprise Architecture-Technical Standards. Moreover Section 2.3.3 of creation of Government ICT Management Documents-Technical Guide requires Public Institutions to have a minimum of nine (9) documents where among others include Enterprise Architecture that defines the structure and operation of a public institution's IT assets, processes, people, skills and resources in alignment with its business goals and objectives.

Enterprise Architecture is not a one-time exercise but a continuous process assessment, refinement and optimization that should be designed to accommodate future growth, scalability and evolving technologies trends. Therefore, public institutions' Enterprise Architectures should be flexible enough to adopt to the changing business requirements, emerging technologies and market dynamics and thus use this Guidebook for Governing and Formulating Enterprise Architecture.

1.2 Purpose

This Guidebook provides a step-by-step and practical approach for architects and ICT professionals in public institutions towards governing and formulating Enterprise Architecture (EA) that:

i. Aligns ICT with business objectives to promote efficiency and reusability, as visualized in ***Figure 1***;
ii. Enhances governance and compliance of the whole enterprise architecture;
iii. Fosters collaboration, and enables continuous improvement; and

iv. Adaptation to changing business landscapes.

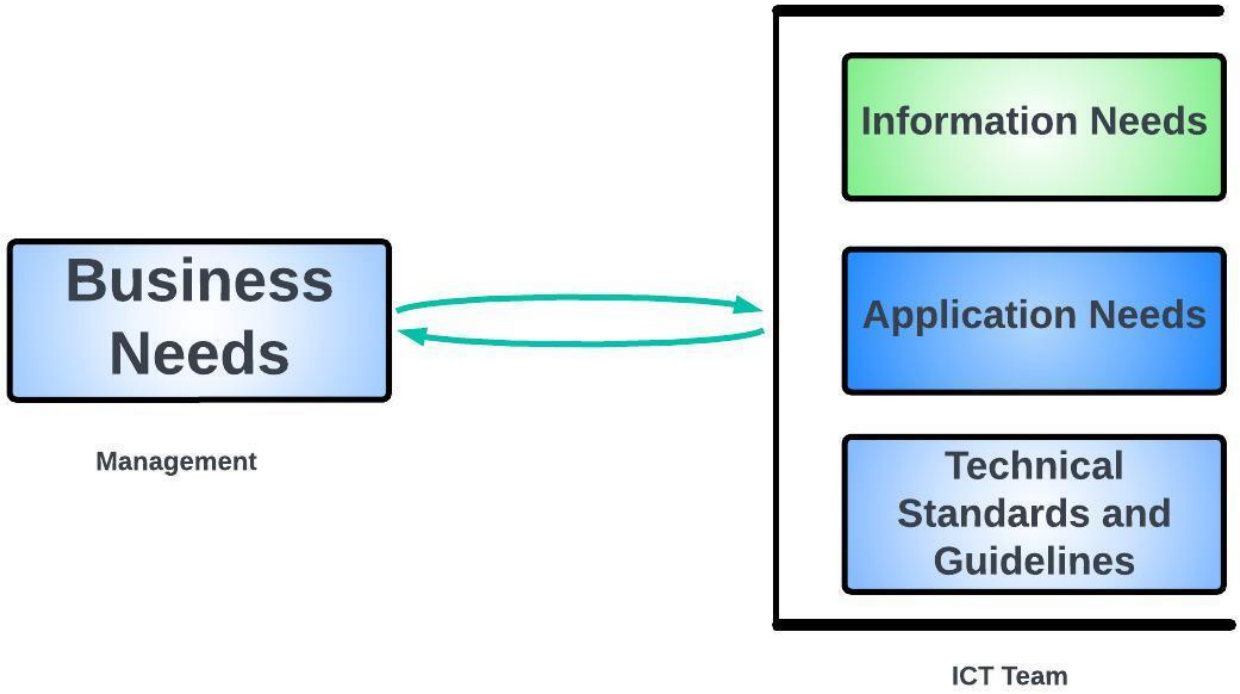


Figure 1 : Aligning Technology with Business

1.3 Rationale

Public Institutions need to align ICT with their business goals and objectives as well as attain better coordination with other Public Institutions' programs and services in order to provide enhanced services to citizens and businesses. Enterprise Architecture will act as the approach and foundation for a citizen-centric, one-stop delivery of government services through a variety of channels. Through Enterprise Architecture, Public Institutions will also benefit from cost savings and/or cost avoidance/ avoiding fragmentation and duplication of efforts by making systems integrate within the government, thus avoiding overlapping of ICT investments.

In a nutshell, a well-developed Enterprise Architecture will serve the following purposes:

- A way to understand what and how public institution operates;
- Models of how operations are undertaken in the public institution;
- Information in a form that helps management make decisions; and
- A way to prevent reinventing the wheel.

The key benefits and expected outcomes of an Enterprise Architecture is summarized in ***Table 1***.

Table 1: Benefits and expected outcomes of an Enterprise Architecture

S/N	Benefits	Outcomes
1.	Captures public institution's mission and business processes in effective and structured manner	Facilitate better planning and decision making
2.	Improve communication between business and ICT groups	Enriches engagement (show interrelationships and dependencies)
3.	Facilitate economies of scale	Sharing common services across public institution
4.	Enhance consistency, accuracy and timeliness of information	Information shared collaboratively across organisation
5.	Provide high level views to communicate complexity of large systems	Understand how different parts (subsystems/ department) work together
6.	Support analysis of alternatives, risks and trade-offs for investment management process to reduce risks	Avoidance of pitfalls: • Building systems that do not meet business needs • Wasting resources on developing duplicated functionality (support re-use)

1.4 Scope

This document shall be used by Public Institutions during governing and formulating Institution's Enterprise Architecture.

2 THE GUIDELINES

This section provides a step-by-step and practical approach for architects and ICT professionals in public institutions towards governing and formulating Enterprise Architecture (EA). ***Figure 2*** is the visualization of the concepts of Enterprise architecture development life circle:

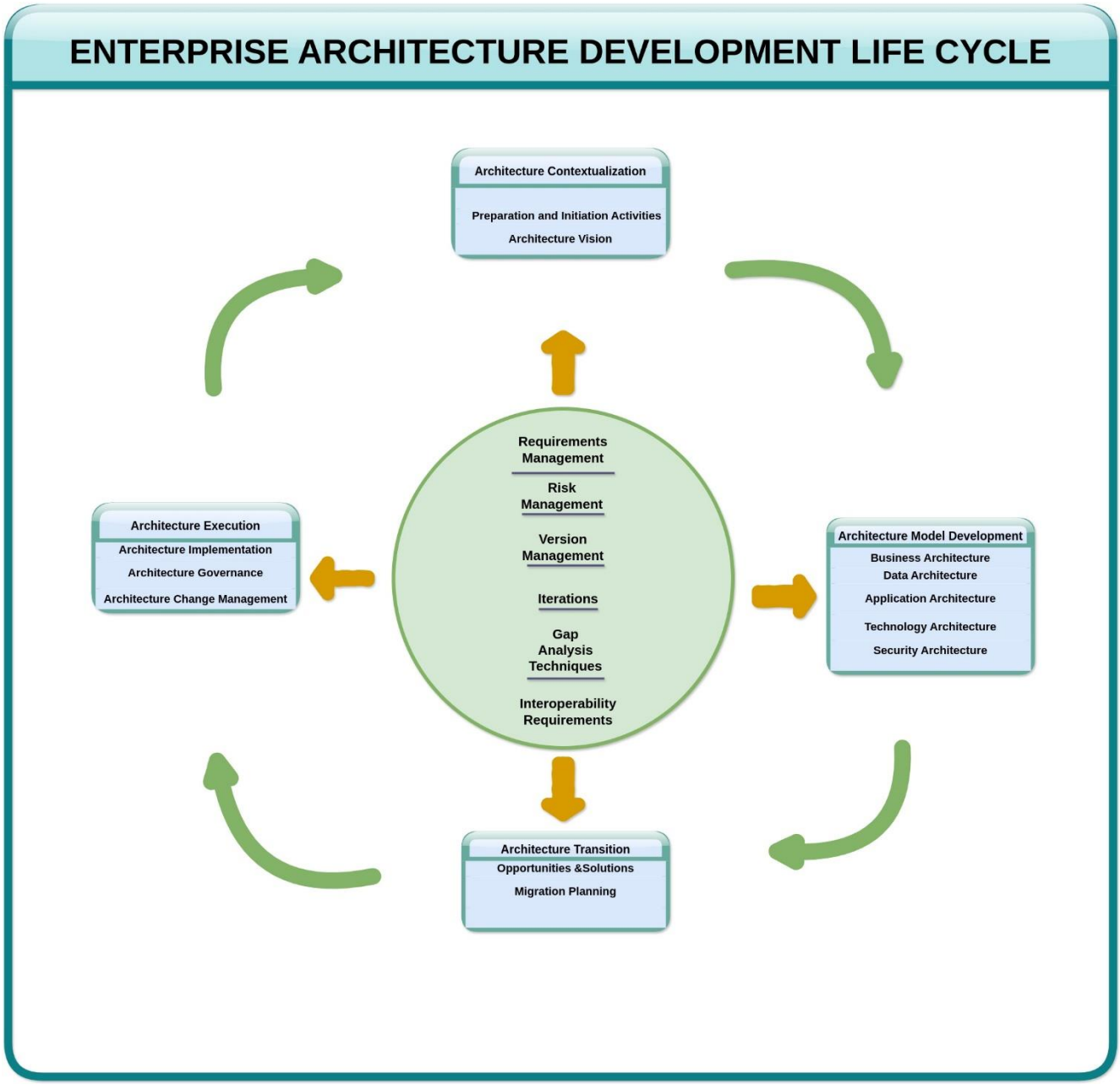


Figure 2 : Visualization of Enterprise Architecture life cycle

In relation to ***Figure 2***, the following are the phases for formulating and governing the enterprise architecture:

A. Architecture Context

i. **Phase 1 - Preparation and Initiation Activities**: This phase focuses on preliminary activities by defining "where, what, why, who, and how we do architecture" of the respective Public Institution;

ii. **Phase 2 - Creation of Architecture Vision**: This phase focuses on providing a high-level aspirational vision of the capabilities and business value to be delivered as a result of the proposed enterprise architecture;

B. Architecture Model Development

iii. **Phase 3 - Development of Business Architecture**: This is a holistic representation of business capabilities, end-to-end value delivery, information and organizational structure along with the relationships to the strategies, products, policies, initiatives, and stakeholders;

iv. **Phase 4 - Development of Data Architecture**: This area focuses on developing data architecture that provide the description of the structure and interaction of the organization's major types and sources of data, logical data assets, physical data assets, and data management resources needed to support the business in a way that can be understood by the stakeholders;

v. **Phase 5 - Development of Application Architecture**: This provides a current applications ecosystem and a blueprint for the individual applications, their interactions, and their relationships to the core business processes and data architecture of the public institution;

vi. **Phase 6 - Development of Technology Architecture**: This phase focuses on developing the technology architecture that provide technology landscape components needed to support the organization's business goals and objectives in a way that addresses stakeholders concerns.

vii. **Phase 7 - Development of Security Architecture**: This phase involves planning and supervising the construction of systems which are free from security threats;

C. Architecture Transition

viii. **Phase 8 - Identification of Opportunities and Solutions**: This phase aims to identify and evaluate programs or projects that can turn the earlier identified target architectures into reality. It identifies opportunities to deliver the target architectures identified in the previous phases, prioritize and sequence programs or projects based on their alignment with business goals and architectural standards and develop an initial implementation and mitigation strategy. Public institutions can ensure that their architecture visions are translated into projects that deliver business value;

ix. **Phase 9 - Migration Planning**: This phase aims to finalize the architecture roadmap and the supporting implementation and migration plan, ensuring that the plan is coordinated with the enterprise's approach to managing and implementing change in the enterprise's overall change portfolio, and that the business value and cost of work packages and transition architectures is understood by key stakeholders;

D. Architecture Implementation

x. **Phase 10 - Architecture Implementation**: This phase focuses on execution of the implementation and migration plan;

xi. **Phase 11 - Architecture Governance**: This phase refers to the set of practices, processes, and mechanisms that ensure the effective management, control, and alignment of institutional architecture activities with its strategic objectives, business goals, policies, standards, and best practices. It provides oversight, decision-making, and accountability to ensure that architectural decisions and implementations are consistent, compliant, and value-driven;

xii. **Phase 12 - Architecture Change Management**: This phase is crucial for ensuring that the architecture continues to meet business needs and objectives over time by managing changes in an organized and controlled manner in line with the architecture governance processes. It establishes and supports the enterprise architecture to provide flexibility to evolve rapidly in response to changes in the technology or business environment.

2.1 General Guidelines

Below are the general guidelines that public institution shall adhere while governing and formulating Enterprise Architecture: -

2.1.1 Institutional Enterprise Architecture Development Guidelines

The Public Institutions shall: -

i. Develop and implement their EA to enable and accelerate the development of effective Digital Government within the Institution by complying with the e-Government Enterprise Architecture – Standards and Technical Guidelines;
ii. Adhere to interoperability standards as defined in e-Government Interoperability Framework – Standards and Technical Guidelines of defining data, application and infrastructure standards;
iii. Adhere to e-Government Technology Roadmap, 2023 – 2027;
iv. When developing the Enterprise Architecture for President's Office – Regional Administration and Local Government (PO -RALG), the EA shall include architecture requirements for Regional Secretariats, Local Government Authorities, Primary Health Facilities and Basic Education Schools;
v. When developing the Enterprise Architecture for the Ministry of Health, the EA shall include architecture requirements for Secondary Health Facilities such as Regional Referral Hospitals (RRHs). Moreover, National, Zonal and Specialized Hospitals shall develop their own Enterprise Architecture based on their business objectives.

2.1.2 Requirements Management

Requirements management is a foundational practice in Enterprise Architecture that bridges the gap between business needs and technical solutions. By effectively managing requirements, Public Institutions can ensure that their architecture decisions are aligned with strategic objectives, deliver tangible business value, and enable agility in response to market dynamics. During requirements management Public Institutions shall:

i. Identify types of requirements that must be met by the architecture in each relevant phase;
ii. When defining requirements, the architect shall consider assumptions for requirements, constraints for requirements, domain-specific principles that drive requirements, policies affecting requirements, standards that requirements must meet, organization guidelines for requirements and specifications for requirements;
iii. Assess and prioritize identified requirements to guide the architecture governing and formulation life cycle and record the decisions related to the requirements;
iv. Create Architecture Requirements Specification that stipulates initial and newly identified requirements and stating measurable criteria to be met during implementation of enterprise architecture as indicated in ***Appendix L-1***.
v. Monitor baseline architecture requirements, identify changed requirements and conduct requirements impact assessment and gap analysis to ensure that requirements that were either removed, added or modified are addressed and documented in the Architecture Requirements Specification, and that the target architecture is revised accordingly; and
vi. Manage requirements throughout architecture governing and formulation life cycle and update the Architecture Requirements Specification accordingly.

2.1.3 Risk Management

In order to effectively manage risks that may occur during governance and formulation of enterprise architecture, ensuring that it remains aligned with the business objectives and resilient to potential threats, Public Institutions shall:

i. Identify, classify and mitigate risks before starting the formulation of enterprise architecture so they are tracked throughout the process;
ii. Collaborate with stakeholders to conduct a comprehensive risk assessment to identify all potential risks related to technology, processes, people and external factors;

iii. Consider two levels of risks namely initial level where risk categorization prior to determining and implementing mitigating actions and residual level of risk where risk categorization after implementation of mitigating actions (if any);

iv. Classify the risks with respect to impact on the organization so that the mitigation of the risks can be executed as expeditiously as possible. Risks can be classified as time (schedule), cost (budget), and scope but they could also include client transformation relationship risks, contractual risks, technological risks, scope and complexity risks, environmental (corporate) risks, personnel risks, and client acceptance risks;

v. Group risks with respect to effect (catastrophic, critical, marginal or negligible) and frequency (frequent, likely, occasional, seldom, unlikely) factors;

vi. Conduct risk impact assessment combining effect and frequency using a heuristically-based but consistent classification scheme for the risks. A potential scheme to assess impact could be as follows Extremely High Risk (E), High Risk (H), Moderate Risk (M) and Low Risk (L);

vii. Document all identified risks, potential impact and proposed mitigation strategies in risk register to be used for decision making and tracking risk mitigation efforts associated with the proposed enterprise architecture as indicated in ***Appendix L-2****;*

viii. Mitigate risks with priority going to frequent high impact risks by identifying, planning and conducting actions that will reduce the risk to an acceptable level;

ix. Re-assess the effect and frequency, recalculate the impacts and see whether the mitigation effort has really made an acceptable difference to obtain residual risk; and

x. Continuously monitor the execution of the mitigation actions to ensure that the enterprise is dealing with residual rather than initial risk.

2.1.4 Version Management

In order to effectively manage versions of enterprise architecture documents during governing and formulation of enterprise architecture as well as streamlining

collaboration among stakeholders and drive alignment between business goals and architecture decisions. Public institutions shall: -

i. Define clear and consistent versioning scheme for the proposed enterprise architecture to track progression from baseline to target architecture. Versioning schemes may include numeric versions such as 0.1 for draft documents and 1.0 for approved documents; and
ii. Maintain a change log that document revisions, updates and modifications made to each version of the enterprise documents and include details such as date of change, its description and the entity responsible for modification

2.1.5 Iterations

Architecture governing and formulation life cycle is an iterative process that evolves over time in response to changing business needs, technological advancements and organizational priorities. Develop enterprise architecture following multiple phases concurrently or cycle between different phases when required. For iterative implementation of enterprise architecture, Public Institutions shall:

i. Consider factors that may influence iterations when formulating enterprise architecture. These factors may include
    a. Order of activities and check points to be carried out through the phases of formulating enterprise architecture;
    b. Level of stakeholder involvement expected within the process;
    c. Number of teams involved and the relationships between different teams;
    d. Maturity of the solution area and the expected amount of re-work and refinement required to arrive at an acceptable solution;
    e. Public institution's attitude to risk; and
    f. Context for development of the enterprise architecture.
ii. Recognize that requirements may evolve over time in response to changing business needs, market conditions or technological advancements; and

iii. Continuously review and update the consolidated requirements to ensure they remain relevant and aligned with the public institution's evolving priorities.

2.1.6 Gap Analysis Technique

Gap analysis is a technique used to compare the current state (baseline architecture) of the enterprise architecture with the desired future state (target architecture) in order to identify gaps, misalignment, deficiencies, and opportunities for improvement. During performing gap analysis, Public Institution shall;

i. Identify domain gaps between the baseline and target architecture by indicating what needs to change. This include what needs to be retained (keep), improved (modify), created (new) and eliminated (redundant or duplicated); and
ii. Perform a comparative analysis between the baseline and target architectures and document the identified gaps with their appropriate recommendations as indicated in the ***Appendix L-3;***

2.1.7 Interoperability Requirements

Defining the degree to which information and services are to be shared is very important, in public institutions. This is a critical aspect of enterprise architecture, ensuring that different systems, applications, and components can work together seamlessly to achieve business objectives. In order to ensure interoperability within the enterprise architecture public institution shall: -

i. Cleary define interoperability requirements to meet the needs of the institution based on below categories: -
    a. Business process or organizational interoperability: which relates to the collaboration between entities in the development, deployment and delivery of e-Government services, and to the interaction between services, and supporting processes;
    b. Information or semantic Interoperability: which relates to ensuring that the exact meaning of information from various applications are understandable by any application even though if the application was not developed for this purpose; and

c. Technical interoperability: which ensure that all the hardware and software components of the network and information system physically communicate and transfer information successfully, and includes key aspects such as open interfaces, interconnection services, data integration and middleware, data presentation and exchange, accessibility and security services.

ii. Ensure security requirements are part of interoperability requirements;

iii. Incorporate interoperability requirements when defining target architectures;

iv. Reconcile interoperability requirements with potential solutions to ensure there are no interoperability conflicts;

v. Conduct interoperability testing across different systems, platforms, and environments to identify and address compatibility issues early during the architecture implementation;

vi. Define compliance criteria and metrics to assess adherence to interoperability standards and ensure consistency with architectural principles and guidelines; and

vii. Continuously monitor the implemented interoperability requirements in relation to emerging technologies trends, and standards related to interoperability and update interoperability practices accordingly.

2.2 Specific Guidelines

2.2.1 Phase 1 - Preparation and Initiation Activities

This phase focuses on preliminary activities by defining "where, what, why, who, and how we do architecture" of the respective Public Institution and preparation of proposal for architecture work. Within this phase, the understanding of the Organization is obtained through identification of core and supporting organization units, identification of impacted internal and external stakeholders and assessment of Enterprise Architecture capability within the Institution.

During the preparation and initiation activities of Enterprise Architecture, Public Institution shall: -

2.2.1.1 Define and Establish Enterprise Architecture Governance Structure and Framework

The following should be considered

i. Assess the enterprise architecture capability within the institution;
ii. Use Institutional ICT Steering Committee to establish an Enterprise Architecture Sub-Committee with its respective roles and responsibilities as specified in ***2.2.1.2 (A)*;**
iii. Use Enterprise Architecture Sub-Committee to establish both enterprise architecture team and extended team with their respective roles and responsibilities as specified in ***2.2.1.2 (B)***;
iv. The Architecture Governance may be structured as depicted in ***Figure 3***;

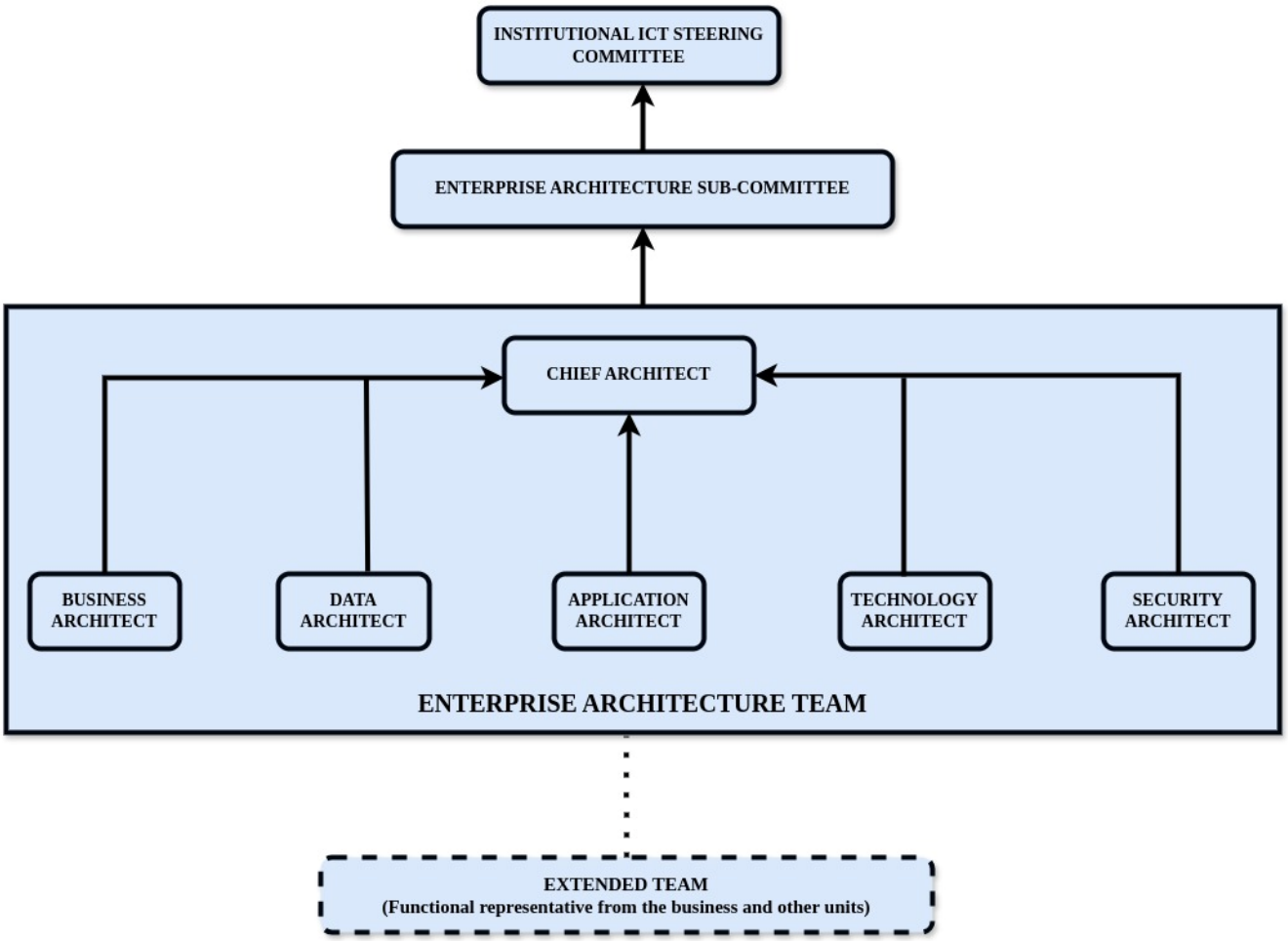


Figure 3 : Architecture Governance Structure

The following are the roles and responsibilities of various parts of the architecture governance**;**

A. Institutional ICT Steering Committee

The Institutional ICT Steering Committee shall be composed of members as outlined in the e-Government Act No. 10, 2019 and Guidelines for Operationalization of Institutional ICT Steering Committee. The Committee shall have the following EA roles and responsibilities: -

i. Provide approval for Architectural work;
ii. Provide senior management guidance and feedback; and
iii. Review and endorse all key EA deliverables.

B. Enterprise Architecture Sub – Committee

This is a sub-committee of Institutional ICT Steering Committee. The Chairperson of the Sub-Committee shall be appointed by the Accounting Officer and the Head/Director of ICT shall provide secretariat to the Sub-committee. The Committee shall have the following EA roles and responsibilities: -

i. Review and provide the basis to the Institutional ICT Steering Committee for all decision making with regards to Enterprise Architecture;
ii. Review Architecture work and request the endorsement to the Institutional ICT Steering Committee;
iii. Define objectives and scope provide access to resources (personnel, information etc.); and
iv. Review all recommendations on EA opportunities, approach and resources.

C. Chief Architect

The Head/Director of ICT of the respective Institution shall serve as Chief Architect. The Chief Architect shall have the following EA roles and responsibilities:

i. Provide technical advice, support and guidance throughout the Enterprise Architecture development and implementation life cycle;
ii. Establish architecture governance and ensure architecture compliance including alignment with organization's business goals, objectives and strategies;
iii. Communicate effectively with stakeholders on Enterprise Architecture benefits, progress, outcomes and results as well as manage stakeholder relationships;
iv. Review and provide inputs and guidance for the EA deliverables developed by the Domain Architects to ensure that deliverables meet required quality standards.

D. Domain Architects

Domain Architects are technical experts with knowledge within the particular domain of their expertise. The domain architects cover areas related to Business, Data, Application, Technology and Security. The Domain Architect shall have the following EA roles and responsibilities: -

i. Provides technical advice, support and guidance in the respective domain of Enterprise Architecture;
ii. Ensure all the stakeholders needs and concerns are addressed and incorporated in the respective domain of Enterprise Architecture;
iii. Develops and maintains architecture in the respective domain of Enterprise Architecture while ensuring its alignment with the overall Enterprise Architecture and submit deliverables to Chief Architect for review, inputs and guidance.

E. EA Stakeholders

These refers to functional representatives from the business and other units. The EA Stakeholders shall have the following EA roles and responsibilities: -

i. Participate in the team meetings, visits and workshops;
ii. Provide operational objectives and surface key challenges;
iii. Provide inputs for current process review;
iv. Review all identified improvement opportunities;
v. Assess feasibility of recommendations in actual operational context.

GENERAL ARCHITECTURE GOVERNANCE BEST PRACTICES

The following should be considered: -

i. Defining governance objectives, scope, and responsibilities;
ii. Establishing governance structures, roles, and decision-making authorities;
iii. Developing governance policies, standards, and guidelines;
iv. Conducting architecture reviews, assessments, and audits;

v. Monitoring compliance with governance requirements and addressing non-compliance issues; and
vi. Continuously improving governance practices based on feedback and lessons learned.

2.2.1.2 Determine Constraints on Enterprise Architecture work

The following should be considered: -

i. Define the constraints that must be dealt with, including organization constraints, financial constraints, business constraints and external dependences constraints; and
ii. Identified constraints should contain likelihood, severity and mitigation strategies.

2.2.1.3 Define Architecture Principles

The following should be considered

i. Define architecture principles that are appropriate to the Public Institution;
ii. Should be expressed in the language that business understand and uses;
iii. Architecture principles should be few in number, future oriented, endorsed and championed by senior management;
iv. Define architecture principles with respect to each architecture domain such as business, data, application, technology and security;
v. Architecture principles should have the following qualities: -
    a. **Understandable:** The underlying tenets can be quickly grasped and understood by individuals throughout the organization. The intention of the principle is clear and unambiguous, so that violations, whether intentional or not, are minimized;
    b. **Robust:** enable good quality decisions about architectures and plans to be made, and enforceable policies and standards to be created. Each principle should be sufficiently definitive and precise to support consistent decision making in complex, potentially controversial situations;

c. **Complete:** Every potentially important principle governing the management of information and technology for the organization is defined — the principles cover every situation perceived;

d. **Consistent:** Strict adherence to one principle may require loose interpretation of another principle. The set of principles must be expressed in a way that allows a balance of interpretations. Principles should not be contradictory to the point where adhering to one principle would violate the spirit of another. Every word in a principal statement should be carefully chosen to allow consistent yet flexible interpretation;

e. **Stable:** Principles should be enduring, yet able to accommodate changes. An amendment process should be established for adding, removing, or altering principles after they are ratified initially.

vi. Identified principles should contain components such as reference number, name, statement, rationale and implications as shown on ***Table 2***.

Table 2: Components of principles

Reference number	This is the number that uniquely identifies the specified architecture principle.
Name	i. Should both represent the essence of the rule as well as be easy to remember; ii. Specific technology platforms should not be mentioned in the name or statement of a principle; iii. Avoid ambiguous words in the Name and in the Statement such as: "support", "open", "consider", and for lack of good measure the word "avoid", itself, be careful with "management", and look for unnecessary adjectives and adverbs (fluff).

Statement	Should succinctly and unambiguously communicate the fundamental rule. For the most part, the principles statements for managing information are similar from one organization to the next. It is vital that the principles statement is unambiguous.
Rationale	i. Should highlight the business benefits of adhering to the principle, using business terminology. ii. Point to the similarity of information and technology principles to the principles governing business operations. Also describe the relationship to other principles, and the intentions regarding a balanced interpretation. iii. Describe situations where one principle would be given precedence or carry more weight than another for making a decision.
Implications	i. Should highlight the requirements, both for the business and IT, for carrying out the principle in terms of resources, costs, and activities/tasks. It will often be apparent that current systems, standards, or practices would be incongruent with the principle upon adoption. ii. The impact to the business and consequences of adopting a principle should be clearly stated. iii. The reader should readily discern the answer to: "How does this affect me?". iv. It is important not to oversimplify, trivialize, or judge the merit of the impact. Some of the

	implications will be identified as potential impacts only, and may be speculative rather than fully analyzed.

2.2.1.4 Develop a Budget Plan and Time Scale

i. Assess budget requirements and prepare budget plan; and
ii. Identify the timeline for completing enterprise architecture work.

2.2.1.5 Prepare Proposal and Obtain Approval for Architecture Work

i. Consolidate the outputs from steps above into a proposal document for undertaking the architecture work as specified in ***Appendix A-1*** and submit to ICT Steering Committee; and
ii. Obtain endorsement for starting execution of architecture work from the ICT Steering Committee.

2.2.1.6 Deliverables

The deliverable for this phase is approved proposal for Architecture work.

2.2.2 Phase 2 - Creation of Architecture Vision

This phase focuses on providing a high-level aspirational vision of the capabilities and business value to be delivered as a result of the proposed enterprise architecture.

2.2.2.1 Initiate Architecture Work

i. Conduct kick-off engagement with relevant stakeholders to mark the beginning of the architecture work;
ii. Collect and make use of pre-existing documents which includes: proposal document for architecture work, organization goals, business principles, business goals, business drivers, institution strategy and ICT strategy; and
iii. Confirm and elaborate architecture principles including business principles.

2.2.2.2 Identify Stakeholders and Concerns

i. Identify stakeholders into the following stakeholder categories namely management, core business units, supporting units, suppliers, regulatory bodies, clients and other external entities as indicated in ***Appendix B-1***;

ii. Classify the identified stakeholders to determine their engagement based on their power, influence and interest as indicated in ***Appendix B-1***. The classification can be mapped into a power /interest matrix as show in the ***Figure 4***;

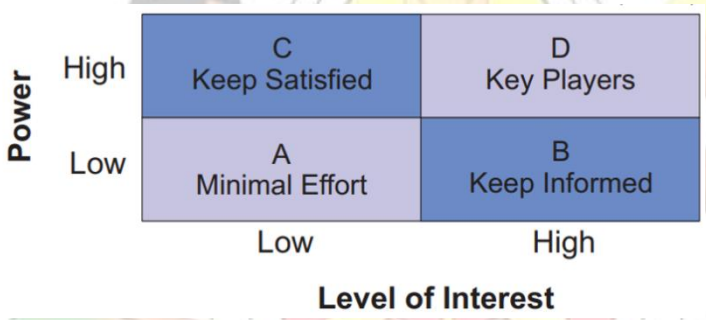


Figure 4 : Level of Interest

iii. Document concerns as expressed by the respective stakeholders' categories regarding architecture work as indicated in ***Appendix B-1***; and

iv. Create a plan showing how each stakeholder group will be engaged. The plan should include communication channel, frequency of interaction and communication objectives ***Appendix B-2***.

2.2.2.3 Identify Business Goals, Drivers and Constraints

i. Identify the business goals and strategic drivers of the organization;

ii. Determine constraints that must be dealt with during the architecture work. These constraints may be newly identified or originated from the proposal of architecture work; and

iii. Ensure the goals, drivers and constraints are current and non-ambiguous.

2.2.2.4 Assess Business Transformation Readiness

i. Assess the capability of Public Institution to undertake architecture work in areas such as information, process, resources and tools;
ii. Assess the organization preparedness towards undertaking business transformation. The assessment involves readiness factors such as vision, desire, willingness and resolve, need, business case, funding, sponsorship and leadership, governance, accountability, ICT capacity to execute, enterprise capacity to execute and enterprise to implement and operate;
iii. The readiness assessment should be jointly performed by business and ICT staff;
iv. Assess the risk for each readiness factor and improvement action to mitigate the risk identified;
v. Identify, classify and mitigate risks associated with business transformation;
vi. Identify the assumptions to be taken into consideration to attain target architecture; and
vii. The results of readiness assessment should be added to a business transformation readiness assessment report.

2.2.2.5 Define Architecture Scope

This area focuses on defining the boundaries of baseline architecture and target architecture;

i. Identify departments, units, branches and sectors impacted by the Architecture work;
ii. Identify and define level of details required based on the intended use of enterprise architecture. The level of details includes analysis of business process, organization structure, strategy, capability and performance metrics;
iii. Ensure enterprise architecture contain minimum of five domains namely; business architecture, data architecture, application architecture, technology and security architecture; and
iv. Determine time period required to reach the desired target Architecture.

2.2.2.6 Define Expected Outcomes

i. Review and agree the benefits of successful implementation of the enterprise architecture; and
ii. Define the performance metrics and measures to meet business needs.

2.2.2.7 Define Architecture Vision Statement

i. Based on stakeholder concerns, capability, requirements, scope, constraints, principles and business goals write a summary vision statement that effectively communicate the target state of proposed enterprise architecture;
ii. Ensure the vision statement is clear and concise understandable to all stakeholders with no technical jargons; and
iii. Validate the vision statement with all key stakeholders.

2.2.2.8 Deliverables

The deliverables for this phase are: -

i. Stakeholders map;
ii. Stakeholder engagement plan;
iii. Business requirements;
iv. Business transformation readiness assessment report; and
v. Architecture vision statement.

2.2.3 Phase 3 - Development of Business Architecture

Business architecture is a holistic representation of business capabilities, end-to-end value delivery, information and organizational structure along with the relationships to the strategies, products, policies, initiatives, and stakeholders.

Business Architecture captures the architectural models of business operation, looking specifically at factors that motivate the public institution, how the public institution is structured, and also what business capabilities the public institution has. The business architecture needs to support the agreed architecture vision. During development of Business Architecture, Public Institutions shall:

2.2.3.1 Initiate Development of Business Architecture

i. Collect and review pre-existing documents related to business which includes proposal for architecture work, business goals, business drivers, business strategies, ICT Strategies and business requirements;
ii. Document business architecture objectives;
iii. Review and validate business architecture related principles from the proposal for architecture work or establish new principles if necessary;
iv. Document the business architecture principles in the business architecture section. Examples of business architecture principles are such as Maximize Benefit to the Enterprise, Business Continuity, Common Use Applications, Service Orientation, Compliance with Law, and IT Responsibility as detailed in ***Table*** ; and
v. Utilize the business architecture principles during the development of the business architecture.

Table 3: Examples of Business Architecture Principles

Principle #B1	**Maximize Benefit to the Enterprise**
Statement	Information management decisions are made to provide maximum benefit to the enterprise as a whole.
Rationale	This principle embodies "service above self". Decisions made from an enterprise-wide perspective have greater long-term value than decisions made from any particular organizational perspective. Maximum return on investment requires information management decisions to adhere to enterprise-wide drivers and priorities. No minority group will detract from the benefit of the whole. However, this principle will not preclude any minority group from getting its job done.
Implications	i. Achieving maximum enterprise-wide benefit will require changes in the way we plan and manage information — technology alone will not bring about this change; and ii. Some organizations may have to concede their own preferences for the greater benefit of the entire enterprise.

Principle #B2	**Business Continuity**
Statement	Enterprise operations are maintained in spite of system interruptions
Rationale	As system operations become more pervasive, we become more dependent on them; therefore, we must consider the reliability of such systems throughout their design and use. Business premises throughout the enterprise must be provided with the capability to continue their business functions regardless of external events. Hardware failure, natural disasters, and data corruption should not be allowed to disrupt or stop enterprise activities. The enterprise business functions must be capable of operating on alternative information delivery mechanisms.
Implications	i. Dependency on shared system applications mandates that the risks of business interruption must be established in advance and managed. Management includes but is not limited to periodic reviews, testing for vulnerability and exposure, or designing mission-critical services to ensure business function continuity through redundant or alternative capabilities; ii. Recoverability, redundancy, and maintainability should be addressed at the time of design; iii. Applications must be assessed for criticality and impact on the enterprise mission, in order to determine what level of continuity is required and what corresponding recovery plan is necessary.
Principle #B3	**Common Use Applications**
Statement	Development of applications used across the enterprise is preferred over the development of similar or duplicative applications which are only provided to a particular organization.
Rationale	Duplicative capability is expensive and proliferates conflicting data.

Implications	i. Organizations which depend on a capability which does not serve the entire enterprise must change over to the replacement enterprise-wide capability; this will require establishment of and adherence to a policy requiring this; ii. Organizations will not be allowed to develop capabilities for their own use which are similar/duplicative of enterprise-wide capabilities; in this way, expenditures of scarce resources to develop essentially the same capability in marginally different ways will be reduced; iii. Data and information used to support enterprise decision-making will be standardized to a much greater extent than previously. This is because the smaller, organizational capabilities which produced different data (which was not shared among other organizations) will be replaced by enterprise-wide capabilities. The impetus for adding to the set of enterprise-wide capabilities may well come from an organization making a convincing case for the value of the data/information previously produced by its organizational capability, but the resulting capability will become part of the enterprise-wide system, and the data it produces will be shared across the enterprise.

2.2.3.2 Define Organization Vision, Mission and Objectives

Define organization vision, mission and objectives as described in other pre-existing documents such as organization strategy.

2.2.3.3 Define Organization Structure and Organization Map

i. Define the organizational structure of the business depicting business units and the decomposition of those units into lower-level functions;
ii. Define the organization map showing key organization units, partners and stakeholder groups that make up the enterprise ecosystem as illustrated in ***Appendix C-1***; and

iii. Ensure the organization map depict working relationship and interaction between the entities.

2.2.3.4 Describe the Organization Business Functions and Services

i. Describe the organization core business functions, and organization-wide support functions;
ii. Decompose the major business functions into their respective sub-functions; and
iii. Describe the services that the organization provides to its clients, both internally and externally.

2.2.3.5 Describe the Organization Value Stream

The primary reason that an organization exist is to provide value to one or more stakeholders. This step includes the ability to decompose the creation, capture and delivery of value into discrete stages of value-producing activities, each of which is enabled by the effective application of business capabilities. The Public Institution shall:

i. Identify the list of value-adding activities. The values-adding activities are represented by value stream stages, each of which creates and adds incremental stakeholder value from one stage to the next;
ii. Ensure that value is defined from the perspective of the stakeholder i.e. the customer, end-user or recipient of the product, service or deliverable produced by the work;
iii. Describe a value stream as illustrated in ***Appendix C-2*** using the following elements:
    a. **Name** - The value stream name must be clearly understandable from the initiating stakeholder's perspective. Value streams use an active rather than passive tense with a verb-noun construct. For example, "Acquire Retail Product" and "Recruit Employee";
    b. **Description** – A short and precise description to provide additional clarity on the scope of activities that the value stream deals with;

c. **Stakeholder** - The person or role that initiates or triggers the value stream; and

d. **Value** – The value that the stakeholders expects to receive upon successful completion of the value stream.

iv. Decompose a value stream into a sequence of value-creating stages as illustrated in ***Appendix C-3*** using the following elements;

a. **Name** – Two to three words identifying what is or will be achieved by this stage;

b. **Description** – A few sentences explaining the purpose and the activities performed during the value stream stage;

c. **Stakeholders** – Actors who receive measurable value from the value stream stage or who contribute to creating or delivering that value;

d. **Entrance Criteria** – The starting condition or state change that either trigger the value stream stage or enables it to be activated;

e. **Exit Criteria** – The end state condition that denotes the completion of the value stream stage i.e. when the required value has been created or delivered to the stakeholders. This information becomes the entry criteria for the next value stream stage; and

f. **Value Item** – The incremental value that is created or delivered to the participating stakeholder(s) by the value stream stage.

v. Draw a value stream diagram as illustrated in ***Appendix C-4***; and

vi. Map capabilities to value stream stages. Identify which business capabilities are required to enable each value stream stage and create a Value Stream Map as illustrated in ***Appendix C-5***.

2.2.3.6 Define Business Reference Model

Business Reference Model (BRM) is a functional framework focusing on providing an organized, tiered hierarchical construct representing the business functions of the Public Institutions. It provides a functional view identifying common business capabilities across the Public Institution required to provide services to internal and external stakeholders. During creation of BRM, the Public Institution shall:

i. Ensure that the BRM contains the following components:
    a. Business Areas – describing the functionality and activities surrounding the operations of the Public Institution. Example of business areas can be core functions and supporting functions;
    b. Line of Business – These are functions within respective business areas; and
    c. Sub-functions under each line of business – relating to the business capabilities under each line of business.
ii. Represent the BRM using diagram as illustrated in ***Appendix C-6***.

2.2.3.7 Group Stakeholder Concerns with Respect to Business Functions

Select and consolidate stakeholders' concerns that need to be addressed in relation to the business functions.

2.2.3.8 Develop Baseline Business Architecture Description

i. Develop a baseline description using textual or graphical description;
ii. Use process flow diagrams to show the baseline sequential flow of business processes;
iii. Use business service/information diagram as illustrated in ***Appendix C-7*** to show the information needed to support one or more business services; and
iv. Identify the challenges affecting the business functions and processes.

2.2.3.9 Develop Target Business Architecture Description

i. Develop target description using textual or graphical description;
ii. Use process flow diagrams to show the target sequential flow of business processes;
iii. Use business service/information diagram to show the target information needed to support one or more business services; and
iv. Ensure the documented target architecture support the architecture vision and addresses the stakeholder's concerns and identified challenges.

2.2.3.10 Perform Gap Analysis

Gap analysis shall be performed based on steps specified on Section 2.1.5 of this document and document the results as illustrated in ***Appendix L-3.***

2.2.3.11 Finalize the Business Architecture

i. Conduct final cross-check on the business architecture documentation's completeness, accuracy, and alignment with feedbacks received from stakeholders and any changes made during the review process; and
ii. Prepare final versions of architecture deliverables, including architectural diagrams, models, descriptions, views, and other documentation that collectively describe the business architecture.

2.2.3.12 Deliverables

i. Business architecture principles;
ii. Organization map;
iii. Value stream map;
iv. Detailed baseline business architecture;
v. Detailed target business architecture; and
vi. Gap analysis results.

2.2.4 Phase 4 - Development of Data Architecture

This area focuses on developing data architecture that provide the description of the structure and interaction of the organization's major types and sources of data, logical data assets, physical data assets, and data management resources needed to support the business.

2.2.4.1 Initiate Development of Data Architecture

Data owners need to be identified to be responsible for common data definition, ensuring data integrity and protecting data from misuse and destruction.

i. Data capture, modeling and analysis of key data entities that will address stakeholders' concerns. These tools and techniques to be used include entity relationship diagram and class diagram;
ii. Collect and make use of pre-existing resources which includes: business architecture, organization goals, architecture principles, institutional

data dictionary if exist, architecture vision, business goals, business drivers, institution strategy and ICT strategy; and

iii. Document data architecture objectives.

2.2.4.2 Review and Confirm Data Architecture Principles

i. Review and confirm the data architecture principles that have been documented in the proposal for architecture work;

ii. Document the data architecture principles in the data architecture section. examples of data architecture principles are: Data is an Asset; Data is Accessible and Data Secured as shown in ***Table*** ; and

iii. Utilize the business architecture principles during the development of the Data Architecture.

Table 4: Examples of Data Architecture Principles

Principle # D1	Data is an Asset
Statement:	Data is an asset that has value to the Institution and is managed accordingly.
Implications:	Stewards must have the authority and means to manage the data for which they are accountable.
Rationale:	Data is the foundation of our decision-making, so we must also carefully manage data to ensure that we know where it is, can rely upon its accuracy, and can obtain it when and where we need it.
Principle # 2	Data is Shareable
Statement:	Users have access to the data necessary to perform their duties; therefore, data is shared across the Authority and Government.
Rationale:	Institution data will be made readily available and accessible in real time to prevent delay of the business processes and enable appropriate timely sharing across the organization.
Implications:	i. Institutional Data Dictionary and Policy to be created and ii. Institution will leverage on the Data Reference Model to define data catalog (a schema that contains the data entities and their definitions), a meta-data model (a schema that defines relationship between the data entities) and a meta-data store (an electronic repository to store it).

Principle # 3	Data Security
Statement:	Data is protected from unauthorized use and disclosure.
Implications:	i. Security must be designed into data elements from the beginning. ii. In order to adequately provide access to open information while maintaining secure information, security needs must be identified and developed at the data level, not the application level
Rationale:	i. Information must be protected to avoid unwarranted speculation, misinterpretation, and inappropriate use. ii. Open sharing of information and the release of information via relevant legislation must be balanced against the need to restrict the availability of classified, proprietary, and sensitive information.

2.2.4.3 Define Data Reference Model (DRM)

The Data Reference Model (DRM) provides a structure that facilitates the development of data that can be effectively shared across Public Institutions for better and more effective service delivery, improved decision making and improved mission performance. The DRM is a service-oriented model that provides the pathway for "services to stakeholders" to become operational. At the same time, the DRM provides motivation for Public Institutions to better understand their data, how it fits in the total empire of Government information design Data Reference Model (DRM) as stipulated in ***Appendix D-1***.

2.2.4.4 Develop Baseline Data Architecture Description

i. Define baseline institutional metadata standards;
ii. Identify and document components of the existing data architecture required by business function, services and application e.g., data entities and data sources;
iii. Identify the assumptions that have been used to document components of the existing data architecture;
iv. Draw baseline ERD as stipulated in ***Appendix D-2***; and
v. Develop baseline Data Entity/Business Function matrices showing which data supports which functions and which business function owns which data as stipulated in **APPENDIX-D3**; and
vi. Identify the challenges affecting baseline data architecture.

2.2.4.5 Develop Target Data Architecture Description

i. Define target institutional metadata standards;
ii. Identify and document components of the target data architecture required by business function, services and application e.g., data entities and data sources;
iii. Identify the assumptions that have been used to document components of the target data architecture;
iv. Draw target ERD as stipulated in ***Appendix D-2****;* and
v. Develop target Data Entity/Business Function matrices showing which data supports which functions and which business function owns which data as stipulated in ***Appendix D-3***.

2.2.4.6 Perform Gap Analysis

Gap analysis shall be performed based on steps specified on Section 2.1.5 of this document and document the results as illustrated in ***Appendix L-3.***

2.2.4.7 Finalize the Data Architecture

i. Conduct final cross-check on the data architecture documentation's completeness, accuracy, and alignment with feedbacks received from stakeholders and any changes made during the review process; and
ii. Prepare final versions of architecture deliverables, including architectural diagrams, models, descriptions, views, and other documentation that collectively describe the data architecture.

2.2.4.8 Deliverables

The deliverables for this phase are: -

i. Data architecture principles;
ii. Detailed baseline data architecture;
iii. Detailed target data architecture; and
iv. Gap analysis results.

2.2.5 Phase 5 - Development of Application Architecture

This phase focuses on crafting the application architecture, which outlines landscape and desired structures and interactions of the institution's ICT systems while

addressing stakeholders' concerns and aligning with institution's goals and objectives.

During the development of application architecture public institution shall: -

2.2.5.1 Initiate Development of Application Architecture

i. Review and validate application architecture related principles such Design of user-centric applications, use of open standards and Data driven from the proposal for architecture work as depicted in ***Table*** or establish new principles, if necessary;
ii. Identify and select relevant application architecture stakeholders' concerns and requirements; and
iii. Document application architecture objectives.

Table 5: Examples of Application Architecture Principles

Principle # A1	**Design of User-Centric Applications**
Statement	Applications should prioritize the needs, preferences, and experiences of users in their design and development processes.
Rationale	i. By focusing on users' needs and preferences, user-centric applications aim to deliver intuitive and engaging user experiences. This can lead to increased user satisfaction, retention, and loyalty. ii. User-centric design emphasizes simplicity, clarity, and ease of use. Applications are designed with user-friendly interfaces and workflows, reducing cognitive load and making it easier for users to accomplish tasks efficiently.
Implications	Users should be involved and engaged in defining their systems requirements based on the established business processes, rules and guidelines.

Principle # A2	**Use of Open Standards**
Statement	Whenever possible, solutions should use or adopt open standards, open-source tools, and open innovations and generate open data.
Rationale	i. To use open standards to reduce technology lock-in and promote sustainability of solutions. ii. To facilitate flexibility and adaptability by enabling organizations to easily integrate new technologies, upgrade existing systems, and scale their operations.
Implications	iii. Solutions should adopt and expand on existing open standards that have been developed, agreed upon, adopted, and maintained by a global community to enable the sharing of data across tools and systems. iv. Should develop modular, interoperable approaches instead of standalone ones, to ensure the ability to adopt and build on components from other software developers or existing applications and the ability of other institutions to perform reciprocal processes in the future
Principle # A3	**Data Driven**
Statement	Application systems should provide the correct information (data) available at the right time and place
Rationale	By leveraging data-driven approaches, application architecture decisions can be grounded in empirical evidence rather than subjective opinions. This leads to more informed, objective decision-making processes that are aligned with business goals and user needs.

Implication	i. Data-driven architectures must be able to handle large volumes of data efficiently. ii. Should use high-quality real-time or timely data to support rapid decision-making, improve programs, and inform strategy. iii. Should integrate data from multiple sources, such as internal databases, third-party APIs, or IoT devices. iv. Should support advanced analytics and machine learning capabilities to derive actionable insights from data v. Should address challenges related to data quality, consistency, and cleanliness.

2.2.5.2 Develop Application Reference Model

Application Reference Model (ARM) is a functional framework focusing on providing an organized, tiered hierarchical construct representing the application functions within the Public Institutions. It provides a logical group of ICT service capabilities (Application/ Service Components) to support the re-use of business components and services across the Public Institutions. During creation of ARM, Public Institution shall: -

i. Prepare ARM which contains the following components:
    a. **Service Domain**: Provides a high-level view of the services and capabilities that support business processes and applications.
    b. **Service Type**: Further sub-categorizes which defines the capabilities of each domain. It defines the business context of a specific service component within a given domain.
    c. **Service Component**: Provides the components to deliver the services and capabilities to the business.
ii. Ensure that the ARM is composed of the following four (4) service domains;
    a. Operational services;
    b. Business support services;

c. Service integration; and
d. Enabling system support services.

iii. Draw the ARM considering the above components as depicted in ***Appendix E-1***.

2.2.5.3 Develop Baseline Application Architecture

i. Prepare a list of existing applications, with their appropriate business functions as indicated in ***Appendix* E-2**;
ii. Prepare graphical representation of the current application ecosystem as depicted in ***Appendix E-3****;* and
iii. Identify and document challenges in baseline architecture.

2.2.5.4 Develop Target Application Architecture

i. Prepare a description for target applications and a catalog of applications with their corresponding desired business functions as indicated in ***Appendix E-2***; and
ii. Prepare graphical representation of the aspired application ecosystem as depicted in ***Appendix E-4***.

2.2.5.5 Perform Gap Analysis

Gap analysis shall be performed based on steps specified on *Section 2.1.5* of this document and document the results as illustrated in ***Appendix L-3.***

2.2.5.6 Finalize the Application Architecture

i. Conduct final cross-check on the application architecture documentation's completeness, accuracy, and alignment with feedbacks received from stakeholders and any changes made during the review process; and
ii. Prepare final versions of architecture deliverables, including architectural diagrams, models, descriptions, views, and other documentation that collectively describe the security architecture.

2.2.5.7 Deliverables

The deliverables for this phase are: -

i. Application architecture principles;
ii. Detailed baseline application architecture;
iii. Detailed target application architecture; and
iv. Gap analysis results.

2.2.6 Phase 6 - Development of Technology Architecture

This phase focuses on developing the technology architecture that provide technology landscape components needed to support the organization's business goals and objectives in a way that addresses stakeholders concerns. the following are the key steps in the development of technology architecture.

2.2.6.1 Initiate Development of Technology Architecture

i. Collect and review pre-existing documents which includes proposal document for architecture work, stakeholder engagement plan, business requirements, business transformation readiness assessment report, architecture vision statement, communications plan, gap analysis results from business, data, and application architectures, and other relevant technical requirements from previous phases;
ii. Document technology architecture objectives;
iii. Review and validate the set of technology principles to be used in the development of technology architecture; and
iv. Document updated set of technology principles in the technology architecture section. ***Table*** outlines examples of technology architecture principles.

Table 6: Examples of Technology Architecture Principles

Principles #T1	**Infrastructure Resilience and Scalability**
Statement	Software and hardware should be built and set up to support business continuity, ensuring that operations can be resumed at the last recorded state despite potential technical and nontechnical failures.
Rationale	i. Resilience entails availability, archival and backup.

	ii. Scalability is required to support the overall SLA requirements. This involves scalability, availability & performance issues.
Implications	i. Scalability: Technology standards chosen will meet the changing and growing Public Institution needs and requirements and the applications and technologies will essentially scale up, to adapt and respond to such requirement changes and demand fluctuations. Server, storage and network capacities must handle user, application and data loads. ii. Availability: The technology infrastructure will exhibit no single point of failure. iii. Archival and Backup: The infrastructure will have data and source spanning across multi years. The archival and backup policy and mechanism will address the archival and backup requirement of the system and be aligned with the regulatory requirements. iv. The system infrastructure will be architected considering failover requirements and ensure, a single server or network link failure does not bring down the entire system (although e.g. performance may degrade). v. The system will handle every request and yield a response and handle error and exception conditions effectively. vi. In the event of failures or crashes, recovery of transactions and data will be possible. vii. The platform solution will support effective disaster recovery. viii. Monitoring of systems health at regular intervals will be possible. Use of central system, monitoring tool would be required to gauge the health of the system all time and

	monitor against the pre-defined SLA.
Principles #T2	**Adherence to Open Standards**
Statement	To enable the various systems to interact and communicate with one another, adhere to open integration standards.
Rationale	i. Avoid vendor lock-in ii. More choices to deliver best-of-breed solutions to meet operational needs
Implications	i. Reduce maintenance complexity ii. Enhance portability of applications from one platform to another
Principle #T3	**Interoperability**
Statement	Software and hardware should conform to defined standards that promote interoperability for data, applications, and technology.
Rationale	i. Standards help ensure consistency, thus improving the ability to manage systems and improve user satisfaction, and protect existing IT investments, thus maximizing return on investment and reducing costs. ii. Standards for interoperability additionally help ensure support from multiple vendors for their products, and facilitate supply chain integration.
Implications	i. Interoperability standards and industry standards will be followed unless there is a compelling academic or administrative reason to implement a non-standard solution. ii. A process for setting standards, reviewing and revising them periodically, and granting exceptions must be established.

	iii. The existing IT platforms must be identified and documented.

2.2.6.2 Technology Reference Model (TRM)

The Technology Reference Model (TRM) serves as a reference guide for categorizing and organizing technology solutions and standards within an enterprise architecture context. The TRM provides a structured framework for understanding, selecting, and integrating technology components that support the organization's business objectives and architectural requirements. The following are the key steps in the development of Technology Reference Model (TRM):

i. Ensure that the TRM contains the following components:
   a. Application Delivery Infrastructure - Web Server, Portal, Application Server, and User Interface Technology;
   b. Middleware Infrastructure - Enterprise Service Bus, Message Brokering and Queuing, Business Logic, Directory and Naming, Time Service Technology;
   c. Database Management Infrastructure - Transactional DBMS, Data Warehouse, Master Data Management, and Metadata Management technology;
   d. Computing Platforms, Peripheral and Sensors - Operating Systems, Servers/Hosts, Storage, End-User Computing, Peripherals, and Data Sensing Technology;
   e. Communication Infrastructure - Transmission / Carrier (WAN, LAN), Data Switching, Internet, Intranet, Extranet, Virtual Private Network, Voice and Video Conferencing Technology;
   f. System Management Infrastructure - Network and Security, Capacity/Performance, Infrastructure configuration, Software License, and Incident/Fault Management Technology;
   g. System Security Infrastructure - Identity and Authentication, Authorization and Access Control Confidentiality / Cryptography, Safeguarding/Integrity, and Security Audit technology; and

h. System Engineering Infrastructure - System Design/Modeling, Software development, and Software configuration technology.

ii. Represent the TRM using diagrams, such as Layered Architecture Diagram - A layered architecture diagram organizes technology solutions into horizontal layers, with each layer representing a different aspect or domain of the TRM. This type of diagram provides a clear separation of concerns and helps visualize the modular structure of the technology landscape, as shown in ***Figure 5***.

Figure 5 : Sample Technology Reference Model

2.2.6.3 Develop Baseline Technology Architecture Description

i. Identify and define the scope of the baseline technology architecture description by stating what will be included in the baseline, such as Application Delivery Infrastructure, Middleware Infrastructure, Database Management Infrastructure, Computing Platforms, Peripheral & Sensors, Communication Infrastructure, System Management Infrastructure, System Security Infrastructure, System Engineering Infrastructure;

ii. Collect and make use of documentation, including system architecture diagrams, network diagrams, inventory lists, configuration documents, and any other relevant sources of information related to current technology landscape;

iii. Identify components of current technology architecture, this may include: -

   a. Application Delivery Infrastructure - Web Server, Portal, Application Server, and User Interface Technology;
   b. Middleware Infrastructure - Enterprise Service Bus, Message Brokering and Queuing, Business Logic, Directory and Naming, Time Service Technology;
   c. Database Management Infrastructure - Transactional DBMS, Data Warehouse, Master Data Management, and Metadata Management technology;
   d. Computing Platforms, Peripheral and Sensors - Operating Systems, Servers/Hosts, Storage, End-User Computing, Peripherals, and Data Sensing Technology;
   e. Communication Infrastructure - Transmission / Carrier (WAN, LAN), Data Switching, Internet, Intranet, Extranet, Virtual Private Network, Voice and Video Conferencing Technology;
   f. System Management Infrastructure - Network and Security, Capacity/Performance, Infrastructure configuration, Software License, and Incident/Fault Management Technology;

g. System Security Infrastructure - Identity and Authentication, Authorization and Access Control Confidentiality / Cryptography, Safeguarding/Integrity, and Security Audit technology; and
h. System Engineering Infrastructure - System Design/Modeling, Software development, and Software configuration technology.

iv. Document and create baseline technology architectural views that illustrate different aspects of the current technology architecture as illustrated in ***Appendix F-1.*** A diagram depicting the baseline technology architecture may be drawn. The diagram can be illustrated in the following ways:
a. Conceptual View: High-level visual representation of the baseline architecture's structure and components;
b. Logical View: Logical decomposition of the baseline architecture into components and their interactions; and
c. Physical View: Physical implementation of the baseline architecture, including hardware, software, and network infrastructure.

v. Document baseline technology architecture challenges.

2.2.6.4 Develop Target Technology Architecture Description

i. Understand and analyze institutional resources that influencing the design of target technology architecture. These resources may include Business Reference Model (BRM), Data Reference Model (DRM), Application Reference Model (ARM), and Security Reference Model (SRM);
ii. Establish principles that will govern the design and implementation of the target technology architecture. Principles should reflect the institution's goals and objective;
iii. Research emerging technology trends and identify new technologies (such as Artificial Intelligence (AI) and Machine Learning, Block chain, etc.) that may be leveraged in the design of target technology architecture;
iv. Define the key components of the target technology architecture, including: -

a. Application Delivery Infrastructure - Web Server, Portal, Application Server, and User Interface Technology;
b. Middleware Infrastructure - Enterprise Service Bus, Message Brokering and Queuing, Business Logic, Directory and Naming, Time Service Technology;
c. Database Management Infrastructure - Transactional DBMS, Data Warehouse, Master Data Management, and Metadata Management technology;
d. Computing Platforms, Peripheral and Sensors - Operating Systems, Servers/Hosts, Storage, End-User Computing, Peripherals, and Data Sensing Technology;
e. Communication Infrastructure - Transmission / Carrier (WAN, LAN), Data Switching, Internet, Intranet, Extranet, Virtual Private Network, Voice and Video Conferencing Technology;
f. System Management Infrastructure - Network and Security, Capacity/Performance, Infrastructure configuration, Software License, and Incident/Fault Management Technology;
g. System Security Infrastructure - Identity and Authentication, Authorization and Access Control Confidentiality / Cryptography, Safeguarding/Integrity, and Security Audit technology; and
h. System Engineering Infrastructure - System Design/Modeling, Software development, and Software configuration technology.

vi. Document and create target technology architectural views that illustrate different aspects of the desired technology architecture as illustrated ***Appendix F-1***. A diagram depicting the target technology architecture may be drawn. The diagram can be illustrated in the following ways: -
a. Conceptual View: High-level conceptual representation of the target architecture's structure and components;
b. Logical View: Logical decomposition of the target architecture into components and their interactions;
c. Physical View: Physical implementation of the target architecture, including hardware, software, and network infrastructure.

2.2.6.5 Perform Gap Analysis

Gap analysis shall be performed based on steps specified on Section 2.1.5 of this document and document the results as illustrated in ***Appendix L-3.***

2.2.6.6 Finalize the Technology Architecture

i. Conduct final cross-check on the technology architecture documentation's completeness, accuracy, and alignment with feedbacks received from stakeholders and any changes made during the review process; and
ii. Prepare final versions of architecture deliverables, including architectural diagrams, models, descriptions, views, and other documentation that collectively describe the technology architecture.

2.2.6.7 Deliverables

The deliverables for this phase are: -

i. Technology architecture principles;
ii. Detailed baseline technology architecture;
iii. Detailed target technology architecture; and
iv. Gap analysis results.

2.2.7 Phase 7 - Development of Security Architecture

Enterprise Security Architecture involves planning and supervising the construction of systems which are free from security threats.

Public institution shall consider following steps in developing the security architecture;

2.2.7.1 Initiate Development of Security Architecture

i. Document security architecture objectives; and
ii. Review and validate security Architecture related principles from proposal of architecture work or establish new principles, if necessary, as depicted in ***Table*** .

Table 7: Examples of Security Architecture Principles

Principle # S1	**Alignment with Security Policies**
Statement	Security policies should drive the implementation of business and technical security controls.
Rationale	Business and technical security controls are put in place to enforce compliance with existing security policies.
Implication	There should be a way to monitor and measure the security compliance of each IT system
Principle # S2	**Least Privilege**
Statement	Every module (such as a process, a user, or a program depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose.
Rationale	It is an important design consideration protecting data and functionality from faults and malicious behavior. Benefits include better system stability, better system security, and ease of deployment.
Implication	User accounts should be given only those privileges essential to that user's work. Applications should only acquire information necessary for their operations.
Principle # S3	**Security Measurement**
Statement	Evaluate, improve, and maintain security posture effectively in the face of evolving cyber threats and regulatory requirements.
Rationale	Allows errors to be corrected and system misuse to be minimized.

Implication	Security controls will be reviewed or audited through qualitative or quantitative means for traceability and to ensure that risk is being maintained at acceptable levels. Be able to prepare a security dashboard which includes all relevant information security KPIs to be presented to management on a regular basis.

2.2.7.2 Define Security Reference Model

i. Ensure that the SRM contains components such as: -
   a. Security Drivers (threat, compliance, business requirements, business opportunities);
   b. Security Governance (policies, standards, guidelines, procedures, security strategies and planning, risk management, education and awareness);
   c. Security Operations (vulnerability assessment, incident management, system and infrastructure monitoring, event management, secure deployment of devices and applications, administration of users, systems and devices); and
   d. Security Technology architecture (secure system design and development, logical and physical architecture, security requirements, encryption mechanism, multi-factor authentication).

ii. Represent the SRM using diagrams as shown in ***Appendix G-1.***

2.2.7.3 Develop Baseline Security Architecture

i. Assess and document current security architecture posture basing on the ten Government ICT security domains. The Government ICT security domains are ICT security governance and management, ICT security operation, Security of ICT assets, identity and assets management, ICT security incident management, information system continuity management, information system acquisition development and

maintenance, human resource security, physical and environment security, ICT security compliance and audit;

ii. Identify and document landscape security services catalog which lists the services that provide security specific functionality as part of overall architecture; and

iii. Identify and document challenges in baseline security architecture.

2.2.7.4 Develop Target Security Architecture

Public Institution Shall: -

i. Define target security architecture posture basing on the ten Government ICT security domains; and

ii. Identify and document the target security services catalog which lists the services that provide security specific functionality as part of overall architecture.

2.2.7.5 Perform Gap Analysis

Gap analysis shall be performed based on steps specified on Section 2.1.5 of this document and document the results as illustrated in ***Appendix L-3.***

2.2.7.6 Finalize the security architecture

i. Conduct final cross-check on the security architecture documentation's completeness, accuracy, and alignment with feedbacks received from stakeholders and any changes made during the review process; and

ii. Prepare final versions of architecture deliverables, including architectural diagrams, models, descriptions, views, and other documentation that collectively describe the security architecture.

2.2.7.7 Deliverables

The deliverables for this phase are: -

i. Security architecture principles;

ii. Detailed baseline security architecture;

iii. Detailed target security architecture; and

iv. Gap analysis results.

2.2.8 Phase 8 - Identification of Opportunities and Solutions

This phase aims to identify and evaluate programs or projects, that can turn the earlier identified target architectures into reality. It identifies opportunities to deliver the target architectures identified in the previous phases, prioritize and sequence projects based on their alignment with business goals and architectural standards and develop an initial implementation and mitigation strategy. Public institutions can ensure that their architecture visions are translated into projects that deliver business value.

During execution of this phase public institutions shall:

2.2.8.1 Determine and Confirm Institution's Key Change Attributes

i. Define the list of factors impacting the architecture implementation and migration decisions, these factors include risks, issues, assumptions, dependencies, actions and impacts;

ii. Create the implementation factor assessment and deduction matrix as indicated in ***Appendix L-4***. The matrix should include a list of the factors, their descriptions with rationale and the deductions (conclusions) that indicate the actions or constraints that have to be taken into consideration when formulating the implementation and migration plan.

2.2.8.2 Determine Business Constraints for Implementation

i. Identify business drivers that may limit the sequence of the target architecture execution. These may include: -
   a. Business objectives and strategies;
   b. Budgetary, skills and technological limitations;
   c. Project timelines and deadlines;
   d. Legal and compliance requirements;
   e. Stakeholders' constraints from power and interest matrix; and
   f. Environmental regulations or sustainability goals that may influence execution.

ii. Document the identified constraints as indicated in ***Appendix H-2.***

2.2.8.3 Review and Consolidate Gap Analysis Results

i. Review gap analysis results from the business, data, application, technology and security architectures and consolidate them in a single list along with potential solutions to the gaps and dependencies as indicated in ***Appendix H-1***; and

ii. Make use of business interaction matrix, data entity/business function matrix and the application/function in the course of determining the dependencies.

2.2.8.4 Review Consolidated Requirements Across Related Business Functions

Assess the requirements, gaps, solutions, and factors to identify a minimal set of requirements whose integration into work packages would lead to a more efficient and effective implementation of the target architecture leading to shared solutions and services across the business functions that are participating in the architecture.

2.2.8.5 Consolidate and Reconcile Interoperability Requirements

i. Consolidate the interoperability requirements that were identified in the previous phases. These may include integration needs, data exchange formats, communication protocols, system compatibility and standards compliance;

ii. Prioritize the consolidated interoperability requirements based on their importance to the organization goals, strategic objectives and operational needs;

iii. Review implementation factor assessment and deduction matrix as well as consolidated gaps, solutions and dependencies matrix to identify any constraints on interoperability required;

iv. Identify and resolve any interoperability conflicts or redundancies among the interoperability requirements by ensuring they are addressed in the architecture and considered across all architecture domains; and

v. Document the updated consolidated and reconciled interoperability requirements.

2.2.8.6 Refine and Validate Dependencies

i. Refine the initial dependencies, ensuring that any constraints on the implementation and migration plans are identified;
ii. Determine the sequence of implementation and coordination required based on the refined dependencies; and
iii. Document the identified dependencies to be used as part of architecture roadmap in the later steps.

2.2.8.7 Formulate Implementation and Migration Strategy

i. Determine approaches to implementing the identified solution and/or exploiting opportunities. The approaches may be a new implementation, implementing a change or running a parallel approach;
ii. Determine strategic directions that will address and mitigate the risks identified in the consolidated gaps, solutions and dependencies matrix; and
iii. Consolidate strategic approaches and directions and agree on the implementation and migration strategy for the enterprise.

2.2.8.8 Identify and Group Major Work Packages

i. Using the consolidated gaps, solutions, and dependencies matrix together with the implementation factor assessment and deduction matrix, logically group the various activities into work packages;
ii. Fill in the "Solution" column in the consolidated gaps, solutions, and dependencies matrix to recommend the proposed solution mechanisms;
iii. Indicate for every gap/activity whether the solution should be oriented towards a new development, or be based on an existing product, and/or use a solution that can be purchased;
iv. Review and refine these work packages with respect to their business transformation issues and the strategic implementation approach; and
v. Group the work packages into portfolios and projects within a portfolio, taking into consideration the dependencies and the strategic implementation approach.

2.2.8.9 Determine Transition Architectures Where Necessary

i. Identify transition architectures when the scope of change to implement the target architecture requires an incremental approach. This identifies clear targets along the roadmap to realizing the target architecture;
ii. Transition architectures will be developed based upon the preferred implementation approach, the consolidated gaps, solutions, and dependencies matrix, the listing of projects and portfolios, as well as the enterprise's capacity for creating and absorbing change; and
iii. Document transition architectures in architecture definition increment table as prescribed in ***Appendix L-5.***

2.2.8.10 Prepare Initial Architecture Roadmap

i. Consolidate the work packages and transition architectures into the architecture roadmap, as specified in ***Appendix L-6***;
ii. Ensure the identified transition architectures and work packages have a clear set of outcomes.

2.2.8.11 Create Implementation and Migration Plan

Create implementation and migration plan that identifies and demonstrate necessary projects and resource requirements necessary to realize the Architecture Roadmap as prescribed in ***Appendix I-1.***

2.2.9 Phase 9 - Migration Planning

Migration planning aims to finalize the Architecture Roadmap and the supporting implementation and migration plan, ensuring that the plan is coordinated with the organization's approach to managing and implementing change in the organization's overall change portfolio, and that the business value and cost of work packages and transition architectures is understood by key stakeholders.
During Migration Planning, Public Institutions shall:

2.2.9.1 Confirm Management Framework Interactions for the Implementation and Migration Plan

Execute the implementation and migration plan in alignment with the existing management frameworks within the organization such as ICT project management procedures.

2.2.9.2 Estimate Resource Requirements, Project Timings and Delivery

i. Determine the required resources and times for each project and their increments and provide the initial cost estimates;
ii. Break down the costs into capital (to create the capability), operations and maintenance (to run and sustain the capability);
iii. Identify opportunities where the costs associated with delivering new and/or better capability can be offset by decommissioning existing systems; and
iv. Assign required resources to each activity and aggregate them at the project increment and project level.

2.2.9.3 Prioritize the Migration Projects

i. Determine the net benefits of all solutions delivered by the projects and their associated costs, then communicate them to stakeholders;
ii. Review the initial identified risks to ensure that the risks for the project deliverables have been mitigated as much as possible;
iii. Have the stakeholders agree upon a prioritization of the projects based on elements identified in creation of the initial Architecture Roadmap in the "Identification of Opportunities and Solutions" phase as well as those relating to individual stakeholders' agendas;
iv. Formally review the risk assessment and revise it to ensure there is a full understanding of the residual risk associated with the prioritization and the projected funding line;
v. Update the project list incorporating risk-related comments; and
vi. Prioritize the projects by ascertaining their business value against the cost of delivering them.

2.2.9.4 Confirm Architecture Roadmap and Update the Architecture Domains Descriptions

i. Review the architecture work to date to assess what the time-spans between transition architecture should be taking into consideration factors such as the increments in business value, capability and risk;

ii. Update the Architecture Roadmap including any transition architectures along with its associated Architecture Definition Increments Table; and

iii. Generate a finalized Architecture Roadmap by utilizing the ***Appendix I-1***.

2.2.9.5 Finalize the Implementation and Migration Plan

Consolidate all sections forming the contents of the implementation and migration plan as depicted in ***Appendix I-1***.

2.2.9.6 Deliverables

i. Finalized implementation and migration plan;
ii. Finalized Architecture Domains Descriptions;
iii. Finalized transition architectures, if any;
iv. Finalized Architecture Roadmap;
v. Updated architecture definition increments table; and
vi. Project portfolio.

2.2.10 Phase 10 - Architecture Implementation

This phase focuses on execution of the implementation and migration plan. During the execution of this phase public institutions shall:

2.2.10.1 Confirm Scope and Priorities for Architecture Implementation with Development Team.

i. Review migration planning outputs to understand the scope of the architecture implementation, efforts, and resources required;
ii. Make use of the transition architectures described in “Migration Planning” phase to guide on functionalities and features to be included in each implementation phase based on priorities; and

iii. Identify and document potential issues that could arise during the architecture implementation and make possible recommendations to ensure successful implementation.

2.2.10.2 Identify Required Implementation Resources and Skills

i. Assess the organization's workforce to identify skillsets and experience of the development and IT teams to determine their capacity to handle the implementation tasks. This involves identifying any gaps between the required skills and the skills currently available within the organization and develop a plan for acquiring the required skills; and

ii. Identify system development methods required for solutions development such as agile, waterfall, Rapid Application Development (RAD) or DevOps development methodology; and

iii. Ensure that the identified methods enable feedback to the architecture team on designs.

2.2.10.3 Guide Development of Solutions Deployment

i. Formulate project recommendation, whereby for each separate implementation and deployment project, do the following: -

   a. Document scope of individual project in impact analysis;
   b. Document strategic requirements (from the architectural perspective) in impact analysis;
   c. Document change requests (such as support for a standard interface) in impact analysis;
   d. Document rules for conformance in impact analysis; and
   e. Document timeline requirements from roadmap in impact analysis.

2.2.10.4 Deliverables

Documentation related to work performed.

2.2.11 Phase 11 - Architecture Governance

Architecture Governance refers to the set of practices, processes, and mechanisms that ensure the effective management, control, and alignment of institutional architecture activities with its strategic objectives, business goals, policies, standards, and best practices. It provides oversight, decision-making, and accountability to ensure that architectural decisions and implementations are consistent, compliant, and value driven. During the execution of this phase public institutions shall:

2.2.11.1 Perform Enterprise Architecture Compliance Reviews

i. The Enterprise Architecture Committee shall establish enterprise architecture compliance review team;

ii. The enterprise architecture compliance review team shall: -

   a. Define the criteria, standards, and guidelines against which compliance will be assessed. This includes adherence to architecture principles, policies and regulatory requirements;

   b. Determine the scope of the compliance review, this may include assessing compliance across different architectural domains such as business architecture, application architecture, data architecture, technology architecture and security architecture;

   c. Collect relevant architectural output, documents, and guidelines, this may include architectural deliverables such as architecture vision, business architecture, data architecture, application architecture, technology architecture, security architecture and others;

   d. Schedule review meetings with all relevant architecture stakeholders, such as business representatives and project managers;

   e. Assess the compliance of enterprise architecture implementation to ensure that the original architecture vision is appropriately realized and that any implementation learning is fed back into the architecture process. periodic compliance reviews of implementation projects provide a mechanism to review project

progress and ensure that the design and implementation is proceeding in line with the strategic and architectural objectives;

f. Document findings of the compliance review by capturing observations, causes, recommendations, and supporting evidence;
g. Communicate the results of the compliance review to the relevant stakeholders, including Enterprise Architecture Committee and ICT Steering Committee by providing clear summaries of findings, highlighting areas of compliance, non-compliance, and recommended actions;
h. Monitor the implementation of corrective actions and follow up on progress to ensure that non-compliance issues are addressed effectively. Conduct regular reviews and assessments to track improvements in compliance and identify any recurring issues or emerging risks; and
i. Continuously review and refine compliance criteria, processes, and practices based on lessons learned, feedback from stakeholders, and changes in organizational needs or standards.

iii. Conduct the enterprise architecture compliance review semi-annually.

2.2.12 Phase 12 - Architecture Change Management

This phase is crucial for ensuring that the architecture continues to meet business needs and objectives over time by managing changes in an organized and controlled manner in line with the architecture governance processes. It establishes and supports the enterprise architecture to provide flexibility to evolve rapidly in response to changes in the technology or business environment. During the execution of change management phase, Public Institutions shall:

2.2.12.1 Develop Change Requirements to Meet Performance Targets

i. Identify and prioritize change requirements that need to be addressed or improved to meet the defined performance targets; and
ii. Document change requirements in an Architecture Requirements Specification document as stipulated in ***Appendix L-1*** detailing the

scope, objectives, and constraints of each requirement ensuring desired performance outcomes are clearly defined, measurable, and achievable through the proposed changes.

2.2.12.2 Determine Architecture Change Approach

The architectural change approach may be one of the following.

i. **Simplification change**: This change approach aims to streamline and optimize the existing architecture by consolidating systems and simplifying processes. These changes often have minimal impact on the overall architecture but can significantly improve efficiency and reduce complexity;
ii. **Incremental change**: This change approach involves making gradual improvements and enhancements to the existing architecture. These changes are planned and executed in small, manageable increments, allowing for continuous improvement without significant disruption; and
iii. **Re-architecting change**: This change involves a fundamental overhaul of the existing architecture. These changes are typically driven by significant shifts in business strategy, technology advancements, or major issues with the current architecture.

2.2.12.3 Approval of Architectural Changes

Obtain approval and guidance on change implementation from the ICT Steering Committee.

2.2.12.4 Implementation of Change

Execute the change as specified in the Architecture Change Requirements Specification document.

2.2.12.5 Perform Monitoring

i. Identify and define specific monitoring requirements based on the objectives, scope, and nature of architecture changes.
ii. Perform monitoring of technology/business changes that could impact the baseline architecture, track business value, monitor enterprise architecture capability maturity, track and assess asset management

programs as well as determine and track business continuity requirements.

2.2.12.6 Deliverables

i. New proposal for architecture work, to initiate another cycle of the ADM (for major changes).
ii. Change management procedures.

2.2.13 Create an Enterprise Architecture Document

Consolidate deliverables from all phases into the Enterprise Architecture document and Obtain approval from the ICT Steering Committee.

3 IMPLEMENTATION, ENFORCEMENT AND REVIEW

This document 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 Continually complied to and any exception to its application must be duly authorized.

4 RELATED DOCUMENTS

4.1 e-Government Guideline, 2017 by President's Office – Public Service Management and Good Governance (PO-PSMGG);

4.2 e-Government Interoperability Framework – Standards and Technical Guidelines (eGA/EXT/GIF/001);

4.3 e-Government Business Architecture – Standards and Technical Guidelines (eGA/EXT/BSA/001);

4.4 e-Government Application Architecture – Standards and Technical Guidelines (eGA/EXT/APA/001);

4.5 e-Government Information Architecture – Standards and Technical Guidelines (eGA/EXT/IFA/001);

4.6 e-Government Integration Architecture – Standards and Technical Guidelines (eGA/EXT/ITA/001);

4.7 e-Government Infrastructure Architecture – Standards and Technical Guidelines (eGA/EXT/IRA/001);

4.8 e-Government Security Architecture – Standards and Technical Guidelines (eGA/EXT/ISA/001);

4.9 e-Government Architecture Processes and Governance – Standards and Technical Guidelines (eGA/EXT/PAG/001); and

4.10 e-Government Act No.10, 2019.

5 DOCUMENT CONTROL

Version	Name	Comment	Date
1.0	e-GA	Creation of new document to align with e-Government Guidelines, 2017.	December 2024

APPENDICES

APPENDICES A – PREPARATION AND INITIATION PHASE

Appendix A-1: Example of Proposal for Architecture Work Document

Contents of the document

1. Understand the Organization
2. Enterprise Architecture team and Governance Structure
3. Constraints on Enterprise Architecture work
4. Architecture Principles
5. Budget plan and Time Scale
6. Approval for Architecture Work

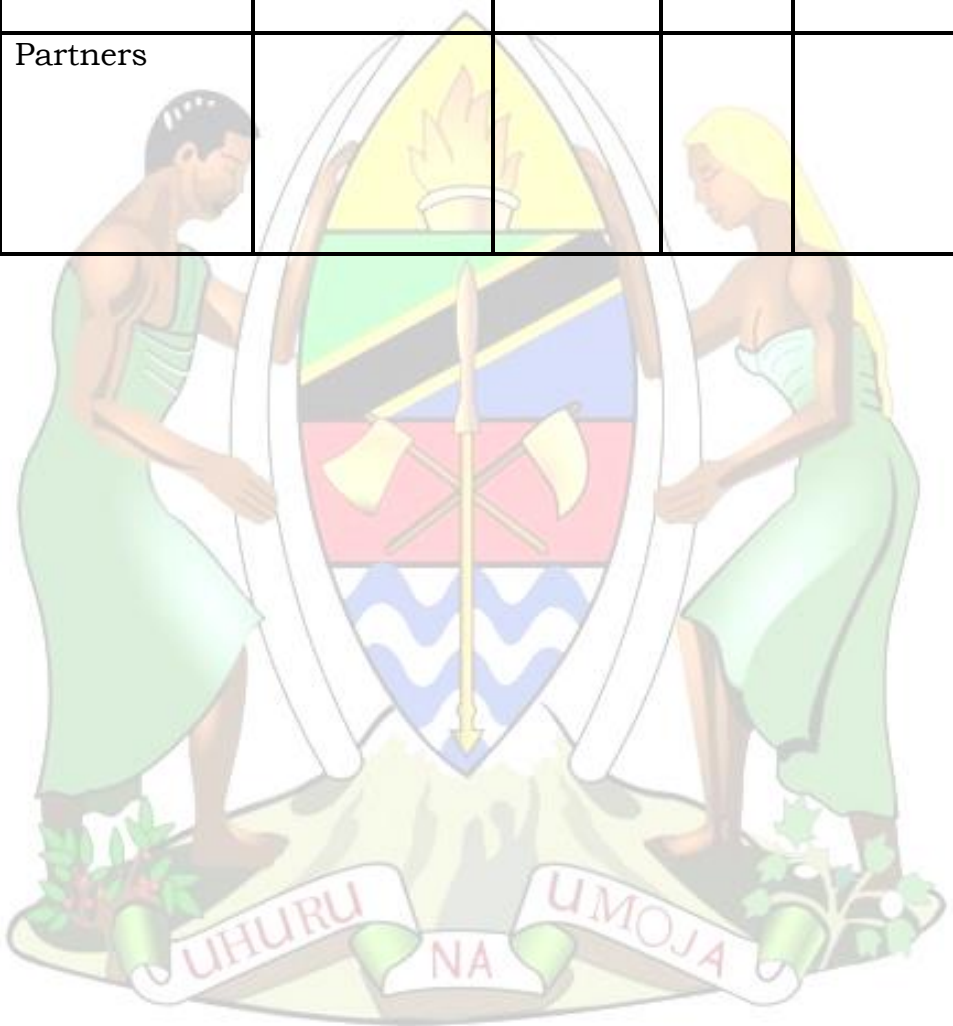
APPENDIX B – ARCHITECTURE VISION PHASE

Appendix B-1: Stakeholder Map

Stakeholders Category	Stakeholders	Involvement	Class	Power	Level of Interest	Key Concerns
Core Functions	Program Management Unit e.g., Project Portfolio Managers	This stakeholder group is interested in the high-level drivers, goals, and objectives of the organization, and how these are translated into an effective process and IT architecture to advance the business.	Keep Satisfied	High	Medium	Prioritizing, funding, and aligning change activity. An understanding of project content and technical dependencies between projects support portfolio management decision making.
Business Support Functions	Human Resources (HR) e.g., HR Managers, Training & Development Managers	Key features of the enterprise architecture are roles and actors that support the functions, applications, and technology of the organization. HR are important stakeholders in ensuring that the correct roles	Keep Informed	Low	Medium	The roles and actors are required to support the architecture and changes to it. The key concern is managing people transitions.

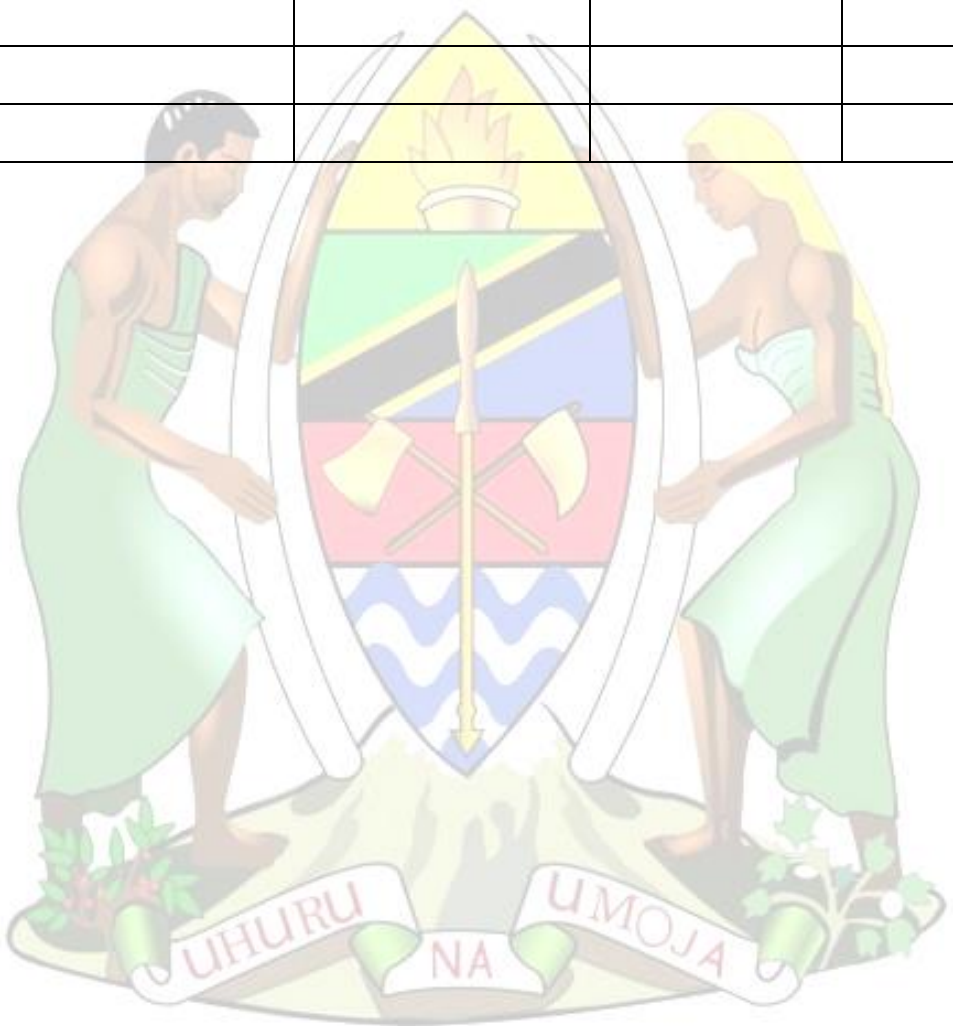
		and actors are represented.				
	Procurement e.g., Acquirers	This stakeholder group is interested in the high-level drivers, goals, and objectives of the organization, and how these are translated into an effective process and IT architecture to advance the business.	Keep Satisfied	High	Medium	Understanding what building locks of the architecture can be bought, and what constraints (or rules) are relevant to the purchase. Acquirers will shop with multiple vendors looking for the best cost solution while adhering to the constraints (or rules) derived from the architecture, such as standards. The key concern is to make purchasing decisions that fit the architecture.

External stakeholders	Customers					
	Regulatory bodies					
	Partners					



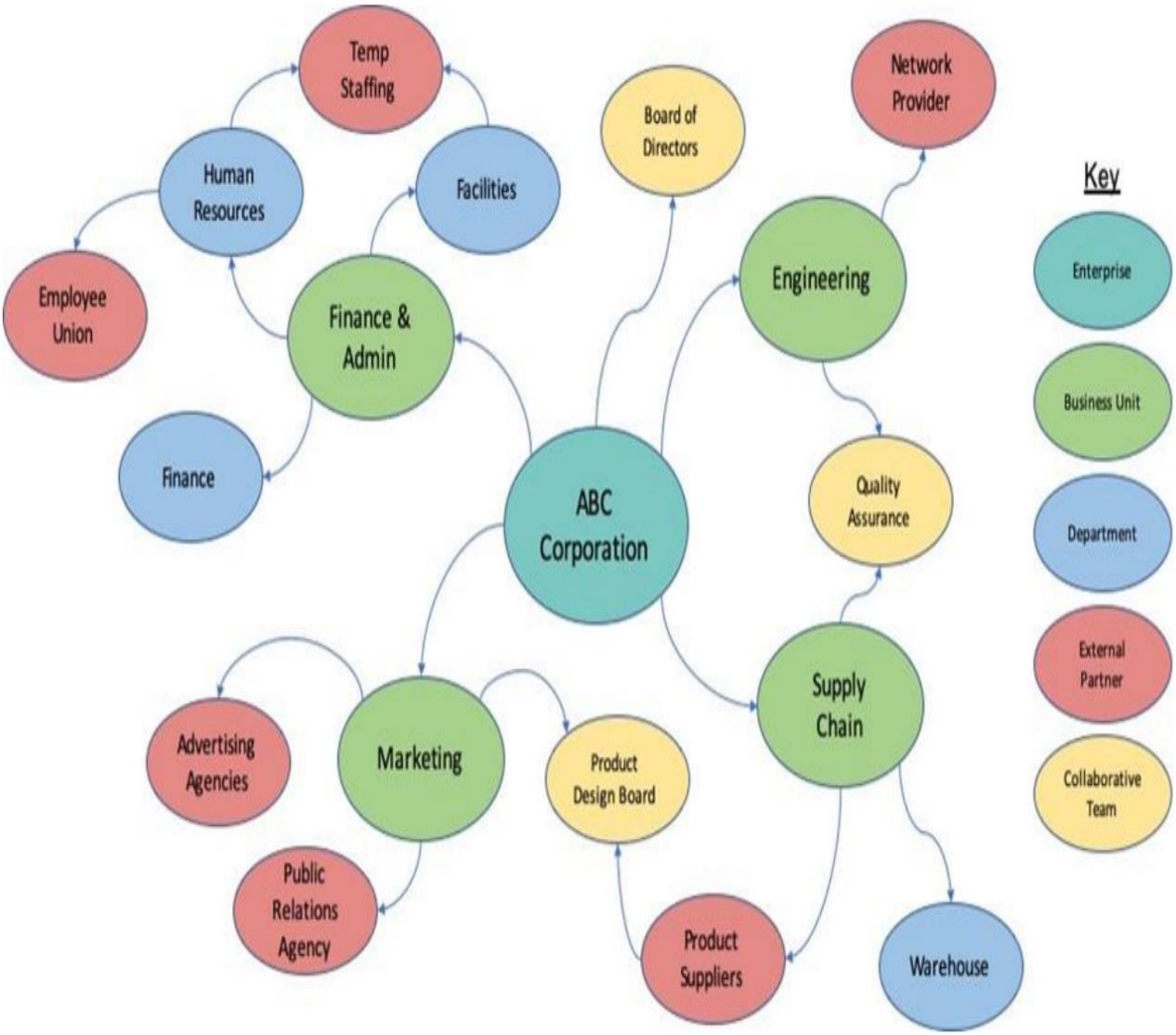
Appendix B-2: Stakeholder Engagement Plan

S/N	Stakeholder Group	Communication Channel/Mode	Frequency of Interaction	Communication Objectives
1.				
2.				
3.				
4.				
5.				
6.				
7.				



APPENDIX C – BUSINESS ARCHITECTURE PHASE

Appendix C-1: Example of Organization Map



Appendix C-2: Example for a List of Value Streams

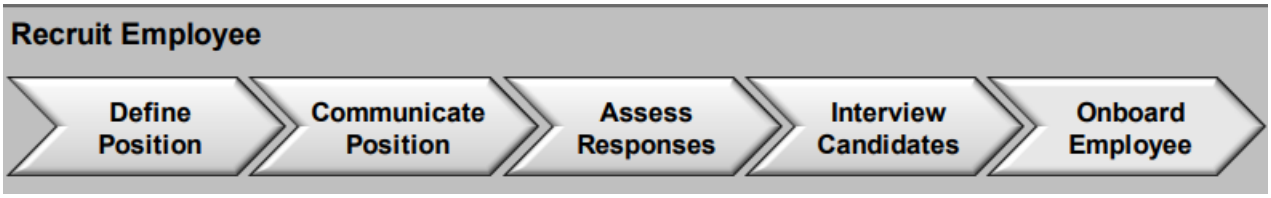
S/N	Name	Description	Stakeholder	Value
1.	**Acquire Retail Product**	The activities involved in looking for, selecting and obtaining a desired retail product.	A retail shopper wishing to purchase a product.	Customers are able to locate desired products and obtain them in a timely manner
2.	**Recruit Employee**	The activities involved in identifying and hiring suitably qualified employees	A Hiring Manager looking to fill a specific position	A new employee with good fit for the job, hired rapidly and working productively

Appendix C-3: Example of Value Stream Stages Regarding "Recruit Employee"

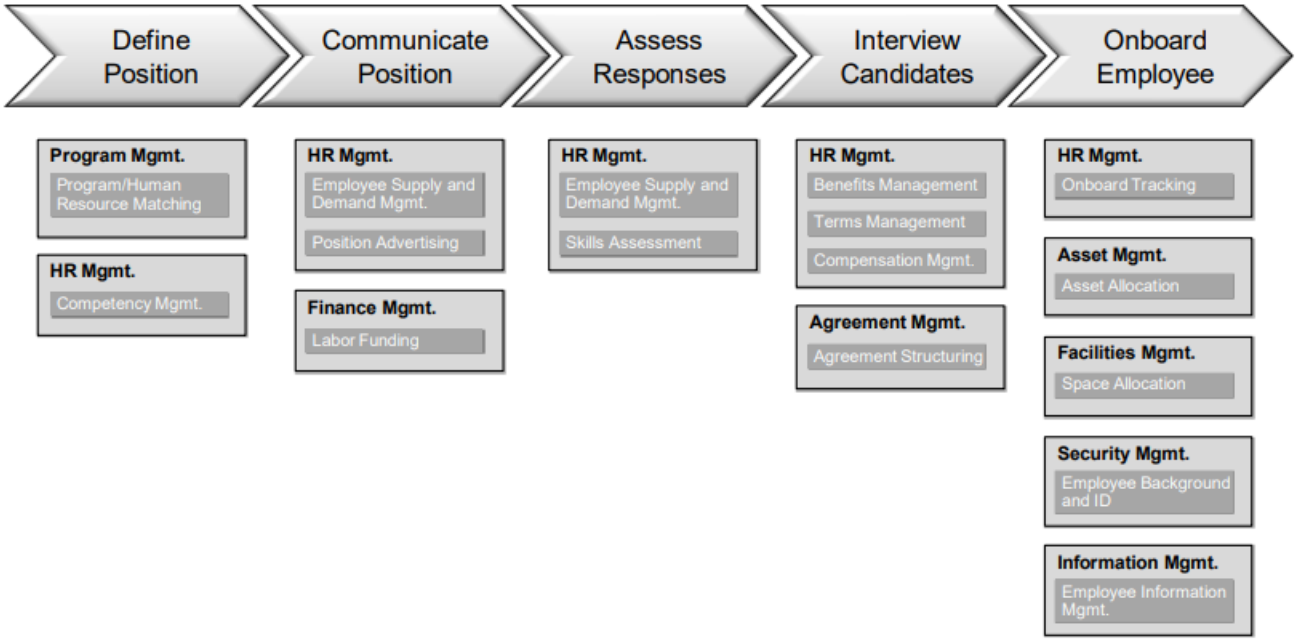
S/N	Value Stream Stage	Description	Participating Stakeholders	Entrance Criteria	Exit Criteria	Value Items
1.	Define Position	The act of determining the need for staffing, identifying skills and qualifications, and documenting them	Hiring Manager HR Recruitment Lead	Staffing changes identified	Recruitment needs identified	Time and expense saved on search for candidates
2.	Communicate Position	The act of advertising, posting, or sending requisition information to available portals and recruitment events.	Recruiter	Recruitment needs identified	Positions communicated	High likelihood of finding qualified candidates
3.	Assess Responses	The act of receiving, logging, distributing, and scoring candidate responses and additional checks.	Hiring Manager Recruiter	Positions communicated	Qualified responses selected	Efficient use of interview time and costs

S/N	Value Stream Stage	Description	Participating Stakeholders	Entrance Criteria	Exit Criteria	Value Items
4.	Interview Candidates	The act of communicating with candidates, arranging transport, and scheduling and conducting interviews.	Hiring Manager Candidate Employee	Qualified responses selected	Hiring decision	Selection of the best employee
5.	Onboard Employee	The act of making an offer, then triggering the embedded value stream for all activities involved in integrating the employee into the work environment.	Employee HR Security Facilities Finance IT	Hiring decision	Employee onboarded	Productive workforce, meeting business commitments

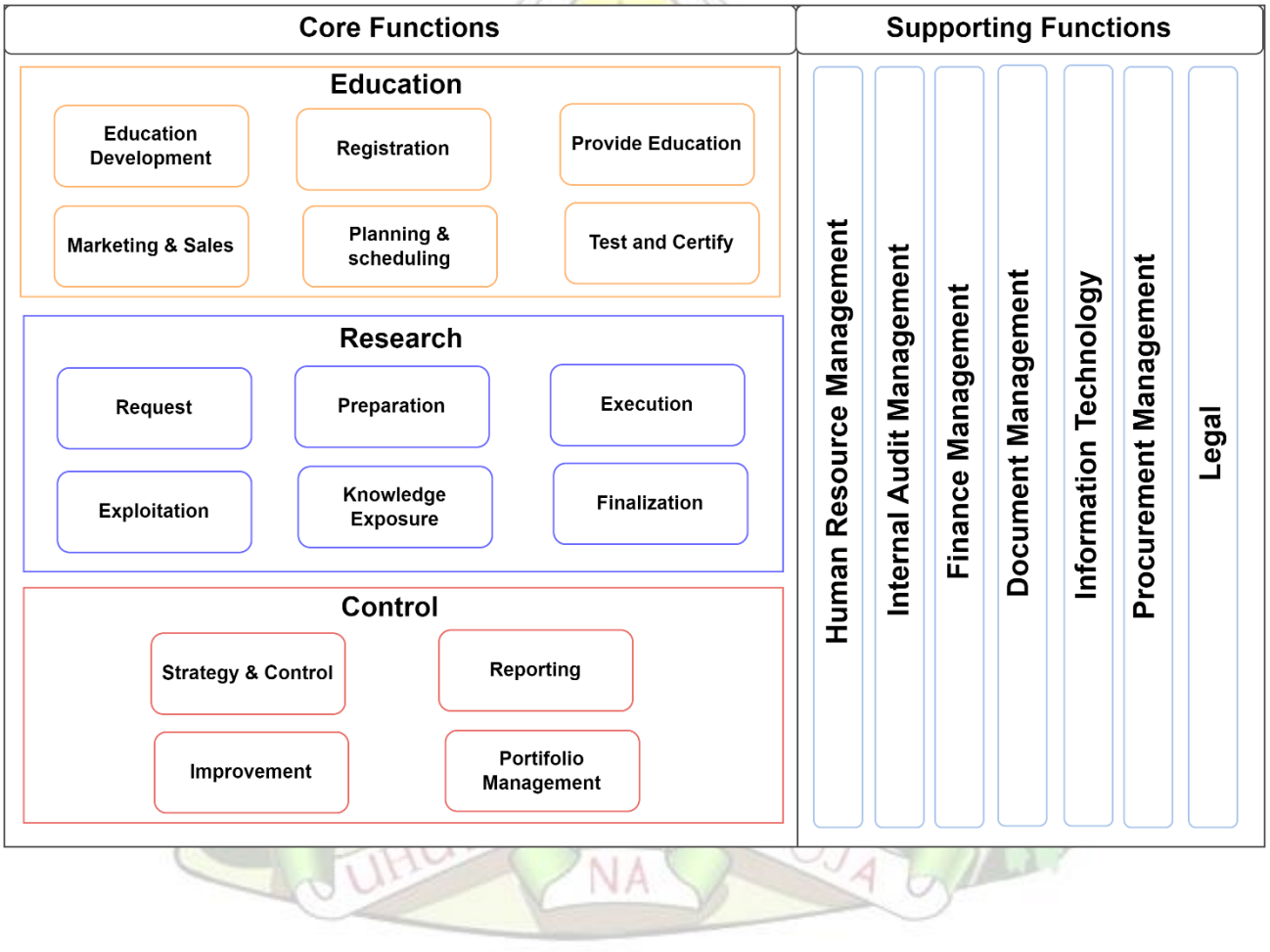
Appendix C-4: Example of a Value Stream Diagram



Appendix C-5: Example of Value Stream Map



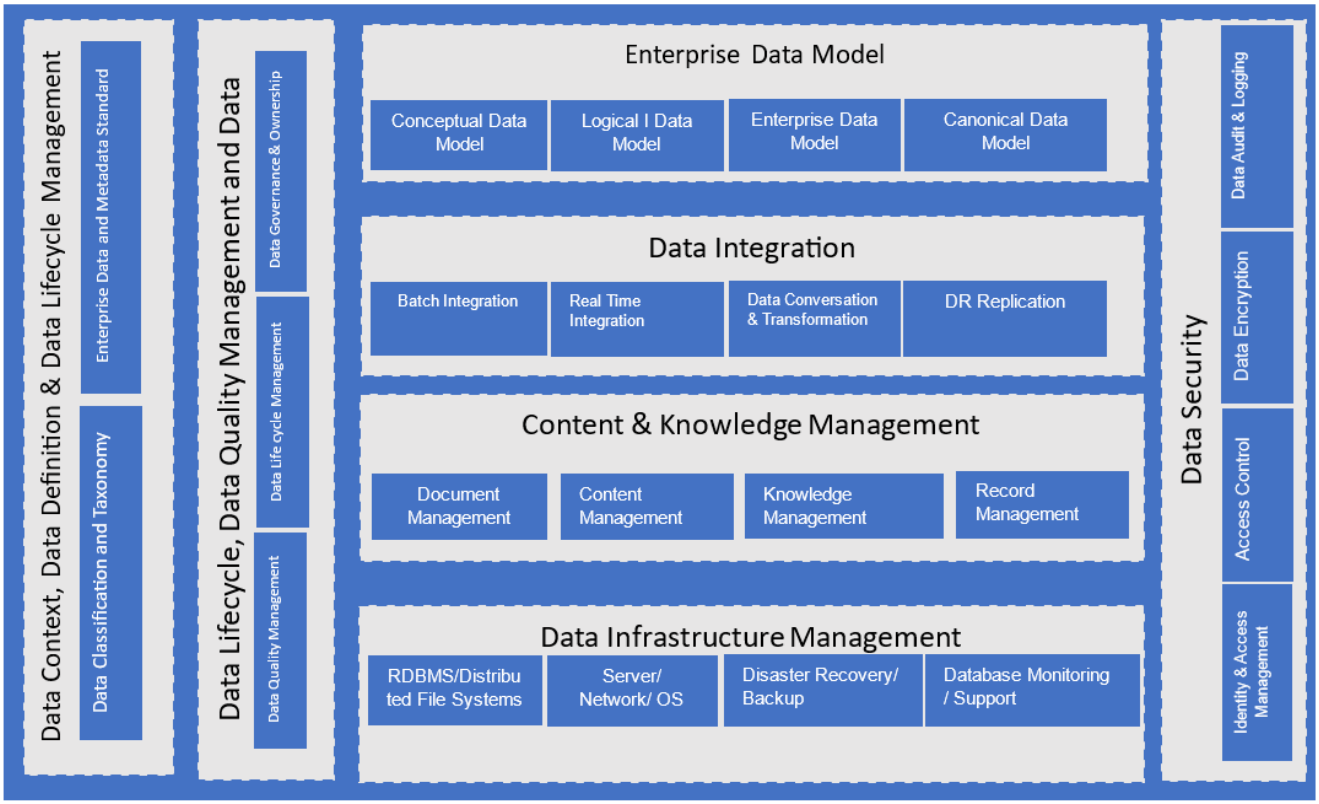
Appendix C-6: Business Reference Model Example



Appendix C-5: Business Service/Information Diagram

APPENDIX D – DATA ARCHITECTURE PHASE

Appendix-D1: Data Reference Model Framework



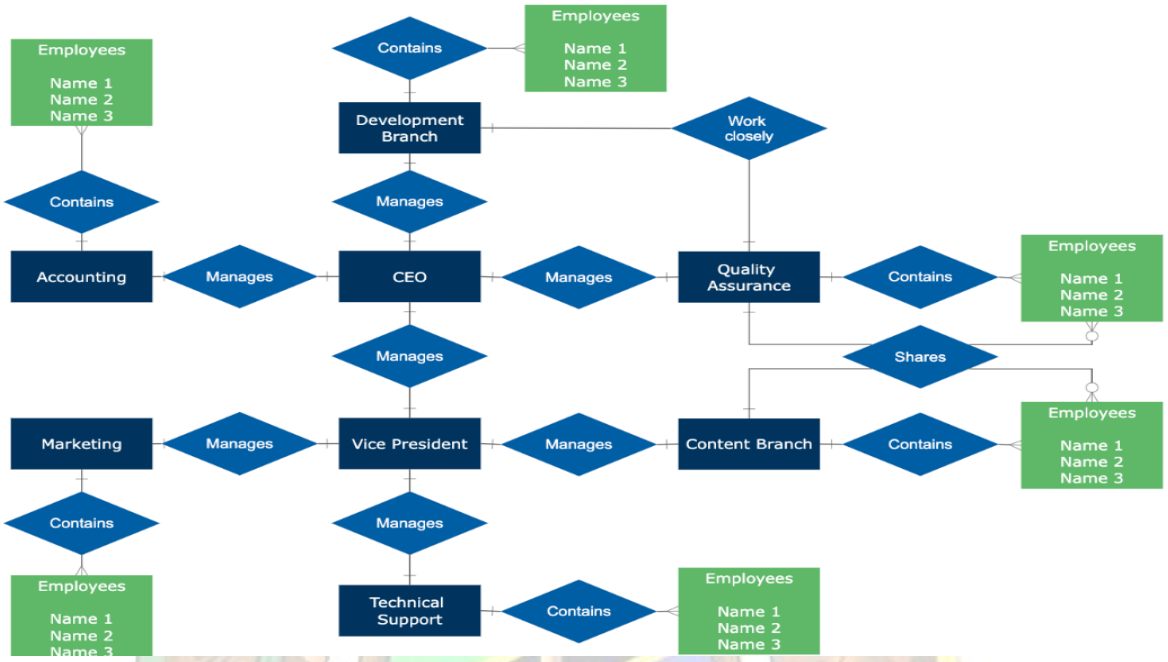
The diagram in Figure I illustrates the Information reference architecture framework with the components in Table D1:

Table D1: Components of Data Reference Architecture Framework

Components	Description
Data context and data definition	This component deals with defining the context of the data by classifying data as per subject area and defining the enterprise data and metadata standards to ensure seamless interoperability by removing ambiguities and inconsistencies in the use of data across Public Institutions.
Enterprise data model	This component deals with data analysis and design of the underlying data structure.

Data life cycle, quality management and data governance	Data life cycle management deals with the management of structured data assets across the data life cycle, from creation and acquisition through archival and purge.
Data Quality	Data quality deals with defining, monitoring and improving data quality.
Data Governance	Data governance deals with planning, oversight, and control over data management and use of data
Data sharing and integration	This component deals with managing data transformation and data exchange across applications and data store, defining capabilities from batch-based to real-time integration (including extract, transform and load (ETL) and extract, load and transform (ELT)), event driven, message-driven, and real-time integration.
Data security	This component deals with managing data privacy, confidentiality and to prevent unauthorized data access, creation and change.

Appendix D-2: Example of Entity Relation Diagram (ERD)

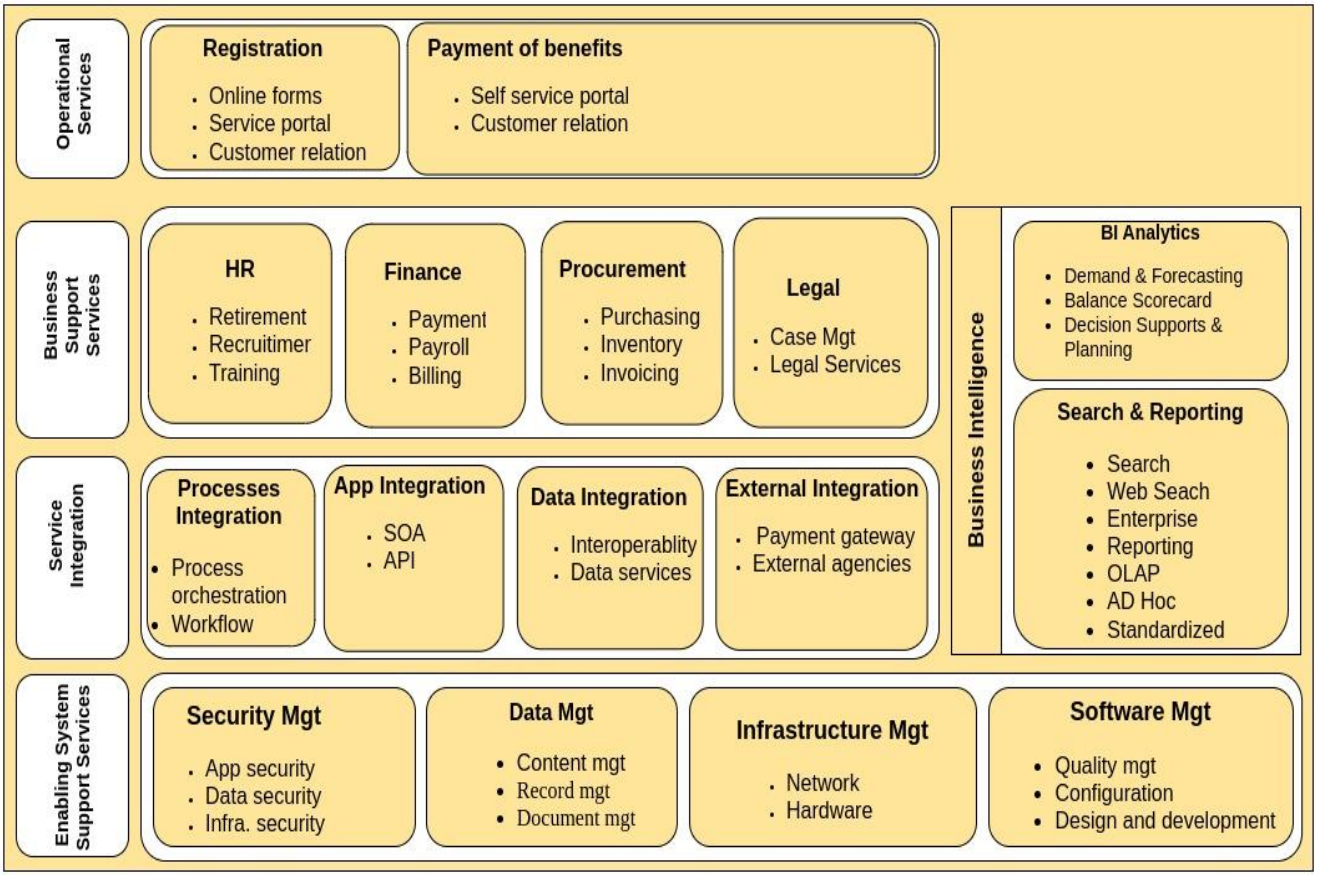


Appendix-D3: Example of Data Entity/Business Function Matrix

Physical Data Components Map to Business Functions		
	Business Function 1	Organization's Unit
Physical Data Entity 1		
Physical Data Entity 2		
Physical Data Entity 3		
Physical Data Entity 4		
Physical Data Entity 5		
Physical Data Entity 6		

APPENDIX E – APPLICATION ARCHITECTURE PHASE

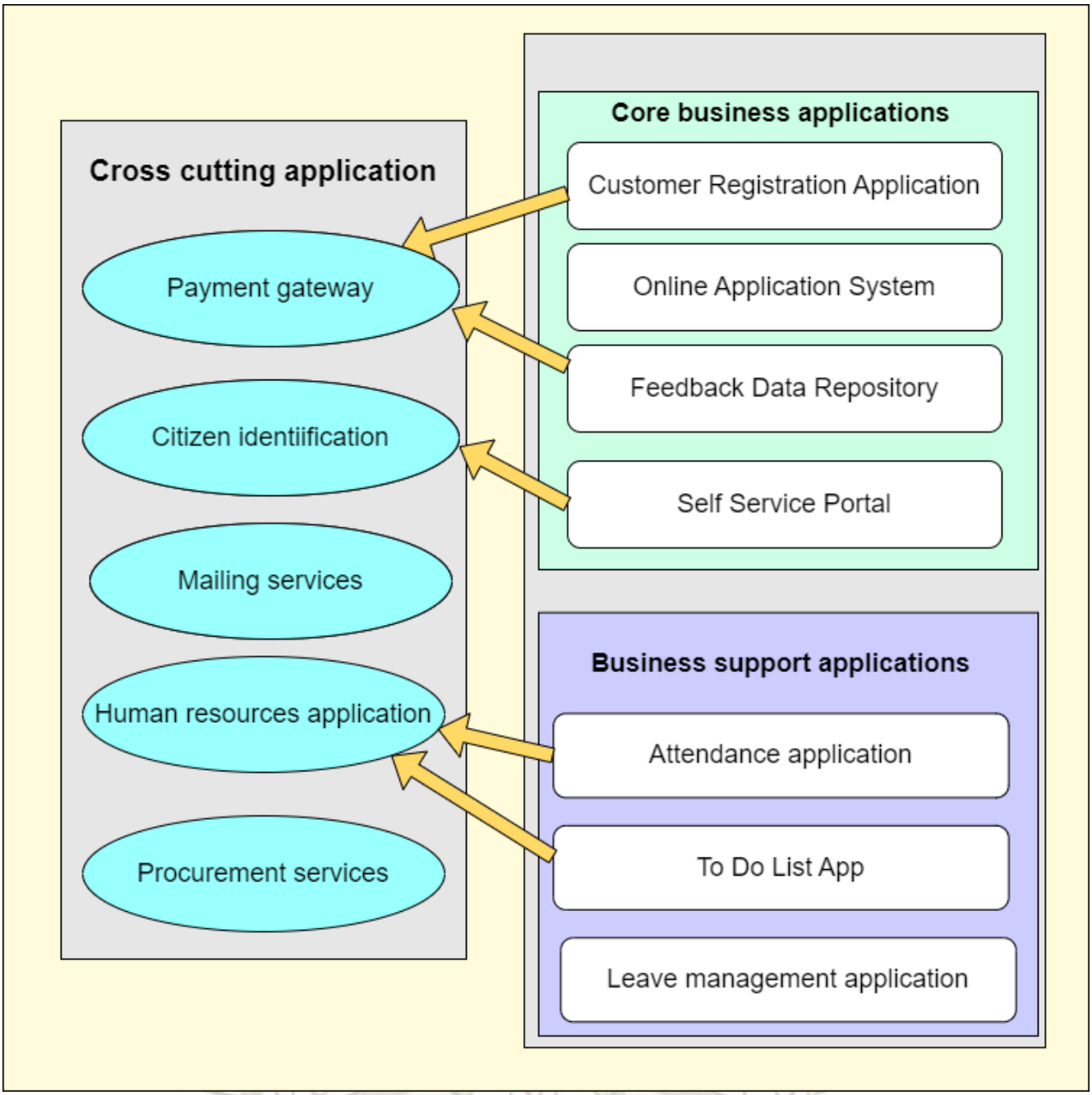
Appendix E-1: Example of Application Reference Model



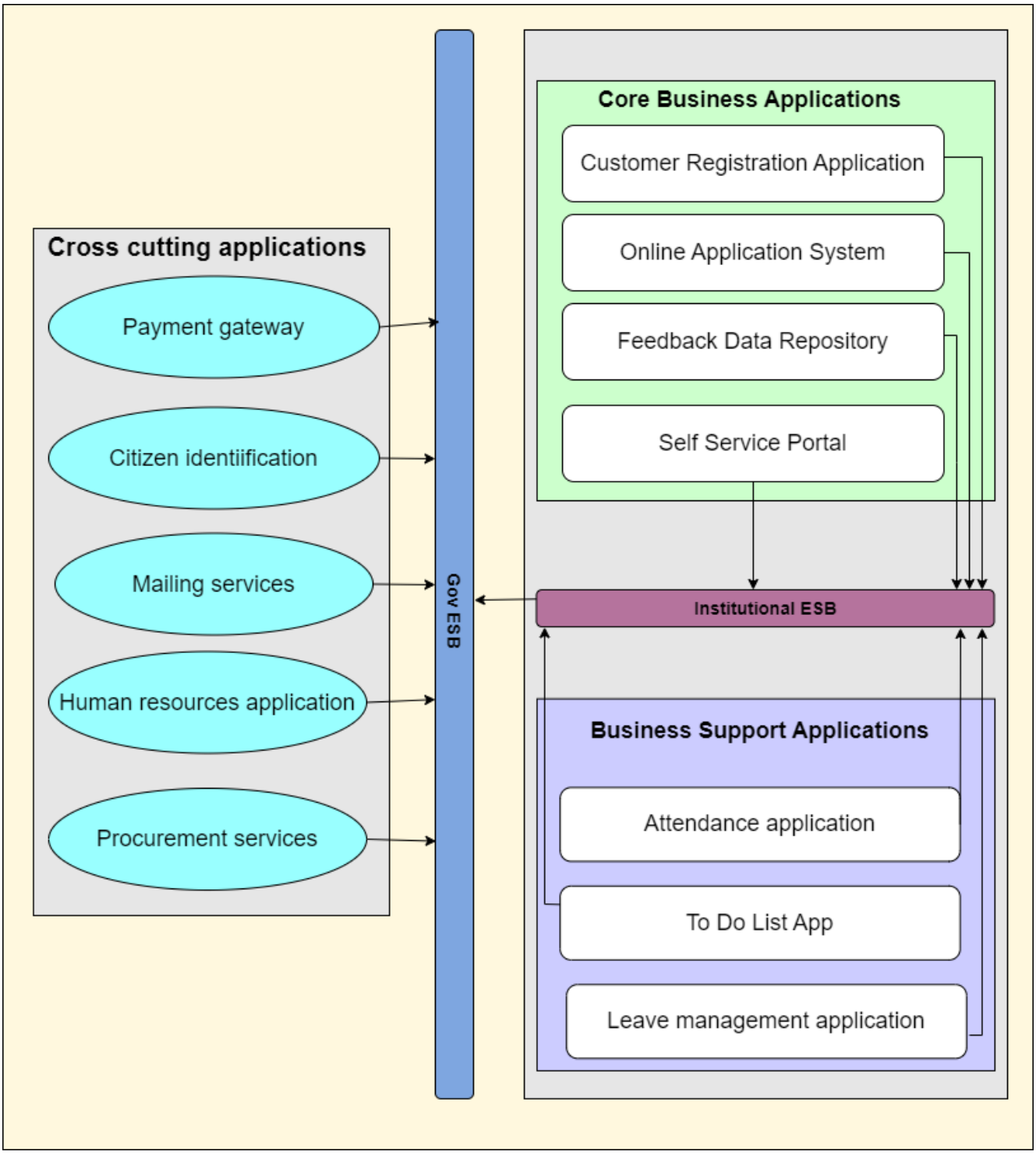
Appendix E-2: Example of application catalogue

Business Function	Sub function	Services	Application
Corporate Services	Planning Management	Budget	PlanRep
		Monitoring	PlanRep
	Human resources management	Recruitment	Ajira Portal
		Benefits processing	HCMIS
Corporate communication			

Appendix E-3: Example of Baseline Application Architecture Diagram



Appendix E-4: Example of Target Application Architecture Diagram



APPENDIX F – TECHNOLOGY ARCHITECTURE PHASE

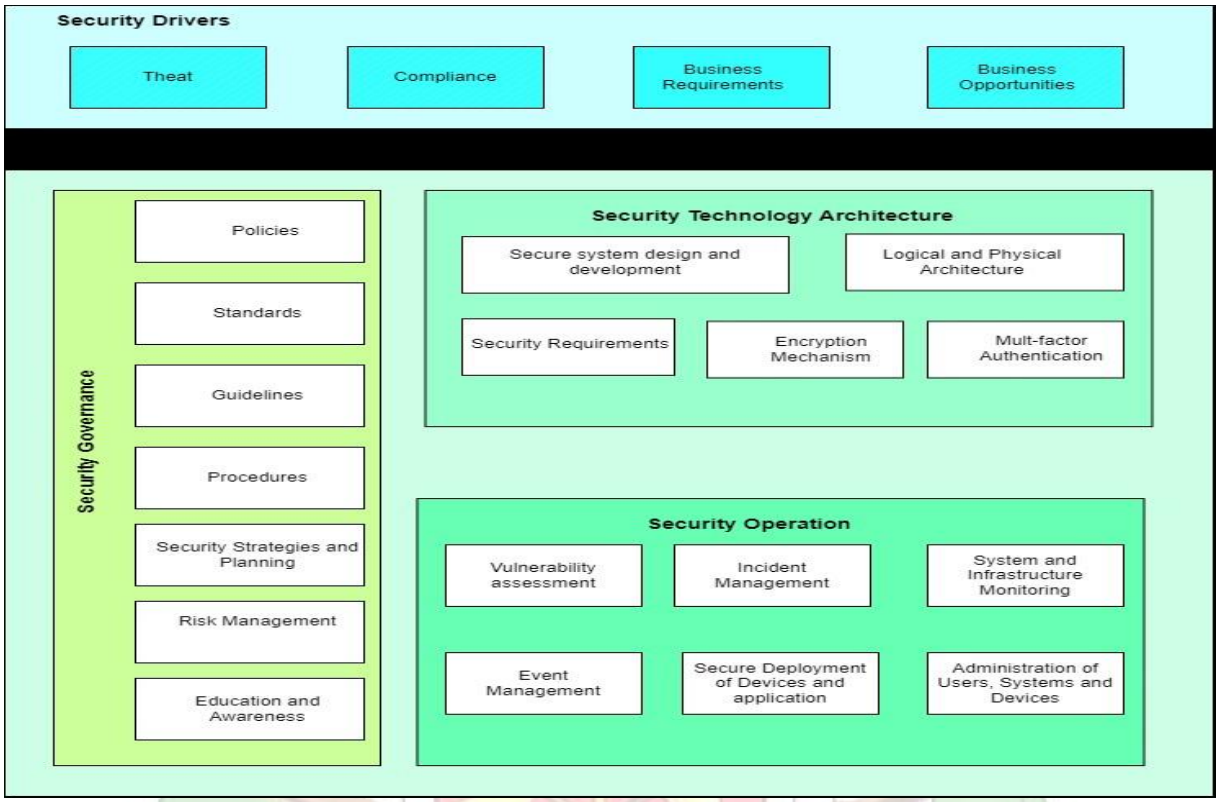
Appendix F-1: Baseline/Target Architecture Table

S/N	Component	Baseline Technology Architecture Description
1.	Service area	a. **Access Channel:** b. **Delivery Channel:** c. **Presentation:**
2.	Application Delivery Infrastructure	a. **Web Servers:** b. **Mail Servers:** c. **Hosting Control Panel:** d. **Client-Side Technology (User Interface):** e. **Server-Side Technology:** f. **Mobile Technology**: g. **Deployment Architecture:**
3.	Middleware Infrastructure	a. **Enterprise Service Bus:** b. **Message Brokering and Queuing:** c. **Application Programming Interface (API):**
4.	Database Management Infrastructure	a. **Database Servers:** b. **Caching Technology: Database Optimization:**
5.	Computing Platforms, Peripheral and Sensors	a. **Operating Systems:** b. **Virtualization:** c. **Containerization:** d. **Container Orchestration:** e. **Servers/Hosts:** f. **Storage (Type: Block/File):** g. **End-User Computing and Peripherals:** h. **Environmental Sensors:** i. **Method of service delivery:** j. **File Sharing:**
6.	Communication Infrastructure	a. **Media of Transmission:** b. **Network Equipment:** c. **Internet Service Provider:** d. **Traffic Routing:** e. **Packet Routing Technique:**

S/N	Component	Baseline Technology Architecture Description
		f. **Network Segmentation:** g. **Protocol:**
7.	System and Infrastructure Management	a. **Performance Monitoring:** b. **Software License Management:** None c. **Incident/Fault Management Technology:** d. **Disk encryption:**
8.	System Security Infrastructure	a. **Identity, Access Control and Authentication:** b. **Encryption Protocols:** c. **Digital Signature, Digital Certificate, SSL Certificate:** d. **Audit Tools:** e. **Assessment Tools:** f. **Verification of DNS information and domains signing:** g. **Security information and event management:** h. **Network security technologies:**
9.	Software and Infrastructure Engineering	a. **System Design/Modeling:** b. **Network Design:** c. **Infrastructure Design:** d. **Integrated Development Environment:** e. **Testing Tools:** a. **Software:** b. **Network:** f. **Configuration Management Software:** g. **Deployment methodology:**

APPENDIX G – SECURITY ARCHITECTURE PHASE

Appendix G-1: Example of Security Reference Model



APPENDIX H-OPPORTUNITIES AND SOLUTIONS PHASE

Appendix H-1: Consolidated gap analysis with their solutions

Consolidated Gaps, Solutions, and Dependencies Matrix				
S/N	**Architecture**	**Identified Gap**	**Proposed Solution**	**Dependencies**
1.	**Business**	Inadequate engagement of external stakeholders in development of shared systems	Analysis and engagement of stakeholders in any shared solution throughout its implementation	Stakeholders' availability
13.	**Technology**	Outdated Operating Systems	Replace all operating systems that have reached end of life with supported ones.	• Availability of trained personnel; • Availability of equipment
24.	**Data**	Interoperability: Lack of standardized data exchange protocols	Adopt and enforce open standards (e.g., XML, JSON, APIs)	Develop comprehensive data governance framework
32.	**Application**	Inadequate System documentations	Ensure all aspects of systems development are well-documented, including requirements, design, code, APIs, test cases,	• Documentation tools; • Business analyst; • Technical writers; • Software Developers cooperation; Continuous integration processes.

			deployment guides, and user manuals.	
35.	**Security**	Enhanced Helpdesk System for Incident Report	Fully operationalized Helpdesk system to cover incident management reports requirements.	• Fund; • Developers; • ICT security expertise; Integration with existing security systems.

Appendix H-2: Implementation Constraints

Implementation Constraints			
S/N	**Factor**	**Description**	**Proposed Action**
1.	Regulatory Compliance	Adherence to laws, standards, and regulations.	i. Take the required steps to abide by the law; ii. Take into account privacy and data protection restrictions.
2.	Technical Skills	Accessibility of required technical expertise and training.	Make a plan for skill development and training.
3.	Cost	The necessary financial resources for implementation and maintenance.	i. Perform a cost-benefit analysis ii. Make long-term financial plans.
4.	Vendor Dependence	Dependence on vendors for hardware, software, or other services.	i. Evaluate the dependability of vendors and their backup plans; ii. Diversify vendor base.

APPENDIX-I: MIGRATION PLANNING PHASE

Appendix I-1: Implementation and Migration Plan

Program	Project	Milestones	Timeline			Resource Requirements and Costs
			Duration	Start Date	End date	
DOCUMENTATION						
INFRASTRUCTURE ENHANCEMENT						

ACQUISITION AND CONFIGURATION						

APPENDIX J- ARCHITECTURE IMPLEMENTATION PHASE

APPENDIX J- ARCHITECTURE GOVERNANCE PHASE

APPENDIX K- ARCHITECTURE CHANGE MANAGEMENT PHASE

APPENDIX L - OTHERS

Appendix L-1: Architecture Requirements Specification

1. Architecture Requirements

1.1 Architecture Requirements
<<List all Architecture requirements >>
eg.
Requirement: Automated invoice processing
Desrption: The system shall automate the processing of invoices to reduce manual effort, improve accuracy, and accelerate the billing cycle

1.2 Interoperability Requirements
<<List interoperability requirements>>
eg.

Requirement: Unified Customer Data Access
Description: Enable seamless access to customer data across all business units and systems to ensure a consistent and unified customer experience

1.3 Constraints
<<List Constraint for requirements >>
eg.:
1. Constraint: Budget constraint
Description: Limited financial resources can restrict the scope of requirements management activities, including stakeholder engagement, tools and technologies for requirements capture, and validation processes.
Impacts: May lead to incomplete or inadequately defined requirements, affecting the overall quality and feasibility of the architecture

1.4 Assumptions
<<list assumptions for requirements>>
eg.
Requirement: Implementation of a Centralized Customer Data Repository
Description: Establish a centralized repository to consolidate customer data from multiple systems, ensuring a single source of truth
Assumptions:
i. Adequate funding will be available throughout the project lifecycle to cover all necessary expenses, including software, hardware, and professional services.

1.5 Success Measures
<<List success measure for architecture requirements>>

2. Service Contracts

2.1 Business Service Contracts
<<List the applicable Business service Contracts>>

2.2 Application Service Contracts
<<List the applicable Application service contracts>>

Appendix L-2: Risk Register

<<Insert name of public institution>>

RISK MANAGEMENT REPORT FOR THE YEAR <<Insert FY>>

- **PERIOD:** <<Insert period>>

RISK MANAGEMENT REPORT FOR QUARTER I (JULY – SEPTEMBER 2021)

1. Risk Management Context

1.1 Factors affecting Operations

i. Fast changing ICT Technology

ii. Inadequate Human Resources

iii. Insufficient Financial Resources

iv. Increase in service demands

v. ICT market trends

vi. Changing ICT requirements

1.2 Risk Appetite

Risk Appetite Categories	Risk Appetite Statements

Strategic	<<Insert name of public institution>> will accept a moderate degree of risk in pursuing a new strategic initiative that is in alignment with the strategic objectives.
Operations	<<Insert name of public institution>> will accept a minimal level of technical staff turnover given the nature of our operations and the industry in general.
Standards	<<Insert name of public institution>> will not accept any deviations from e-Government Standards and Guidelines as well as internal ICT rules and procedures.
Compliance	<<Insert name of public institution>> will not tolerate non-compliance with any legal or regulatory or professional compliance.

1.3 Risk Tolerance

Response	Threat	Opportunity
Action required	Unacceptable risks; <<Insert name of public institution>> will not tolerate threats whose consequences coupled with likelihood is acceptably high.	Opportunities; <<Insert name of public institution>> must pursue opportunities whose positive consequences coupled with the likelihood are so large because it cannot afford to forego the associated benefits.
Potential action	<<Insert name of public institution>> can tolerate the threat at their current levels if the costs associated with implementing additional control measures outweigh the associated benefits.	<<Insert name of public institution>> may wish to pursue opportunities if the benefits outweigh the costs associated with implementing the strategies required to realize the opportunity.

No action required	Acceptable risks; <<Insert name of public institution>> can tolerate the threats at their current levels after existing controls.	<<Insert name of public institution>> will give a low priority to opportunities if the benefits are not sufficient to expand resources on pursuing.

2. RISK ASSESSMENT

Risk Title: Possibility of cyber-attacks that may result into destruction of ICT infrastructure, systems and data as well as financial loss.						**Risk ID: r-001**
Risk	Possibility of destruction of ICT infrastructure, systems and data as well as financial loss.					
Principal risk owner	<<Insert Unit/Directorate/department etc>>					
Supporting owner(s)	Manager of <<<<Insert Unit/Directorate/department etc>>>>					
Risk Category	Strategic					
Objective/Plan	D: Compliance to policies, laws, regulations, standards and guidelines related to e-Government initiatives in Public Institutions enhanced.					
Process/ Section:	ICT Security Management					
Causes: - Less consideration on e-Government security standards and guidelines. - Inadequate cyber-security skills and awareness - Inadequate sophisticated tools for handling cyber security management		**Consequences:** - Failure of e-services delivery, - Financial Loss. - .				
Inherent risk analysis (tick the appropriate rating basing on the scenarios that current controls do not exist or completely fail)						
Inherent risk	**Consequence:**	VERY HIGH ✓	HIGH	MODERATE	LOW	VERY LOW
	Likelihood:	VERY HIGH	HIGH ✓	MODERATE	LOW	VERY LOW
Risk rating	**Consequence x Likelihood**					
Key risk mitigation/controls currently in place and their weaknesses: 1. Deployment of semi-automated security monitoring tools. 2. Provision of trainings to ICT officers responsible for security management.						

3.						
Residual risk analysis (tick the appropriate ratings basing on remaining risk levels after the above existing controls)						
Residual risk	**Consequence:**	VERY HIGH ✓	HIGH	MODERATE	LOW	VERY LOW
	Likelihood:	VERY HIGH	HIGH	MODERATE ✓	LOW	VERY LOW
Risk rating	**Consequence x Likelihood**					
Actions/mitigating controls to be taken: (actions to be put in place to reduce the risk at tolerable levels, including resources required for each action – financial, physical assets or human)						
Treatment Actions: 1. Application of automated tools to improve security management and monitoring of Government systems 2. Enhancing ICT security assessments. 3.				**Resources Required:** 1. Financial resources. 2. Hardware and software (Human resources.		

Risk Title:						**Risk ID:**
Principal risk owner						
Supporting owner(s)						
Risk Category						
Objective/Plan						
Process/Section:						
Causes: -			**Consequences:** -			
Inherent risk analysis						
Inherent risk	**Consequence:**		✓			
	Likelihood:			✓		
Risk rating	**Consequence x Likelihood**					
Key risk mitigation/controls currently in place and their weaknesses: 1.						
Residual risk analysis (tick the appropriate ratings basing on remaining risk levels after the above after the above existing controls)						
Residual risk	**Consequence:**			✓		
	Likelihood:			✓		
Risk rating	**Consequence x Likelihood**					

Actions/mitigating controls to be taken:	
Treatment Actions: 1. Research on emerging technologies. 2.	**Resources Required:**

Compiled By:
Name:
Signature:
Date:

Approved By:
Name:
Signature:
Date:

Reviewed By:
Name:
Signature:
Date:

Appendix L-3: Gap analysis sample table

S/N	Gaps	Recommendations
1.	Database Management Infrastructure improvement	▪ Deploy NoSQL Databases and use them to run unstructured data; and ▪ Deploy data management tools for big data analysis.
2.	Enhanced Helpdesk system	Enhance Helpdesk system to automate knowledge base management processes to improve customer service, support, and statistics processes.
3.		
4.		
5.		
6.		
7.		
8.		

Appendix L-4: Implementation Factor Assessment and Deduction Matrix

Implementation Factor Assessment and Deduction Matrix			
SN	**Factor**	**Description**	**Deduction**
1	Change in Technology	Shut down the message centers, saving 700 personnel, and have them replaced by email	Need for personnel training, re-assignment • Email has major personnel savings and should be given priority
2	<<Insert factor>>	<<insert description>>	<<insert deduction>>

Appendix L-5: Architecture Definition Increment Table

Architecture Definition - Project Objectives by Increment

Project	April 2021/2022	April 2022/2023	April 2023/2024	Comments
	Transition Architecture 1: Preparation Transition	Architecture 2: Initial Operational Capability Transition	Architecture 3: Benefits	
Enterprise e-Services	Training and Business Process	e-Licensing Capability	Capability e-Employ	<<Insert comment>>
<<Insert project>>				