GOVERNMENT DIGITAL ENTERPRISE ARCHITECTURE (GEA) DOCUMENT

Government Enterprise Architecture Guidelines

3rd Edition
ICTA GEA: 001:2025

REPORT PREPARED BY:

nicoza africa

The ICT Authority is a State Corporation under the State Corporations Act 446

www.icta.go.ke

SUMMARY SHEET

Project Type	Information, Communication Technology (ICT)	**Reporting Period:**	**From:** **To:**	April 2025 December 2025
Project Name:	**TITLE: DEVELOPMENT OF GOVERNMENT DIGITAL ENTERPRISE ARCHITECTURE AND E-GOVERNMENT INTEROPERABILITY FRAMEWORK**			
Project Description:	Strategy, Project Planning & Design, Institutional Development, and Capacity Building			
Offices:	**NAIROBI, KENYA** Physical Address: Teleposta Towers 12th Floor Kenyatta Avenue, Nairobi P.O. Box 27150 - 00100, Nairobi, Kenya **Phone Numbers:** (+254) 793 879629 (+254) 20 6676999 (+254) 20 2211960 (+254) 20 2211961 **E-Mail Addresses:** General Inquiries - Communications: communications@icta.go.ke **Website:** https://www.icta.go.ke/	**Document prepared by:**	**NICOZA AFRICA LIMITED** 1st Floor, Nyumba Bora, Karen, Nairobi E: info@nicoza.co.ke W: www.nicoza.co.ke	
Executing Authority		**Project Office**	**Contractor Contacts**	
Name:	**ICT AUTHORITY**	**Physical Address:** Teleposta Towers, 12th Floor Kenyatta Avenue, Nairobi, Kenya P.O. Box 27150 - 00100, Nairobi, Kenya **Phone Numbers:** (+254) 793 879629 (+254) 20 6676999 (+254) 20 2211960 (+254) 20 2211961 **E-Mail Addresses:** info@icta.go.ke **Website:** https://www.icta.go.ke/	**NICOZA AFRICA LIMITED** 1st Floor, Nyumba Bora, Karen, Nairobi E: info@nicoza.co.ke W: www.nicoza.co.ke	
Contact Persons:	**Terry Ong'amo**		**Monte Kajamaa**	
Email:	Terry.ongamo@moict.go.ke +254 721 140710		monte@nicoza.co.ke +254 722 589625	
Report Date:	**25th February 2026 (iteration 3)**			

PREAMBLE

The Government of Kenya recognizes that digital transformation is fundamental to achieving national development objectives, strengthening public sector performance, enhancing transparency and improving the quality of services delivered to citizens, businesses and investors. As Kenya advances toward its long-term development aspirations, digital government is no longer optional; it is a strategic necessity for building a responsive, efficient, and globally competitive nation.

Guided by national priorities articulated in Kenya Vision 2030, the Digital Economy Blueprint, and the National Digital Master Plan 2022–2032, the Government is committed to establishing a modern digital public sector that operates as a single, coordinated enterprise. This commitment reflects the recognition that effective governance in the digital era requires integrated institutions, shared platforms, trusted data, and secure digital infrastructure.

Despite significant progress in digitization initiatives, structural challenges persist across the public sector. Fragmented systems, siloed data environments, duplication of investments, vendor lock-in, inconsistent standards, and limited interoperability continue to constrain service delivery and reduce the efficiency of public expenditure. These challenges undermine the ability of government institutions to operate cohesively and limit the realization of a seamless citizen experience.

To address these challenges, the Government of Kenya through the KDEAP programme is instituting a revised Government Enterprise Architecture (GEA) framework as the authoritative national blueprint for planning, designing, governing, and integrating digital capabilities across all Ministries, Departments, Counties, State Corporations, and Agencies (MCDA). GEA establishes a structured and standardized approach that aligns policy objectives, business processes, information assets, applications, technology infrastructure, and governance mechanisms to ensure coherent and sustainable digital transformation.

The GEA framework embodies key national principles, including citizen-centric service delivery, Whole-of-Government integration, data-driven decision-making, security and privacy by design, reuse of shared capabilities, fiscal prudence, and adherence to open standards. Through this framework, the Government seeks to eliminate fragmentation, strengthen institutional coordination, and enable the delivery of secure, interoperable, and high-quality digital services.

By institutionalizing enterprise architecture across government, Kenya will enhance its ability to implement national programmes effectively, improve policy execution, strengthen resilience against emerging risks, and foster trust in digital government. The GEA therefore serves as a critical enabler for achieving national development priorities and advancing Kenya's position as a regional innovation leader in the digital economy space.

EXECUTIVE SUMMARY

Kenya's commitment to digital governance is a cornerstone of its national development agenda and a key driver for economic growth, public sector modernization, and social inclusion. The Government Enterprise Architecture (GEA) framework provides the strategic and operational foundation required to transform government into an integrated, agile, and citizen-focused enterprise.

The GEA establishes a common architecture framework, standards, and governance mechanisms that enable government institutions to align their strategies, business processes, data assets, and technology investments. By providing a unified approach to digital services development, data and application lifecycle management and infrastructure deployment, the framework reduces duplication, improves interoperability, strengthens cybersecurity, and optimizes the use of public resources.

GEA also strengthens governance by providing clear oversight mechanisms for architecture compliance, investment planning and digital programme execution to ensure that major national initiatives are implemented consistently, aligned with national priorities, and designed for long-term sustainability.

By embedding enterprise architecture into the fabric of government operations, Kenya will accelerate the delivery of digital services, enhance institutional coordination, improve accountability, and support evidence-based policymaking. Thereby positioning MCDAs to respond effectively to emerging technological opportunities and risks while advancing inclusive and resilient national development.

KENYA'S DIGITAL TRANSFORMATION JOURNEY

Kenya's digital transformation journey is anchored in its long-term national development blueprint, **Kenya Vision 2030**, which seeks to transform the country into a globally competitive and prosperous nation with a high quality of life for all citizens. The vision recognizes Science, Technology and Innovation and Public Sector Reform as foundational enablers for achieving economic growth, social development, and effective governance.

The Government's digital transformation agenda is further articulated through the **Digital Economy Blueprint** and operationalized through the **National Digital Master Plan 2022–**

2032, which provide a comprehensive roadmap for leveraging digital technologies to enhance service delivery, strengthen institutional capacity, and drive innovation across the economy.

Further supporting priorities, the Kenya Digital Economy Acceleration Project (KDEAP) is advancing investments in digital infrastructure, digital government services, and digital skills development. These initiatives are expanding connectivity, enabling the digitization of public services, and strengthening the digital capabilities required for inclusive growth.

GEA provides the structural and governance foundation necessary to ensure that these initiatives are implemented in a coordinated, interoperable, and sustainable manner through the establishment of common standards, reference models, and integration mechanisms ensuring that investments in digital infrastructure and services contribute to a coherent national digital ecosystem rather than isolated initiatives.

Through the adoption of GEA, the Government will strengthen alignment between national programmes, improve coordination across institutions, and ensure that digital transformation efforts collectively advance national development goals.

PURPOSE OF DOCUMENT

This framework is intended for a broad spectrum of stakeholders involved in the planning, implementation, governance, and advancement of Enterprise Architecture (EA) and Interoperability initiatives across the public and private sectors. It is specifically targeted at the persona below:

Audience	Description
Government Entities at National and County Levels	Ministries, departments, state corporations and agencies (MCDA) regardless of their current level of enterprise architecture maturity.
Senior Government Officials and Executive Sponsors	All individuals tasked with overseeing, championing, and guiding EA and digital transformation programs. This document is designed to augment their understanding and encourage active leadership participation and policy alignment.
Enterprise Architects, Solution Architects, Business Analysts, and Developers	Professionals responsible for designing, integrating, and optimizing government systems and services, who require

	standardized, scalable, and efficient frameworks to enhance service delivery to citizens and other stakeholders.
Consultants and Technology Practitioners	Organizations or Individuals engaged in designing and delivering innovative solutions for public sector clients, including those working on interoperability, systems integration, and digital transformation projects within the broader government ecosystem.
Public Policy Managers, ICT Trainers, and Educators	Individuals and institutions seeking to disseminate knowledge on enterprise architecture, interoperability, and digital government principles as part of curriculum development, capacity building, or policy formulation.
Government ICT Professionals and Planners	Individuals and institutions involved in strategic ICT planning, digital governance, procurement, program management, and advisory roles, who play a pivotal part in shaping and implementing government-wide digital strategies.

The ICT Authority (ICTA) under the Ministry of ICT and the Digital Economy (MICTDE) is vested with the mandate to establish and enforce comprehensive ICT standards and guidelines throughout the entire public service sector organizations. This mandate is crucial for fostering a coherent and unified approach to the acquisition, deployment, management, and operation of ICTs, ultimately aiming for secure, efficient, flexible, integrated, and cost-effective digital environments by virtue of being the implementer and custodian of the GEA framework and governance.

TABLE OF CONTENTS

TABLE OF FIGURES

ABBREVIATIONS AND ACRONYMS

GEA	Government Enterprise Architecture
GIF	Government Interoperability Framework
MICDE	Ministry of ICT and the Digital Economy
ICTA	Information and Communication Technology Authority
MCDA	Ministries, Counties, Departments, and Agencies
WoG	Whole of Government
EA	Enterprise Architecture
API	Application Programming Interface
BPR	Business Process Reengineering
BRM	Business Reference Model
ARM	Application Reference Model
DRM	Data Reference Model
TRM	Technology Reference Model
SRM	Security Reference Model
GRM	Governance Reference Model
MDM	Master Data Management
JSON	JavaScript Object Notation
DCAT	Data Catalog Vocabulary
AI	Artificial Intelligence
TOGAF	The Open Group Architecture Framework
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
EGDI	e-Government Development Index
ARB	Architecture Review Board
PGB	Program Governance Board

INTRODUCTION

WHAT IS GOVERNMENT ENTERPRISE ARCHITECTURE (GEA)?

Government Enterprise Architecture (GEA) is the Government of Kenya's authoritative Whole-of-Government framework and management discipline for planning, designing, integrating, and governing the evolution of public sector institutions, services, information, and technology. It provides a structured approach for understanding how government currently operates and directing its transformation toward a coordinated, efficient, secure, and digitally enabled future state in which government functions as a single, integrated enterprise.

GEA establishes the principles, standards, reference models, and governance mechanisms that guide how MCDAs plan and implement digital initiatives, manage information assets, and deliver public services. By aligning strategy, policy objectives, business processes, data, applications, and technology investments, GEA ensures that government operates cohesively rather than as a collection of independent systems and initiatives.

Through a disciplined enterprise architecture practice, GEA assesses the current ("as-is") environment, including institutional mandates, policies, services, processes, data ecosystems, applications, infrastructure, and operational capabilities, and defines a clear pathway toward a desired ("to-be") architecture that supports national development priorities, improves service delivery outcomes, strengthens accountability, and optimizes the use of public resources.

GEA adopts an enterprise-wide perspective that ensures business capabilities, information assets, digital platforms, and technology infrastructure are coherently designed, integrated, and governed across institutional boundaries. It promotes interoperability, reuse of shared platforms and services, standardization, and evidence-based decision-making, enabling government to respond effectively to evolving policy demands, technological change, and emerging risks.

As both a strategic planning framework and a governance instrument, GEA enables government to deliver seamless and citizen-centred digital services, reduce duplication and fragmentation, strengthen cybersecurity and resilience, enhance transparency, and support coordinated implementation of national programmes. It provides the foundation for managing complexity across the public sector while ensuring that digital transformation initiatives contribute to a unified national vision.

GEA FRAMEWORK STRUCTURE

The GEA framework is structured as a set of interconnected architecture domains that collectively provide a comprehensive view of how government plans, delivers, secures, and governs public services across the Whole-of-Government ecosystem. These domains function as complementary layers that together define the operating model of government as an integrated enterprise, ensuring that strategic intent, service delivery, information management, and technology capabilities are aligned. See *Figure 1* below.

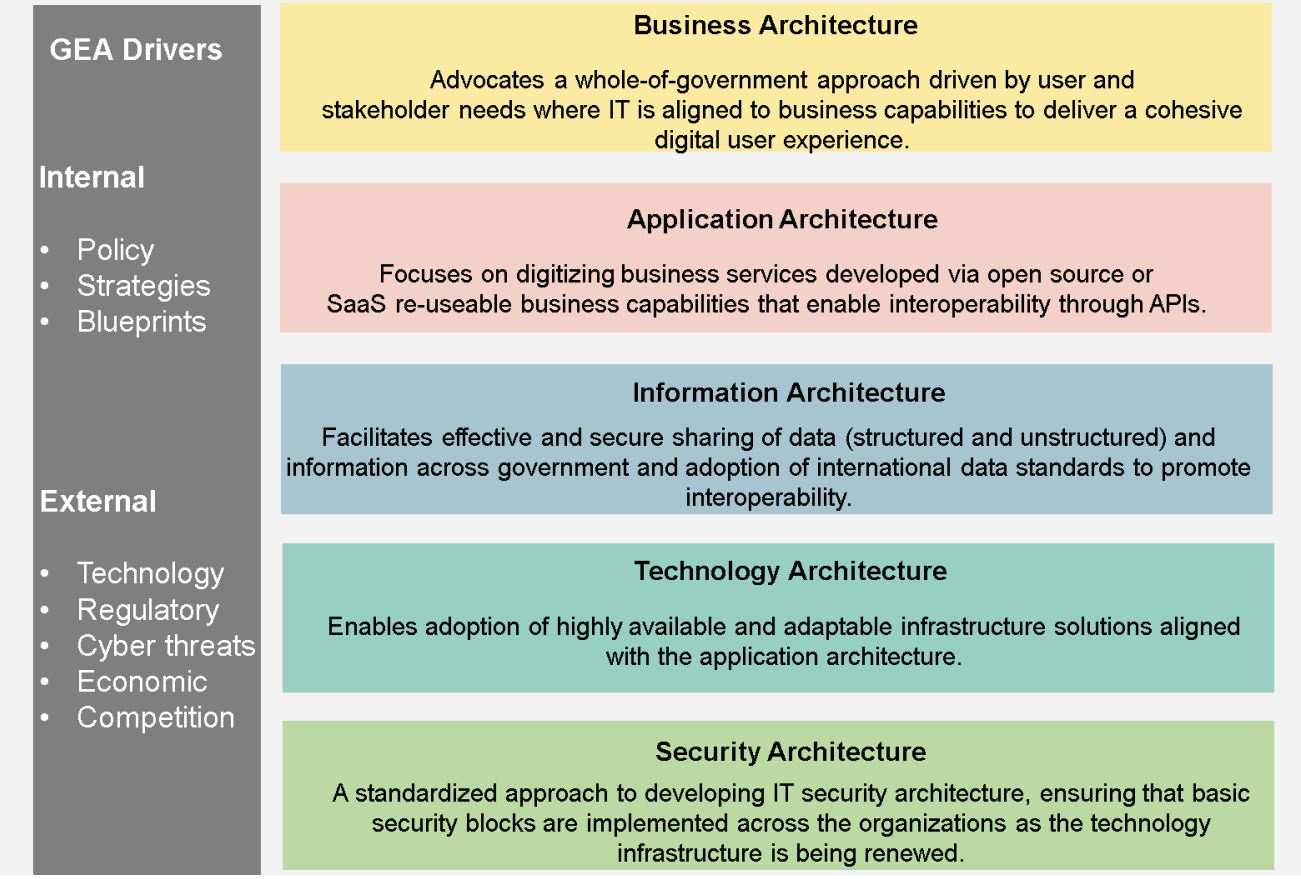

Figure 1 – GEA Holistic View

Business Architecture defines government's strategic objectives, policy priorities, service portfolios, and business capabilities. It ensures that public services are designed around the needs of citizens, businesses, and stakeholders and aligned with national development goals. Business Architecture provides the foundation for prioritizing initiatives, improving service outcomes, and ensuring policy coherence across institutions.

Application Architecture defines the portfolio of digital systems, shared platforms, and application services that enable government to deliver its mandates. It ensures that systems are designed for interoperability, reuse, scalability, and integration, enabling seamless service delivery and efficient collaboration across agencies.

Information Architecture establishes how government data and information are governed, managed, shared, protected, and leveraged as strategic national assets. It supports trusted data exchange, analytics, and evidence-based policymaking while ensuring that information is accurate, secure, and accessible to authorized users across government.

Technology Architecture defines the infrastructure, networks, cloud environments, platforms, and technical services required to support secure, reliable, and scalable digital operations. It provides the technological foundation that enables government systems to operate efficiently and adapt to changing needs.

Security Architecture is a cross-cutting domain that safeguards government systems, protects sensitive information, ensures compliance with legal and regulatory obligations, and maintains trust in digital services. It embeds security, privacy, and resilience considerations across all architecture domains.

Government priorities and architectural evolution are shaped by internal drivers, including national strategies, policies, fiscal considerations, and institutional mandates, as well as external factors such as regulatory developments, technological innovation, emerging risks, and global trends. These influences ensure that the framework remains responsive and adaptable to changing circumstances.

Together, these components show how government works as one connected system where services, information, and technology are aligned to deliver seamless, efficient, secure, and high-quality public services.

Enterprise Architects, under the governance of the national architecture function, develop and maintain authoritative “as-is” and “to-be” views of MCDAs and capabilities. These views inform strategic planning, investment decisions, and transformation initiatives, providing a clear understanding of current capabilities and future direction.

Through structured gap analysis, institutions can identify capability shortfalls, manage risks, and prioritize initiatives in a coordinated manner, ensuring that transformation efforts are aligned with national priorities and deliver measurable public value. This disciplined approach strengthens coordination between policy leadership, operational management, and technical delivery teams.

Without the adoption of the GEA framework, digital initiatives risk becoming fragmented, duplicative, and inefficient, leading to increased costs, inconsistent service delivery, and reduced ability to achieve Whole-of-Government outcomes. The framework therefore provides an essential foundation for coherent, sustainable, and accountable digital transformation across government.

GEA VISION AND MISSION

VISION STATEMENT

To cultivate a unified and trusted national digital ecosystem where data flows seamlessly and securely across the Whole-of-Government to deliver value through, citizen-centric services that are efficient, accessible, and responsive to the needs of all Kenyans.

MISSION STATEMENT

To design, implement, and govern a standardized, secure, and interoperable enterprise architecture framework for the Government of Kenya.

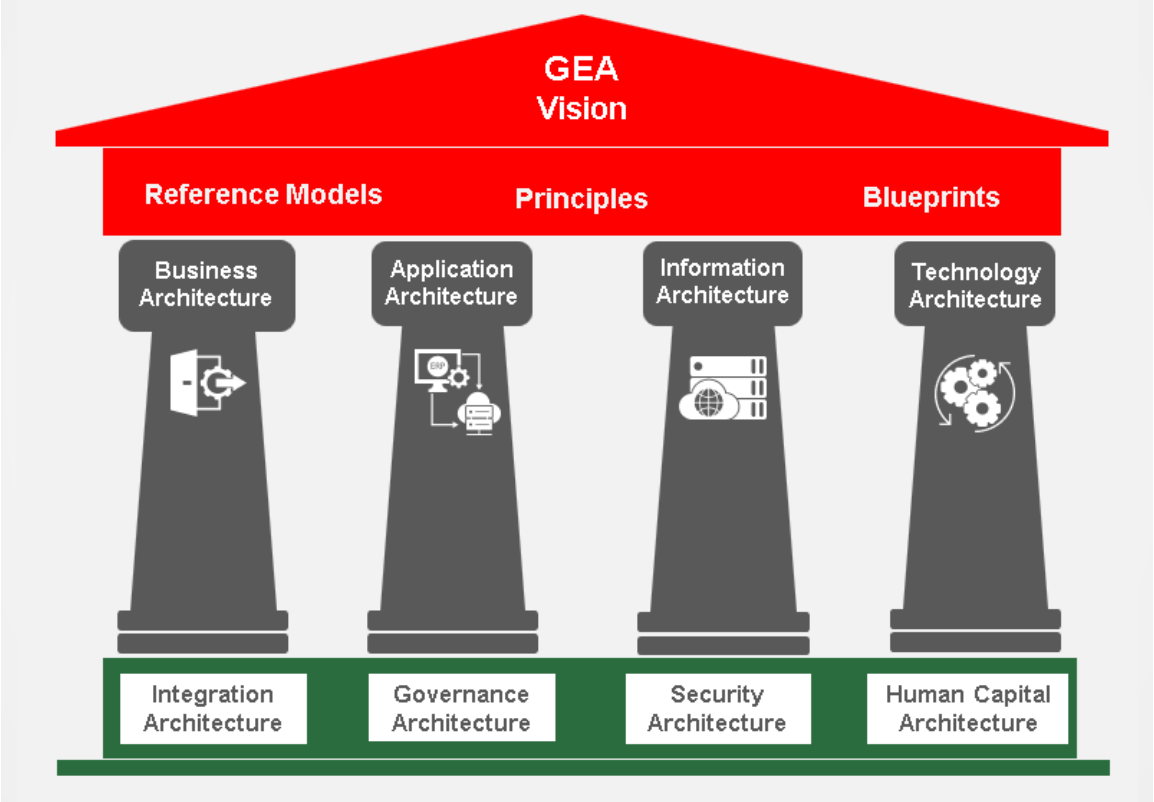

Figure 2 - GEA Framework Structure

WHOLE OF GOVERNMENT (WOG) APPROACH

The 'Whole-of-Government' (WoG) approach is a concept that underscores the critical need for enhanced collaboration and coordination across sectoral and departmental boundaries within public administration. Its primary objectives are multifaceted: to eliminate redundant

efforts, optimize the allocation and utilization of resources, foster synergistic relationships across diverse government ecosystem, and ultimately, deliver integrated and seamless services to both citizens and businesses.

This concept represents a paradigm shift in public administration by moving away from fragmented, siloed operations intentionally towards integrated, collaborative public administration.

It requires MCDAs to operate collectively, align priorities, and jointly design solutions to address complex public policy and service delivery challenges that cut across institutional mandates. This approach inherently involves cross-boundary operations and often necessitates structural, operational, and governance reforms to enable shared planning, shared execution, and shared accountability.

A core aim of WoG, therefore, is to fundamentally address and overcome the pervasive issue of 'departmentalism' or 'silos.' This refers to the rigid separation of mandates, systems, data, and decision-making structures that has historically characterized public institutions. These silos result in duplicated investments, inconsistent policies, fragmented service delivery, inefficient use of public resources, and limited visibility across the government ecosystem.

By alignment of common interests, actively preventing the duplication of tasks, reducing operational costs, and enhancing overall productivity, the WoG approach strives to achieve a coherent and unified line of action across the entire governmental apparatus by promoting:

- Alignment of national priorities and institutional objectives
- Prevention of duplication in systems, platforms, and services
- Reduction of operational and ICT lifecycle costs
- Improved productivity, responsiveness, and service quality

Furthermore, WoG approach promotes the establishment of shared resources, common platforms, interoperable systems, and standardized information exchange mechanisms to support integrated decision-making and coordinated service delivery. This transition is not merely organizational; it is systemic, requiring common governance structures, shared capabilities, and enforceable standards.

As a result, WoG is not merely an organizational preference but a strategic imperative for modern, effective public service delivery, without which, digital transformation initiatives risk enhancing the existing digital silos, leading to further fragmentation of digital services and prevent the realization of the full potential of significant public investments in technology.
WoG approach serves as the foundational organizational philosophy that must precede and guide the design and implementation of any comprehensive Government Enterprise Architecture and national digital transformation agenda.

GEA AS A STRATEGIC ENABLER OF WoG CONCEPT

GEA is the primary strategic instrument through which the Whole-of-Government approach is operationalized by providing a unified, enterprise-wide perspective that integrates all MCDAs into a single coherent architectural vision encompassing business processes, information assets, applications, technology infrastructure, governance mechanisms, and strategic direction.

The primary objective of GEA is to guide the planning, investment, and implementation of ICT systems, digital platforms, and infrastructure in alignment with MCDA strategic goals and national digital transformation priorities. Through a structured and standards-based framework, GEA streamlines the management of complex digital environments, facilitates the integration of disparate systems, reduces operational redundancies, and ensures that ICT capabilities are directly aligned with business objectives and service delivery outcomes.

The GEA framework provides the architectural foundation comprising blueprints, reference models, standards, best practices and alignment mechanisms needed to implement shared resources, seamless services, and cross-boundary cooperation envisioned under the WoG approach. In essence, GEA defines the architectural "***how"*** that enables the WoG "***what"***, translating policy intent into implementable structures and enforceable design constraints.

By applying systematic baseline ("as-is") and target-state ("to-be") architecture analysis, GEA enables MCDAs to:

- Identify duplication, fragmentation, and capability gaps
- Rationalize applications, data assets, and infrastructure
- Define coherent transformation roadmaps aligned to national priorities

- Coordinate investments across institutional boundaries

This structured approach directly addresses the recurring challenges of fragmented strategies, isolated system development, and ambiguous digital investment decisions that undermine public sector transformation efforts.

GEA, therefore, serves as the architectural backbone of the WoG operating model, ensuring that all digital initiatives whether sector, department or agency specific or cross-cutting the government ecosystem, contribute to a coherent, interoperable, and reusable government digital services that deliver measurable value to citizens and all stakeholders.

EXTENDING GEA ECOSYSTEM AND CROSS-BORDER ARCHITECTURE

Modern government service delivery operates beyond the traditional public sector boundaries and include strategic areas such as digital trade, regional integration, financial inclusion, identity assurance, and cross-border service delivery which require governments to interact seamlessly with private sector partners, development partners, platform providers, regional institutions, and other governments.

As such, the Whole-of-Government approach must evolve from an inward-facing coordination model to an ecosystem-oriented operating model, enabled and governed through GEA using ecosystem architecture and boundaryless information flow concepts.

GEA extends its scope to encompass and governance by defining government as an enterprise rather than a closed, self-contained entity and together multiple categories of participants (enterprises) as stakeholders in the ecosystem, including:

- Private sector service providers and technology vendors
- Financial institutions and payment service providers
- Identity, trust, and authentication service providers
- Regional and international digital platforms
- Development partners and PPP operators

GEA establishes architectural boundaries, roles, and responsibilities for each ecosystem participant, ensuring that integration occurs in a controlled, secure, and regulatory and policy-compliant manner. These boundaries are not barriers, but governance gates or interfaces that

enable cohesive collaboration while preserving sovereignty, accountability, and risk management.

By adopting and complying with established architecture reference models and standards, GEA streamlines the government operations and services to ensure that participation and contribution in the digital transformation within ecosystem is:

- Business-driven and outcome-oriented
- Data-consistent and semantically aligned
- Application and platform-agnostic
- Technically interoperable and standards-based
- Governed through clear accountability and compliance mechanisms

BOUNDARYLESS INFORMATION FLOW AND INTEROPERABILITY

Boundaryless Information Flow ensures that data, the essential resource that drives decisions and processes, can move freely across different systems and service. This is realized within GEA through the Government Interoperability Framework (GIF), which defines the legal, organizational, semantic, technical, and security conditions under which information can be securely exchanged across institutional and national boundaries.

Boundaryless information flow does not imply uncontrolled data sharing. Rather, it signifies the intentional removal of unnecessary structural, technical, and organizational barriers to information exchange, while maintaining strict controls over data ownership, privacy, consent, and security.

GEA, working in concert with GIF, enables:

- Secure data sharing between MCDAs and external partners
- Reuse of national digital platforms (Digital ID, payments, registries) by ecosystem actors
- Interoperability across sectoral and national systems in areas such as supply chain and logistics integration
- Policy-aligned information exchange across borders

This approach ensures that digital services can be composed and delivered across multiple organizations and jurisdictions as paperless, cashless, faceless, seamless digital experience for citizens and businesses.

PUBLIC–PRIVATE PARTNERSHIPS AND PLATFORM INTEGRATION

GEA provides the architectural and governance foundation for Public–Private Partnerships (PPPs) in the digital domain. Rather than treating PPP solutions as standalone or vendor-controlled systems, GEA mandates their alignment to national architecture standards, interoperability requirements, and platform strategies.

All PPP-driven digital solutions are required to:

- Integrate through the Government Integration Platform (GIP) using standardized APIs and shared services
- Conform to GEA reference architectures and GIF standards
- Support portability, reuse, and future extensibility in their digital services
- User open systems and standards to avoid proprietary lock-in and duplication of national capabilities

This ensures that private sector innovation and partnerships are harnessed in a manner that strengthens, rather than fragments, the government digital ecosystem.

CROSS-BORDER DIGITAL SERVICES AND REGIONAL INTEGRATION

As Kenya advances its regional and continental integration agendas, including trade facilitation, mobility, and digital economy initiatives, GEA provides the architectural basis for cross-border digital services.

GEA supports cross-border integration by:

- Defining interoperable identity, payments, and data exchange patterns
- Aligning national standards with regional and international frameworks
- Enabling trusted data exchange agreements and federated service models
- Supporting mutual recognition of digital credentials and services

Through this approach, GEA positions government systems to participate effectively in regional and global digital ecosystems, while maintaining national control over architecture, data, and policy enforcement.

GEA AS THE GOVERNING MECHANISM FOR THE DIGITAL ECOSYSTEM

GEA serves not merely as a design framework, but as the authoritative governance mechanism for managing participation, integration, and evolution of the government digital ecosystem. It establishes:

- Entry and onboarding criteria for ecosystem participants
- Mandatory compliance with interoperability and security standards
- Architecture conformance assessment and certification processes
- Continuous oversight of ecosystem risks, dependencies, and performance

By extending GEA beyond the government boundaries, the Whole-of-Government approach is transformed into a Whole-of-Ecosystem operating model, enabling the creation and delivery and support of integrated, scalable, and future-ready digital services at national, regional, and international levels.

OBJECTIVES OF GOVERNMENT ENTERPRISE ARCHITECTURE

GEA establishes the strategic foundation for planning, governing, and coordinating digital transformation across government enabling the Whole-of-Government approach by ensuring that policies, business processes, data, applications, and technology investments are aligned to national priorities, operate as an integrated ecosystem, and deliver measurable public value.

GEA provides the framework through which MCDAs design and implement digital initiatives in a consistent, secure, and interoperable manner. It strengthens governance, promotes reuse of shared capabilities, enhances investment discipline, and supports the delivery of seamless, citizen-centric services while safeguarding national digital assets.

1. **Ensure Strategic Alignment**

Ensure that all government digital and technology investments are aligned with national development priorities, Whole-of-Government principles, and approved sector strategies, delivering measurable outcomes and public value.

2. Establish a Unified Architecture Framework

Provide a coherent enterprise architecture framework that guides the planning, design, implementation, and evolution of digital initiatives across all MCDAs.

3. Strengthen Architecture Governance and Compliance

Enforce architecture governance processes, standards, and review mechanisms to ensure compliance with national policies, interoperability frameworks, and cybersecurity requirements.

4. Enable Integrated and Citizen-Centric Service Delivery

Support the design and delivery of integrated services by promoting coordinated business processes, shared platforms, and seamless user experiences across government.

5. Promote Interoperability and Secure Data Exchange

Enable secure and trusted information sharing across institutions through standardized interfaces, common data models, and interoperability mechanisms.

6. Enhance Digital Investment Governance

Embed architecture assurance within project approval, procurement, and funding processes to improve investment decisions, reduce duplication, and optimize the use of public resources.

7. Drive Reuse of Shared Platforms and Capabilities

Promote adoption of common digital platforms, shared services, and reference architectures to accelerate delivery, improve consistency, and reduce costs.

8. Elevate Data as a Strategic National Asset

Strengthen data governance, standardization, quality management, and lifecycle oversight to support evidence-based decision-making and responsible data sharing.

9. Ensure Security, Privacy, and Resilience by Design

Integrate cybersecurity, privacy protection, and resilience considerations across all architecture domains to safeguard government systems and build public trust.

10. Build Institutional Architecture Capability

Develop enterprise architecture skills, tools, and communities of practice across government to support effective implementation and continuous improvement.

11. Monitor Performance and Benefits Realization

Establish mechanisms to track compliance, measure outcomes, and assess the benefits of digital initiatives to ensure accountability and continuous optimization.

12. Support Innovation Within Governed Guardrails

Enable adoption of emerging technologies through clear standards and risk-managed experimentation while maintaining alignment with national priorities and architecture principles.

ADDRESSING KEY CHALLENGES - FROM SILOS TO SEAMLESS SERVICE DELIVERY

Kenya's GEA framework is designed to directly address several long-standing challenges that have historically impeded public sector efficiency and digital service delivery. These include:

These challenges along with their impact and solution within the GEA framework are summarized in the table below.

Challenge	GEA Solution	Impact
Siloed Systems & Departmentalism	• GEA Framework Architectures • Government Interoperability Framework (GIF) • Integration Architecture Principles.	Enhanced interoperability, seamless data exchange, cross-departmental collaboration, unified service delivery.

Duplication of ICT Investments & Suboptimal Resource Use	• GEA holistic approach and economies of scale • IT Governance Standard • Enterprise Architecture Principles	Significant cost efficiencies, optimized resource allocation, reduced duplication of projects, improved ROI on technology
Fragmented Service Delivery	• Digital one-stop-shop initiatives Government Interoperability Framework (GIF) • Application Architecture Principles (AAP) • Systems & Applications Standard.	Seamless, integrated, and citizen-centric services, improved accessibility and efficiency for citizens and businesses.
Lack of IT-Business Alignment	• Enterprise Architecture Principles • IT Governance Standard • GEA Framework (aligning business processes, information flows, and technology).	IT solutions directly support business goals, increased value delivery from IT investments, clear strategic and operational needs identification.
System Heterogeneity & Ineffective Data Sharing	• Government Interoperability Framework (GIF) • Information/Data Architecture Principles • Data Governance Framework.	Accurate and consistent data sharing, improved information flow across systems, reduced data redundancy.
Unclear Strategic & Operational Needs	• GEA's 'as-is' and 'to-be' architectural processes • digital transformation roadmaps.	Clear identification of current gaps and future requirements, systematic planning for digital transformation.

Table 1 - GEA Challenges, Solutions and Impact

These are not merely technical issues but deeply rooted systemic challenges that GEA is specifically designed to counteract. This reinforces GEA's strategic value beyond just IT, positioning it as a critical tool for fundamental public services reform and a key driver of the National Digital Transformation objectives.

GEA'S SUPPORT FOR KENYA'S STRATEGIC GOALS

Government continues to invest significantly in digital systems and technology platforms to improve service delivery, enhance revenue collection, and support national development. However, without a strong coordinating framework, there remains a risk of fragmented systems, duplication of investments, inconsistent standards, and limited interoperability across MCDAs.

GEA provides the structured framework through which digital initiatives are planned, governed, and aligned across government. It supports the Whole-of-Government approach by ensuring that systems work together, investments are coordinated, and services are delivered efficiently and securely.

By linking enterprise architecture capabilities with key government strategies GEA provides the mechanism through which ICT investments, digital capabilities, and innovations are coordinated, implemented and governed across the government ecosystem. This ensures the effective execution of public policy, fosters transparency, eliminated information silos and enhances value for citizens and stakeholders.

GEA ALIGNMENT WITH KENYA VISION 2030

Kenya Vision 2030 is national long-term development blueprint that aims to transform Kenya into a globally competitive and prosperous nation with middle-income economy and a high quality of life by 2030.

GEA enables the creation of agile, service oriented and citizen-centric government services, which are essential for fostering economic growth, industrialization, and inclusive service access. It empowers public institutions to deliver efficient, transparent, and secure services, contributing directly towards sustainable development, and a globally competitive digital economy.

By promoting interoperability, standardization, and coordinated ICT investments, GEA ensures that digital transformation initiatives are aligned with national priorities across all public sector entities.

ALIGNMENT WITH THE DIGITAL ECONOMY BLUEPRINT

The Digital Economy Blueprint is a conceptual masterplan adopted by the Government of Kenya in its quest towards the realization of a successful and sustainable digital economy with strategic focus on five key pillars - Digital Government, Digital Business, Infrastructure, Innovation-Driven Entrepreneurship, and Digital Skills.

Supported Pillar	GEA Enablement
Digital Government	GEA enables the development of citizen-centric e-services, streamline processes, and enhances data sharing, making government more efficient, transparent, and responsive by establishing a unified framework for interoperability, data sharing, and service integration across MCDAs.
Digital Business	By enabling open standards, secure data exchange, and consistent digital infrastructure, GEA fosters innovation, integration, and transaction with government systems more effectively.
Infrastructure	GEA guides the design, planning, and governance of national ICT infrastructure, including data centers, cloud platforms, networks, and digital identity systems, forming a strong foundation for digital services and innovation.
Innovation-Driven Entrepreneurship	GEA lowers barriers to entry for innovators and startups to build and scale solutions within the government ecosystem through the support of API-driven integration and building of modular, reusable, and open digital platforms.
Digital Skills	GEA promotes capacity building and knowledge sharing through standardized practices, EA training programs, and a common framework that enhances institutional understanding of digital transformation and broaden digital literacy within the public sector.

SUPPORT FOR THE NATIONAL DIGITAL MASTER PLAN 2022–2032

GEA framework in its structure defines a comprehensive transition plan to move from the current operational state to a desired target architecture. This envisioned future state, articulated within Kenya's National Digital Master Plan 2022-2032, outlines a highly integrated and advanced digital government.

GEA being a foundational framework for guiding the implementing the National Digital Master Plan (NDMP), identifies the following initiatives as key flagship projects:

- Digital identity and authentication (e.g., Maisha Namba)
- Interoperable e-government services
- National cloud and shared infrastructure
- Data centers and government-wide integration platforms

Through structured architecture and governance, GEA will support these NDMP priorities by establishment and enforcement of standards, security policies, and lifecycle management activities.

Recurring themes of **one-stop-shop**, **digital ID**, **cloud services**, and **cybersecurity** across the Kenya national blueprints indicate a clear strategic intent towards a highly centralized, secure, and user-friendly digital government.

This represents the practical manifestation of the Whole-of-Government concept in a digital context, where the architectural design directly enables the policy vision of integrated and accessible public services.

ALIGNMENT WITH INTERNATIONAL GOALS AND COMMITMENTS

GEA supports Kenya's obligations under regional and global frameworks by providing the structural foundation and strategic alignment needed to support the effective implementation of key frameworks and initiatives, including:

- **United Nations Sustainable Development Goals (SDGs)**
  GEA strengthens institutional frameworks and promotes transparency, accountability, and efficient service delivery directly supporting **Goal 16** (Peace, Justice, and Strong Institutions). It also facilitates innovation and infrastructure development aligned with **Goal 9** by ensuring coordinated ICT investments and scalable digital solutions.

- **African Union Digital Transformation Strategy**
  GEA underpins data governance, standardization, and digital inclusion by promoting harmonized ICT policies and architectures. This fosters regional interoperability and enables African countries to build cohesive and resilient digital economies.

- **Smart Africa Manifesto**

GEA advances the vision of an integrated digital ecosystem through the support of cross-border interoperability, shared infrastructure, and collaborative digital platforms. It enables member states to align national digital initiatives with broader continental goals for economic and social transformation.

By adopting open standards, reusability principles, and citizen-centric service delivery, GEA positions Kenya to align itself against international digital frameworks and promoted worldwide government interconnectivity.

GEA CURRENT-STATE ASSESSMENT

The current digital landscape in Kenya is characterized by a strong policy intent for digital transformation, underpinned by several strategic masterplans and initiatives such as Vision 2030, The Kenya National Digital Master Plan 2022-2032 which serve as the blueprints outlining strategic objectives across digital infrastructure, government service delivery, skills, and innovation.

Despite comprehensive policy documents and frameworks, the digital transformation journey at the MCDA level remains hindered by siloed systems, duplicated ICT investments, vendor lock-in, and fragmented service delivery that limit efficiency and effectiveness.

There is a need to revise and augment existing policy frameworks, address dependencies, and implement more inclusive digital governance measures. The concept of 'human interoperability' has also been identified as an area requiring significant development to nature crucial relationships and establish institutional structures that promote human capital development and collaboration.

It is therefore imperative to understand the current landscape of digital systems, processes, data and application management as well as the supporting infrastructure across Kenya's government institutions to identify gaps, inefficiencies, and opportunities for transformation.

The summary below of the current-state assessment provides a baseline from which the design of the target-state architecture can be built. The comprehensive current state assessment is documented in the *'GEA-GIF 'As-Is' Architecture Assessment Report'*

BUSINESS ARCHITECTURE

The government's digital transformation efforts are mainly focused on enhancing citizen, business, and inter-governmental interactions. The approach to Government service delivery and interactions can be broadly categorized into: Government-to-Citizen (**G2C**), Government-to-Business (**G2B**), Government-to-Government (**G2G**), and Government-to-Employee (**G2E**) models.

A major strategic initiative is underway to automate core government services through the 'Paperless Office Strategy,' anchored by the ambitious objective of digitizing five billion

manual records representing a critical step toward enhancing service delivery efficiency and substantially reducing the dependency on physical storage.

The eCitizen platform greatly exemplifies this progress through the digitization of approximately 20,000 services, cutting across 100+ MCDAs, offering citizens easy, convenient, and efficient access to government services.

Despite these advancements, fundamental challenges persist:

- Most MCDAs continue to operate autonomously, leading to duplication of functions, siloed services, poor coordination and a fragmented digital experience in public service delivery.
- The push for extensive digitization of services, risks digitizing existing inefficiencies rather than transforming service delivery if underlying interoperability and 'human interoperability' challenges are not fully addressed.
- Citizen services are fragmented across multiple MCDAs which are already struggling from disjointed user experiences and redundant information requests, perpetuating the inefficiencies of traditional departmentalism
- Across MCDAs, performance measurement and management systems are either inconsistent or absent, limiting the ability to accurately track and analyze the effectiveness and efficiency of public service KPIs
- Although initiatives such as the e-Citizen platform and Huduma Centres have introduced elements of service integration, progress remains fragmented, with integration still limited in scope and far from a universal omnichannel experience.

APPLICATION ARCHITECTURE

The application landscape is in theory guided by the ICT Authority's **'Systems and Applications Standard'**, which provides a common framework for software lifecycle processes, covering the acquisition, supply, development, operation, maintenance, and disposal of software systems.

Despite these established standards and frameworks, the government continues to grapple with challenges such as siloed systems, duplication of ICT investments, and vendor lock-in, indicating a disconnect between policy intent and practical outcomes. This suggests that the current standards and frameworks may not be sufficiently prescriptive or rigorously enforced

through legislation to address these issues, or that there is a significant gap in their practical application during procurement and development cycles.

In summary, challenges include:

- Applications are largely monolithic and developed in isolation by individual agencies.
- Low levels of modularity and reusability; each MCDA builds or procures its own systems.
- Legacy systems dominate in many sectors, lacking API access or integration capability.
- A low number of shared platforms and applications exist (e.g., IFMIS, e-Citizen, g-Procurement), meaning that many MCDAs still rely on stand-alone solutions.

The ICT Authority's governance mandate should be strongly backed up legislatively to drive a unified approach to ICT acquisition and deployment to mitigate these problems across all MCDAs as described in the proposed **Government Regulations for GEA/GIF Coordination** document.

The GEA framework should extend beyond the definition of principles to establishing clear, mandatory mechanisms for their adoption, potentially through centralized architectural review boards for all major ICT projects, standardized procurement clauses preventing vendor lock-in, and robust compliance audits that penalize deviations from established architectural guidelines.

DATA / INFORMATION ARCHITECTURE

In response to the recognition for the necessity of defining common identifiers and data standards to enhance information flow and minimize data duplication across MCDAs, notable sector-specific initiatives have been established such as the Kenya Health Information Systems Interoperability Framework (KHISIF), which aims to facilitate the interoperability of health information systems to support patient-centric, joined-up health services.

Significant challenges persist in the practical implementation of these standards including:

- Government systems currently generate massive pools of data at different levels, often stored in different formats across various systems and locations, which severely hinders access, sharing, and analysis.

- Data is inconsistently classified and governed due to lack universal data catalog and authoritative data source registry across MCDAs.
- Data quality issues persist due to lack of data governance processes to identify and address instances where data quality is low or remediation is necessary.
- Fragmented data storage and inconsistent formats indicate a significant gap in the data governance and limited adoption of metadata standards or common vocabularies.
- Inadequate sharing of data due to policy restrictions, lack of a legal interoperability framework, and desire to maintain data autonomy
- Personal data is often collected multiple times by different MCDAs, against the desired the 'Once-Only' interoperability principle.

TECHNOLOGY ARCHITECTURE

The government has laid out ambitious plans for establishing a pervasive and ubiquitous national ICT infrastructure. This includes the extensive installation of 100,000 km of high-speed fiber optic infrastructure and the creation of 25,000 internet hotspots, aimed at universal connectivity across the country. Flagship programs are underway for building a national data center and establishment of cloud services for use by both government and the private sectors including smart city Konza Technopolis and regional ICT hubs.

Strategic plans such as Artificial Intelligence (Kenya Artificial Intelligence Strategy 2025-2030), Internet of Things (IoT), and Blockchain (National Digital Master Plan 2022–2032) encourage the adoption of cutting-edge technologies.

However, several challenges persist including:

- Lack of standardized infrastructure environments; on-premise data centers, third-party hosting, and increasing adoption of cloud services.
- Redundant investments in similar technologies across departments and agencies due to lack of central application and system catalogues.
- Limited adoption of the government cloud infrastructure initiative.
- Connectivity disparities exist between urban and rural counties despite NOFBI and County Connectivity initiatives.

GEA's Technology Architecture will define the target state technologies and inherently incorporate principles of resilience, environmental sustainability, and equitable access as core

design considerations, moving beyond simple deployment metrics to ensuring operational effectiveness, widespread usability, and long-term societal impact.

INTEGRATION ARCHITECTURE

MCDAs continue to function as a 'set of silos,' which significantly hinders effective information exchange and interoperability as far as system integrations are concerned. Disparate systems store data in different formats across various locations, making access, sharing, and analysis exceptionally difficult the existing despite functional commonality,

While the technical definitions for interoperability may be in place at some levels, their practical adoption, semantic alignment (ensuring a shared understanding of data), and the necessary organizational and cultural shifts do not exist across MCDAs.

GEA's Integration Architecture extends beyond technical interoperability, such as APIs, shared protocols, and common data formats, to fully incorporate semantic interoperability by ensuring consistent interpretation and shared meaning of data across government and strengthening organizational interoperability through the adoption of the **Government Interoperability Framework (GIF)**. This includes the rationalization of cross-agency processes, the establishment of clear collaboration and data-sharing agreements, and the implementation of strong governance and cultural change measures aimed at eliminating siloed operations.

The adoption of the Government Interoperability Framework (GIF) as the standard reference for data exchange provides a unified, practical approach to enhancing data collaboration and system interoperability across MCDAs and supports a clear vision for seamless, citizen-centric service integration enabled by inter-departmental cooperation, ICT standardization, and consistent alignment with Whole-of-Government digital transformation goals.

SECURITY ARCHITECTURE

The Government places strong emphasis on achieving a secure, efficient, flexible, integrated, and cost-effective use of ICT across public service. This commitment is reinforced through a comprehensive set of legal and policy instruments, including the Data Protection Act (2019), the Kenya Information and Communication Act, the Public Finance Management Act (2012), the National ICT Policy (2020), and the National Cybersecurity Strategy (2022). These

frameworks collectively establish the foundation for protecting national digital assets and ensuring responsible ICT deployment.

Security cannot be addressed through technical controls alone rather effective protection of government digital assets (systems and data) requires robust policy and legal frameworks, transparent data-handling practices, and sustained public awareness efforts that respond to ethical and societal expectations. Security extends beyond defending systems against external threats by encompassing data privacy, ethical data use, transparency in government information practices, and the safeguarding of citizens' digital rights as integral components of national digital trust.

Key challenges currently affecting the government's security posture include:

- Fragmented security implementation across MCDAs, resulting in uneven protection levels and leaving critical systems vulnerable to cybersecurity threats or non-compliance with national security and ICT standards.
- Limited maturity in the enforcement of the Data Protection Act, with many MCDAs lacking designated Data Protection Officers (DPOs) and other essential governance roles required for effective oversight of privacy obligations.
- Use of outdated or insufficient authentication mechanisms, with several critical systems still lacking modern controls such as multi-factor authentication (MFA), PKI-based identity, and centralized access management.
- Inconsistent incident response, auditability, and threat detection capabilities, leading to delayed detection of security events, inadequate forensic visibility, and varied response effectiveness across government entities.

Information Security Standards is a key component of the GEA framework whose commitment promotes public trust through the safe, secure and responsible adoption and use of digital technologies.

HUMAN CAPACITY ARCHITECTURE

The Kenya Digital Master Plan features the ambitious 'Digital Skills' pillar which targets digital literacy capacity-building for 20 million citizens, including specialized training for 10,000 ICT professionals and 300,000 public servants and 350,000 teachers.

Through the ICT Human Capital and Workforce Development Standard (2023), the government attempts to systematically strengthen the skills and competencies required for effective e-service delivery across the public sector. This standard addresses the capability needs of technical personnel, operational staff, end-users, and the broader public, promoting interoperability of ICT resources, supporting uniform skill development, and ensuring consistent, high-quality delivery of government services nationwide.

Programmes such as DigiTalent and broader public service capacity building initiatives, covering areas like Business Process Re-engineering (BPR), Project Management, IT System Management (ITSM), and Cybersecurity can potentially accelerate the plan to bridge the skills gap.

Challenges currently experienced include:

- Inadequate Human Resource capacity, values and culture, with insufficient ICT skills across the broader public sector workforce relative to demand across all industry sectors.
- Areas such as enterprise architecture, cybersecurity, data science, system integration lack sufficient skill and capacity to meet the demands required to guide advanced digital transformation initiatives.
- Training, mentoring, and professional development initiatives are not properly coordinated and in many cased lack budgets or are externally driven (donor-based).
- Increasing the number of trained individuals in areas such as enterprise architecture may not necessarily translate into the required specialized skills, a broader cultural transformation is needed to drive digital ways of working and collaboration.
- Recruitment and retention challenges persist especially in rural-based and under-resourced MCDAs.

Human Capacity Architecture focuses on strategic workforce planning, targeted high-end skill development, continuous learning pathways, and robust talent attraction and retention strategies, such as competitive compensation and professional development incentives and addresses the cultural transformation required to foster a digitally enabled public service.

GOVERNANCE ARCHITECTURE

Despite established formal structures, characterized by the ICT Authority's oversight role and responsibility for the management, enforcement, and review of ICT standards, there is a significant risk of failing to align ICT initiatives to real business needs of the MCDAs.

The ICT Authority's mandate enables a robust governance structure and standards enforcement mechanisms and audit processes. However, persistent challenges related to IT-business alignment, efficient resource utilization, and vendor management indicate that governance needs to evolve from a purely compliance-focused approach actively drive value and strategic alignment.

Existing challenges are summarized below:

- Oversight of ICT initiatives are fragmented across MCDAs, with unclear mandates and duplicated functions.
- Limited visibility of ongoing IT projects and EA initiatives across the public sector.
- Compliance with GEA or GIF is not systematically monitored, nor are MCDAs audited against a common architecture maturity assessment model.
- Lack enforcement powers in certain areas such as procurement decisions and strategy management).

GEA's Governance Architecture emphasizes performance measurement, clear accountability for value delivery, and strategic oversight that moves beyond policy enforcement to proactive management of ICT as a strategic asset that directly supports government objectives and optimizes public investment.

GEA ALIGNMENT WITH GLOBAL EA FRAMEWORKS

GEA framework is structured to align with internationally accepted best practices and standards to ensure consistency, interoperability, and sustainability across public sector digital transformation initiatives. GEA adapts and contextualizes leading Open reference frameworks explained in detail below.

I. National ICT Interoperability Framework (NICTIF)

GEA is influenced by the National ICT Interoperability Framework (NICTIF), forming the backbone of the Government Interoperability Framework (GIF) outlining interoperability

across the Technical, Semantic, Legal and Organizational dimensions. Other frameworks such as India Stack, and the UK's Government Digital Service (GDS) have also influenced the GEA and GIF frameworks.

II. Inspiration from Best Practice Frameworks

Globally recognized best practices in GEA are characterized by a constellation of key attributes, including a strong emphasis on stakeholder engagement and alignment to ensure that architectural initiatives are driven by and serve the diverse needs of citizens, government agencies, and other stakeholders.

A thorough research exercise was undertaken to build a strong evidence base for GEA through review and analysis of published books and peer-reviewed academic journals from industry thought leaders. industry publications and case studies, academic databases and global knowledge repositories as official government publications and policy papers from recognized institutions.

The research incorporated case studies and comparative analyses of established Enterprise Architecture frameworks from around the world, including:

- Kingdom of Bahrain's National Enterprise Architecture Framework (NEAF): Demonstrating how EA can drive digital transformation and support national economic visions.
- United States Federal Enterprise Architecture Framework (FEAF): Highlighting federal-level coordination, efficiency, and accountability.
- Australian Queensland Government Enterprise Architecture (QGEA): Focusing on interoperability and shared services across government entities.
- India's IndEA and IndEA Stack: Emphasizing citizen-centricity, scalability, and the reuse of digital building blocks.

A detailed report on this research and analysis is contained in the *GEA-GIF International Best Practices & Local Applicability and Relevant Global Practices and Suitability for Kenya*

TOGAF ADM AS GEA's FOUNDATIONAL METHODOLOGY

The GEA methodology is underpinned by TOGAF Architecture Development Method (ADM) as the overarching lifecycle for implementation of Enterprise Architecture within the MCDAs.

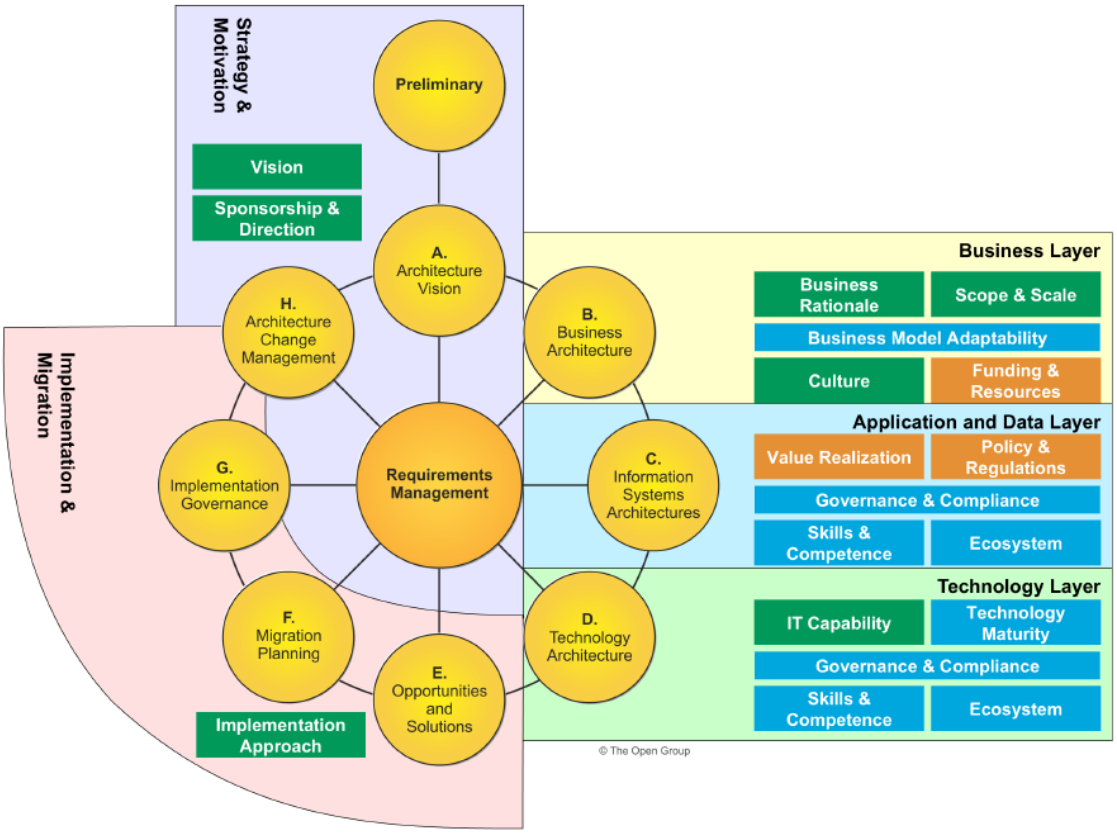

Figure 3 - TOGAF high-level approach

Within the GEA context, TOGAF aligns naturally with the GEA Reference Models - Business, Data, Application, Technology, Security, Integration, Human Capital and Governance as shown in Figure 3 above. GEA reference models are systematically embedded into each phase of the Architecture Development Method (ADM), ensuring that every MCDA develops its architecture in a manner that:

- Maintains interoperability across agencies
- Ensures compliance with GIF and national ICT standards
- Supports citizen-centric service delivery
- Enables reusable, modular, and secure architectures
- Facilitates efficient, coordinated digital transformation

For more details see *the GEA Framework Components* section. The ADM and its adoption as the guiding GEA implementation methodology are described in further detail in the *GEA Implementation Roadmap and Adoption Guide* including specific guidelines how MCDAs can use ADM lifecycle to develop their respective Enterprise Architectures aligned with the GEA.

GOVERNMENT ENTERPRISE ARCHITECTURE (GEA) FRAMEWORK

GEA is a unified, strategic framework composed of interrelated architecture reference models that define and guide the design, planning, and implementation of government digital transformation initiatives. These reference models embody proven best practices, industry standards, and governance principles to support solution delivery teams in MCDAs to make informed and consistent design and technology decisions in their digital transformation initiatives.

GEA promotes architectural coherence, interoperability, and agility across government by providing a structured blueprint that accelerates the design and delivery of digital public services in alignment with national priorities and supports transition toward the target-state digital government architecture.

GEA ARCHITECTURE PRINCIPLES

GEA Principles are enduring, authoritative rules that govern how Government plans, designs, acquires, integrates, and operates digital capabilities across the public sector and the broader digital ecosystem. These principles are intended to inform and guide the manner in which an organization sets about fulfilling its strategic objectives through implementation of digital transformation initiatives.

The principles establish a common architectural discipline for all MCDAs, as well as ecosystem participants including private sector partners, Public–Private Partnerships (PPPs), and cross-border service providers to ensure that all digital initiatives are coherent, interoperable, secure, inclusive, and aligned to national priorities.

Compliance with these principles is mandatory and forms the basis for architecture governance, investment approval, procurement, and solution assurance across Government.

Principle	Description
Citizen-Centricity	Digital public services shall be designed and delivered around the needs, life events, and experiences of citizens and businesses, rather than institutional structures. Services must be simple, transparent,

	accessible, and capable of being composed across multiple government and ecosystem actors.
Whole-of-Government (WoG) Approach	Government shall operate as a single enterprise, prioritizing national outcomes over institutional or sectoral optimization. Digital initiatives must align to shared platforms, common capabilities, and cross-government service models, with ecosystem participation governed through GEA.
Ecosystem by Design	All digital solutions shall be designed to operate within a governed digital ecosystem that includes external partners, PPPs, and regional or international platforms. Standalone or closed architectures are not permitted unless formally approved through GEA governance.
Interoperability by Design and Default	Interoperability across legal, organizational, semantic, technical, and security layers shall be embedded from inception. All systems must comply with the Government Interoperability Framework (GIF) to enable seamless information exchange within government and across borders.
Boundaryless Information Flow with Control	Information shall flow securely across organizational and national boundaries where legally permitted, while preserving data sovereignty, accountability, privacy, and security. Barriers to information sharing must be justified, not assumed.
Security and Privacy by Design	Security, privacy, identity assurance, and trust mechanisms shall be integral to all architectures from inception, including ecosystem and cross-border integrations, to protect public data, maintain confidence, and meet national security and regulatory obligations.
Reuse and Modularity	Existing national platforms, shared services, data assets, and ecosystem capabilities shall be reused before new solutions are developed or procured. Duplication of capabilities already available within the government ecosystem is prohibited.
Standards-Driven and Open Architecture	Open, internationally recognized standards shall be adopted to ensure compatibility, portability, vendor neutrality, and long-term sustainability across government and ecosystem solutions.
Lifecycle-Based Governance	Digital investments shall be governed across their full lifecycle from concept and design to operation, modernization, and retirement ensuring architectural alignment, value realization, and controlled evolution of the ecosystem

Technology Neutrality	Digital architectures shall remain vendor-agnostic and technology-neutral, avoiding proprietary lock-in and enabling fair competition, substitution, and long-term flexibility across the ecosystem.
Data as a Strategic Asset	Data shall be managed as a shared national asset, supporting policy formulation, service innovation, and performance management. Data quality, semantic consistency, stewardship, and responsible use are mandatory across the ecosystem.
Cloud-First and Mobile-First	Digital solutions shall prioritize cloud-based infrastructure and mobile-accessible delivery models to enhance scalability, resilience, agility, and reach, subject to national security and data classification requirements.
Inclusivity and Universal Accessibility	Digital initiatives shall be inclusive and accessible to all users, regardless of ability, geography, or socio-economic status, ensuring equitable access to government services and preventing digital exclusion.
Cross-Border Readiness and Regional Alignment	Government digital architectures shall be designed to support regional and international interoperability where strategically required, enabling cross-border services, mutual recognition, and participation in regional digital ecosystems.

These principles are binding on:

- All MCDAs and sector architectures
- National digital platforms
- PPP-driven and outsourced digital solutions
- Ecosystem and cross-border integrations

Non-compliance with these principles should result in withholding approval for participation in the government digital ecosystem in accordance with GEA governance and enforcement mechanisms defined within the framework and various supporting regulations.

GEA FRAMEWORK COMPONENTS

GEA is structured around 3 core layers – **Strategy, Models and Operations**, supported by a crosscutting Governance Model as shown in *Figure 4* below:

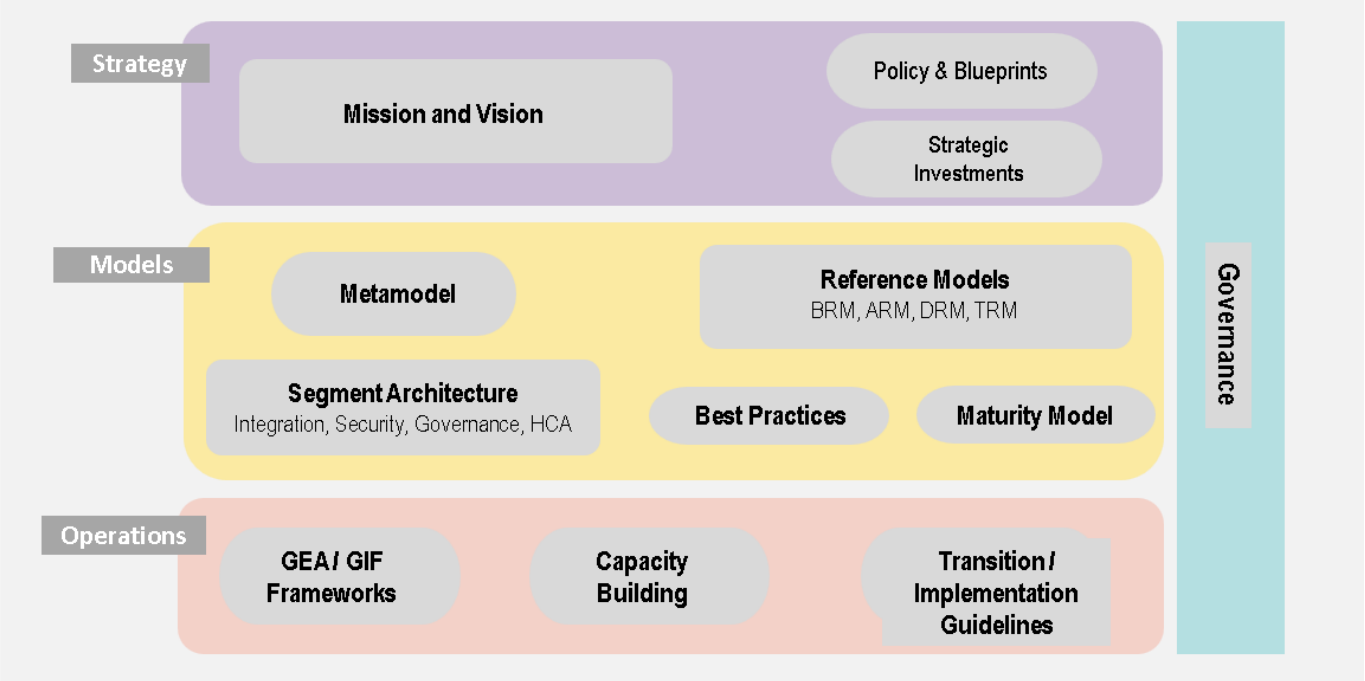

Figure 4 - GEA Framework Components

The table below describes each of the components in the GEA structure in detail:

Component Layer	Description
Strategy	Strategy defines the foundational alignment between enterprise architecture and national digital transformation objectives. It ensures that all architecture initiatives are guided by a clearly articulated vision, shaped by national digital transformation priorities and development strategies. It translates the strategic intent of government into actionable enterprise architecture plans, both short-term and long-term, supported by relevant policies, regulatory frameworks, legal instruments, and strategic investments providing a structured roadmap anchored in a shared future-state vision.
Models Layer	The GEA Models Layer provide the living reference artefacts that guide MCDAs in adopting and implementing Government Enterprise Architecture (GEA) using the defined best practices.

	They provide structured views that organize and classify the core components of enterprise architecture, with each domain offering a standardized lens for analyzing and designing enterprise capabilities. GEA domains are included in this layer: Business Architecture, Application Architecture, Data/Information Architecture, Technology Architecture, Security Architecture, Integration Architecture, Human Capital Architecture and Governance Architecture
Operations	Focuses on execution, coordination, and continuous improvement of the government's digital service delivery. It encompasses the design, implementation, and control of operational processes to ensure that public services are efficient, citizen-centric, and aligned to the highest architectural standards. Activities are supported by established methodologies, tools, key performance indicators (KPIs), and operations management.
Governance	Establishes the leadership, accountability, and oversight mechanisms necessary to guide and sustain the implementation of GEA by defining: • A strategic governance structure with defined roles, responsibilities, and decision-making authority. • A management framework for enforcing compliance, quality assurance, and value realization. • Mechanisms for monitoring, evaluation, and continuous feedback, ensuring responsiveness to evolving social, economic, and technological conditions. Governance ensures that architecture initiatives remain aligned to national priorities and strategies, and are executed in a transparent, agile, and results-driven methodology.

GEA METAMODEL

The GEA Content Metamodel provides a standardized structure for defining and relating architectural elements across the Business, Data, Application, and Technology core layers. It serves as the foundational model that ensures consistency, traceability, and interoperability across all MCDAs.

By establishing common definitions and relationships i.e. the linkage of strategic goals to business capabilities, processes, and enabling technologies, the metamodel enables coherent architecture development, promotes system and data integration, and embeds governance through principles, standards, and requirements. Its adoption within GEA supports capability-based planning, effective resource alignment, and measurable progress toward a unified, interoperable, and digitally empowered government.

The interconnections and relationship between the various GEA components and models are shown in *Figure 5* below.

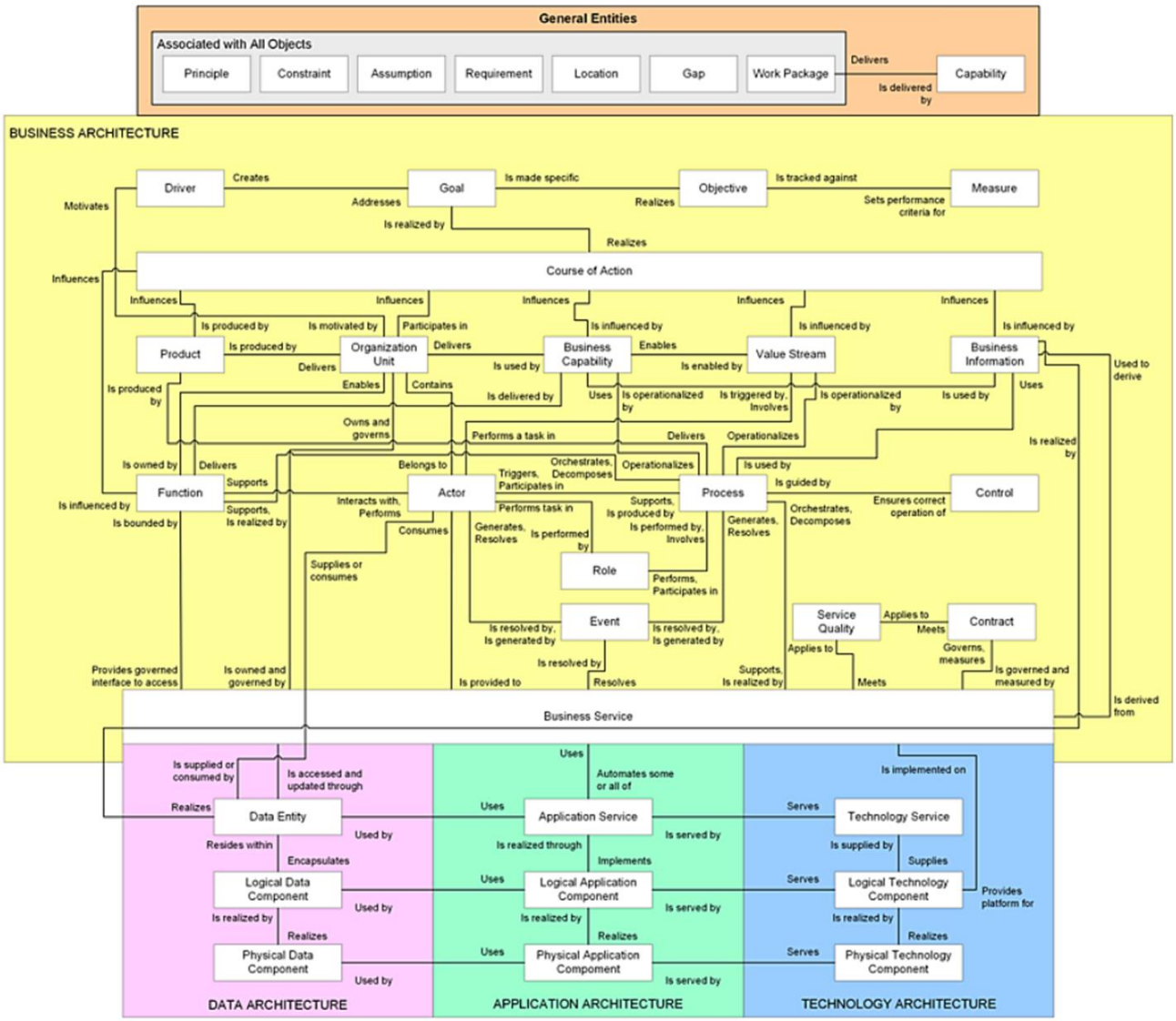

Figure 5 - GEA Content Metamodel

The GEA meta-model is organized into four primary architectural layers, that provide a view of the government enterprise from distinct perspectives in their focus areas but also deeply interconnected to ensuring that technology is always aligned with business needs by supporting business processes. This section provides a high-level conceptual overview of these perspectives and their critical linkages.

The four Architectural layers are described in the table below:

Business Layer	The Business Architecture layer defines the enterprise's strategic direction and operational structure in a technology-agnostic manner by focusing purely on the business model, value streams, and organizational design required to meet strategic objectives. It provides a stable reference point for understanding how the business creates value and allows architects to trace every technical component back to the Driver (motivation) or business requirement.
Data Layer	Data layer describes the structure, storage, and management of an enterprise's logical and physical data assets. It defines the metadata and key business information (Data entities like "Customer" or "Application") and maps out how this data is organized and accessed using the Data Reference Model, then translates the information requirements into a logical plan that applications can use to store, retrieve, and process data consistently.
Application Layer	The Application Architecture layer outlines the portfolio of applications, their interactions, and their relationship to the business processes they support. It defines the Application Services that directly fulfill Business Services and specifies the logical and physical software components that deliver this functionality.

	This layer promotes the reuse of common components and manages the interfaces between different applications to ensure that the software ecosystem is efficient, integrated, and aligned with business processes.
Technology Layer	Technology Architecture layer describes the underlying platforms, hardware infrastructure and software solutions that host and support the application and data layers, the foundation upon which the entire enterprise architecture is built. A robust technology architecture provides the stable and powerful environment necessary for applications to run effectively, providing an infrastructure to support current and future business demands in a cost-effective and secure manner.

The connections that bind the architecture together are illustrated in the relationships between key entities from each layer. These connections ensure that every application and infrastructure component supports a specific business process that uses specific data to deliver a valuable service to a stakeholder, in fulfillment of a government function aligned with national strategic goals.

This integrated view is essential for making informed decisions about investment, modernization, and cross-agency collaboration. The subsequent parts of this document will define the entities and relationships within each of these layers in detail.

GEA REFERENCE MODELS

The Content Metamodel serves as the conceptual foundation from which GEA derives its Architectural Reference Models. By defining standardized entities, relationships, and dependencies across business, data, application, and technology domains, the metamodel enables the structured development of each reference model.

- **Business Reference Model (BRM)** is derived from entities such as drivers, goals, capabilities, and processes

- **Data Reference Model (DRM)** from data entities, information flows, and data governance relationships
- **Application Reference Model (ARM)** from application services and their realization of business capabilities
- **Technical Reference Model (TRM)** from technology services and components supporting the application layer.

This derivation ensures that all reference models are conceptually aligned, interoperable, and governed by the same architectural logic, thereby providing a cohesive and reusable foundation for digital transformation.

Within the GEA framework, reference models have been defined to adopt to the local context, providing a shared language, structure and best practice guidelines for designing and implementing enterprise architecture across MCDAs.

Each of these models have following characteristics

- **Abstraction**: GEA reference models are a high-level generic representation of a specific section of an area of interest in an MCDA, deliberately avoiding sector-specific or implementation-level detail. This ensures the framework remains broadly applicable diverse use cases across MCDA.
- **Standards-Based**: Each Reference Model incorporates recognized industry and government best practice and open standards, to drive consistency, compliance, and interoperability across all digital government initiatives.
- **Technology-Neutrality**: GEA is deliberately agnostic to specific technologies and platforms. It focuses on architecture principles and patterns that are open, independent of vendor solutions or implementation choices, enabling interoperability, flexibility and future scalability.

Each Reference Model within the GEA framework provides:

- Graphical representations, using standard modeling notations such as UML, ArchiMate, or BPMN, to visually depict architectural entities and their relationships.
- Descriptive components, outlining the roles, capabilities, and governance requirements of each entity within the model.

- Prescribed standards and guidelines for interaction, integration, and communication among components.

The reference models provide a robust foundation and guidelines to support a wide spectrum of digital transformation initiatives within MCDAs and provide the capability to maintain architectural consistency, build resilience, eliminate information silos, reduce duplication of capabilities, and promote interoperability and integrated digital public service delivery.

GEA REFERENCE MODEL STRUCTURE

GEA reference model structure maps the overall structure of an organization and uses it as the basis to plan and manage business and technical transformation in each organization. The reference model structure is composed of two primary dimensions:

- **Architectural Layers** - Provides a hierarchical view of the enterprise, defining the core domains from high-level strategy down to the underlying technology.
- **Architectural Pillars -** Representing the cross-cutting domains that support, secure, and govern all the architectural layers to ensure a cohesive framework.

This structure is underpinned by a set of foundational requirements that drive compliance, standardization, and provide a clear implementation path and measurable outcomes as shown in *Figure 6* below.

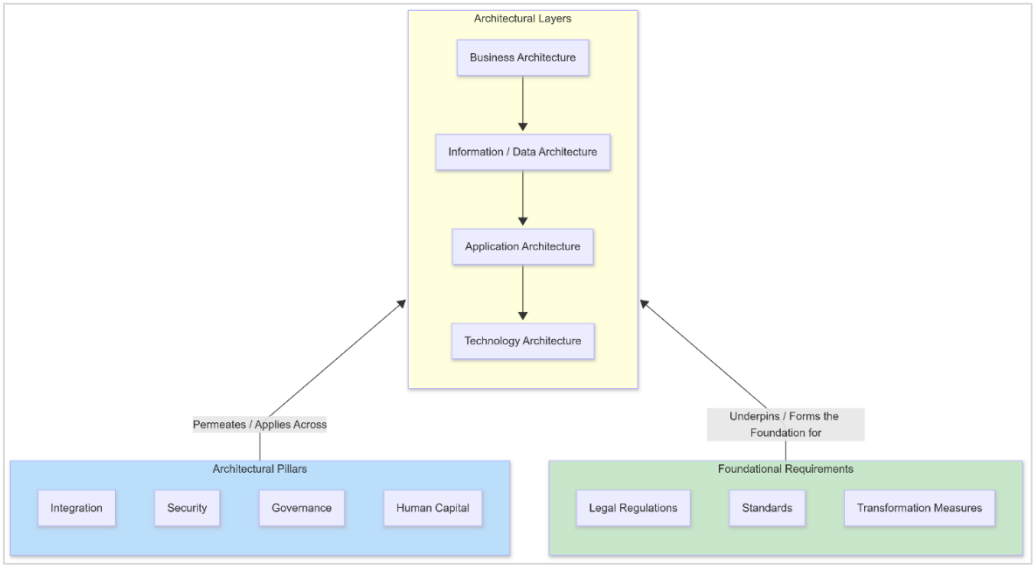

Figure 6 - GEA Architectural Layers and Supporting Pillars

ARCHITECTURAL LAYERS

The Architectural Layers provide a hierarchical decomposition of GEA, moving from the high-level strategic 'why' and 'what' to the detailed 'how' implementation. Each domain layer is distinct but intrinsically linked to the layers above and below it.

Below is a summary of the Architectural Layers

Domain / Layer	Focus	Key Components
Business Architecture	Defines *what* the MCDA does, its strategic goals, and its services, independent of technology.	Strategic Goals, Channels, Services, Processes, Organizational Units
Information / Data Architecture	Describes the government's core data assets and how they are managed and utilized.	Business Components, Logical Data Models, Data Management, DBMS Standards.
Application Architecture	Details the software applications and systems that automate processes and manage data.	Application Systems, Databases, Application Interfaces (APIs).
Technology Architecture	Outlines the underlying hardware, software, and network infrastructure that hosts applications.	Infrastructure, Networks, Platforms, Middleware & Development Tools.

ARCHITECTURAL PILLARS

Architectural Pillars are cross-cutting disciplines that are essential for the success and sustainability of the entire GEA framework permeating across all architectural layers.

Pillar	Focus	Key Components
Integration Architecture	Ensuring seamless data flow, process orchestration, and communication across government entities and systems.	Inter-Ministry Reporting, Workflow & Data Integration, Messaging Tools.
Security Architecture	Protecting the confidentiality, integrity, and availability of government information and technology assets.	Infrastructure Security, Access Management, Data Security, Cybersecurity Competencies.

Governance Architecture	Establishing decision-making structures, policies, and processes to manage and enforce the GEA.	GEA Oversight Board, Architecture Review Board (ARB), Policies & Standards, Compliance, Monitoring and Reporting.
Human Capital Architecture	Developing the necessary skills, competencies, and culture to support a digitally transformed government.	Skills Development, Workforce Planning, Change Management.

IMPLEMENTATION GUIDELINES USING TOGAF ADM

TOGAF ADM is consistently and iteratively adopted as the standard, repeatable lifecycle for developing, governing, and evolving GEA across three distinct but interdependent perspectives:

- **Whole-of-Government (WoG) Approach** - sets direction, standards, and shared capabilities across the whole of government.
- **MCDA Approach** - implements MCDA architectures and solutions within approved boundaries.
- **Solution Implementations Approach** - Translates of solution architecture into operational systems and services

Figure 7 below shows the **Whole-of-Government (WoG) Approach** mapping the entire process when the national or county government is aiming to build a government-wide enterprise architecture at the WoG level.

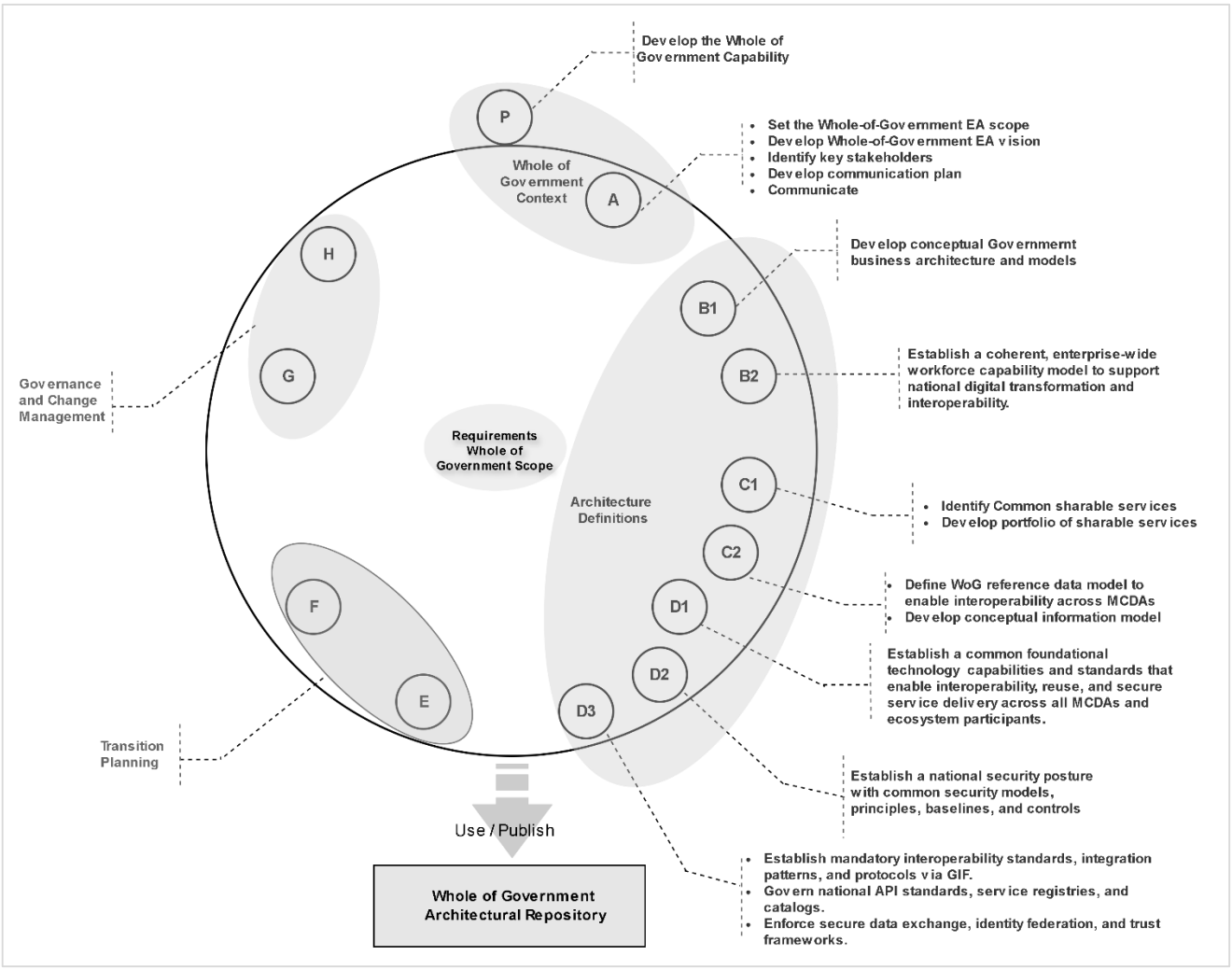

Figure 7 - GEA WoG level implementation using ADM

See the *GEA Implementation Roadmap and Adoption Guide* for specific guidelines MCDA and Solution Implementation approaches using ADM lifecycle to develop Enterprise Architectures aligned with the GEA.

DEVELOPING ENTERPRISE ARCHITECHTURE IN AN AGILE WAY

Developing architecture in an agile way is essential to ensure that GEA remains responsive, outcome-driven, and capable of supporting continuous digital service delivery, while preserving WoG coherence, interoperability, and governance.

GEA adopts this approach allowing architecture to be incrementally and iteratively developed, without weakening architectural authority or introducing service fragmentation. Agility within GEA deliberately evolves in-step with policy priorities, service needs, and delivery cycles to

remain within the guardrails of nationally defined standards and controls. This approach ensures that individual digital transformation initiatives do not outpace governance, and that rapid delivery does not result in new digital silos.

To enable agility at scale, GEA adopts architecture partitioning across three levels of detail, as defined in TOGAF framework. Each level is explicitly mapped to GEA's operating model to ensure clarity of responsibility, decision rights, and governance.

These levels of detail can be used for partitioning architecture development as shown in *Figure 8* below:

- Enterprise Strategic Architecture
- Segment Architecture
- Capability Architecture

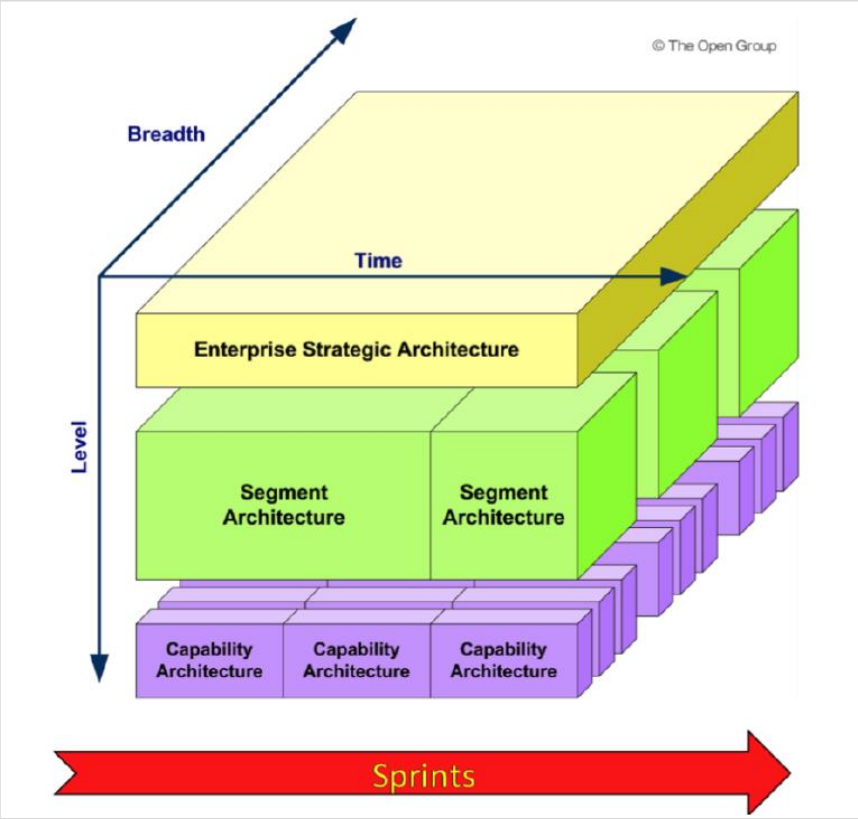

Figure 8 - GEA Enterprise Architecture Development Levels

1. Enterprise Strategic Architecture (Whole-of-Government Focus)

The Enterprise Strategic Architecture establishes the authoritative national architectural direction enabling understanding of the overall strategic direction of the government digital transformation at a high level. It must be sufficiently broad to establish the context within which the segments (MCDAs) and capabilities (Solutions) fit. It defines:

- National digital vision and outcomes
- Whole-of-Government value streams and shared capabilities
- Enterprise-wide principles, reference models, and standards
- Mandatory interoperability, security, and data governance requirements
- Governance structures and decision rights

Changes at this level are implemented through formal policy or controlled architecture change management processes providing the non-negotiable guardrails within which all other architecture-related activities are done.

2. Segment Architecture (MCDA Focus)

Segment Architecture translates the Enterprise Strategic Architecture into domain-specific and sector-specific architectures aligned to the mandates of individual MCDAs. Segment Architectures will typically provide direction at the portfolio, program level. These large-scale segments are often aligned to natural boundaries of the organization.

At this level, MCDAs:

- Define sector and agency value streams and services
- Design business, data, application, integration, technology, security, and human capital architectures relevant to their domain
- Identify shared service opportunities and dependencies
- Plan transformation roadmaps aligned to national priorities

Segment Architecture allows controlled flexibility, enabling MCDAs to innovate and modernize services while remaining compliant with Whole-of-Government standards and interoperability requirements.

3. Capability Architecture (Solution Implementation Focus**)**

Capability Architectures are detailed descriptions of (increments of) business capabilities through digital solutions, platforms, and services. These may align to delivery sprints, or multiple sprints may be needed to deliver a capability and sufficiently detailed to be handed to implementers and developers for action. Sprints may be undertaken at any level but are mostly associated with the delivery of capabilities or increments of capability and can be implemented in parallel. At this level:

- Architecture is developed in short sprint cycles aligned to delivery iterations
- Capabilities are designed, implemented, tested, and refined incrementally
- Architecture requirements are embedded directly into solution design and procurement
- Continuous compliance with GEA and GIF is enforced throughout delivery

Capability Architecture is where agile methods are most actively applied, ensuring rapid delivery of citizen value without compromising enterprise integrity.

INTEGRATING AGILE PRACTICES WITH THE TOGAF ADM LIFECYCLE

ADM remains the primary lifecycle framework for architecture development across MCDAs while agile delivery frameworks (e.g., SAFe, Scrum) are applied as execution mechanisms for implementing architecture-defined capabilities and solutions.

Agile methods do not replace the ADM Lifecycle but operate within ADM guardrails to accelerate delivery, improve responsiveness, and enable incremental realization of architectural outcomes. These guardrails and decision rights are described in detail in the Phase G – Implementation Governance of the *GEA Implementation Roadmap and Adoption Guide.*

Agile practices are applied within and across ADM phases, particularly during:

- Capability-based architecture development
- Opportunities and Solutions
- Migration Planning
- Implementation Governance
- Architecture Change Management

This ensures that architecture is continuously refined based on feedback from implementation and operations, while maintaining alignment with the approved target states as shown in the table below.

ADM Phase	Agile Application	Governance & Control Point	Outcome
Phases A–D Architecture Vision, Business, Application, Data Architecture	• Capabilities decomposed into features, and value streams • Architecture backlog established to guide delivery • Progressive elaboration without over-design	• Architecture Review Board (ARB) validates capability models and target-state alignment • PGB endorses strategic scope and priorities	Stable architectural intent with flexibility for incremental solution design
Phase E Opportunities & Solutions	• Architecture roadmaps translated into Program Increments (SAFe) or release plans (Scrum) • Prioritization driven by value, risk, and dependency	• ARB confirms solution options and reuse of shared platforms • PGB approves investment and sequencing	Agile planning explicitly driven by approved architecture
Phase F Migration Planning	• Iterations and sprints planned within approved migration waves • Incremental releases mapped to roadmap milestones	Governance gates ensure releases advance the approved target architecture	Controlled, incremental transformation without fragmentation
Phase G Implementation Governance	• Architecture compliance embedded into sprint reviews and PI reviews • Incremental conformance assessments rather than end-stage audits	• ARB conducts lightweight, frequent compliance checks • Compliance required for procurement, deployment, and funding release	Rapid delivery with enforced architectural discipline

ADM Phase	Agile Application	Governance & Control Point	Outcome
Phase H Architecture Change Management	• Feedback from delivery informs backlog refinement • Legitimate change requests raised from agile teams	• Formal change control assesses enterprise impact • Approved changes, update baselines and standards	Continuous improvement without architecture drift

Agile architecture development does not reduce governance obligations. On the contrary, it requires stronger and more continuous oversight.

Accordingly:

- All architecture work is subject to continuous architecture review and assurance
- Compliance with GEA and GIF is enforced throughout the solution lifecycle
- Deviations and exceptions require formal approval
- Architecture changes are managed through structured change control processes

Vendors and system integrators are required to operate within the defined agile architecture framework within clearly defined decision rights and mandatory guardrails for each architecture partition to ensure that agile architecture development does not dilute Whole-of-Government (WoG) authority, compromise interoperability, or introduce fragmentation or solution silos.

Decision rights establish who is authorized to decide what while the Mandated Guardrails define what cannot be violated, regardless of delivery speed or implementation method.

Phase G – Implementation Governance Section of the *GEA Implementation Roadmap and Adoption Guide contains* detailed guidelines.

GEA FOUNDATIONAL REQUIREMENTS

The foundational requirements below define the mandatory legal, governance, operational, and technical conditions required to ensure GEA is implemented consistently across MCDAs. These requirements establish the minimum controls needed to enforce interoperability, eliminate duplication, secure government assets, and translate architecture into coordinated programmes and measurable outcomes.

Category	Description	Key Components
Legal and Regulatory Compliance	All architectural decisions, digital services, data processing, and cross-government integrations shall comply with applicable Kenyan laws and regulatory obligations.	Constitution of Kenya (2010); Data Protection Act (2019); Access to Information Act (2016); Computer Misuse and Cybercrimes Act; Public Archives and Documentation Service Act; Public Finance Management Act; Evidence Act; sector-specific laws and regulations.
Architecture Governance and Decision Rights	GEA implementation must be governed through formal decision rights, accountability structures, and enforcement mechanisms to prevent fragmentation and non-compliance.	Central GEA Oversight Authority / EA Management Office; Architecture Review Board (ARB); Programme Governance Board (PGB); Project Steering Committees (PSCs); escalation paths; deviation and waiver management; compliance reporting rules.
Interoperability Requirements (GIF Enforcement)	All systems must be interoperable by design through mandatory legal, organizational, semantic, technical, and security interoperability requirements as defined by GIF.	Government Interoperability Framework (GIF) compliance; canonical data models and shared vocabularies; API standards; integration patterns; interface registries; interoperability certification and scoring.
Standards and Reference Models	Architecture must be based on approved open standards and reference models to ensure consistency, reuse, portability, and long-term sustainability across government.	GEA reference models (BRM, DRM, ARM, TRM, IRM, SRM, GRM); open standards approved patterns and technology baselines; vendor-neutral requirements.
Security, Privacy, and Trust Baselines	Security and privacy requirements are mandatory across all architecture domains to maintain managed risk, citizen trust, and national resilience.	Security architecture baseline controls: IAM, encryption, logging, monitoring, auditability; privacy-by-design requirements; risk management; incident response alignment; security accreditation for systems; GIF security controls.

Category	Description	Key Components
Data Governance and Information Management	Data must be governed as a strategic national asset with clear ownership, quality standards, and lifecycle controls, including retention and archival obligations.	Data ownership and stewardship; data quality standards; authoritative data domains and registries; metadata standards; retention schedules; archival policy; lawful sharing agreements; controlled access and classification.
Shared Platforms and Reuse Mandates	Foundational shared platforms and common services must be reused to reduce duplication and enable Whole-of-Government service delivery.	National platforms (e-Citizen, Digital ID, Payments, Integration platforms, registries); shared services catalogue; reuse-by-default rules; common infrastructure services; service catalog governance.
Procurement and Investment Controls	ICT funding and procurement must be architecture-driven to prevent misalignment, duplication, and vendor lock-in.	Architecture compliance as a pre-condition for budgeting; ARB approvals at procurement stages; EA conformance clauses in RFPs/contracts; milestone payments tied to compliance evidence; vendor exit/portability requirements.
Transformation Measures (Roadmaps and Delivery Governance)	Implementation must follow structured transformation planning that sequences delivery, manages dependencies, and ensures measurable progress toward target architecture.	Approved project portfolio; time-phased roadmaps; dependency mapping; migration waves; implementation governance (Phase G); post-implementation assurance; benefits realization tracking.
Human Capital Architecture (HCA) Readiness	GEA implementation requires skilled and accountable workforce structures to design, govern, deliver, and sustain enterprise-wide services.	Defined EA roles (service owners, capability owners, data stewards, security leads, integration leads); training and certification; change management capability; cross-agency collaboration mechanisms; operational readiness planning.

Category	Description	Key Components
Monitoring, Measurement, and Assurance	GEA implementation must be measurable, auditable, and continuously improved to prevent architecture drift and ensure value realization.	KPI dashboards aligned to value streams; compliance scorecards; architecture conformance reviews; periodic audits; benefits realization reporting; corrective action plans.

All MCDA digital initiatives including new systems, upgrades, integrations, and procurements shall demonstrate minimum compliance with these foundational requirements before approval, funding, deployment, or integration into government platforms

GOVERNMENT ENTERPRISE ARCHITECTURE DOMAINS

The Government Enterprise Architecture (GEA) Framework is structured around a set of interrelated **Reference Models (RMs)**. Each Reference Model addresses a specific architectural domain and functions as a blueprint for guiding the design, development, and governance of enterprise-wide systems and services within the MCDAs.

REFERENCE MODEL - DEFINITION

A Reference Model refers to an abstract yet authoritative representation that captures the core entities, their interrelationships, and the standards applicable within a given architectural domain.

It prescribes a uniform set of representations and specifications for consistency, standardization, and interoperability across architectural domains. When aligned with the GEA Reference Model, it provides an authoritative basis for designing, integrating, and governing Enterprise Architecture initiatives.

The main objectives of the reference models are to:

a) **Offer descriptive specifications** outlining the capabilities, roles, and responsibilities of each architectural component.
b) **Provide conceptual clarity** through structured graphical representations (e.g., using Unified Modeling Language – UML, BPMN, etc.).
c) **Prescribe open standards and guidelines** to ensure consistency, interoperability, and compliance.

The deliberate abstraction and neutrality characteristics of the GEA Reference Models provide scalability, adaptability, and reusability attributed across diverse governmental contexts and use cases.

A reference model therefore is used to describe, demonstrate and explain at a high-level the main architectural elements or components so that different stakeholders can reference it to understand and make relevant architectural decisions that apply to their local context.

ARCHITECTURE - DEFINITION

TOGAF defines an architecture as:

I. A formal description of a system, or a detailed plan of the system at component level, to guide its implementation (source: ISO/IEC 42010:2007)
II. The structure of components, their inter-relationships, and the principles and guidelines governing their design and evolution overtime.

In Enterprise Architecture, the architecture describes the relevant elements or components from the reference model, and further designs the details based on available data and circumstances to meet the architectural objectives.

GEA comprises the following seven Reference Models, each supporting a distinct architectural domain:

Reference Model	Purpose
Business Reference Model (BRM)	Defines the core and support business functions of MCDAs.
Application Reference Model (ARM)	Guides the classification, development, integration, and reuse of applications.
Data Reference Model (DRM)	Standardizes data representation and sharing across departments.
Technology Reference Model (TRM)	Provides the technology foundation required to support application and data components.
Security Reference Model (SRM)	Establishes security principles, policies, and controls across all architectural layers.
Integration Reference Model (DRM)	Enables interoperability and information exchange across systems and departments.
Governance Reference Model (GRM)	Provides structure for managing and overseeing enterprise architecture implementation.

BUSINESS ARCHITECTURE

Business Architecture defines how Government organizes its capabilities, services, value streams, and operating model to deliver measurable public value in alignment with national policy, fiscal priorities, and Whole-of-Government mandates. It establishes a common blueprint that ensures coherence across MCDAs.

Business Architecture is a mandatory reference for planning, investment, service design, and institutional reform across government and shall guide decision-making throughout the policy, budgeting, and implementation lifecycle.

At the core of the Business Architecture is the '**Service'** concept whether it is citizen-facing, partner-oriented, or internal anchored in clearly defined business capabilities and supported by shared national platforms.

The purpose of Business Architecture is to ensure that government services are designed, delivered, and continuously improved in a coordinated, outcome-driven manner that advances national development priorities, improves service quality, reduces duplication, and strengthens accountability. It provides the basis for aligning policy priorities, institutional mandates, and public expenditure with measurable outcomes.

It is technology-agnostic and attempts to answer key enterprise questions:

- Why do we exist (purpose)?
- What services and functions do we perform?
- Who are the stakeholders involved?
- How fast and effectively can services be delivered?
- How much value do these services generate in relation to cost and outcomes?
- What capabilities must government build or strengthen to deliver strategic outcomes?
- How are services funded and governed across their lifecycle?
- What risks could affect service delivery continuity?

Business Architecture (BA) forms the foundational layer of GEA, defining its core functions, services, and strategic objectives from a citizen-centric perspective and provides the base

upon which the other architecture domains, Information, Application, Technology, Security, and Governance are built and aligned.

OBJECTIVES OF BUSINESS ARCHITECTURE

The objectives of the Business Architecture (BA) are:

Objective	Description
Define and Map Government Functions	To create a comprehensive blueprint of ***what*** the government does, documenting all its core services and capabilities independent of the specific ministries or technology used.
Ensure Citizen-Centric Service Design	Re-design services around the citizen's needs and life events, rather than around the government's internal structures and processes, for example, starting a business or birth a child.
Align Operations with National Strategy	Ensure that every government service directly supports and links to the high-level objectives the national strategies such as the Kenya Vision 2030 and the National Digital Master Plan.
Improve Efficiency and Collaboration	Map all business capabilities and identify redundant services, overlaps between MCDAs, opportunities to create common shared services foster the whole-of-government approach.
Guide Technology Investments	Define business requirements and priorities that will be used to inform all future technology and application investments ensuring ICT investments deliver value.
Governance Objective	Establish enforceable governance mechanisms that ensure all government initiatives comply with GEA principles, standards, and service design requirements.
Interoperability Objective	Institutionalize cross-government interoperability through standardized business processes, shared services, and coordinated value stream management.
Capability Development	Define and mature core government business capabilities to support sustainable service delivery and policy execution.
Funding Alignment	Ensure that funding approvals and investment decisions are contingent upon demonstrated alignment with Business Architecture and value stream priorities.
Workforce Transformation	Strengthen institutional capacity, skills, and change readiness required to implement and sustain Business Architecture.

PRINCIPLES OF BUSINESS ARCHITECTURE

These principles are binding and shall be enforced through architecture governance, procurement controls, and investment review processes.

Principle	Description
Citizen-Centricity by Design	All government functions and services must be designed from the perspective of the citizen, prioritizing their needs, experiences, and ease of access.
Enterprise-Wide Value Optimization	All business and information management decisions must be made with the intent of maximizing value for the entire government ecosystem.
Strategic Alignment	Business architecture initiatives must prioritize development programs aligned with the Government's digital transformation agenda and strategic masterplans and policies.
Service Orientation	Government operations shall be viewed as a portfolio of services that can be defined, measured, and continuously improved, rather than a collection of siloed departmental functions.
Business Process Optimization	Legacy processes must be critically evaluated and re-engineered to eliminate inefficiencies and aligned with modern service delivery models.
Transparency and Accountability	Business architecture will be documented and made accessible to ensure accountability, governance and visibility into government operations and performance including publication of service performance metrics and accountability reporting.
Adaptability and Agility	Business architecture must be a living model, capable of evolving in response to changing citizen needs, policy directives, and strategic priorities. Changes to Business Architecture shall follow formal change governance processes approved by the Architecture Review Board.
Whole-of-Government Collaboration	Business architecture shall promote the breakdown of organizational silos by identifying cross-cutting functions and shared services to foster cross-sector integration and shared capabilities
Open & Evidence-Driven	Business architectures shall be designed and evolved based on openness, transparency, and verifiable evidence. Decisions must be informed by reliable data, performance metrics, service usage patterns, and policy outcomes, rather than assumptions or institutional silos.
Resilient & Adaptable	Business architectures shall be resilient to disruption and adaptable to changes arising from policy shifts, fiscal constraints, emergencies, or

	technological advances. Capabilities and processes must be designed to scale, be reconfigured, or be repurposed with minimal disruption to service delivery.
Engaged & Participatory	Business architecture shall be developed and governed through active engagement of stakeholders across government, the private sector, civil society, and citizens where appropriate. Collaboration across MCDAs is mandatory for end-to-end service design, while participatory mechanisms must be used to incorporate user feedback and operational insights.
Compliance by Design	All programs and initiatives must demonstrate compliance with Business Architecture before funding approval and implementation.

To break down the business vision and principles into an implementable and workable structure, GEA utilizes the Business Reference Model to provide standardized, abstract views of government operations, enabling consistent analysis, planning, and communication across all MCDAs.

BUSINESS REFERENCE MODEL

The Business Reference Model (BRM) is an architecture tool that aligns an organization's operations and results with the government strategy vision.

Its primary objective is defining the business services and capabilities required to fulfill the vision, independent of the underlying technology used to implement them. The central organizing principle of the BRM is the concept of **Service**, which can be either customer-facing or internal.

BRM provides a structured approach for the MCDA to answer fundamental strategic questions:

- **WHY** are we performing these activities? (Vision and Goals)
- **WHAT** business services and capabilities do we need? (Service Portfolio)
- **WHO** is responsible for delivering them? (Organizational Alignment)

This ensures that every initiative, from national programs to departmental projects, directly contributes to strategic goals and measurable public value.

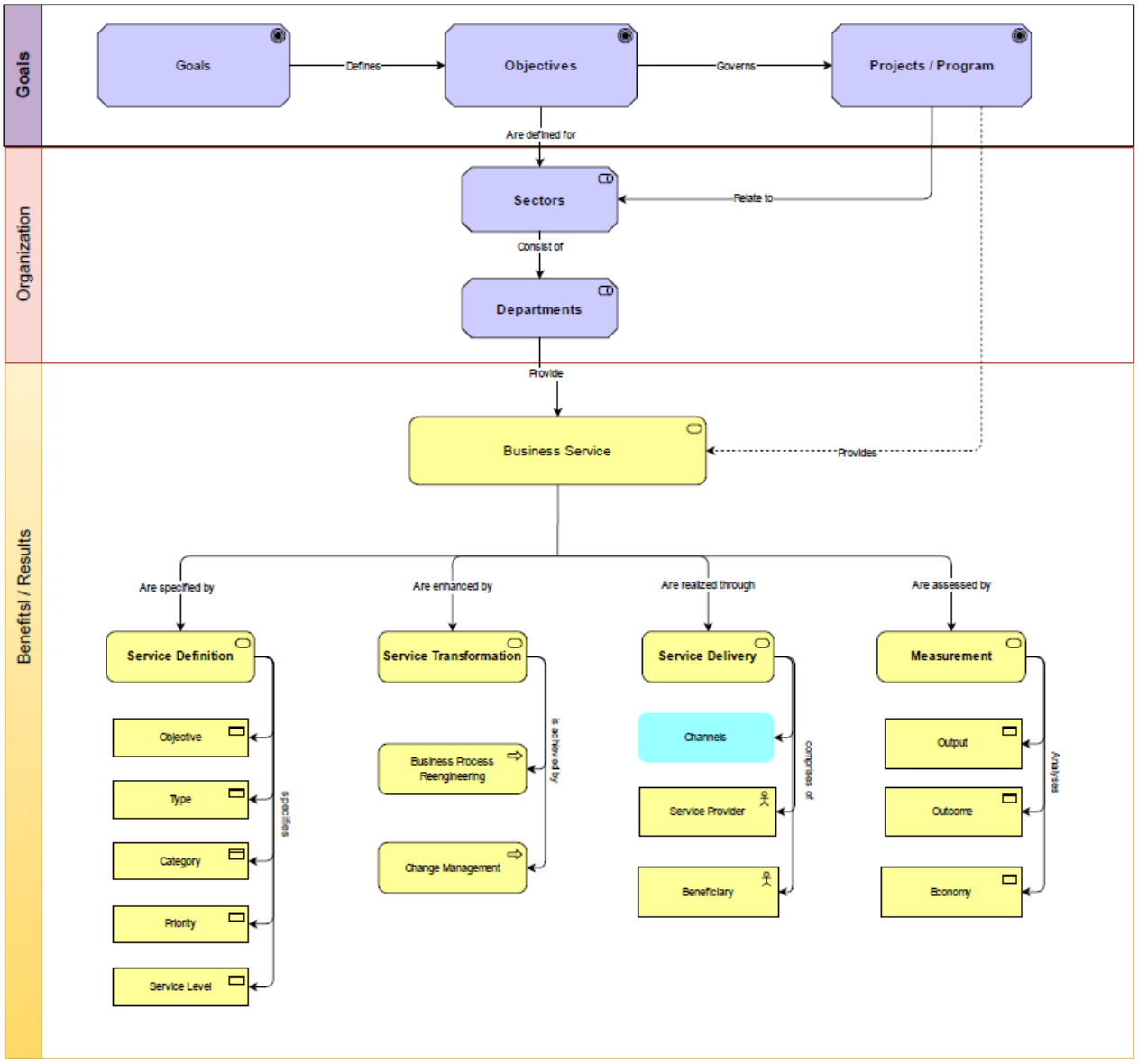

Figure 9 - GEA Business Reference Model

The Business Reference Model, shown in Figure 9 above, acts as a blueprint that connects strategy with organizational structure and tangible results to ensure that every activity, from a high-level program to a specific departmental task, is directly traceable to a strategic goal and delivers measurable value through services. It has been segmented into 3 layers as described below:

a) Goals Layer

Goals layer is the strategic driver for the enterprise (MCDA) because it defines it aims to achieve to fulfill its vision.

Goals	Broad, often qualitative statements that describe a desired future state.
Objectives	Goals are broken down into specific, measurable, achievable, relevant, and time-bound (SMART) Objectives.
Programs / Projects	Concrete initiatives are undertaken to ensure that resources are directed only in activities that directly contribute to strategic objectives.

b) Organization Layer

This layer represents the operational structure of the enterprise and shows how the organization is arranged to deliver on the programs and projects defined in the Goals layer.

- **Sectors:** These are the major divisions or functional groupings of the organization. E.g. Health, Education, Agriculture, etc. could be considered as sectors.
- **Departments:** Sectors are comprised of MCDAs i.e. various state departments and agencies within the different sectors

This model helps in restructuring the organization to eliminate silos and align departments more effectively around the services they collectively provide by linking the organizational structure to its purpose of service delivery.

c) Benefits/Results Layer

This layer transforms strategy into measurable outcomes through services. **Service** is the cornerstone, acting as the central hub that connects all components.

A service is a repeatable activity with a specific outcome that provides value to a beneficiary (e.g., a citizen, business or another MCDA).

The model breaks down the service lifecycle into four key components:

Component	Objective	Description
Service Definition	Defines the specific purpose of the service before it's delivered	• **Service Type** - transactional, informational, or regulatory service • **Service Category/SLA** (Service Level Agreement) - How is the service

		categorized, and the committed performance levels
Service Transformation	Defines how services evolve and are enhanced to become more efficient and effective throughout the lifecycle	• **BPR (Business Process Re-engineering):** This involves redesigning the processes behind a service to achieve efficiency and improvements. • **Change Management**: This addresses the human element of transformation, ensuring that stakeholders (employees and users) adopt the new processes and systems smoothly.
Service Delivery	Describes how the service is realized or provided to the end-user; the goal of the delivery process itself (e.g., accessibility, user satisfaction)	• Type - What channel is used for delivery (e.g., online portal, in-person, mobile app, etc.) • **Category**: How the specific delivery classified (i.e. Government to Citizens (G2C), Government to Business (G2B), Government to Government (G2G), Government to Employee (G2E)
Service Measurement	It closes the strategic loop by Objective - What is being measured (e.g., cost-effectiveness, citizen satisfaction) and ensures that services are assessed for performance and value.	• **Type** - What kind of metric is being used (e.g., quantitative KPI, qualitative survey) • **Category** - How are the measurements grouped for analysis

The results from Measurement provide feedback that informs future Goals and drives the need for further Service Transformation, creating a cycle of continuous improvement.

A rationalized and optimized Service catalog derived from this model becomes the primary input for designing the Enterprise Application Architecture.

By understanding the **Services** a particular MCDA needs to provide (**Service Definition**), how they should be continually improved (**Service Transformation**), and how they are delivered (**Service Delivery**) and their effectiveness evaluated (**Measurement)**, architects are able to design an application portfolio and robust technology infrastructure that avoids duplication, optimizes resources and promotes interoperability.

ESTABLISHING BUSINESS ARCHITECTURE

The Business Reference Model (BRM) provides a systematic approach to defining the Business Architecture by aligning government strategy, services, and outcomes. The following structured steps below serve as a practical guide to initiating the Business Architecture phase within the GEA initiative.

a) Define and align with GEA Vision

The EA initiative begins by identifying and articulating the strategic value the government intends to deliver. These plans are included in various strategic master plans and blueprints that explain these high-level goals in detail.

A visioning workshop with Architecture Review Board officials, stakeholders from the MCDA, policymakers and stakeholders to align on a unified Whole-of-Government (WoG) approach is conducted at this stage. The output creates a vision document that reflects the specific objectives of the government, serving as a reference point throughout the digital transformation roadmap.

b) Determine the Scope of the EA Initiative

Given the complexity and scale of government operations, the scope of the EA effort must be based on available capacity and strategic importance. Scope decisions shall consider risk exposure, national impact, and service criticality.

c) Identify Business Goals

Establish clear goals that will guide the development and implementation of Business Architecture categorized as follows:

- Enterprise-Level Goals: Broad objectives that span the entire scope of the GEA program.
- Domain-Specific Goals: Sectoral or departmental targets aligned with service outcomes or mission mandates.

d) Define the Portfolio of Services

The portfolio of services refers how the government delivers value to its citizens, businesses, and internal stakeholders.

The services need to be Identified, catalogued, and prioritized with key focus on:

- Reusability of service components across departments.
- Integration of services to minimize fragmentation and redundancy.

The outcome is well-structured Service Portfolio, which becomes the anchor for Application and Integration Architecture.

e) Design Delivery Architecture

Service delivery ensures that services are both high-performing and feedback-driven. Specifically aiming to:

- Align service delivery with clearly defined performance benchmarks.
- Establish continuous feedback loops to capture user satisfaction and operational effectiveness, thereby closing the value loop and informing future improvements.
- Ensure continuity of service under disruption scenarios including emergencies and system failures

f) Establish Performance Measurement and Continuous Improvement

This step embeds measurement, learning, and adaptation into the architecture process, ensuring the Business Architecture is continuously optimized for value, performance, and citizen impact.

Key activities include:

- Define KPIs: Establish clear, measurable KPIs and outcome metrics for each service, aligned with citizen satisfaction, cost efficiency, and policy outcomes.
- Implement Feedback Mechanisms: Integrate service analytics, citizen feedback, and operational performance dashboards to collect real-time insights.

- Conduct Capability Maturity Assessments: Schedule quarterly or annual reviews to assess whether business capabilities and services are delivering intended outcomes.
- Drive Continuous Improvement: Use insights from performance reviews to refine business processes, update service definitions, and reprioritize initiatives.

WHOLE-OF-GOVERNMENT VALUE STREAMS

Value Streams describe how the government delivers value end-to-end to citizens, businesses, and other stakeholders by orchestrating services, capabilities, and actors across MCDAs and the wider digital ecosystem. Value streams focus on outcomes and value realization, cutting across institutional boundaries to reflect how services are actually experienced by the stakeholders.

Within GEA, value streams provide the critical bridge between national goals and service delivery, ensuring that strategic objectives are translated into coherent, measurable, and citizen-centric outcomes by establishing a common Whole-of-Government (WoG) view of how value is created, independent of organizational silos or technology implementations.

Value Streams in Business Architecture

Value streams act as a unifying construct within the Business Architecture by:

- Translating national goals and policy objectives into end-to-end value delivery flows
- Enabling cross-MCDA coordination around shared outcomes rather than isolated mandates
- Providing a basis for capability planning, service design, and investment prioritization
- Supporting performance management by linking outcomes to services and measurable indicators

Each value stream spans multiple services and capabilities and may involve internal government actors, delivery agencies, ecosystem partners, and cross-border participants, consistent with the Whole-of-Government and ecosystem operating model.

Structure of GEA Value Stream

Each value stream is defined at an abstract, architecture level and comprises of the elements below:

Element	Description
Trigger	An event or need that initiates the value stream (e.g. a life event, regulatory requirement, or policy obligation).
Outcome	The intended result that delivers value to a beneficiary (citizen, business, or government).
Participating Services	A logical grouping of services that collectively realize the outcome.
Capabilities	The business capabilities required to enable the value stream across MCDAs.
Stakeholders	Key actors involved in value delivery, including ecosystem participants.
Performance Measures	High-level indicators used to assess effectiveness, efficiency, and experience.

Detailed process flows and system implementations are intentionally excluded at this stage and are addressed in Phase B1 of the *GEA Adoption and Implementation Guide*.

KEY VALUE STREAMS

The following WoG value streams represent the primary, cross-cutting mechanisms through which Government delivers public value. They provide a stable foundation for service portfolio design and sector architecture alignment.

Value Stream	Description
Citizen Identity and Lifecycle Management	Enables the recognition, registration, and management of citizens across key life events, including birth, education, employment, social protection, and civil status changes.
Business Formation and Compliance	Supports the end-to-end establishment, operation, regulation, and dissolution of businesses, including licensing, taxation, and regulatory compliance.
Service Access and Digital Engagement	Enables citizens and businesses to discover, access, and interact with government services through integrated digital and physical channels.

Value Stream	Description
Revenue Collection and Financial Management	Facilitates the assessment, collection, management, and reporting of government revenues, fees, and payments in a transparent and efficient manner.
Social Protection and Benefits Delivery	Enables the identification of beneficiaries, eligibility determination, and timely delivery of social assistance and welfare programs.
Public Safety, Justice, and Security	Supports prevention, enforcement, adjudication, and correctional services to maintain public order, safety, and rule of law.
Trade, Mobility, and Cross-Border Services	Enables cross-border movement of goods, people, and services through interoperable identity, customs, immigration, and trade facilitation systems.
Policy Formulation, Monitoring, and Oversight	Supports evidence-based policy development, implementation tracking, and performance oversight across government.

Value streams shall be periodically reviewed to reflect emerging national priorities and evolving service demands.

Value Streams, Services and Capabilities

Value streams do not replace services; they organize services around outcomes. Each value stream is realized through multiple services, which are defined, delivered, and measured within the Business Reference Model. Services, in turn, depend on reusable business capabilities that may be shared across value streams and sectors. This relationship ensures:

- Services are designed in the context of end-to-end value delivery
- Capabilities are prioritized based on strategic impact
- Duplication across MCDAs is identified and eliminated
- Investment decisions are aligned to national outcomes
- Use of Value Streams in Governance and Planning

Within the GEA governance framework, value streams are used to:

- Guide Business Architecture scoping and prioritization
- Align sector and MCDA architectures to Whole-of-Government outcomes
- Support investment appraisal and funding decisions

- Provide a reference point for performance measurement and continuous improvement

Institutionalizing value streams within Business Architecture, establishes a shared language of value, enabling coordinated action, measurable outcomes, and sustainable digital transformation across the entire government ecosystem.

Below is a Value Stream, Service, Capability, KPI mapping

Value Stream	Key Services	Core Business Capabilities	Representative KPIs
Citizen Identity & Lifecycle Management	Civil Registration, Digital ID Issuance, Status Updates (birth, death, marriage), Identity Verification	Identity Management, Population Registry Management, Data Validation & Quality Management, Inter-Agency Data Sharing	• % of population with verified digital identity • Identity issuance turnaround time • Identity verification success rate • Duplicate identity rate
Business Formation & Compliance	Business Registration, Service & Permits, KRA Registration, Regulatory Reporting	Business Registry Management, Licensing & Compliance Management, Regulatory Coordination, Digital Payments Enablement	• Time to start a business • % licenses issued digitally • Compliance rate • Cost of regulatory compliance
Service Access & Digital Engagement	Service Discovery, Online Applications, Omnichannel Support, Notifications	Service Catalog Management, User Experience Management, Channel Management, Digital Communications	• % services accessible digitally • User satisfaction score • Digital inclusion index • Service completion rate • Channel adoption rate • Service reliability
Revenue Collection & Financial Management	Tax Assessment, Fee Collection, Payment Processing, Revenue Reporting	Revenue Administration, Financial Transaction Management, Payment Integration, Financial Analytics	• Revenue leakage rate • Collection efficiency • % payments processed digitally • Reconciliation cycle time

Value Stream	Key Services	Core Business Capabilities	Representative KPIs
			• Cost-to-serve reduction
Social Protection & Benefits Delivery	Beneficiary Registration, Eligibility Determination, Benefits Disbursement, Grievance Management	Beneficiary Management, Eligibility & Rules Management, Funds Disbursement, Case Management	• Targeting accuracy • Benefits delivery timeliness • Leakage/fraud rate • Beneficiary satisfaction
Public Safety, Justice & Security	Incident Reporting, Case Management, Prosecution, Correctional Services	Law Enforcement Operations, Case Lifecycle Management, Judicial Administration, Inter-Agency Coordination	• Case resolution time • Crime clearance rate • Backlog reduction • System interoperability rate
Trade, Mobility & Cross-Border Services	Customs Clearance, Immigration Processing, Trade Certification, Cross-Border Payments	Trade Facilitation, Border Management, Credential Verification, Regional Interoperability	• Clearance time at borders • % automated declarations • Cross-border transaction success rate • Compliance with regional SLAs
Policy Formulation, Monitoring & Oversight	Policy Development, Data Analytics, Performance Reporting, Audit & Oversight	Policy Analysis, Performance Management, Data Analytics, Compliance Monitoring	• Policy outcome achievement rate • Data timeliness • % programs meeting targets • Audit resolution rate

STAKEHOLDER & ROLE MAPPING

This mapping defines the key stakeholders and roles involved in the design, delivery, governance, and oversight of government services across the Whole-of-Government (WoG) digital ecosystem.

It clarifies decision rights, accountabilities, and responsibilities, ensuring effective coordination across MCDAs, national platforms, ecosystem partners, and cross-border actors.

This role model is architecture-binding and applies to all services, platforms, and digital initiatives governed under the GEA.

Stakeholder Category	Role	Primary Responsibilities
Citizens & Businesses	Service Consumers	• Consume government services. • Provide feedback and consent for data use • Participate in digital engagement channels.
Policy Authorities	Policy Owners	• Define national policies, legal frameworks, and strategic objectives aligned to Vision 2030.
Executive Leadership	Strategic Sponsors	• Provide strategic direction • approve priorities, funding envelopes, and major reforms.
Ministries, Counties, Departments & Agencies (MCDAs)	Service Owners	Own and are accountable for end-to-end service outcomes, regardless of how many entities contribute.
Sector Leads	Sector Coordinators	Coordinate sector-wide services and capabilities; align sector architectures to GEA.
Business Capability Owners	Capability Owners	Own and mature shared business capabilities used across services and value streams.
Data Governance Bodies	Data Owners / Stewards	Define data standards, ownership, quality, access rules, and stewardship.
Digital Delivery Units / ICT Authorities	Solution Delivery Leads	Design, build, integrate, and operate digital solutions in compliance with GEA and GIF.
GEA/GIF Oversight Authority	Architecture Authority	Acts as custodian of GEA, responsible for standards, oversight, and coordination across government.
Architecture Review Board (ARB)	Architecture Authority	Enforce GEA principles; approve architectures; conduct conformance and compliance review and empowered to approve, reject, or require remediation of non-compliant initiatives.
Treasury / Budget Authorities	Investment Authorities	Approve funding based on architectural alignment, value streams, and performance impact.

Stakeholder Category	Role	Primary Responsibilities
Procurement Authorities	Procurement Gatekeepers	Ensure procurement aligns to GEA, interoperability standards, and vendor neutrality.
Security & Oversight Agencies	Security Authorities	Define and enforce security, privacy, and trust requirements across the ecosystem.
Public–Private Partners (PPPs)	Ecosystem Service Providers	Deliver services or capabilities under defined contracts and architecture constraints.
Private Sector & FinTechs	Ecosystem Integrators	Integrate with government platforms to deliver value-added services.
Regional & Cross-Border Bodies	Cross-Border Partners	Enable regional interoperability, mutual recognition, and shared services.
Audit & Oversight Institutions	Independent Oversight Bodies	Audit performance, compliance, and value realization across digital initiatives.

Kenya's digital transformation strategy will only succeed if clear accountability exists for outcomes and not only projects or systems. This accountability model assigns decision rights, ownership, and performance responsibility across the entire digital ecosystem to ensure that:

- Services deliver measurable value to citizens and businesses
- Investments are aligned to national priorities
- Duplication is eliminated and interoperability enforced
- Public–Private Partnerships and ecosystem actors operate under clear government control

VALUE STREAM RACI MATRIX

The Value Stream RACI Matrix provides a consolidated view of roles, responsibilities, and accountabilities across the key government value streams. It establishes clear ownership for value delivery, decision-making, and performance outcomes, ensuring that responsibilities are explicitly assigned and understood across MCDAs, and ecosystem partners.

By organizing accountability around value streams rather than institutional silos, the matrix reinforces the Whole-of-Government operating model and enables coordinated action across organizational boundaries. It clarifies who is **Responsible** for execution, who is **Accountable**

for outcomes, who must be **Consulted** in decision-making, and who must be **Informed** for transparency and oversight. RACI assignments shall be reviewed annually to ensure alignment with evolving mandates.

Value Stream	Executive Leadership	Service Owner (MCDA)	Architecture Review Board	National Treasury	Security & Data Authorities	Ecosystem / PPP Partners
Citizen Identity & Lifecycle Management	I	R	C	C	A	C
Business Formation & Compliance	I	R	C	C	C	R
Service Access & Digital Engagement	I	A	C	I	C	C
Revenue Collection & Financial Management	I	R	C	A	C	R
Social Protection & Benefits Delivery	I	R	C	C	A	C
Public Safety, Justice & Security	I	R	C	I	A	C
Trade, Mobility & Cross-Border Services	I	R	C	C	A	R
Policy Formulation, Monitoring & Oversight	A	R	C	C	C	I

This consolidated RACI matrix serves as a mandatory governance reference for architecture approval, investment prioritization, procurement, and performance management. All services, platforms, and digital initiatives must demonstrate alignment with the defined roles and accountabilities to ensure effective execution, eliminate duplication, and deliver measurable value in line with national priorities.

DATA / INFORMATION ARCHITECTURE

Data Architecture establishes a Whole-of-Government framework for governing, managing, sharing, protecting, and leveraging data as a strategic national asset. The primary objective is to ensure that government data is trusted, secure, interoperable, and accessible to support effective governance, economic development, national security, and citizen-centric service delivery.

Data architecture positions data as a strategic asset and a foundational capability for achieving national development priorities, including improved public service outcomes, evidence-based policy, enhanced revenue mobilization, digital innovation, and strengthened public trust.

By adopting a unified approach, government ensures that data is managed consistently across MCDAs, enabling seamless collaboration and eliminating data siloes and fragmentation.

This architecture governs the full data lifecycle from creation through use, sharing, archival, and disposal and applies to all government data, including:

- Operational data
- Master and reference data
- Analytical data
- Geospatial data
- External partner data
- Open data
- Archived records
- Emerging data sources such as IoT and digital platforms

OBJECTIVES OF DATA ARCHITECTURE

The primary objective is to harness the power of trusted, secure, and ethically-managed government data as a unified national asset that drives policy, empowers citizens, and delivers intelligent, proactive public services.

MCDAs shall pursue the following objectives:

a) Treat data as a national strategic asset that supports policy, service delivery, and economic growth.
b) Establish authoritative data sources for core national entities such as citizens, businesses, and locations.
c) Enable seamless and secure data sharing across government through standardized interfaces.
d) Improve data quality, reliability, and timeliness across all systems.
e) Strengthen data governance and accountability at national and institutional levels.
f) Protect privacy, confidentiality, and national security through robust safeguards.
g) Support advanced analytics, artificial intelligence, and evidence-based decision-making.
h) Promote innovation through controlled and responsible access to data.
i) Preserve government records and institutional memory.
j) Build public trust through transparent and ethical data practices.

INFORMATION ARCHITECTURE PRINCIPLES

The effectiveness of the Information Architecture is underpinned by a set of core principles that guide its implementation and use to manage data as a critical enterprise asset.

Principle	Description
Data as a Strategic Asset	Data is recognized as a critical asset with specific and measurable value. It must be made available for sharing across the government, subject to legal and security controls, to maximize its value.
Data Sharing and Reuse	Data should be shared across government entities to prevent duplication, reduce inefficiencies, and enable integrated service delivery; subject to clearly defined rights, roles, and privileges, conforming to the principles of data security, privacy, and confidentiality.
Data Stewardship and Accountability	Every dataset must have a designated data steward responsible for ensuring the quality, accuracy, integrity, and security of the data.
Data Security and Privacy	Data must be safeguarded against loss, unauthorized access, and corruption. Privacy and security are paramount as well as compliance the Kenya Data Protection Act, 2019

Standardized Data Definitions	All data must be defined once and consistently across government entities using common vocabulary, taxonomy, and metadata standards to ensure that information can be consistently interpreted and exchanged between MCDAs
Ethical and Transparent Data Use	The collection and use of citizen data will be transparent, purposeful, and ethical. Citizens have a right to know how their data is being used and to control its dissemination where legally applicable.

DATA REFERENCE MODEL (DRM)

The Data Reference Model provides a common framework for describing, governing, managing, sharing, and assuring the quality of government data across its lifecycle to establish the semantic foundations, governance structures, and interoperability principles required to treat data as a trusted national asset. *Figure 10* below shows a diagrammatic depiction of the Data Reference Model

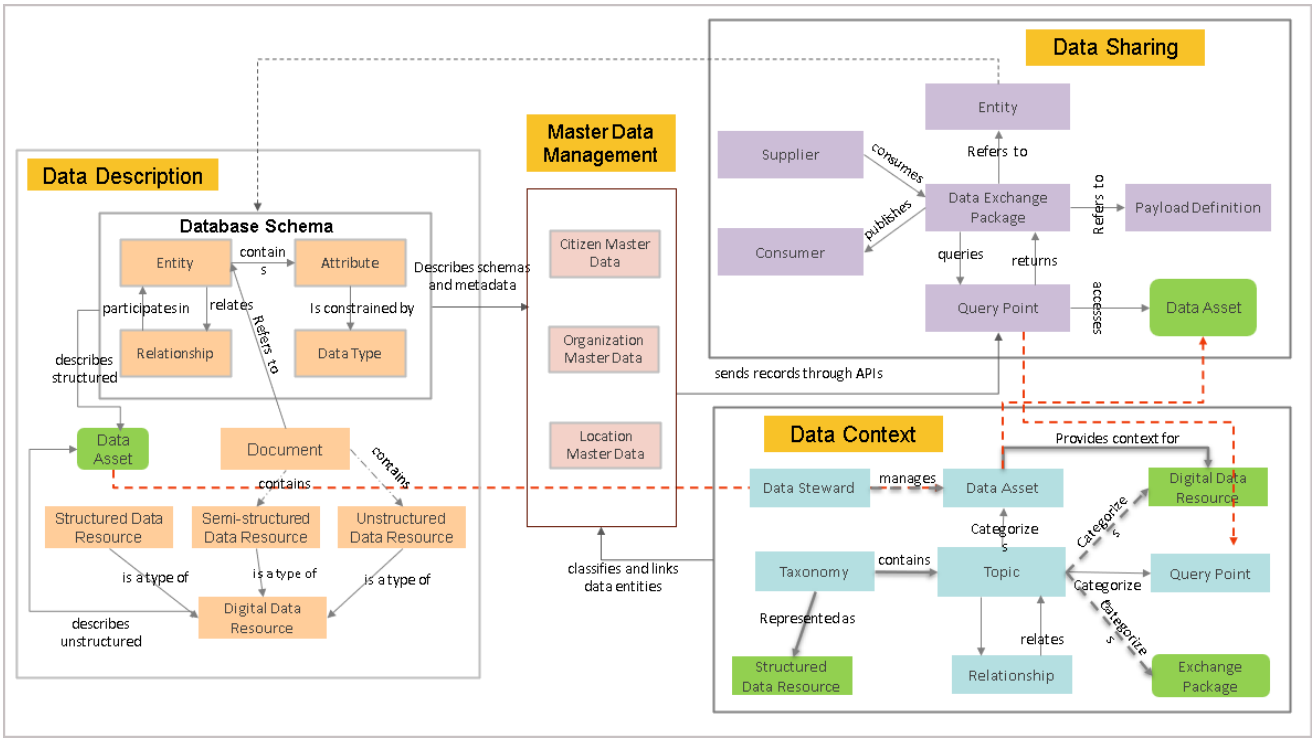

Figure 10 - Data Reference Model

a) Data Description

Data Description refers to the formal definition, structuring, and semantic articulation of data. It ensures that data elements used across various government systems are understood in a uniform and consistent manner. It defines what each data element means, how it should be represented, and how it can be identified, classified, and reused.

Data Description scope includes:

- Metadata definitions
- Data models (conceptual, logical, canonical)
- Data dictionaries
- Naming conventions
- Semantic definitions

Standardizing data descriptions eliminates ambiguity in data interpretation and ensures that different systems can exchange and use data without requiring manual reconciliation. The key elements are:

Element	Description
Metadata Specification	Using internationally accepted metadata standards (e.g., ISO/IEC 11179), each data element is described in terms of its name, format, permissible values, units, data type, and definition.
Data Modeling	Logical and conceptual data models define relationships between data entities. These models help architects visualize the structure of data across agencies and align it with business processes.
Data Dictionaries and Glossaries	Repositories of agreed-upon definitions and data elements used across the government which act as a reference point for developers, data stewards, and system integrators.

b) Data Context

Data Context defines how data relates to its business purpose, relevance, and usage within specific government domains or functions. While Data Description focuses on what data is, Data Context focuses on why the data matters and how it is used.

Contextualizing data is essential for assigning meaning based on the function or process it supports, providing the basis for prioritizing high-value datasets, alignment between the DRM

and the Business Reference Model (BRM) and ensuring that data supports the actual business goals and services of the government.

Data context involves the key elements below:

Element	Description
Domain-Specific Classification	Data is categorized according to business domains (e.g., agriculture, transport, public health, etc), enabling its use to be aligned with the strategic goals of the respective sectors.
Ontologies and Taxonomies	Government-wide classification systems and controlled vocabularies are developed to support meaningful interpretation of data. These include industry-standard taxonomies for sectors like healthcare (e.g., ICD codes) or education (e.g., NEMIS standards).
Data Stewardship and Ownership	Each dataset is assigned a data owner or trustee responsible for the data's quality, relevance, and security. This enhances accountability and governance in data management.

c) Data Sharing

Data Sharing governs the flow and controlled exchange of data between systems and departments at all levels of government, ensuring that data can be reused securely, efficiently, and in compliance with applicable policies and laws.

By promoting interoperability and breaking down data silos, effective data sharing facilitates seamless integration across diverse systems, departments, and jurisdictions. This principle ensures that data is consistently and efficiently reused while complying with relevant security policies, privacy regulations, and legal frameworks.

Data sharing component includes the elements below:

Element	Description
Interoperability Standards	Technical protocols (e.g., RESTful APIs, XML, JSON) and data exchange formats and standards that enable seamless system-to-system communication as defined in the GIF framework.
Access Control and Authorization	Policies defined for granting access to datasets based on roles, privileges, and sensitivity classifications. Identity and access management tools used to enforce these controls.

Data Sharing Agreements and SLAs	Formal agreements or contracts that define how data will be shared, for what purpose, under what conditions, and with what guarantees on availability, integrity, and confidentiality.
Privacy and Consent Frameworks	Mechanisms established to ensure that personal and sensitive data is handled according to data protection regulations, and that data subjects' consent is obtained and respected where required.

d) Master Data Management (MDM)

The Master Data Management (MDM) component extends the Data Reference Model by providing the mechanisms, governance structures, and technology patterns required to create and maintain authoritative, consistent, and reusable core data entities across MCDAs. These master data entities such as citizen, organization, and location form the backbone of interoperable and data-driven digital government services.

MDM ensures that critical data entities are:

- Defined once and used consistently across all MCDAs.
- Stored and managed through authoritative systems that act as the “single source of truth.”
- Governed through standardized lifecycle policies, version control, and change management processes.
- Synchronized across systems through controlled data sharing and integration mechanisms.

Centralized MDM Design Patterns

GEA adopts a hybrid centralized MDM architecture, combining national-level authoritative registries with domain-specific extensions at MCDA level. The design patterns for key master data domains are as follows:

Master Data Domain	Centralized Design Pattern	Description
Citizen Master Data	**National Population Register (NPR)**	The NPR serves as the authoritative source for all person-related data, including identifiers (e.g., National ID), demographic details, and verification attributes. It exposes standard APIs for authentication and identity validation across government systems.
Organization Master Data	**National Business and Institution Registry (NBIR)**	A centralized repository that maintains master records of legal entities, institutions, and businesses. It integrates with systems like eCitizen, the Business Registration Service (BRS), and KRA to ensure consistency of organizational information across government.
Location Master Data	**National Geospatial Reference Registry (NGRR)**	Provides authoritative geolocation, address, and administrative boundary data. It is managed in alignment with the Kenya National Spatial Data Infrastructure (KNSDI) standards to support location-based analytics, planning, and service delivery.

Each master data domain is integrated through standardized APIs, metadata definitions, and interoperability protocols defined in the *Government Interoperability Framework (GIF).*

MDM Governance and Integration Principles

- Authoritative Ownership: Each master dataset has a clearly defined owner responsible for its accuracy and governance.
- Syndication and Synchronization: Data replication across systems occurs through secure, standardized data services, ensuring real-time consistency without redundancy.
- Data Versioning and History Tracking: All changes to master records are version-controlled to maintain historical traceability.
- Data Quality Monitoring: Automated validation and profiling tools continuously assess accuracy, completeness, and integrity of master data.
- Interoperability Alignment: All MDM entities and APIs conform to the metadata standards and data exchange protocols of the DRM and GIF.

Implementation Recommendations

The following tools and technologies can support centralized and federated MDM deployment within the GEA ecosystem:

- Platforms: Informatica MDM, Talend MDM, IBM InfoSphere MDM, or open-source alternatives like WSO2 MDM or Pimcore.
- Integration Frameworks: RESTful API gateways and message queues (e.g., Apache Kafka, MuleSoft, or WSO2 ESB) to synchronize master data between systems.
- Metadata Alignment: All master data definitions must be registered and maintained in the National Metadata Registry (NMR) for discoverability and governance consistency.

Incorporating MDM within Data Reference Model ensures that the most critical data assets citizen, organization, and location are unified, accurate, and consistently applied across systems.

DATA ARCHITECTURE CONTEXTUAL MODEL

The Data Architecture Contextual Model in *Figure 11* below illustrates the structural layers and enabling platforms required to manage data as a strategic national asset within GEA. It shows how data is collected from operational environments and aggregated into repositories where it is managed and governed. Through governance and sharing platforms, data becomes discoverable, standardized, and reusable across government.

The layered structure ensures clear separation of responsibilities while enabling integration across the ecosystem enabling digital services and open data initiatives to deliver value to citizens and institutions while maintaining compliance with policies and security requirements.

The model serves as a bridge between conceptual architecture (see the *Data Reference Model* in the previous section) and real operational environments.

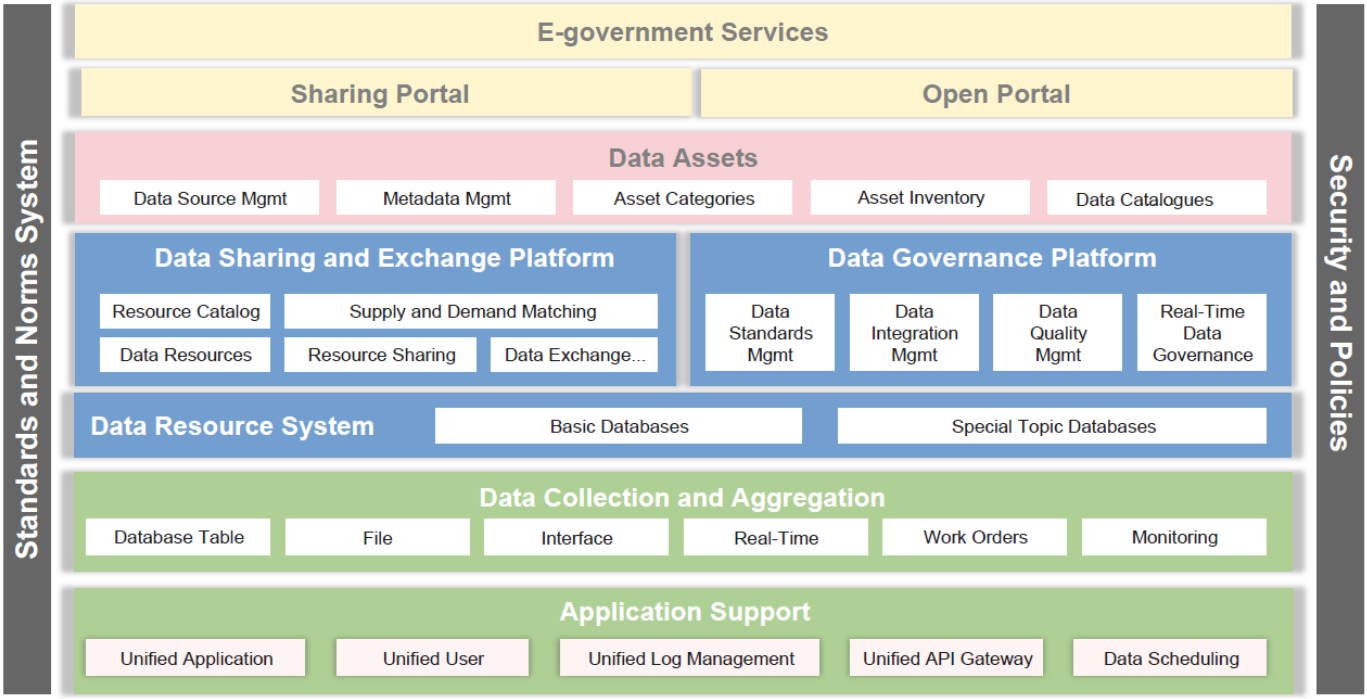

Figure 11- Data Architecture Contextual Model

The model is organized into horizontal layers representing the lifecycle of data, supported by vertical pillars that enforce governance, standards, and security across all layers.

a) E-government Services Layer

The top layer represents the delivery of digital services to citizens, businesses, and public sector users. All digital services delivered by an MCDA (permits, welfare applications, licenses, etc.) interface here. This is the ultimate beneficiary of effective data management.

Key elements include Government service portals, Digital service platforms, Cross-agency service delivery channels which are supported by:

- Sharing Portal which facilitates the exchange of information and services among government entities.
- Open Data Portal to provides public access to government data and services, promoting transparency and citizen engagement.

b) Data Assets Layer

This layer represents the government's data resources which are treated as managed assets which ensure that government maintains visibility, ownership, and control over its data holdings, supporting discoverability, reuse, and governance. They include:

Component	Description
Data Source Management	Processes for managing the origin and collection of data.
Metadata Management	Standardized descriptions of data to improve discoverability and understanding.
Asset Categories & Asset Inventory	Classification and cataloging of data assets to ensure they are properly managed and utilized.
Data Catalogues	Centralized, organized inventory of MCDA data assets, utilizing metadata to help users discover, understand, and trust data

c) Data Sharing and Exchange Platform & Data Governance Platform

This platform enables controlled and standardized data exchange across institutions and aligns with GIF to ensures that data sharing occurs through governed channels rather than ad-hoc integrations.

Data Sharing and Exchange Platform	This platform enables controlled and standardized data exchange across institutions. Capabilities include: • Resource catalogues • Data discovery • Supply-and-demand matching • Data exchange services • Resource sharing mechanisms.
Data Governance Platform	Enforces policies, standards, and oversight across the data ecosystem to ensure compliance with national policies, legal requirements, and architecture standards. Functions include: • Data Standards Management • Data integration oversight • Data quality management

	• Real-time governance monitoring

d) Data Resource System Layer

This layer represents the operational repositories where MCDA data is stored supporting both transactional operations and analytical needs.

- **Core operational Databases:** Standard databases that support general government operations (e.g., citizen service requests, birth records)
- **Sector Specific Repositories**
- **Specialized Datastores:** Specialized databases for specific purposes and functions, such as spatial, environmental data or public health records.

e) Data Collection and Aggregation Layer

This layer captures data from legacy systems, field operations, and ecosystem platforms into operational repositories from multiple sources and channels using:

- Database Tables, Files, Interfaces; represent the traditional methods for data collection.
- Real-Time, Work Orders, Monitoring: More modern, dynamic methods for continuous data acquisition and processing.

f) Application Support Layer

This layer provides shared application services that enable data processing and integration. It provides the capabilities below to improve consistency, reduce duplication, and strengthen operational resilience including:

- Unified application services
- Identity and user management
- Logging and monitoring
- API management
- Scheduling and orchestration

g) Cross-Cutting Pillars

These vertical pillars that span the entire model highlighting their universal functions and importance in data management.

Standards and Norms System	Represent the overarching policies, regulations, and best practices that govern all layers. It ensures: • Alignment with national standards • Consistent implementation across MCDAs • Compliance with legal and regulatory requirements • Adoption of common data practices
Security Assurance System	Security controls apply across all layers to safeguard information and maintain trust reinforcing the security-by-design principle across the data ecosystem. Controls include: • Access management • Encryption • Monitoring and auditing • Privacy safeguards • Risk management

This layered structure supported by standards and security controls reinforces the WoG approach to interoperability, evidence-based decision-making, and citizen-centric service delivery.

DATA STANDARDS

Data standards define the common conventions and specifications for representing, structuring, formatting, tagging, transmitting, and using data across government systems. They serve as the "**rules of engagement**" that govern how information is recorded, processed, and exchanged, establishing the foundation for interoperability and consistency across MCDAs.

The main objectives of data standards within the GEA framework are to:

- Ensure accuracy and consistency in data capture and representation.
- Enable seamless data sharing and exchange across systems and institutions.
- Reduce redundancy and minimize errors in data handling.
- Provide a standardized foundation for interoperability within and across government entities.

Standardizing Data Elements

In an integrated e-Government environment, services frequently span multiple domains such as health, taxation, education, agriculture, land administration, etc. each managing distinct data entities and systems. To ensure cross-domain consistency:

- Each data element must be defined as an independent, well-described unit with a clear contextual meaning.
- Common data elements (e.g., National ID, date of birth, land parcel number) should be standardized and reused across domains to prevent duplication and inconsistency.
- Associated metadata must clearly define meaning, format, constraints, and permissible values.

Standardizing data elements and metadata in this manner promotes interoperability, eliminates data silos, enhances accuracy, and improves the reliability and efficiency of public service delivery across domain-specific applications.

Reference Publications and Standards

The following publications and standards provide mandatory guidance on data governance and management across government and enforcement within the GEA framework. These can be accessed from the ICT Authority portal at https://icta.go.ke/ict-standards

Publication	Purpose
Data Governance	The Kenya Data Protection Act, 2019 is the foundational legal standard for all data processing activities.

Data Classification Policy	A mandatory government-wide policy defining the criteria and handling procedures for Secret, Internal, and public data classifications.
Master Data Management (MDM)	Policy defining the process for identifying and managing authoritative data sources.
Data Exchange Format	JSON is the mandatory standard for data payloads in all new API-based data sharing.
Open Data Standard	The Data Catalog Vocabulary (DCAT) standard for publishing public datasets on the Kenya Open Data Portal to ensure discoverability and interoperability.
Geospatial Data	KSDI (Kenya National Spatial Data Infrastructure) standards for all geospatial information.

Enforcing common data and metadata standards, GEA ensures that information is interoperable, trustworthy, and reusable across public sector entities laying the foundation for integrated, data-driven, and citizen-focused digital government services.

METADATA MANAGEMENT

Metadata management refers to the systematic organization, optimization, and use of metadata to enhance the accessibility, quality, and governance of an organization's information resources includeing descriptive details such as authorship, creation timestamps, structural characteristics, lineage, classification, and security attributes.

Metadata is the descriptive context required to understand, govern, and effectively use data across government by defining the structure, meaning, and permissible values of data elements, ensuring that information assets remain coherent, traceable, and consistently applied across MCDAs.

Once data standards are established, metadata management becomes the primary mechanism for enabling discoverability, integration, interoperability, and reuse across the government ecosystem by:

1. Describing the structure, content, and relationships of data elements.
2. Defining the purpose, usage constraints, formats, and controlled vocabularies associated with each element.

3. Enabling efficient retrieval, exchange, and integration of information resources across organizational boundaries.
4. Establishing accountability through documented ownership, stewardship responsibilities, and lifecycle constraints.

Metadata Architecture Contextual Model

The Metadata Architecture Contextual Model defines the hierarchical structure through which data meaning, structure, and governance are consistently defined, managed, and enforced across the government ecosystem establishing a formal foundation that ensures all government data from conceptual definitions to operational systems is aligned to common semantics, standards, and modelling rules.

By structuring metadata across abstraction layers as shown in *Figure 12* below the model ensures that government systems evolve without losing semantic consistency, thereby reducing fragmentation and strengthening Whole-of-Government integration.

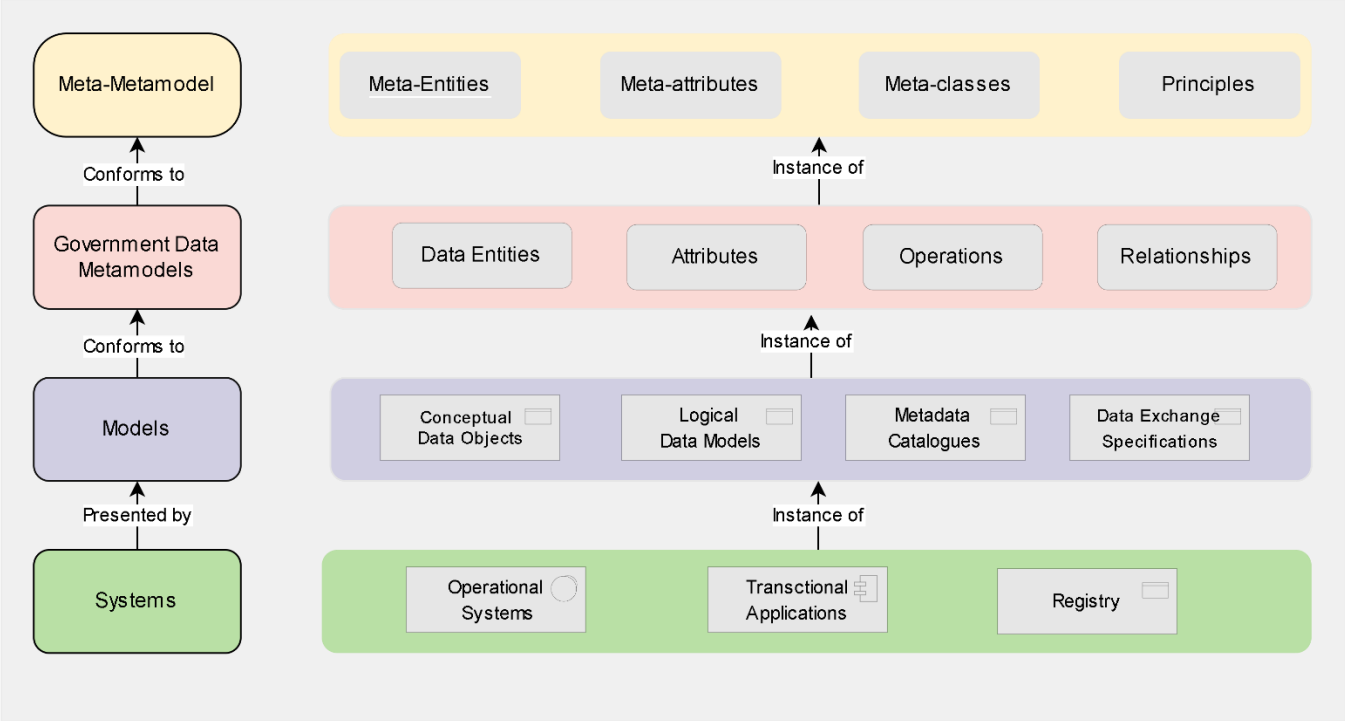

Figure 12 - Metamodel Architecture

The model is structured as a hierarchy of four abstraction layers, each representing a different level of semantic definition and implementation to ensure separation of concerns, allowing

policy, modelling standards, and operational systems to evolve independently while remaining aligned. These layers are described in further detail below.

Meta-Metamodel Layer (Foundational Modelling Rules)

The top-most layer defines the fundamental language and principles used to construct government data models. It establishes the formal constructs that govern how modelling frameworks are defined. Key elements include:

- Meta-entities
- Meta-attributes
- Meta-classes
- Modelling principles

The layer ensures that all government modelling approaches conform to internationally recognized foundations and remain consistent across domains to guarantee semantic coherence across the entire data architecture landscape.

Government Data Metamodel Layer (Government Modelling Standard)

This layer defines the Government Data Metamodel, which specifies the constructs used to build data models across government. It includes the components below:

- Data entities
- Attributes
- Operations
- Relationships

The metamodel provides standardized vocabulary and structure used to represent government data consistently across sectors, enabling harmonization and reuse and ensuring that sectoral models are built using common definitions and modelling conventions.

Model Layer (Domain and Solution Models)

The Model Layer defines the formal representations of government data domains, capturing the core concepts, structures, relationships, and rules that describe how information is

understood and used across government. It represents the design-time view of data, translating business meaning into structured models that guide solution design and integration.

This layer serves as the point where abstract modelling constructs defined in the Government Data Metamodel are applied to specific domains ensuring that all data representations are built using standardized entities, attributes, relationships, and constraints, enabling consistency and semantic alignment across MCDAs.

The Model Layer provides a stable, technology-independent view of information, ensuring that system implementations are grounded in agreed definitions and that stakeholders maintain a shared understanding of key concepts. For example, defining a "**Citizen**" entity with agreed attributes and relationships ensures that all systems interpret and use citizen information consistently.

Artefacts within this layer include:

- **Conceptual Data Models** that capture high-level business concepts and relationships
- **Logical Data Models** that define structured representations independent of specific technologies
- **Canonical Sectoral Data Models** that standardize data structures across domains
- **Master Data and Reference Data Models** that define authoritative entities and controlled vocabularies
- **Metadata Catalogues** that document definitions, lineage, and classifications
- **API and Data Exchange Specifications** that formalize how data is structured and exchanged

All artefacts in this layer are instances of the constructs defined in the Government Data Metamodel, ensuring uniform modelling practices, semantic consistency, and interoperability across the government enterprise

Systems Level (Operational Instances)

The Systems layer represents operational environments where data is created, stored, and processed. These are objects containing actual values, such as a specific citizen record in a database.

Components include:

- Operational systems
- Transactional applications
- Registries

These systems implement the models defined above, ensuring that real-world data aligns with enterprise definitions supporting data integrity, consistency, and interoperability.

The Contextual Metamodel Architecture establishes clear conformance relationships to provide traceability from operational data back to architectural standards and policy intent, strengthening governance and accountability.

- Systems conform to models
- Models conform to the government metamodel
- The metamodel conforms to foundational modelling principles

Metadata Registry

To operationalize metadata governance across government, we recommend the establishment of a National Metadata Registry (NMR) within the existing structures of the Ministry of ICT and Digital Economy's (MICDE) and ICTA to serve as the single authoritative repository for all government data element definitions, classifications, and relationships. The implementation approach below detail how this will be actualized

Implementation Step	Description
Centralized Governance, Federated Management	The NMR will be centrally governed by MICDE allowing MCDAs to register, update, and maintain their domain-specific metadata through controlled interfaces and approval workflows.
Standards Alignment:	Metadata structures will conform to international standards such as ISO/IEC 11179 (Metadata Registries) and DCAT (Data Catalog Vocabulary) to ensure compatibility and interoperability with open data and cross-border systems.

Integration and Access	APIs and automated synchronization mechanisms will enable integration with sectoral systems, master data repositories, and the Kenya Open Data Portal to ensure metadata consistency across platforms.
Lifecycle Management	Version control, change management, and approval workflows will govern how metadata evolves from initial registration to review, archival, or deprecation ensuring traceability and accountability.

Metadata Management Tools

Metadata management tools (also called enterprise metadata management or EMM systems) are software solutions that help capture and manage government Metadata. These solutions packaged as modules of data governance, digital asset management, or data management platforms aim to improve discoverability, governance processes and data-driven decision-making. The features of enterprise metadata management tools include:

Tools / Features	Description
Standalone data catalogs	Centralized platforms that consolidate and organize metadata to improve searchability and enable self-service access to data silos and increase user trust in shared data assets.
Metadata-enhanced ETL and data integration	Data integration and extract, transform, load (ETL) tools help organizations automate metadata extraction while managing data transformations to that metadata flows seamlessly alongside data, improving real-time analytics, data quality and compliance.
Enterprise data governance	Comprehensive platforms offering policy enforcement, data quality controls, and regulatory compliance features embedded within metadata governance workflows.
Cloud-native metadata catalogs	Cloud-native metadata catalogs provide automated metadata discovery, lineage tracking and security controls to support

	scalable and interoperable metadata management and smooth integration across multi-cloud and hybrid environments.
Open-source metadata tools	Open-source metadata tools offer flexible metadata management and support custom workflows, collaboration and governance customization to allow organizations to tailor metadata management to their unique data architecture and avoid vendor lock-in.

DATA GOVERNANCE FRAMEWORK

Data Governance is the authoritative system through which government establishes decision rights, accountability structures, policies, and control mechanisms to ensure that data is managed as a strategic national asset across all MCDAs

Within the GEA, Data Architecture defines what structures, standards, and models must exist, while the Data Governance Framework defines who is accountable, how compliance is enforced, and how data practices evolve in a controlled and coordinated manner across the Whole-of-Government environment.

Data Governance establishes oversight, authority, and control mechanisms that guide how data is created, classified, stored, shared, archived, and disposed, ensuring that data management practices are consistent, lawful, secure, and aligned to national priorities.

The objectives of Data Governance under the GEA are to:

- Ensure consistency, quality, security, and interoperability of data across systems and institutions
- Institutionalize accountability for data ownership and lifecycle management
- Establish enforceable mechanisms for adopting and evolving data standards
- Enable lawful, ethical, and transparent use of government data
- Provide measurable oversight of data performance and maturity

The Data Governance Framework operationalizes these objectives through clearly defined governance structures, policies, processes, controls, monitoring mechanisms, and performance indicators and creates a coordinated governance ecosystem that balances central authority with institutional responsibility, ensuring that all MCDAs operate within a unified national data governance model.

The data governance framework can be broken down into following core areas:

a) People and Oversight: Establishing Clear Roles

Effective Data Governance requires clearly defined authority, accountability, and coordination across institutional and technical functions. A clear separation of responsibilities is critically important in ensuring that strategic direction, operational stewardship, and technical custody are aligned while avoiding ambiguity in decision-making. This reinforces the principle that data governance is a shared responsibility across business leadership, data domain owners, and technology teams.

Within each MCDA formal governance structures shall be established to oversee data priorities, enforce standards, resolve issues, and promote responsible data practices. These roles collectively ensure that data is treated as an institutional asset rather than a by-product of systems.

Role	Stakeholders	Primary Responsibilities
Data Governance Council	Senior leaders from different departments within the MCDA (e.g., Permanent Secretaries, Directors, Heads of Departments or designated executives).	• Set strategic direction for data management aligned with GEA and institutional mandates. • Approve data policies, standards, and governance priorities. • Resolve cross-functional data conflicts and escalation issues. • Oversee compliance with national data governance requirements. • Promote a culture of data accountability and responsible use. • Provide executive sponsorship for data initiatives.
Data Stewards	Business or domain experts responsible for specific datasets or data domains.	• Define business meaning, rules, and classifications for data. • Establish and monitor data quality requirements.

		• Ensure datasets comply with standards and policies. • Approve and review access requests in line with governance policies. • Maintain metadata and documentation. • Act as the primary point of accountability for data within their domain.
Data Custodians	ICT and platform teams responsible for data infrastructure and operations	• Implement technical controls including security, access management, and monitoring. • Manage storage, backup, recovery, and operational integrity. • Enforce data protection and resilience measures. • Execute access decisions as authorized by Data Stewards. • Ensure systems comply with architecture and security standards

To ensure effective governance across the Whole-of-Government environment, the following role alignment principles shall apply:

- Business Ownership of Data: Accountability for data meaning and quality resides with business units, not technology teams.
- Separation of Duties: Strategic oversight, data stewardship, and technical operations are distinct but coordinated functions.
- Federated Governance: MCDAs manage domain data while aligning with national standards and oversight mechanisms.
- Escalation Pathways: Unresolved issues shall be escalated through governance structures to ensure timely resolution.
- Traceability: Decisions regarding data definitions, access, and changes shall be documented and auditable.

b) Policies and Standards

Policies and standards provide formal rules and guidance that translate the principles of the GEA into consistent and enforceable practices across MCDAs. They establish the regulatory and operational framework through which data is governed, ensuring that data is handled lawfully, securely, and in alignment with digital transformation priorities.

Within the Data Governance Framework, policies define what must be done, while standards define how it must be implemented. Together, they ensure uniformity in data practices, reduce ambiguity, and enable coordinated action across institutional boundaries.

The Data Governance Council, supported by Data Stewards and relevant technical and legal stakeholders, is responsible for establishing, approving, and periodically reviewing data policies to ensure they remain aligned with evolving legal requirements, operational needs, and technological developments.

Policies shall be aligned with national laws, including data protection, access to information, records management, and cybersecurity obligations, as well as with GEA standards and interoperability requirements. Where national-level policies exist, MCDAs shall adopt and operationalize them rather than develop divergent rules.

The policy framework aims to

- Establish clear and enforceable rules governing the use and management of data
- Ensure compliance with legal, regulatory, and architecture requirements
- Promote consistent practices across government institutions
- Safeguard privacy, confidentiality, and national interests
- Enable secure and responsible data sharing
- Support high data quality and reliability
- Maintain authoritative sources of critical data

Policy	Description
Data Quality Policy	Defines required quality levels for critical data elements and establishes measurement criteria (accuracy, completeness, consistency, and timeliness). It specifies processes for monitoring quality, reporting issues, and correcting errors at the source to ensure data remains fit for operational and analytical use.

Data Access & Sharing Policy	Defines how users request, approve, and manage access to datasets and how data may be shared within and across MCDAs. It aligns with the government information classification framework and ensures that access decisions are based on roles, legal mandates, and security considerations.
Data Usage Policy	Establishes rules governing the lawful, ethical, and appropriate use of government data. It ensures adherence to data protection principles, including purpose limitation, proportionality, and transparency, and prevents misuse or unauthorized exploitation of data.
Master Data Management (MDM) Policy	Defines governance for authoritative data entities, including processes for creation, validation, maintenance, version control, and retirement of master records. It ensures the integrity of core datasets and supports the "single source of truth" principle across government.

To ensure effective implementation, the following policy governance principles shall apply:

- **Alignment with National Frameworks:** Policies shall conform to national laws, GEA standards, and interoperability requirements.
- **Consistency Across Institutions:** Policies shall be harmonized to avoid conflicting rules between MCDAs.
- **Clarity and Accessibility:** Policies shall be clearly documented and communicated to all relevant stakeholders.
- **Periodic Review:** Policies shall be reviewed regularly to reflect changes in legislation, technology, or operational needs.
- **Enforceability:** Compliance shall be monitored through governance reviews, audits, and reporting mechanisms.

c) Data Management Processes and Controls

Effective Data Governance depends on well-defined processes and operational controls that translate governance intent into day-to-day practice. Data Management Processes and Controls establish the procedural mechanisms through which MCDAs implement policies, enforce rules, and ensure that data is managed consistently across its lifecycle.

Within GEA, these processes ensure that governance is operational enabling institutions to manage access, resolve issues, maintain transparency, and uphold accountability enabling MCDAs move from ad-hoc data handling toward disciplined management of data as a strategic asset, strengthening trust in government information and enabling seamless collaboration across agencies.

Process	Description
Data Access Request Workflow	Establishes a formal mechanism through which users request access to datasets process (e.g., using a ticketing system or request form). Requests are reviewed by the relevant Data Steward to ensure alignment with legal mandates, classification policies, and business need before the Data Custodian grants technical access. All approvals and actions are recorded to maintain auditability and accountability.
Data Issue Resolution Process	Provides a structured workflow for identifying, reporting, and resolving data quality or integrity issues (e.g. using an incident management process). Issues are logged, assessed, assigned to the appropriate Data Steward, and tracked through resolution, with corrective actions applied at the source to prevent recurrence.
Data Catalog	Requires each MCDA to maintain an up-to-date inventory of datasets, including descriptions, ownership, classification, lineage, and access procedures. The catalog promotes discoverability, supports governance oversight, and enables controlled sharing across government.

To ensure consistency and effectiveness, the following Operational Control principles shall guide implementation:

- Traceability: All data actions (including access approvals, changes, and issue resolutions) shall be recorded and auditable.
- Separation of Responsibilities: Approval, execution, and oversight roles shall remain distinct to prevent conflicts of interest.
- Lifecycle Awareness: Processes shall align with data lifecycle stages, from creation through archival and disposal.

- Integration with Governance: Processes shall support governance reviews, compliance monitoring, and reporting.
- Continuous Improvement: Feedback from operational processes shall inform policy updates and process refinement.

The data management processes shall integrate with the following Architecture and Compliance systems to provide workflows that support issue management, decision-making, enable traceability, and ensure that data activities are auditable and aligned with legal, security, and interoperability requirements.

- Metadata and catalog platforms to ensure visibility of data assets
- Identity and access management systems to enforce access decisions
- Data quality monitoring tools to detect and address issues proactively
- Architecture governance processes to ensure compliance with GEA standards
- Audit and risk management functions to support oversight

d) Data Cataloging and Marketplace

This is a foundational capability within the Data Governance Framework that provides the capability to systematically discover, govern, share, and reuse data assets across the Whole-of-Government ecosystem. It enables a structured environment through which data is made visible, accessible, and usable under controlled conditions, supporting interoperability, transparency, and innovation while safeguarding legal and security obligations.

They serve as the central mechanism for publishing data assets, managing access, and enabling collaboration across MCDAs, as well as with authorized external stakeholders.

The catalog provides authoritative visibility into government data holdings, while the marketplace enables controlled exchange and consumption of datasets, APIs, and data services. Together, they reduce duplication, improve coordination, and support data-driven decision-making across government. The Data Catalog and Marketplace aim to:

- Provide a comprehensive view of government data assets
- Enable secure and governed access to datasets and APIs

- Promote reuse of existing data to reduce duplication and costs
- Support interoperability across institutions through standardized discovery mechanisms
- Facilitate collaboration with researchers, innovators, and partners
- Improve transparency and accountability in data management
- Generate insights into data demand and usage patterns

Below are the key components:

Component	Purpose
Enterprise Data Catalog (EDC):	Provides a centralized, searchable inventory of datasets, APIs, and data services across all MCDAs. It enables users to discover data assets, understand their meaning and classification, identify ownership, and request access through governed workflows.
Data Marketplace:	Serves as a controlled digital exchange environment where authorized users can access, share, and reuse datasets and APIs in accordance with legal, policy, and licensing requirements. It supports both internal government collaboration and approved external use cases.
Metadata Integration:	Ensures synchronization with the National Metadata Registry (NMR) so that all datasets maintain standardized definitions, lineage, classifications, and version history, supporting consistency and governance across the ecosystem.
Integration with GIP	Enables direct linkage between the catalog and data exchange infrastructure, allowing datasets and APIs to be accessed through secure integration channels, including real-time and batch data services.

Usage Analytics	Provides monitoring and reporting on dataset usage, demand trends, and access patterns to support governance oversight, inform policy decisions, and identify opportunities for optimization and increased reuse.

The Data Catalog and Marketplace provides a common discovery and exchange environment and establish a coherent national data ecosystem serving as the operational hub connecting:

- Data producers across MCDAs
- Data consumers within government
- Shared services and integration platforms
- Metadata governance structures
- Open data initiatives
- Analytics and policy functions

It shall operate under the following principles:

- Authoritative Registration: All critical datasets and APIs shall be registered and maintained within the catalog.
- Controlled Access: Access to data shall be governed by classification, legal mandates, and approved **use** cases.
- Transparency: Metadata shall be visible to promote discovery while protecting sensitive information.
- Interoperability: Catalog entries shall conform to national standards and integrate with shared platforms.
- Accountability: Data owners remain responsible for the accuracy, classification, and lifecycle of published datasets.
- Compliance: All exchanges shall comply with applicable laws, policies, and security requirements

e) Automated Data Discovery and Self-Service Access

Automated Data Discovery and Self-Service Access capabilities enable government to scale data governance while improving accessibility, efficiency, and transparency across the Whole-of-Government ecosystem. These capabilities ensure that data assets are continuously identified, classified, and governed, while providing authorized users with streamlined mechanisms to discover and request access to data in a secure and controlled manner.

Automation reduces reliance on manual processes, improves visibility into distributed data environments, and strengthens governance by embedding controls directly into discovery and access workflows. It supports the principle that data should be discoverable and usable by authorized users, while ensuring compliance with legal, privacy, and security requirements.

By combining automated discovery with governed self-service access, accelerated data sharing, reduce bottlenecks, and improve responsiveness to operational and analytical needs without compromising oversight. These capabilities aim to:

- Continuously identify and classify data assets across government environments
- Improve visibility into datasets and reduce hidden or unmanaged data repositories
- Enable timely and secure access to data for authorized users
- Reduce manual effort in cataloging and governance processes
- Strengthen compliance through automated controls and auditability
- Support innovation and data-driven decision-making
- Maintain alignment with data protection and security policies

Core Capabilities

1. Automated Discovery

Automated discovery mechanisms use intelligent scanning tools to monitor data repositories, platforms, and integration points to identify new or modified datasets. These tools enhance governance by ensuring that data assets are registered, classified, and evaluated as part of routine operations providing an up-to-date understanding of the government data landscape.

Key functions include:

- Periodic scanning of databases, file systems, APIs, and data platforms
- Automatic classification of datasets based on sensitivity and content
- Metadata enrichment, including source, structure, lineage, ownership, and quality indicators
- Detection of personal or sensitive data elements
- Validation workflows to ensure new datasets are reviewed before publication
- Synchronization with the Enterprise Data Catalog and National Metadata Registry

2. Self-Service Access Portals

Self-service portals provide a unified interface through which authorized users, including government staff, academia, researchers, and approved partners, can discover, preview, and request access to datasets and data services.

Key features include:

- Search and discovery across registered datasets and APIs
- Dataset previews and metadata visibility
- Automated access request workflows aligned with classification and governance policies
- Approval routing to Data Stewards and relevant authorities
- Integration with Identity and Access Management systems to enforce role-based access controls
- Audit logging of requests, approvals, and data usage activities
- Access to APIs, data services, and event streams through the Government Integration Platform for programmatic consumption

Automated discovery and self-service access shall operate under strict governance to ensure that increased accessibility does not introduce risk. Key controls include:

- Enforcement of data classification and access policies
- Continuous monitoring of access and usage patterns
- Alerts for unusual or unauthorized access activities

- Compliance with privacy and data protection requirements
- Periodic reviews of access permissions and usage
- Approval workflows for sensitive or restricted datasets

Automation strengthens governance by embedding safeguards into operational processes.

f) Key Performance Indicators (KPIs)

KPIs provide a structured mechanism for measuring the effectiveness, maturity, and impact of data governance across MCDAs by enabling leadership to assess whether data is being managed as a strategic asset, identify areas requiring improvement, and ensure accountability for governance outcomes.

KPIs serve as a critical feedback loop, linking governance policies and operational practices to measurable results. They support evidence-based oversight, facilitate continuous improvement, and provide visibility into the health of the government data ecosystem.

KPIs shall be monitored through automated dashboards and reporting mechanisms integrated with metadata registries, master data platforms, data quality tools, and governance workflows. Results should be reviewed regularly by governance bodies to inform decision-making, prioritize remediation actions, and track progress toward national data objectives.

The KPI framework aims to:

- Measure the effectiveness of data governance practices
- Monitor data quality and reliability across systems
- Assess compliance with policies and standards
- Identify risks and improvement opportunities
- Support performance reporting to leadership
- Promote accountability across institutions
- Track progress toward Whole-of-Government data maturity

KPIs are evaluated using automated data quality monitoring tools integrated into the metadata registry and master data systems. They include:

KPI / Metric	Definition	Measurement / Method	Target / Threshold
Authoritative Source Coverage	Proportion of critical national data entities (e.g., Citizen, Business, Land) with an established authoritative source.	Derived from metadata registry and master data coverage reports.	≥ 80% coverage of all defined critical entities within three years.
Data Quality Index (DQI)	Composite score measuring data accuracy, completeness, and timeliness.	Automatically computed through data quality dashboards and monitoring tools	≥ 95% for all authoritative datasets.
Data Accuracy	Percentage of data records that are correct and free from errors.	Random sampling, automated validation scripts, and reconciliation checks.	≥ 98%.
Data Completeness	Extent to which all required data fields are populated.	Automated profiling and completeness assessments.	≥ 97%.
Data Consistency	Degree to which data values are uniform across systems and sources.	Cross-system reconciliation and integrity checks.	≥ 95%.
Data Timeliness	Frequency of data refresh or update in line with defined SLAs.	System logs, refresh schedules, and timestamp audits.	≥ 90% compliance with SLA update frequency.
Data Accessibility	Percentage of datasets discoverable and accessible through approved governance processes.	Monitored via Metadata registry and catalog usage analytics.	≥ 90% discoverability of registered datasets.
Data Issue Resolution Rate	Percentage of reported data issues resolved within service levels	Governance workflow and ticketing system analytics.	≥ 95% resolution within SLA.

Data Reuse Rate	Measures the extent to which datasets are reused across systems, programs, or institutions rather than recreated or duplicated.	Analysis of catalog usage logs, API consumption records, and integration reports to track reuse across MCDAs.	Year-on-year increase in reuse of priority datasets.
Cross-Agency Data Exchanges	Tracks the volume and frequency of data sharing transactions between MCDAs through approved integration channels.	Monitoring transactions through the Government Integration Platform, API gateways, and data exchange logs.	Continuous growth in compliant cross-agency exchanges.
Service Delivery Improvements	Assesses improvements in service efficiency, responsiveness, or user experience attributable to better data availability and integration.	Service performance metrics such as processing time reductions, error rate reductions, and customer satisfaction indicators.	Measurable improvements in priority digital services.

Regular reporting ensures that governance remains proactive rather than reactive. KPI results shall be used to:

- Inform governance reviews and performance discussions
- Identify systemic weaknesses in data management
- Prioritize improvement initiatives
- Support audit and compliance activities
- Guide resource allocation and capacity building
- Demonstrate progress toward national digital transformation goals

MCDAs shall maintain dashboards that provide visibility into key data governance metrics with the reported periodically to data governance bodies and aligned with institutional performance management frameworks. Where performance falls below agreed thresholds, corrective actions shall be initiated, including process improvements, policy reviews, or targeted interventions.

g) Data Quality Monitoring

Data Quality Monitoring provides the continuous oversight mechanisms required to ensure that government data remains accurate, complete, consistent, timely, and fit for purpose across its lifecycle. It operationalizes the defined KPI (*see previous section*) by embedding automated controls and monitoring capabilities within data environments, enabling proactive detection and remediation of quality issues.

Data Quality Monitoring ensures that data governance is sustained through ongoing measurement rather than periodic review, supporting the principle that trusted data is essential for effective service delivery, sound policy decisions, regulatory compliance, and public confidence.

To achieve this, GEA recommends the implementation of an Automated Data Quality Monitoring Framework integrated with the National Metadata Registry, Master Data systems, and MCDA operational platforms. This framework enables continuous visibility into data health across the Whole-of-Government ecosystem.

The Data Quality Monitoring capability aims to:

- Continuously assess the reliability and fitness of government data
- Detect and resolve data issues early to prevent downstream impacts
- Support accountability for data quality across institutions
- Enable evidence-based governance and performance management
- Strengthen interoperability by ensuring consistency across systems
- Provide assurance to leadership on the integrity of critical datasets

Key Capabilities

1. **Real-Time Data Profiling**: Continuous scanning of datasets to identify anomalies, missing values, duplicates, and deviations from defined quality rules, enabling early detection of issues.
2. **Quality Dashboards**: Centralized dashboards that visualize Data Quality Index scores, trends, and compliance across domains, providing governance bodies and Data Stewards with actionable insights.

3. **Alerting and Notification**: Automated alerts triggered when quality thresholds are breached, enabling timely intervention by responsible stakeholders.
4. **AI-Based Anomaly Detection**: Advanced analytics to identify unusual patterns or emerging risks that may indicate data integrity issues, supporting proactive remediation.
5. **Data Lineage Tracking**: End-to-end visibility into data origins, transformations, and usage to support traceability, root cause analysis, and auditability.

Data Quality Monitoring shall integrate with:

- Metadata and catalog systems to maintain consistent definitions
- Master Data Management platforms to enforce authoritative sources
- Data governance workflows to trigger issue resolution processes
- Identity and access controls to protect sensitive datasets
- Reporting mechanisms to inform leadership and oversight bodies

By embedding measurable KPIs and automated quality monitoring within the governance framework, MCDAs can continuously assess data reliability, enforce accountability, and improve information quality across systems through data-driven oversight ensures that all MCDAs operate from trusted, standardized, and interoperable datasets strengthening evidence-based decision-making a key enabler of a resilient Whole-of-Government digital ecosystem.

GEA DATA ARCHIVAL POLICY

Kenya's digital transformation has significantly increased the volume of data and records across the government ecosystem. While retention schedules address time-bound storage obligations for privacy and compliance, the Government currently lacks a comprehensive Data Archival Policy that ensures the long-term preservation of public records of enduring legal, administrative, fiscal, cultural, and historical value.

It is acknowledged that additional archival and records management policies are currently under development within MICDE and may, upon approval, supersede or refine elements of this policy. However, such policies will be integrated into the GEA framework as the authoritative policies and standards, ensuring alignment with Whole-of-Government interoperability requirements, shared platforms, and national governance mechanisms.

Accordingly, this policy establishes the foundational architectural and governance controls required immediately, while remaining adaptable to future statutory or policy enhancements.

Archival Policy Objectives

The Data Archival Policy ensures that:

- Government records of enduring value remain authentic, accessible, and intelligible over time
- Maintain evidentiary integrity, authenticity, and chain of custody for legal and audit purposes
- Digital heritage and institutional memory are preserved
- Archived data remains protected, governed, and searchable
- Reduce operational risk arising from system retirement and vendor exit

Data retention determines when data stops being operational while the archival policy determines whether the State remembers or forgets.

ARCHIVAL PRINCIPLES

The archival principles below establish the mandatory foundation for preserving government information of enduring value in a manner that remains lawful, secure, accessible, and usable over time. These principles ensure that archiving is executed consistently across all MCDAs and platforms, safeguarding evidentiary integrity, supporting accountability, and preventing loss of institutional memory as technologies and systems evolve.

1. **Archival by Design** - Archival requirements must be defined during data and application design (ADM Phases C2 and D).
2. **Separation of Active and Archival Data** - Archived data must be logically and physically separated from operational systems.
3. **Format Sustainability** - Archived data must use open, non-proprietary, and preservation-ready formats.
4. **Legal and Evidentiary Integrity** - Archived records must retain evidentiary value, authenticity, and chain of custody.

5. **Controlled Access** - Archived data is not public by default; access is governed by law and policy.
6. **Technology Independence** - Archival data must remain usable independent of specific vendors or platforms.

DATA ARCHIVAL LIFECYCLE

The Data Archival Lifecycle defines the standardized end-to-end process through which government records move from active operational use to long-term preservation. It ensures that archival decisions are consistent, auditable, and legally defensible, while maintaining security, metadata integrity, and controlled access through identification, transfer, preservation, and retrieval.

Stage	Description	Governance Control
Identification	Identify data eligible for archiving based on value, law, and policy	Data Owner / Archivist
Appraisal	Assess archival value (legal, fiscal, historical, cultural)	National Archives + Data Authority
Transfer	Secure transfer from operational system to archival environment	ARB + Security Authority
Preservation	Long-term storage, format normalization, integrity checks	National Archives
Access & Use	Controlled retrieval for legal, audit, and research purposes	Legal + Data Governance
Review / Declassification	Periodic review for access, declassification, or disposal	Archives Authority

Archival Data Categories

Archived data shall be classified as:

1. **Permanent Archives:** Acts, regulations, cabinet decisions, National registries and foundational records, historical datasets of national significance

2. **Long-Term Archives (10–50 years):** Financial, land, procurement, personnel, judicial records
3. **Event-Based Archives:** Records remained until a legal or administrative event concludes
4. **Restricted Archives:** Sensitive, classified, or personal data requiring special controls

Archival Formats

The approved archival formats below establish mandatory requirements for structured data, documents, and multimedia records, ensuring that archived information remains readable, verifiable, and usable throughout its preservation lifecycle.

Category	Supported Formats
Structured Data	• CSV (RFC 4180) • XML (W3C compliant) • JSON (UTF-8 encoded) • RDF / OWL (for semantic datasets)
Unstructured and Document Records	• PDF/A-1, PDF/A-2, PDF/A-3 (archival PDF standards) • ODF (OpenDocument Format)
Multimedia	• Images: TIFF, PNG • Audio: WAV • Video: MP4 (H.264/H.265)
Metadata	• Descriptive metadata (title, creator, subject) • Structural metadata (relationships, versions) • Administrative metadata (ownership, rights) • Preservation metadata (checksums, format history)

Legal and Regulatory Alignment

The Data Archival Policy is grounded in Kenya's constitutional, statutory, and regulatory obligations governing public records preservation, accountability, privacy, access to information, and evidentiary integrity. This section clarifies the legal basis that mandates archiving as a Whole-of-Government requirement, while ensuring that preservation practices remain compliant with data protection, security, and lawful access controls.:

Legal Instrument	Archival Obligation
Constitution of Kenya (2010)	Accountability, transparency, access to information
Public Archives and Documentation Service Act	Custody and preservation of public records
Data Protection Act (2019)	Lawful processing, storage limitation, safeguards
Access to Information Act (2016)	Controlled public access to records
Public Finance Management Act	Preservation of financial and audit records
Evidence Act	Integrity and admissibility of records
Cybercrimes and Computer Misuse Act	Protection against tampering and loss

Roles and Responsibilities

The policy establishes clear custodianship, accountability, and operational responsibilities across government to ensure archival records are preserved with integrity, completeness, and lawful access controls.

Role	Primary Accountability	Key Responsibilities (Summary)
MCDA Data Owner	Business and legal accountability for records	Identify archival candidates, approve transfer, ensure completeness and continuity, confirm alignment to statutory obligations.
Data Steward (MCDA	Operational data quality and metadata integrity	Validate data quality, ensure metadata completeness, package records in approved archival formats, maintain transfer registers, support retrieval and audit requests.
National Archives / Custodial Authority	Long-term custody and preservation	Appraise archival value, preserve records permanently/long-term, manage format migration and integrity checks, provide controlled access and retrieval services.
GEA Authority / Architecture Review Board (ARB)	Architectural compliance and enforcement	Enforce archival standards in solution design and decommissioning, approve archival readiness,

Role	Primary Accountability	Key Responsibilities (Summary)
		embed archival requirements into procurement and governance gates.
Security & Data Protection Authorities	Privacy, confidentiality, and managed risk	Apply classification and access controls, enforce encryption and audit trails, validate lawful processing and safeguards for archived data.
Audit & Oversight Institutions	Independent assurance and compliance	Audit archival compliance, validate chain of custody and admissibility, require corrective action for gaps or non-compliance.

Enforcement and Compliance

Compliance is enforceable through governance, procurement controls, funding gates, and audit mechanisms. Archiving shall not be treated as an optional records management activity; it is a national obligation for accountability, evidentiary integrity, continuity of government, and long-term preservation of public records.

All MCDAs and national platforms shall comply with the following minimum requirements:

- **Archival Readiness by Design**: Every new or modernized system must define archival requirements during solution design, including archival triggers, required metadata, approved formats, access restrictions, and preservation controls.
- **Archival Transfer Obligations:** Records identified as archival shall be transferred to the approved archival environment in accordance with defined processes and schedules.
- **Preservation Integrity**: Archived records must be stored with integrity controls including checksums, version management, and chain-of-custody logs to maintain authenticity and admissibility.
- **Format Compliance:** Records must be archived using approved open and sustainable formats. Where data originates in proprietary formats, a normalized archival copy must be created and preserved.

- **Metadata Completeness**: Archived content must include mandatory descriptive, structural, administrative, and preservation metadata to ensure long-term discoverability and usability.
- **Controlled Access**: Archived records must remain governed by classification, privacy, and access control policies, with audit trails for all retrieval and access events.

Auditing, Monitoring, and Reporting

Compliance shall be continuously monitored through operational dashboards and formal audits:

- **Compliance Dashboards:** Each MCDA shall maintain reporting on archival readiness, transfer progress, and preservation status for critical systems.
- **Periodic Compliance Audits:** Joint audits shall be conducted by the GEA Authority, National Archives, and relevant oversight bodies to verify:
  - Completeness of archived records
  - Metadata integrity
  - Preservation controls and access restrictions
  - Evidence of lawful disposal where applicable
- **Non-Compliance Reporting:** Failure to comply shall be formally recorded and escalated through governance mechanisms.

Evidence, Documentation, and Records of Compliance

Compliance shall be proven through mandatory documentation, including:

- Archival transfer registers and custody receipts
- Format validation and normalization records
- Metadata completeness checklists
- Integrity verification reports (e.g., checksum validation)
- Access and retrieval audit logs
- Disposal certificates for records approved for destruction

Policy Integration and Continuous Improvement

This policy shall be treated as a living governance instrument:

- The GEA Authority review and update archival standards periodically to reflect evolving technologies, risks, and regulatory requirements.
- Improvements shall be implemented through formal architecture change governance processes to preserve consistency and prevent uncontrolled variation across MCDAs.

EXTERNAL DATA INTEGRATION POLICY

This policy establishes the mandatory framework governing how MCDAs acquire, ingest, validate, integrate, share, and manage data originating from external sources. It ensures that external data is handled in a manner that protects national interests, preserves data integrity, and supports effective service delivery and decision-making. External data ingestion is recognized as a controlled national capability and shall be conducted under formal governance oversight.

This policy applies to all external data ingested into MCDA systems and platforms, including both batch and real-time data flows, including

- Private sector data (financial institutions, telecommunications, utilities, insurers, logistics providers)
- Public-private partnership and outsourced service data
- Development partner and donor datasets
- Cross-border and regional data exchanges
- Commercial or licensed datasets

MCDAs as data owners shall ensure that external data ingestion:

- Is legally compliant and explicitly licensed for intended use
- Does not compromise data privacy, national security, or sovereignty
- Improves service delivery outcomes and decision-making integrity
- Maintains data quality and reduces contamination of authoritative government datasets
- Enables controlled reuse of external data across MCDAs, where permitted
- Provides a full audit trail from source to consumption (“lineage”)

Core Governance Rules

1. **No External Data Without Legal Basis** - External data shall not be ingested without a documented legal basis, consent (where required), and licensing terms permitting intended processing.
2. **Staging Before Production** - All external datasets must first enter an ingestion staging zone and shall not be directly injected into operational systems or master data stores.
3. **Quality Controls Before Use -** External data must pass mandatory quality, integrity, and validation checks prior to operational use.
4. **External Data Never Becomes Authoritative by Default -** Authoritative government registries remain the primary sources of truth unless governance explicitly approves external augmentation.
5. **Security and Privacy by Design –** Classification encryption, access control, and audit logging are mandatory for all ingestion pipelines.
6. **Metadata and Lineage Are Mandatory -** No data may enter analytics or operational usage without full metadata and lineage capture.

External Data Ingestion Architecture

The External Data Ingestion Architecture defines the authoritative Whole-of-Government pattern through which MCDAs acquire, onboard, validate, and prepare data originating outside government-controlled environments. It establishes a controlled “trust pipeline” that ensures external data is governed, secure, and semantically aligned before it is made available for operational or analytical use.

This architecture operates in close alignment with the Government Integration Platform (GIP). The ingestion pipeline is responsible for establishing trust, quality, and governance over external data, while the GIP serves as the mandatory enterprise platform for publishing, exchanging, and orchestrating approved data services across MCDAs. This separation ensures that onboarding and trust establishment functions do not duplicate enterprise integration capabilities.

External data shall enter government environments only through this controlled pipeline, ensuring that data is verified, traceable, and compliant with legal, security, and architecture requirements before being exposed through GIP to consuming systems.

This architectural design feature prevents the most common risks associated with external data integration, including:

- direct injection of external data into production systems without validation,
- ingestion of data with unclear licensing or unlawful processing basis,
- contamination of authoritative government data domains with poor-quality or inconsistent records.
- inability to trace data lineage for audit, legal disputes, or service accountability,
- security breaches arising from unmanaged data channels.

External data shall not be written directly into authoritative registries, operational databases, or shared government data domains without passing through the full ingestion lifecycle staging, validation, governance approval, and controlled integration. *Figure 13* below shows how the lifecycle will flow

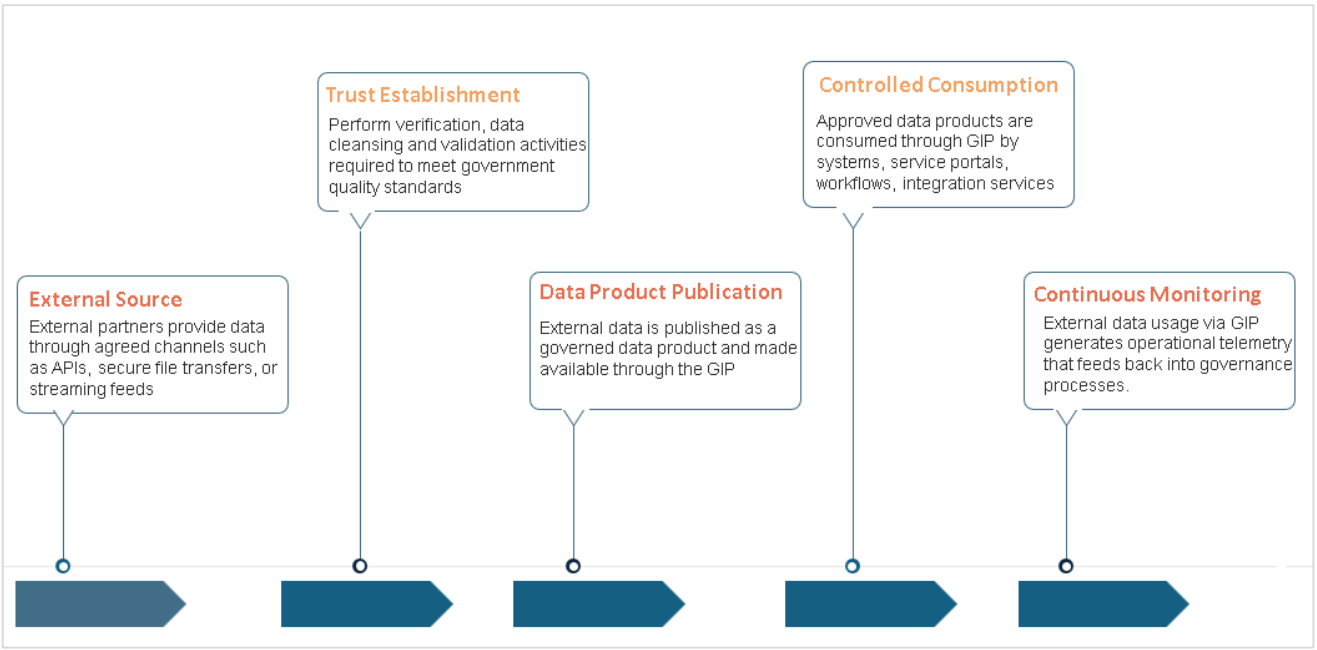

Figure 13 - Data Ingestion Lifecycle

The External Data Ingestion Architecture and the GIP operate together as complementary capabilities with different clearly defined roles while the governance remains centralized within GEA as shown in the table below.

External Data Ingestion Architecture	Government Integration Platform (GIP)
• Data onboarding and validation • Quality assurance and transformation • Semantic alignment with Data Reference Model • Risk assessment and governance approval • Creation of approved data products • Preservation of lineage and evidence	• Enterprise service exposure • Integration mediation and routing • Identity and access enforcement • Traffic management and reliability • Interoperability across institutions • Operational monitoring

The ingestion architecture (shown in *Figure 14* below) establishes trust, governance, and semantic readiness of external data, while GIP provides the enterprise backbone for secure exchange, orchestration, and controlled consumption across the WoG ecosystem.

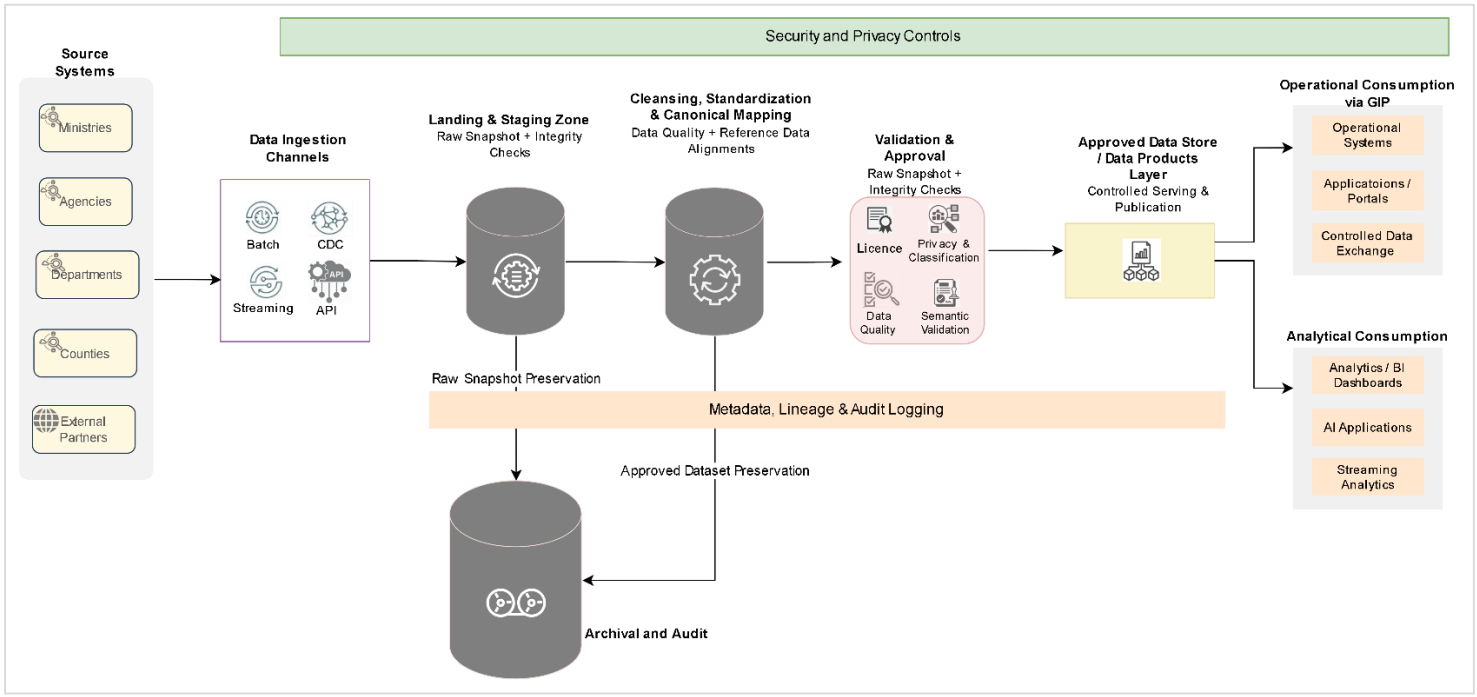

Figure 14 - External Data Ingestion Architecture

Ingestion Architecture Layer	Description
Systems (External Parties)	Represent the origin of data and include private sector partners, PPP operators, cross-border entities, development partners, and open data providers. These sources exist outside government control and are treated as untrusted until validated. Data may be delivered through APIs, secure transfers, partner platforms, or event streams. All sources must be uniquely identified, contractually governed, and registered before integration. Typical sources include: • Financial institutions and payment providers • Telecommunications and digital service providers • Utilities and regulated service operators • PPP and outsourced delivery platforms • Regional and international data exchanges • Commercial data vendors • Academic and open data repositories External connections terminate at the ingestion layer. Ongoing operational exchanges occur through GIP.
Landing and Staging Zone	Mandatory entry point where external data is received in isolation for quarantine and inspection. Its purpose is to prevent premature exposure of government systems to unverified data. Core functions include: • Secure receipt and containment of incoming datasets • Preservation of immutable “as-received” snapshots • Logging of ingestion events for traceability • Early detection of integrity or security risks No downstream consumption is permitted at this stage. Data proceeds only after initial checks.
Cleansing and Standardization Zone	This layer transforms raw data into a form aligned with government standards and canonical models defined by the Data Reference Model. Activities include: • Format and field standardization • Deduplication and validation checks • Reference data alignment • Semantic mapping to canonical entities

Ingestion Architecture Layer	Description
	• Identification of sensitive data elements • Preparation of masking or tokenization where required Outputs include versioned datasets, transformation logs, and quality metrics. This layer ensures data is structurally and semantically consistent before governance review.
Validation and Approval	This zone serves as the formal governance checkpoint where data is assessed for lawful use, quality, and readiness. Controls include: • Legal and licensing verification • Privacy and classification assessment • Data quality threshold evaluation • Semantic conformance validation • Stewardship and security approvals Approval outcomes determine whether data may be used, restricted, or rejected. Only approved datasets may proceed to publication.
Approved Data Product Layer (Published via GIP)	Once approved, external data is packaged as governed data products. These products are not exposed directly to consumers; instead, they are published through the GIP, which provides enterprise-level mediation, access control, and exchange capabilities. GIP functions include: • API and service publication • Access enforcement and authentication • Traffic management and monitoring • Cross-agency exchange • Event streaming and orchestration • Operational systems, portals, and integration services consume external data exclusively through GIP, ensuring consistency and centralized oversight. Analytical platforms may access curated datasets directly under governed conditions, while operational interactions remain mediated by GIP.
Archive and Audit Zone	Preserves evidence required to demonstrate lawful and controlled use of external data. It supports long-term accountability, audit readiness, and dispute resolution.

Ingestion Architecture Layer	Description
	• Preserved artefacts include: • Raw and processed dataset versions • Metadata and lineage records • Approval and validation documentation • Licensing and contractual evidence • Access and usage logs Retention aligns with the archival policy and legal obligations.
Cross-Cutting Controls	Throughout all layers, the following apply: • Security and privacy safeguards • Metadata and lineage capture • Monitoring and audit logging • Compliance with governance policies • Alignment with GEA standards

Roles and Responsibilities

Clear accountability is maintained across governance and operational functions:

- Data Owner defines purpose and approves use cases
- Data Steward validates quality and semantic alignment
- Integration Owner ensures alignment with GIP and interoperability standards
- Security and Privacy Authorities approve safeguards
- Legal and Procurement validate licensing
- Architecture Review Board (ARB) enforces compliance

Performance Monitoring

Each external ingestion must report the following KPIs:

- Data Quality Score (completeness, accuracy, consistency)
- License Compliance Status (pass/fail)
- Ingestion Success Rate
- Time-to-Availability

- Number of consuming services
- Incidents related to ingestion (privacy breaches, mismatches)

Enforcement and Non-Compliance

Compliance with the ingestion pipeline and GIP alignment is mandatory. External data shall not be integrated into operational environments without completing staging, validation, approval, and publication through GIP.

Non-compliance may trigger governance escalation, suspension of integration activities, or corrective action.

APPLICATION ARCHITECTURE

Application Architecture domain defines the principles, models, and standards for the design, implementation, integration, operation, and lifecycle management of application systems across all MCDAs. It provides the principles, models, and standards necessary to guide the design, acquisition, and lifecycle management of all government systems, ensuring they are interoperable, secure, resilient, and cost-effective and aligned with Whole-of-Government objectives.

The primary goal is to shift from siloed, duplicative systems to a rationalized application portfolio that leverages shared platforms and services and promotes reuse across government to efficiently support MCDA business functions and enable coordinated service delivery.

The Application Architecture domain is critical in addressing pertinent challenges faced by MCDAs, such as system redundancy, poor integration, and fragmented user experiences through guidance in the development of scalable, interoperable, and reusable applications that promote consistency, reliability, and cost efficiency.

The outcomes enable citizens and businesses to enjoy a seamless, secure, and unified digital experience through an agile, interoperable, and sustainable portfolio of applications, anchored by common platforms and shared services and supported by standardized integration mechanisms.

APPLICATION ARCHITECTURE PRINCIPLES

The Application Architecture is guided by principles that ensure consistency, interoperability, and long-term sustainability. These principles, derived from the GEA principles, are adapted specifically for the application domain and are intended to guide decision-making across planning, procurement, development, and operations.

Principle	Explanation
Reuse before Buy, Buy before Build	MCDAs should first seek to reuse existing applications or shared services and only if a suitable solution is not available is preference given to acquiring a solution from the market over

	custom development. Justification should be documented where reuse is not feasible.
Shared Platforms First	Core functions common to multiple MCDAs (e.g., identity verification, payments, notifications) must be consumed from designated central platforms like e-Citizen or Huduma Namba, rather than being re-developed.
API-Led Interoperability	All new applications must expose business functions and data through secure, well-documented APIs. Systems should be designed to communicate and share data seamlessly, breaking down information silos.
Technology Independence	Applications should be designed to be loosely coupled with underlying technology infrastructure, using open standards and modular approaches (including containerization where appropriate) to reduce vendor lock-in and improve portability.
Mobile-First Experience	All citizen-facing applications must be designed with a mobile-first approach, ensuring they are accessible, responsive, and provide optimal user experience on mobile devices.
Security by Design	Security and privacy considerations must be integrated into every stage of the application lifecycle, from design and development to deployment and decommissioning, adhering to a DevSecOps approach.
User-Centric Design	Applications should be intuitive, accessible, and designed to meet the needs of their target users, including citizens, government employees, and other stakeholders, with attention to usability and inclusive access.

APPLICATION REFERENCE MODEL

Application Reference Model (ARM) serves as a critical part of the GEA Reference Model component, providing a structured foundation for automating government services that are identified as identified through the Business Reference Model (BRM). By aligning application capabilities with business functions, ARM enables MCDAs to deliver efficient, citizen-centric services, support coordinated service delivery, and enhance collaboration and information exchange across institutional boundaries.

The Application Reference Model diagram in *Figure 15* below illustrates how government applications are structured, integrated, and governed within the broader WoG architecture. It shows the relationships between users, applications, interoperability mechanisms, and supporting reference models that collectively enable the delivery of secure and interoperable digital public services.

The model should be interpreted as a layered architecture that ensures applications are designed, implemented, and operated in a consistent and governed manner across all MCDAs.

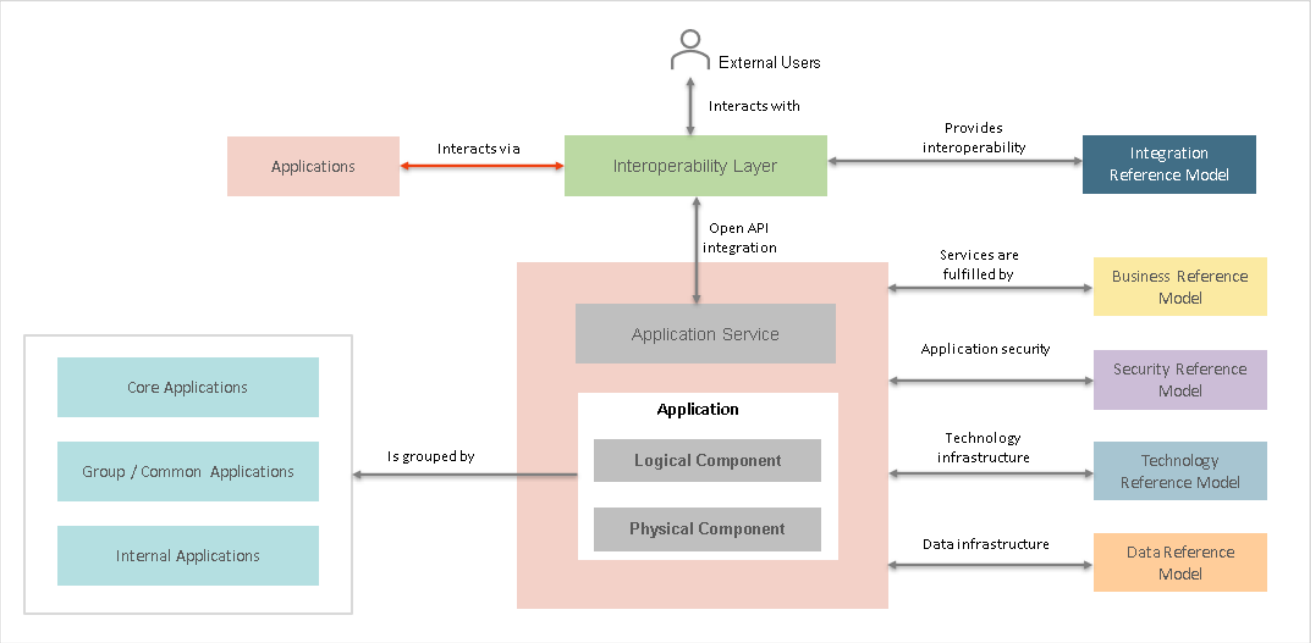

Figure 15 - Application Reference Model

External Users	Includes citizens, businesses, government employees, and partner organizations who interact with government digital services through applications that expose services via secure digital channels. This interaction represents the service consumption layer where government services are delivered and accessed.
Interoperability Layer	Acts as the central mechanism that enables secure communication, data exchange, and service orchestration across government systems. It

	operationalizes interoperability policies and enables coordinated service delivery across institutional boundaries. It provides: • Standardized API mediation • Service routing and orchestration • Secure data exchange • Protocol transformation • Controlled exposure of services Applications interact through this layer rather than through direct system-to-system connections, ensuring consistency, security, and governance of integrations.
Applications and Application Services	Applications implement business capabilities and deliver digital services. Each application exposes its functionality through application services, which represent the operational capabilities made available to users and other systems. The ARM highlights how applications: • Consume shared services • Provide reusable services • Integrate through standardized interfaces • Support business processes defined in the Business Reference Model Application services form the bridge between business needs and technical implementation.
Application Structure (Logical and Physical Components)	Each application is composed of: 1. **Logical Components** define how the application is structured conceptually. These represent functional modules such as: • Business logic • Workflow processing • Service interfaces • Integration components

	2. Physical Components define how the application is implemented and operated. These represent deployed artifacts such as: • Application servers • Containers • Databases • Runtime environments
Application Categorization	Applications are grouped into categories - Core, Common/Group, and Department-Specific, to reflect their scope of use and governance expectations. This helps MCDAs understand which systems are shared assets versus agency-specific solutions. This classification supports: • Portfolio rationalization • Reuse • Standardization • Investment prioritization

CATEGORIZATION OF ENTERPRISE APPLICATIONS

Within the government ecosystem, many business processes and supporting systems are either common across multiple departments or unique to specific agencies. ARM facilitates systematic identification and classification of systems as Core, Common/Group, and Department-Specific applications.

The reference table below provides a structured classification system to guide the standardization, procurement, development, and deployment of software applications across government entities. The classification supports enterprise alignment, interoperability, cost-efficiency, and scalable reuse across the government application portfolio.

Category	Application Type	Description	Examples
Core Applications	Enterprise-wide, foundational applications	Used across all MCDAs for government-wide functions. Mandatory compliance and integration.	eCitizen, Huduma Platform eGP Portal, IFMIS, etc.
Common / Group Applications	Shared across sector-specific departments or related entities	Support functions common to a group of departments within a sector (e.g., health, education).	NEMIS, SHA, HRMIS, G-Pay, Document Mgmt.
Department-Specific (Internal) Applications	Tailored to individual MCDA mandates	Serve unique requirements of a single department or agency. Subject to architectural compliance.	Land Registry System, iTax, etc.

To ensure seamless interoperability and data consistency, the Government ICT Standards and GIF (application interoperability) define and enforce a set of standards, integration protocols, and compliance guidelines through the available regulatory frameworks. These directives are binding across all MCDAs and must be adhered to during the design, procurement, and development of applications.

The ARM facilitates this by offering a structured methodology to:

- Group applications by their type (e.g., Core, Common, Department-Specific) and capabilities (e.g., transactional, analytical, integration-oriented).
- Categorize applications based on strategic parameters such as priority, service alignment, compliance requirements, and deployment criticality.
- Align applications with business services defined in the Business Reference Model (BRM) to ensure that automation initiatives are tightly coupled with actual service delivery needs.

ARM also incorporates deployment guidance by capturing essential application deployment parameters such as hosting environment, delivery model (on-premises, cloud, hybrid), scalability requirements, and interoperability constraints. These deployment insights are

integrated with the Technology Reference Model, enabling the design of a cohesive and scalable Technology Architecture that supports application execution.

APPLICATION PORTFOLIO CATALOG (APC)

APC is the definitive, government-wide inventory of all software applications. Each application is cataloged and mapped to the business capabilities it supports (from the Business Capability Model), the organizational units that own it, and its underlying technology.

This application catalog is the primary tool for identifying redundancy and assessing the application landscape to gain a clear view of what exists, where gaps are, and where consolidation or modernization is required. A template for the APC is provided in the GEA Adoption and Implementation Guide.

While the ARM encourages the reuse and sharing of standardized applications, it also provides sufficient flexibility-controlled flexibility for individual MCDAs to acquire or develop applications tailored to their specific operational needs, provided such initiatives conform to the overarching architectural standards and governance frameworks defined in the GEA and GIF.

APPLICATION ARCHITECTURE STANDARDS

Enterprise Application Architecture must ensure interoperability of all the applications within the MCDA along with seamless upgrade migration and addition of new applications to the system. The Enterprise Application Architecture must adhere to:

- Government Interoperability Framework (GIF)
- ICTA - Systems and Applications Standard

ALIGNING GEA STRATEGY WITH ARTIFICIAL INTELLIGENCE (AI)

Artificial Intelligence (AI) has shifted from an emerging technology to a core strategic enabler of modern public administration. Globally, advanced governments are transitioning into Agentic States governments that deploy AI not only for automation, but for autonomous reasoning, proactive service delivery, and continuous public-sector optimization.

Within the Kenyan context, AI represents a major opportunity to modernize the public service, especially when architected within the Government Enterprise Architecture (GEA) and implemented through the Government Interoperability Framework (GIF). AI can:

- Improve the efficiency and quality of public services
- Enable proactive, citizen-centric experiences
- Enhance decision intelligence for policy and operational management
- Strengthen transparency, accountability, and trust
- Automate regulatory and administrative processes
- Strengthen GovTech capabilities and productivity across the public sector

GEA establishes a national, architecture-aligned approach for integrating AI across MCDAs, ensuring AI investments remain secure, ethical, interoperable, scalable, and aligned with national development priorities.

Benefits of AI Adoption

a) Enhanced Citizen Experience

AI enables the government to deliver more responsive, personalised and accessible public services through AI powered tools like chatbots and virtual assistants that can provide enabling conversational service assistants, context-aware routing and case resolution, personalized public service recommendations and 24/7 multilingual digital front offices

b) Improved Efficiency and Reduced Costs

AI drives automation of routine administrative tasks such as forms processing, claims validation and internal document handling, significantly reducing operational bottlenecks. AI enabled workflows can be mapped against existing service architectures to streamline processes and reduce redundancies resulting in faster service delivery at lower costs.

c) Data Driven Decision Making

AI excels in extracting insights from large and complex datasets; AI models can analyse trends in the utilization of public services, identify underserved populations and flag anomalies or inefficiencies in delivery among other use cases. GEA provides the structure

to ensure that such AI driven insights are fed into strategic processes, system design and cross departmental coordination, supporting more informed and effective decision making.

d) Increased Transparency and Accountability

AI-based systems enhance transparency in how decisions are made, and services are delivered. Automated audit trails, anomaly detection, risk scoring of irregular transactions, flag bias, and ensure fairer access to services. Within EA, AI governance mechanisms such as policies on data ethics, model transparency, and system interoperability, can be integrated into the architecture to support accountability, compliance, and public trust.

e) Improved Interoperability Across Government Services

AI can play a critical role in breaking down data and operational silos across government departments by analyzing and linking fragmented information systems. This unlocks Citizen 360 and Business 360 views enabling more integrated and coordinated public services

AI supports interoperability by automating data harmonization, identifying redundancies, and facilitating seamless information exchange between MCDAs resulting in a more unified, efficient, and citizen-centric public service ecosystem.

AI ADOPTION IN PUBLIC ADMINISTRATION

Frameworks such as The Agentic State framework identify 10 functional layers of government which can be revamped using AI including:

- Public Service Delivery - virtual agents, omni-channel assistants
- Back-Office Operations - automated workflows, document processing
- Case Handling & Adjudication - decision support, priority scoring
- Regulatory Compliance - algorithmic monitoring, anomaly detection
- Policy Intelligence - simulation, forecasting, modelling
- Procurement - automated evaluation, risk analysis
- Finance & Public Expenditure - fraud analytics, predictive allocation
- HR & Talent Management - competence matching, career pathways
- Citizen Engagement - 24/7 conversational interfaces, behaviour insight
- National Security & Resilience - threat detection, misinformation control

These capabilities require well-governed, interoperable, scalable AI architecture, not isolated pilots or departmental deployments.

Challenges Facing AI Adoption within GEA Framework

Challenge Area	Description
Skills Gap	Shortage of applied AI engineers, ML ops, data scientists, and AI governance experts.
Regulatory Gaps	Kenya lacks a comprehensive AI Act; unclear obligations for algorithms, fairness, and governance.
Data Quality & Availability	Fragmented, siloed MCDA datasets; inconsistent metadata; lack of semantic standards.
Security & Privacy Risks	Model poisoning, prompt injection, identity fraud, synthetic data misuse.
Integration Complexity	AI must work across legacy systems, varied APIs, and inconsistent data schemas.
Ethical Governance	Need for transparency, explainability, impact assessments, and accountability structures.
Infrastructure Demands	Requires scalable compute, robust storage, secure cloud environments, GPUs, accelerators.

AI can pose a lot of challenges when it comes to deriving a strategy that works for an MCDA organization. For example:

- How will AI be aligned with overall business architecture goals?
- How will AI be integrated with the rest of the enterprise without any risk of a siloed and isolated approach?
- How will AI resolve integration issues, such as compatibility issues, data inconsistencies, etc., or solve interoperability issues?
- How will AI ensure solution scalability and data governance?
- How does AI address the ethical concerns, biases, and security vulnerabilities in models?

Leveraging an enterprise architecture framework for AI implementations helps overcome these challenges by providing a structured, strategic, and holistic approach to integrating AI technologies into the overall organizational landscape.

GUIDE TO GEA/AI ALIGNMENT

Preparing for AI adoption in MCDAs using Enterprise Architecture (EA) requires a structured, top-down approach to align AI initiatives with strategic objectives, governance, technology infrastructure, and compliance requirements.

Below are steps to guide the alignment effectively.

	Step Activity	Description
1.	**Align AI Strategy with GEA Mission and Vision**	Link to Strategic Goals - Ensure AI supports national digital transformation, policy goals, and public sector values like transparency and equity Define Use Cases - Identify specific public service challenges AI can solve (e.g., fraud detection, citizen services automation, predictive maintenance).
2.	**Extend the Enterprise Architecture**	Introduce AI as a Capability: Model AI as a service or capability layer, defining how it interacts with data, processes, and applications. Create an AI Reference Architecture: Define standardized components such as ML pipelines, model registries, ethical review checkpoints, etc.
3	**Strengthen Data Architecture & Governance (DRM)**	Data Readiness: Ensure availability, quality, and accessibility of data. AI is only as good as the data it consumes. Metadata Management: Implement semantic standards and taxonomies for interoperability. Ethical & Legal Compliance: Build governance models for privacy (GDPR, local laws), bias mitigation, explainability, and accountability.
4.	**Establish Required Technology & Integration Infrastructure**	Cloud & Edge Enablement: Leverage cloud platforms for scalable AI workloads, with edge computing where latency or data residency is critical.

		AI Toolchain Integration: Integrate AI/ML platforms with existing enterprise systems via APIs, event-driven architectures, and service buses. Model Lifecycle Management: Plan for model development, testing, deployment, monitoring, and retirement within your EA.
5.	**Build Workforce & Organizational Capabilities**	Skills Gap Analysis: Use EA capability models to assess current vs. required skills in AI/ML, data science, and AI governance. Organizational Structures: Create roles such as Chief AI Officer, AI ethics boards, or AI centers of excellence.
6.	**Strengthen Security, Ethics, and Risk Controls**	Identify and mitigate potential risks associated with AI, such as security vulnerabilities, system failures, or unintended consequences of AI-generated content. Zero Trust Security: Integrate AI into the security architecture. Model Risk Management: Use EA to model AI-related risks such as data poisoning, adversarial attacks, or model drift and define mitigation controls. Auditability & Traceability: Create models that can be audited and decisions traced, essential for public accountability.
7.	**Align Procurement & Vendor Management**	Evaluate the total cost of ownership, including implementation, maintenance, and scalability costs associated with AI solutions. Standardized Procurement Guidelines: EA should guide consistent requirements for AI solutions across MCDAs. Interoperability Mandates: Use architecture principles to require open standards, APIs, and data portability in AI procurements.
8	**Monitor and Evolve AI Architecture**	Implement mechanisms for continuous monitoring, evaluation, and improvement of AI applications to maintain their effectiveness and relevance KPIs and Metrics: Track AI outcomes including efficiency, service quality, user satisfaction, and compliance.

		Continuous Architecture Evolution: EA teams must regularly update and train models as AI algorithms and regulations change.

AI has the potential to profoundly transform public service delivery if adopted strategically, responsibly, and within a coherent architectural framework. GEA provides the necessary foundation to ensure AI is:

- Aligned with national development priorities
- Ethical, transparent, and secure
- Interoperable and reusable across MCDAs
- Built on strong data and technology foundations
- Integrated into whole-of-government digital transformation

AI should not be viewed as a standalone domain, but as a cross-cutting capability embedded to strengthen the enterprise architecture within the digital government ecosystem**.** As AI becomes an important tool for digital enterprises, it introduces transformative capabilities such as automating repetitive tasks, improving decision-making through rapid data analysis, enhancing creativity in content generation, and providing valuable data insights. The ability of Gen AI to handle complex tasks and generate content makes it a valuable solution for optimizing processes and fostering innovation within MCDAs.

TECHNOLOGY ARCHITECTURE

Technology Architecture establishes the authoritative structural framework, standards, and operating model for the design, deployment, and management of the underlying ICT infrastructure required to support the development, deployment, and delivery of digital government services across the Whole-of-Government ecosystem.

It provides a consistent, interoperable, scalable, and secure national technology foundation that enables the integration and operation of enterprise applications, platforms, and data services across MCDAs and ensures seamless service delivery across institutional boundaries.

Technology Architecture acts as an enforceable blueprint and governance instrument within GEA to guide the design and implementation of technology components while ensuring mandatory alignment with national ICT strategies, the Government Interoperability Framework (GIF), the Government Integration Platform (GIP), and ongoing digital transformation initiatives.

OBJECTIVES

The primary objective of Technology Architecture is to establish a cohesive, secure, resilient, interoperable, and cost-efficient national technology environment that underpins digital transformation, supports integrated service delivery, and enables Whole-of-Government collaboration.

It enables efficient resource utilization, technology standardization, and innovation while ensuring operational continuity and compliance with security, interoperability, and data sovereignty requirements.

The table below outlines the key objectives.

Objective	Description
Design of Target Technology Architectures	Define standardized, modular reference architectures aligned with the GEA vision, WoG operating model and the Application Architecture domain, ensuring consistent and interoperable implementations across all MCDAs.

Define Architectural Building Blocks (ABBs)	Identify and describe the logical and physical components including infrastructure, platforms, and tools required to implement the enterprise's technology landscape including shared national platforms and GIP enablement components.
Support Architecture Documentation	Provide the necessary structure and content to develop comprehensive Architecture Definition Documents (ADDs) aligned with TOGAF ADM and government governance requirements.
Standardize Technology Components	Define and enforce open technical standards, specifications, and integration protocols to ensure uniform, secure, and interoperable technology deployments across the national ICT landscape.
Promote Use of Open-Source Technology	Drive adoption of open-source products and tools where they meet security, sustainability, and operational requirements, to reduce costs, enhance flexibility, and avoid vendor lock-in.
Map Stakeholder Concerns	Provide a systematic approach to align stakeholder needs (security, cost, performance, availability, interoperability, resilience) with appropriate technological configurations and architectural solutions.
Ensure Non-Functional Quality Attributes	Define measurable KPIs and performance benchmarks that ensure the deployed technology landscape meets critical enterprise attributes such as performance, reliability, scalability, maintainability, security, and availability.
Cloud Strategy Adoption	Formalize a 'cloud-first, cloud-smart' strategy, including clear guidelines for selecting public, private, or hybrid cloud models, addressing data residency and sovereignty concerns, and outlining secure migration and modernization paths for legacy workloads.
Emerging Technologies Roadmap	Develop a strategic roadmap and governance guidelines for the responsible adoption and integration of emerging technologies such as AI, IoT, and distributed ledger technologies guided by ethics, risk management, and sustainability principles.
Enable Shared Platforms and GIP Integration	Ensure that technology infrastructure supports national shared services, API-based integration, secure connectivity, and interoperability through the GIP

Technology Lifecycle Management	Establish policies and processes for technology lifecycle governance including acquisition, operation, modernization, and retirement to manage technical debt and ensure sustainability.
Operational Resilience and Continuity	Ensure national platforms are supported by disaster recovery, business continuity, high availability architecture, and operational monitoring capabilities.

PRINCIPLES OF TECHNOLOGY ARCHITECTURE

Principle	Description
Cloud Smart	Government will adopt a cloud-first approach for new initiatives and a cloud-smart approach for existing systems, selecting the appropriate cloud model (public, private, or hybrid) based on security, cost, and mission requirements.
Secure by Design	All infrastructure components must be designed, configured, and managed with security as a primary requirement from the outset, enforcing continuous monitoring, encryption, and vulnerability management.
Shared Infrastructure First	The use of centrally provided, shared infrastructure platforms (e.g., GoK Private Cloud, shared data centers) before procuring new, agency-specific hardware will be prioritized to optimize cost, promote reuse, and simplify management.
Open Standards and Vendor Neutrality	Technology Architecture will adopt open standards and technologies to prevent vendor lock-in, promote interoperability, and ensure long-term flexibility.
Automation and Orchestration	Infrastructure provisioning, configuration, and management will be automated using Infrastructure as Code (IaC) and orchestration tools to increase efficiency, improve reliability and compliance.
Data Sovereignty and Residency	Sensitive and personal data of Kenyan citizens and government operations will be stored and processed within the borders of Kenya, complying to national data residency and protection laws.
Resilience and Scalability	The technology infrastructure must be designed for fault tolerance, redundancy, and elastic scalability to support high service availability and continuity under variable demand.

Green ICT and Sustainability	Prioritize energy-efficient technologies, virtualization, and sustainable data center operations to minimize environmental impact
Interoperability by Default	All technology solutions must support integration through national interoperability platforms and standards to enable seamless data exchange across government.
Reuse Before Build	Existing shared platforms and capabilities must be reused before new infrastructure investments are approved.

TECHNOLOGY REFERENCE MODEL (TRM)

TRM provides the standardized technology stack and baseline architecture that guides the selection, deployment, integration, and management of technology capabilities across the government ecosystem

It defines the mandatory technology components required to support interoperable, secure, resilient, and scalable digital government services, provides alignment with GEA, GIF frameworks and national digital government priorities.

The TRM positions shared platforms, integration infrastructure, and common services as foundational capabilities to enable Whole-of-Government service delivery and cross-agency collaboration as shown in *Figure 16* below.

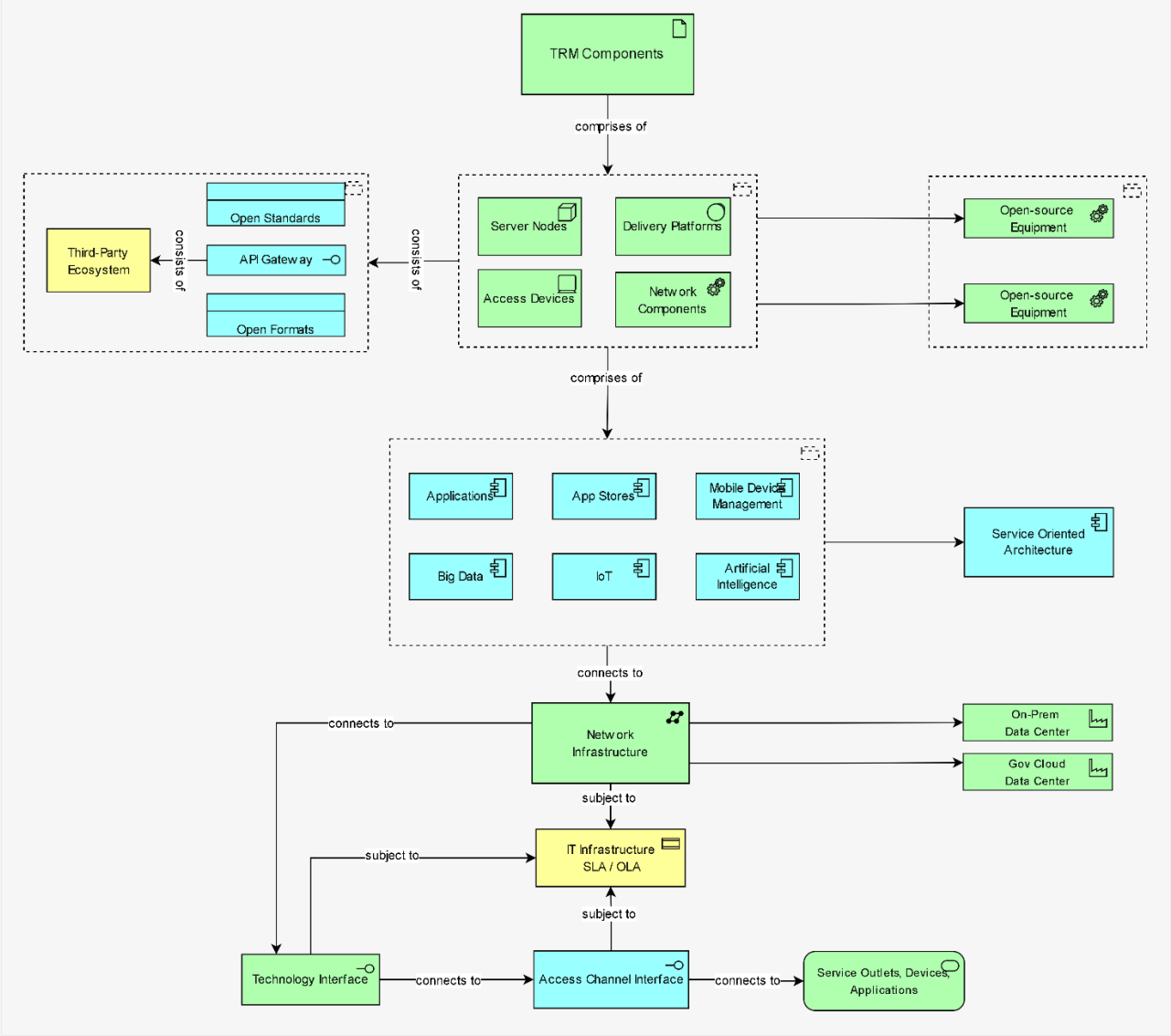

Figure 16 - Technology Reference Model

The core TRM components are described in the table below:

Stack	Component	Description
IT Infrastructure	Servers, storage systems, cloud and virtualization environments and backup/recovery solutions.	Provides compute, storage, hosting, and resilience capabilities for enterprise workloads across shared government platforms including the Government Cloud and data centers.

Applications Platforms & Middleware	Operating systems, databases, application servers, integration platforms (ESB, API gateways), and container orchestration frameworks (e.g., Kubernetes)	Supports interoperability, portability, and scalability of enterprise applications and enables standardized runtime and platform services.
Integration & Interoperability Layer	API management, service orchestration, message brokers, event streaming, service registry, and data exchange services aligned with the Government Integration Platform (GIP).	Enables secure, standardized data exchange and service integration across MCDAs and external ecosystems.
Security & Trust Services Layer	Identity and access management, authentication services, PKI, encryption services, security monitoring, vulnerability management, and threat detection.	Ensures confidentiality, integrity, availability, and trusted access to government systems and data.
Smart Devices & Edge Layer	End-user devices such as desktops, mobile devices, kiosks, and other edge computing.	Delivers services at the last mile and extends compute closer to data sources while supporting endpoint security and device management controls.
Communication & Network Layer	Network fabrics, broadband connectivity, VPNs, SD-WAN, messaging protocols, and IoT connectivity.	Ensures secure, high-speed, and reliable interconnectivity.
Service Delivery Channels Layer	Web portals, mobile applications, IVRs, SMS gateways, and emerging omnichannel interfaces (e.g., chatbots, voice assistants).	Provides citizens and businesses with accessible digital channels for services.
Data Platform Layer	Data storage platforms, analytics platforms, data integration pipelines, metadata services, and master data services.	Supports data-driven decision making, analytics, and trusted data sharing across government.
Operations & Management Layer	Monitoring, logging, observability platforms, configuration management, automation, and service management tooling.	Supports operational resilience, performance management, and continuous service improvement.

TRM mandates the adoption of approved open standards, protocols, and specifications (e.g., REST, JSON, OpenAPI Specification, OAuth 2.0, TLS, Kubernetes) to ensure interoperability, portability, security, and long-term sustainability across government systems.

All MCDAs shall comply with approved technology standards unless an approved exception is granted through the architecture governance process.

TRM serves as a foundational reference for technology planning, procurement, solution design, and operational management. It provides a common language and framework to ensure that technology decisions across MCDAs contribute to a cohesive national digital ecosystem.

By establishing clear technology layers and standards, the TRM enables interoperability, improves security posture, enhances operational efficiency, and supports scalable digital service delivery.

ARCHITECTURE AND DEPLOYMENT APPROACH

All digital services delivered through the Government Integration Platform (GIP and shared government platforms shall adhere to the following mandatory architectural principles to ensure interoperability, scalability, security, and operational resilience across the Whole-of-Government environment.

Architecture Principle	Description
Service Orientation	Services exposed internally or externally shall be implemented as API-first services using RESTful microservices, event-driven patterns, or service-oriented architectures aligned with GIF specifications and approved API standards.
Containerization and Virtualization	Applications shall be deployed using standardized container or virtualization platforms approved under the TRM to ensure portability, scalability, and consistent operations across government hosting environments.
Application Modernization	Legacy systems shall be progressively modernized through structured transformation programs including refactoring, re-platforming, or encapsulation using APIs to support integration with GIP and shared platforms.

Automated Infrastructure	Infrastructure provisioning, configuration, and compliance enforcement shall be automated using approved Infrastructure as Code approaches to ensure repeatability, auditability, and rapid recovery.
Integration by Default	All systems shall integrate through GIP or approved interoperability mechanisms to ensure consistent data exchange and service orchestration.
Security by Design	Security controls shall be embedded across design, development, deployment, and operations in accordance with national cybersecurity policies.

SERVICE MANAGEMENT AND MONITORING

All infrastructure components and services operate under shall operate under formally approved Service Level Agreements (SLAs), Operational Level Agreements (OLAs), and Technical Interoperability Agreements (TIAs) to guarantee availability, performance, security, and resilience.

The Management Infrastructure provides shall provide centralized operational oversight through integrated monitoring, observability platforms, security monitoring, and automated compliance validation mechanisms.

Real-time dashboards track critical KPIs such as:

- Service uptime ≥ 99.9%
- Average response time ≤ 200 ms
- Mean Time to Recovery < 4 hours
- Security compliance coverage ≥ 95%
- Integration availability via GIP ≥ defined national threshold
- Patch compliance ≥ defined baseline

Performance insights and audit metrics shall be shared with governance bodies to support oversight, accountability, and continuous improvement.

Technology Architecture shall continuously and iteratively address architectural risks, scalability requirements, interoperability obligations, security controls, and opportunities for

reuse of shared platforms to ensure sustainable and coordinated technology evolution across government guided by the TRM,

TECHNOLOGY ARCHITECTURE STANDARDS

Technology Reference Model establishes mandatory standards and approved technology baselines governing infrastructure, platforms, integration, data, security, and service delivery components across all MCDAs. These standards ensure secure, efficient, interoperable, and reliable service delivery across government cloud environments, national data centers, and citizen-facing digital platforms.

Adoption of open standards and open formats is mandatory to ensure interoperability, portability, and long-term sustainability of government technology investments. Exceptions shall be subject to formal architecture governance approval.

The Ministry of ICT and Digital Economy through the ICT Authority publishes shall publish and maintain authoritative standards and implementation guidance to ensure consistent adoption across government. These are periodically reviewed based on the evolvement of technology and the needs on the MCDA and the ecosystem stakeholders through the prescribed governance structures.

Some examples of these standards include:

Cloud Services	All public cloud services must be procured from providers accredited by the ICT Authority and who have a physical data center presence in Kenya.
Data Center	All government data centers must adhere to the TIA-942 (Rated-3 or higher) and relevant ISO standards (ISO 27001/22301) for security and availability.
Networking	IPv6 is the mandatory standard for all new network deployments. All external-facing services must be IPv6-enabled.
Operating Systems	Approved enterprise Linux distributions and supported operating systems shall be used in accordance with ICT Authority standards.
Databases	PostgreSQL is the standard for all new relational database deployments. NoSQL (MongoDB, Cassandra) for unstructured or high-velocity data workloads.
Containerization & Orchestration	Docker and Kubernetes as mandated standards for deploying and managing containerized applications.

Infrastructure as Code	Use of tools like Terraform and Ansible is the standard for automating infrastructure provisioning.
Middleware & API Integration	WSO2, Kong, or equivalent for API management; Kafka or RabbitMQ for event streaming.
Identity & Access Management	OAuth 2.0 / OpenID Connect, integrated with centralized IAM and PKI.
Backup & Disaster Recovery	Automated, geo-redundant backup and failover systems tested quarterly.

Compliance with the Technology Reference Model shall be mandatory for all technology initiatives. Architecture reviews, compliance audits, and periodic assessments shall be conducted to ensure adherence.

Enforcement of the Technology Reference Model architectural will ensure the following outcomes:

- Unified technology standards across all MCDAs.
- Enhanced interoperability through GIP
- Reduced costs and complexity through reuse of shared platforms and open technologies.
- Increased agility for deploying, scaling, and maintaining digital services.
- Stronger security and compliance posture through standardized controls and continuous monitoring.

By standardizing infrastructure, embracing cloud and open technologies, and embedding automation and security by design, the digital transformation objectives of a future-ready digital foundation capable of supporting continuous transformation, scalability, and citizen-centric service delivery.

TRANSITION FROM TRM TO TECHNOLOGY ARCHITECTURE

To translate the Technology Reference Model (TRM) into a practical and implementable Enterprise Technology Architecture, the following structured approach is recommended, aligned with the GEA framework:

Focus Area	Key Activities

From Reference to Realization	• Evolve the Technology Reference Model (TRM) from a conceptual guide into a practical, executable Technology Architecture. • Define logical and physical components mapped to each technology domain (compute, storage, network, middleware, endpoints). • Develop architecture blueprints, deployment patterns, and reference implementations aligned with enterprise objectives and GEA principles.
Domain-Driven Design and Service Catalog Development	• Apply Domain-Driven Design (DDD) to define bounded contexts and decompose government services into logical domains (e.g., citizen services, taxation, land management). • Develop a unified Service Catalog for RESTful microservices and SOA-based services to support modular and reusable digital service delivery. • Assign domain ownership for governance, traceability, and lifecycle management.
API Gateway and Integration Guidelines	• Implement a robust Open API Gateway based on GEA/GIF guidance. • Enforce OAuth 2.0, OIDC, and PKI-based authentication for secure access. • Enable interoperability across cloud, on-premise, and hybrid environments. • Integrate API Gateway with the Government Integration Platform (GIP) and event-driven architecture for real-time and batch data exchange.
Component Identification Across Technology Layers	• Identify and document logical and physical components across all TRM layers. • For each component, define its function, applicable open standards, and recommended technologies (open-source or proprietary). • Map interdependencies and integration interfaces across layers.

Conformance with Standards and Baselines	• Align technology implementations with the Government Interoperability Framework (GIF), National ICT Standards, and GEA compliance baselines. • Use Service Standards Tables to verify conformance at the application and data layers. • Establish regular review cycles to update technology baselines and ensure continuous compliance.
Cross-Referencing Implementation Guidance	• Reference the Implementation Approach and GEA Adoption Guide for detailed methodologies. • Follow step-by-step procedures for translating TRM into operational technology designs. • Use prescribed templates for architecture documentation, service catalogs, and compliance reporting.

DISASTER RECOVERY & BUSINESS CONTINUITY

GEA Technology Architecture – Mandatory Resilience Requirements

Disaster Recovery and Business Continuity (DR/BC) defines the mandatory capabilities, controls, and operational practices required to ensure that Government digital services remain available, recoverable, and resilient in the event of disruption. Disruptions may include cyberattacks, infrastructure failures, cloud outages, human error, natural disasters, or operational incidents affecting national platforms and MCDA systems.

Within GEA, DR/BC is a Whole-of-Government requirement that applies to:

- National platforms (e-Citizen, Digital ID, Payments, Registries, Integration Platforms)
- Critical MCDA operational systems
- Shared services and data exchange platforms
- External ecosystem integrations that support essential services

DR/BC requirements are mandatory and enforceable through GEA governance decision gates (ADM Phase G) and change controls (ADM Phase H).

Objectives

The DR/BC framework ensures that:

- Government services can be restored within approved time thresholds (RTO)
- Government data loss remains within acceptable limits (RPO)
- Critical services continue through alternative channels during major disruptions
- National platforms and shared services maintain resilience against localized failures
- Recovery processes are tested regularly and continuously improved
- Recovery readiness is measurable, auditable, and contractually enforced for vendors and PPP partners

Definitions

- **Business Continuity (BC):** The ability to continue delivering critical services during disruption through alternate arrangements and processes.
- **Disaster Recovery (DR):** The technical capability to recover systems, infrastructure, and data following a disruption.
- **RTO (Recovery Time Objective):** Maximum acceptable time to restore service after disruption.
- **RPO (Recovery Point Objective):** Maximum acceptable period of data loss measured in time (how far back recovery is allowed).
- **DR Site:** Secondary environment used to restore services (warm/hot/cold).
- **Backup:** A protected copy of data or systems to support recovery.

Service Criticality Tiering

All systems and services shall be categorized by criticality to determine minimum DR/BC requirements.

Tier	Service Type	Examples	Minimum DR Standard
Tier 0 – National Critical	Services essential for national stability and trust	Digital ID, Payments, e-Citizen core access, national registries, integration gateway	Hot/Warm DR, strong RTO/RPO, continuous monitoring
Tier 1 – Essential Public Services	High-volume or essential citizen services	Health service access, licensing, customs, revenue, justice	Warm DR, daily backups, tested recovery
Tier 2 – Important Support Services	Operational continuity services	HR, internal finance, document systems	Warm/Cold DR, scheduled backups
Tier 3 – Non-Critical / Low Impact	Non-essential or low dependency services	informational portals, low priority tools	Basic backup and restore

RTO / RPO Requirements

RTO/RPO must be defined per system, approved by governance, and tested.

Tier	RTO (Target)	RPO (Target)	Notes
Tier 0	≤ 1 hour (target)	≤ 15 minutes (target)	Requires replication and high availability
Tier 1	≤ 4 hours	≤ 1 hour	Requires defined DR failover procedures
Tier 2	≤ 24 hours	≤ 24 hours	Restoration priority after Tier 0/1
Tier 3	≤ 72 hours	≤ 72 hours	Basic restore acceptable

No Tier 0 or Tier 1 system may go live without documented and tested RTO/RPO capability.

Backup Policy and Schedules (Mandatory Minimum Standard)

Backups shall be automated, encrypted, access-controlled, and regularly verified. Backups must include:

- Production databases and object stores
- Configuration and infrastructure as code
- Application binaries and deployment pipelines (where applicable)
- Audit logs and security logs (per retention and archival policy)
- Encryption keys and secrets management (protected and controlled)
- Integration configurations (API gateways, message brokers)

Backup Frequency and Retention (Minimum Baseline)

Data / System Type	Backup Frequency	Retention (Minimum)	Protection Requirements
Tier 0 transactional databases	Continuous/near real-time replication + daily full	90 days minimum	Immutable snapshots, encryption, restricted access
Tier 1 operational databases	Hourly incremental + daily full	60–90 days	Encrypted backups, tested restore
Tier 2 systems	Daily incremental + weekly full	30–60 days	Controlled storage, access logging
Tier 3 systems	Weekly full	30 days	Basic controls
Logs (security/audit)	Daily snapshot or centralized SIEM retention	Per policy	Tamper-resistant storage

Backups must support immutable storage or write-once controls to protect against ransomware and insider threats. This is a mandatory requirement for Tier 0/1

The 3-2-1 backup rule is a widely accepted resilience standard used to reduce the risk of data loss caused by hardware failure, corruption, cyberattacks (including ransomware), human error, or site-level disasters. Under the GEA DR/BC requirements, it provides a minimum baseline for protecting critical government data.

- 3 copies of data
- 2 different media/storage types
- 1 copy stored offsite / isolated

Disaster Recovery Sites and Recovery Architecture

DR Site Types (Standard Definitions)

- **Hot Site**: Fully operational, near-real-time replication, rapid failover

- **Warm Site**: Partially operational, restored within hours
- **Cold Site**: Infrastructure and storage available, long restore window

Minimum DR Site Requirements by Tier

Tier	DR Site Type	DR Capability Requirement
Tier 0	Hot or Warm	Automated failover + tested recovery
Tier 1	Warm	Documented cutover procedure and rehearsal
Tier 2	Warm/Cold	Restore procedure validated
Tier 3	Cold	Basic backup restore acceptable

Site Separation and Resilience Controls

- DR environments must be separated by geography and risk profile (where feasible)
- DR infrastructure must be isolated from primary environments to reduce simultaneous compromise
- DR access is restricted and monitored, including privileged access controls
- The DR site must be treated as production-grade infrastructure for Tier 0 and Tier 1 services.

Business Continuity Requirements

DR restores technology; BC ensures services continue. Each Tier 0 and Tier 1 service must define:

- Alternate service channels (manual/assisted where required)
- Emergency operating procedures for service delivery
- Communication plans to citizens and businesses during outages
- Continuity of critical staff roles and escalation contacts
- Dependencies on national platforms (ID, payments, integration)

BC plans must be aligned to value streams, not departmental silos.

Testing, Drills, and Assurance

DR Testing Requirements

- Tier 0 and Tier 1: Minimum annual full failover drill, plus quarterly recovery validation
- Tier 2: Annual restore testing
- Tier 3: Basic verification and restore sampling annually

Mandatory Drill Components

Each annual drill must validate:

- Failover activation and service restoration
- Data integrity against RPO targets
- Application functionality and integration connectivity
- Security controls during recovery (IAM, logging, monitoring)
- Ability to resume operations without uncontrolled risk

Evidence and Reporting

Each drill must produce:

- Drill report (success/fail against RTO/RPO)
- Root cause analysis for gaps
- Corrective action plan with owners and deadlines
- Updated DR playbooks and runbooks

A drill that produces no corrective actions is not credible governance.

Governance, Compliance, and Enforcement

Design and Approval Controls

DR/BC requirements must be defined during solution architecture (ADM Phases D and E).

- ARB must validate DR/BC readiness before procurement and deployment (Phase G)
- Any deviation from baseline targets requires formal approval and risk acceptance

Continuous Monitoring

DR readiness must be monitored through dashboards tracking:

- backup success rates

- restore test success rates
- replication status
- DR drift (config mismatch)
- incident and outage history

Minimum Outputs / Artefacts (Required per System)

Each system shall maintain the following artefacts:

- DR/BC classification tier and criticality rating
- Approved RTO/RPO targets and supporting design
- Backup schedules and retention configuration
- DR site architecture and connectivity design
- Runbooks for failover/failback and restore
- Annual drill results and corrective action logs
- DR readiness report as part of governance compliance

No Tier 0 or Tier 1 digital service shall be approved for production unless its DR/BC capability has been defined, implemented, tested, and certified in accordance with GEA resilience requirements.

INTEGRATION ARCHITECTURE

Integration Architecture establishes the authoritative, government-wide framework that defines how public sector institutions connect, exchange information, coordinate processes, and securely interact to deliver seamless, end-to-end public services. It provides the structural, technical, and governance foundation required to enable interoperability across MCDAs, ensuring that government operates as a cohesive and coordinated enterprise rather than a collection of isolated systems.

As government increasingly delivers services through digital channels, effective integration becomes a critical national capability. Integration Architecture ensures that systems, platforms, and data sources can interact reliably, securely, and consistently to support policy implementation, service delivery, regulatory oversight, and evidence-based decision-making.

The Integration Architecture defines the standards, patterns, platforms, and governance mechanisms that enable systems to communicate through secure interfaces, reusable services, and shared integration infrastructure. It promotes the reuse of capabilities, reduces duplication, and establishes consistent mechanisms for orchestrating business processes that span institutional boundaries.

Public service delivery effectiveness relies on coordination and governance mechanisms within multiple MCDAs. Integration Architecture provides the structural and technical foundation to support interoperability and cohesion across the various architectural domains by defining how systems interact, share data, and collectively enable end-to-end service delivery.

Integration architectural layer defines the standards, protocols, messaging patterns, and API management approaches, enabling the reuse of services and promoting data-driven operations across the government ecosystem. It supports the orchestration and choreography of business processes that span across agency boundaries, underpinned by a shared governance framework.

Through the Government Integration Platform (GIP) and associated shared services, the architecture provides a controlled and auditable environment through which all cross-

government integrations are implemented, ensuring alignment with national interoperability standards and strengthening trust in digital government operations.

OBJECTIVES OF INTEGRATION ARCHITECTURE

Integration Architecture functions as the connective layer that links Business, Data, Application, Technology, and Security domains and operationalizes Whole-of-Government coordination by enabling information flows, process integration, and service orchestration across institutional boundaries.

Integration Architecture ensures that:

- Business processes can be coordinated across MCDAs to support integrated service delivery.
- Applications can interact through standardized and secure interfaces.
- Data can be exchanged in a governed and interoperable manner.
- Shared digital platforms can be leveraged consistently across government.
- Security controls are applied uniformly across inter-system interactions.

By enabling controlled interaction among architectural domains, Integration Architecture supports the realization of citizen-centric services, improves operational efficiency, and strengthens institutional collaboration across all levels of government.

It enables national and county systems to interoperate through common standards, shared platforms, and coordinated governance, ensuring that citizens and businesses experience government as a single, integrated service provider regardless of institutional boundaries. It reduces fragmentation, minimizes duplication of technology investments, and supports coordinated implementation of national development priorities.

The objectives of the Integration Architecture can be summarized as below:

Objective	How objective is achieved
Enable Seamless Public Service Delivery	Guide MCDAs in the conceptualization, design, and deployment of integrated public services that are cashless, paperless, and faceless to provide citizens with a unified, WoG experience through platforms like e-Citizen, Huduma, etc.

Promote Interoperability Across Layers and MCDAs	Define and structure the various integration layers; business process, data exchange, application interfaces, and infrastructure connectivity and elucidate the relationships among them.
Provide Technical Implementation Guidance	Provide implementation guidance and strategies for integration at the application layer including comparative analysis of integration approaches such as Enterprise Service Buses (ESBs), API Gateways, Event-Driven Architectures (EDAs), and Service-Oriented Architectures (SOA), Micro Services Architecture, etc.
Reduce Redundancy and Cost	Eliminate costly, custom point-to-point integrations and promote the use of a central, standardized integration platform.
Improve Business Process Efficiency	Automate cross-agency business processes by enabling systems to trigger actions and exchange information without manual intervention.
Enhance External Collaboration	Establish secure and standardized methods for integrating with external partners, such as banks, telecommunication companies, and international bodies.

INTEGRATION ARCHITECTURE PRINCIPLES

The Integration Architecture is guided by the following principles that ensure scalability, interoperability, resilience, security and trust across all layers:

Principle	Description
Openness and Transparency	Government systems shall enable appropriate data sharing and service accessibility by default, subject to legal, security, and privacy safeguards, to promote transparency, accountability, and public value
Standards-Based Interoperability	All integration mechanisms shall conform to standards defined in GIF, ensuring consistent technical implementation across institutions.
API-First Design	All new applications must expose their functions and data through well-documented, secure, and standardized APIs.
Asynchronous and Loosely Coupled	Integrations should be designed to be asynchronous where possible using event-driven patterns enhancing resilience and scalability.

User-Centric Design	Integration initiatives must prioritize citizen and end-user experience by enabling unified, intuitive, and inclusive multi-channel service delivery.
Secure by Design	All integrations shall enforce strong authentication, authorization, encryption, and auditing controls in alignment with national cybersecurity policies.
Full Lifecycle Management	Integration services and APIs shall be managed throughout their lifecycle, including design, approval, deployment, monitoring, versioning, and retirement.
Centralized Integration, Decentralized Execution	Shared integration platforms shall provide common capabilities while allowing institutions to retain ownership of their systems and business processes.

INTERRELATIONSHIP WITH GOVERNMENT INTEROPERABILITY FRAMEWORK (GIF)

The Integration Architecture and the Government Interoperability Framework operate as complementary constructs that together enable effective interoperability across government.

GIF defines the policy, governance, and compliance requirements that guide how institutions share information and collaborate. Integration Architecture translates these requirements into technical mechanisms, platforms, and standards that enable their practical implementation. Through this relationship:

- The GIF defines '**what'** and '**why'** - the policy and governance rules for interoperability.
- The Integration Architecture defines '**how**' - the technical mechanisms and standards that implement those rules

GIF Policy Objective - (What, Why)	Integration Architecture Response – (How)
The Mandate for Data Sharing & Governance GIF establishes the high-level policy that MCDAs *must* share data in a standardized and secure way by defining the governance	**Implemented through Government Integration Platform (GIP)** The central, mandatory platform defined in the reference model as the technical enforcement point

rules for creating and consuming shared services.	for the GIF's mandate, preventing ad-hoc, insecure integrations.
Rules for Secure Access & Authentication: GIF specifies that only authorized systems and users can access shared data, and this access must be audited.	**Enforced through API Gateway using OAuth 2.0 & OIDC** The architecture mandates the use of an API Gateway as the single-entry point. This gateway technically enforces GIF's security rules using OAuth 2.0 and OpenID Connect (OIDC) standards for authenticated and authorized access.
Standards for Data Formats & Semantics GIF defines what data should look like to be understood by any other government system to provide semantic interoperability.	The architecture provides specific technical standards to fulfill GIF's requirement. It mandates JSON as the data format and OpenAPI Specification (OAS) 3.0 for describing APIs, ensuring every MCDA builds and consumes data in the exact same, consistent way
Need for Discoverability and Reuse The core goal of GIF is to promote the reuse of existing services to save time and money. MCDAs need a way to find out what data-sharing services already exist.	**API Management Portal** This component of the GIP serves as a central, searchable catalog where developers can discover, understand, and subscribe to existing government APIs, as per the 'Full Lifecycle Management' principle.
Requirements for Resilient & Efficient Exchange GIF requires that data exchange be reliable and not cause system failures if one part of the government network is slow or unavailable.	**Asynchronous and Loosely Coupled Principle & ESB/Message Broker:** Achieved through Asynchronous and Loosely Coupled Integration Patterns implemented via ESB or Message Broker components supporting publish–subscribe mechanisms.

At the GIF level, the Government Integration Platform (GIP) serves as the primary enforcement point, ensuring that all integrations adhere to approved standards for security, data exchange, service discovery, and lifecycle management. API management capabilities provide centralized visibility, monitoring, and governance, enabling institutions to discover and reuse existing services while ensuring secure and reliable interactions.

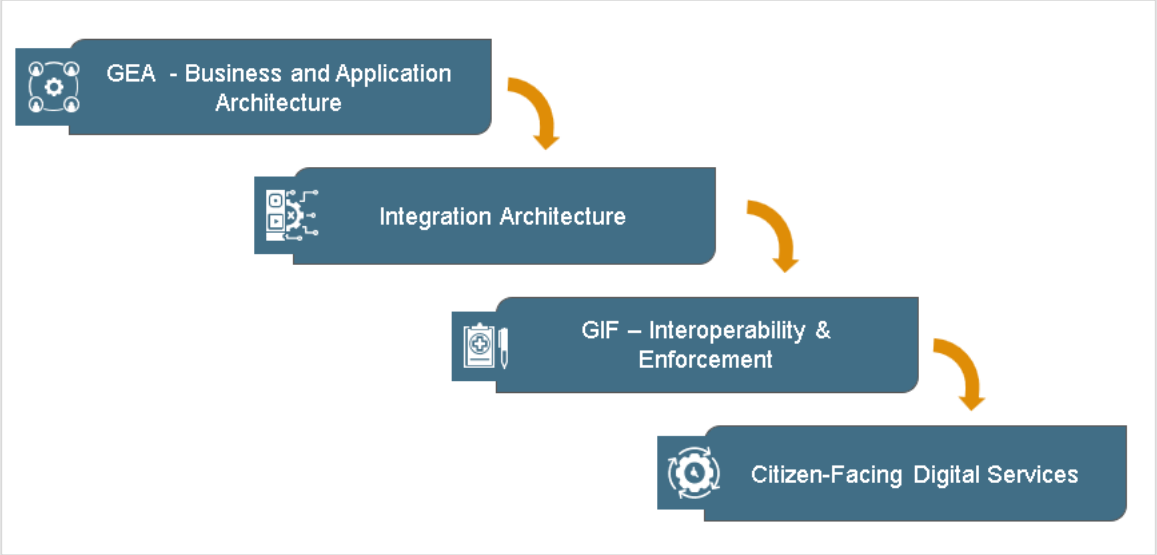

Figure 17 - GEA-GIF transition to digital services

Together, Integration Architecture and GIF create a unified framework that enables government systems to interoperate seamlessly, supporting coordinated service delivery, efficient operations, and a consistent Whole-of-Government digital experience as shown in *Figure 17* above.

INTEGRATION REFERENCE MODEL (IRM)

The Integration Reference Model (IRM) establishes the authoritative blueprint for enabling secure, standardized, and scalable interoperability across government systems, platforms, and stakeholders. It defines the structural layers, integration capabilities, and shared services required to support seamless information exchange and coordinated business processes across MCDAs, as well as with private sector partners and external stakeholders.

The IRM provides a unified integration fabric that supports multiple interaction patterns including synchronous APIs, asynchronous messaging, event-driven communication, and managed data exchange. By standardizing how systems interact, the model reduces complexity, eliminates fragmented integrations, and enables government to operate as a coordinated digital enterprise as shown in *Figure 18* below

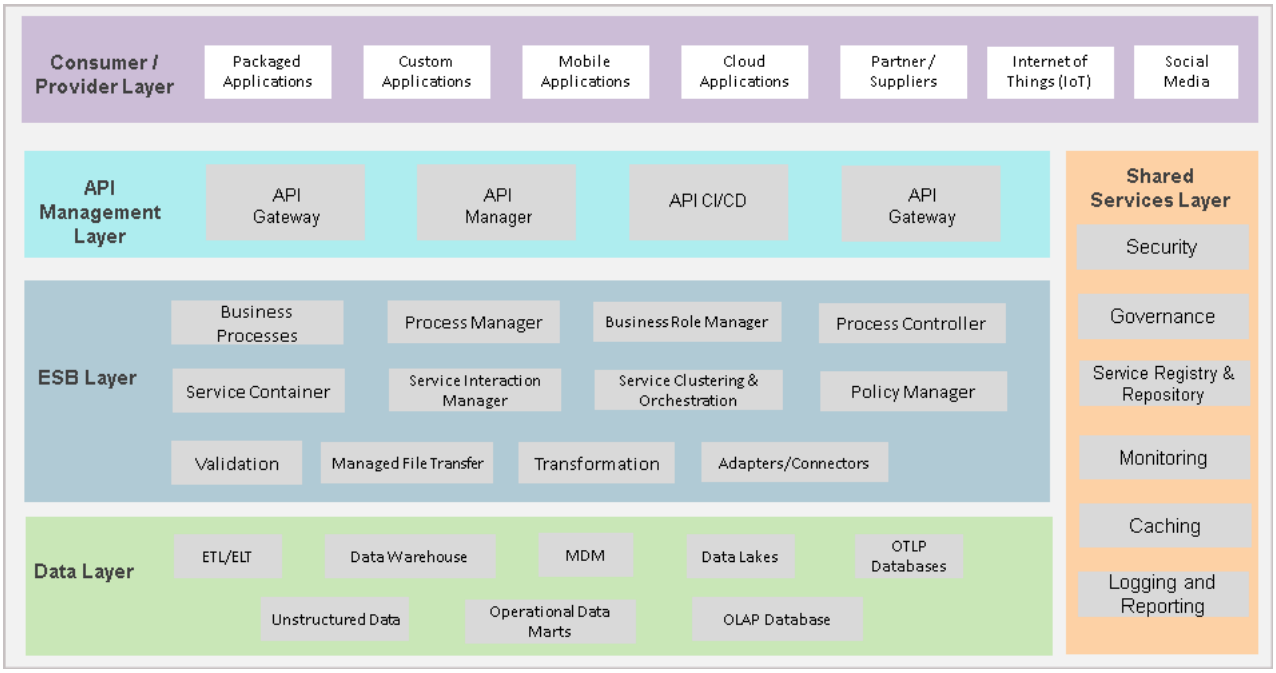

Figure 18 - Integration Architecture Contextual Model

The IRM is structured into logical layers that together form a comprehensive integration stack. Each layer provides distinct capabilities while working cohesively through the GIP

Consumer/Provider Interaction Layer	This layer represents all entities that consume or expose government services including internal systems, external partners, and digital channels interacting with government platforms. Participants in this layer include: • Government business systems and line-of-business applications • Mobile and web applications • Cloud-hosted solutions • County government systems • Partner and supplier platforms • Financial institutions and payment networks • Internet of Things devices • Regional or international data exchange platforms Interactions at this layer are mediated through secure entry points provided by the GIP, ensuring that all access is authenticated, authorized, and monitored.

API Management Layer	This Layer provides controlled exposure of services and enforces consistent access policies across all integrations. It enables API-led connectivity and supports the full lifecycle of API management. Capabilities include: • API gateway services for traffic management, security enforcement, and protocol mediation • API lifecycle management including design, publishing, versioning, and retirement • Developer portal for discovery and reuse of government APIs • Access control, throttling, and subscription management • API analytics and performance monitoring • Continuous integration and deployment support for API services
Integration Fabric (SOA / ESB Layer)	The Integration Fabric provides the core mediation, orchestration, and service interaction capabilities required for system-to-system integration, enabling government systems to interact in a loosely coupled manner, reducing dependencies and supporting incremental modernization. Key capabilities include: • Service orchestration and workflow coordination • Protocol mediation and routing • Message transformation and validation • Policy enforcement • Service discovery and registry integration • Managed file transfer and batch integration • Adapter frameworks for legacy system integration.
Event-Driven Integration Layer	Supports real-time responsiveness and high scalability by incorporating an Event-Driven Architecture through GIP messaging and streaming services; supporting scenarios such as real-time notifications, policy triggers, and cross-agency workflows. Key Components include: • Event producers that publish business events • Event brokers providing durable and scalable message distribution • Event consumers that subscribe to and process events • Schema registry for standardizing event formats

	• Event monitoring, replay, and audit capabilities
Data Integration Layer	Supports the movement, synchronization, and controlled access to data across heterogeneous environments, ensuring data exchanged through the GIP is consistent, governed, and available to authorized consumers. Capabilities include: • Data transformation and mapping • Data virtualization and federation • Extract, transform, and load processes • Change data capture • Data quality validation • Integration with operational and analytical data platforms This layer supports both transactional exchanges and analytical data flows required for reporting and decision-making.
Shared Services Layer	Provides cross-cutting capabilities that support all integration activities and ensure consistency across the integration ecosystem. Services include: • Identity and access management • Security services including encryption and key management • Logging, monitoring, and observability • Audit and compliance tracking • Service registry and repository • Notification and messaging services • Performance monitoring and reporting • Configuration and policy management These shared services are delivered through the GIP to ensure centralized governance and operational visibility.

All MCDAs shall align new system implementations and modernization initiatives with the IRM and leverage the GIP for exposing services and integrating with other systems. Point-to-point integrations that bypass approved platforms shall be avoided unless formally approved by the Architecture Review Board.

MCDAs shall adopt standardized integration patterns defined under this model and participate in centralized governance processes to ensure interoperability across the government ecosystem.

GOVERNMENT INTEGRATION PLATFORM (GIP)

GIP provides the common, governed interoperability backbone that enables secure, reliable, and semantically consistent exchange of information and services across MCDAs, as well as with authorized external stakeholders in the government ecosystem.

Within the IRM, the GIP serves as the operational integration fabric through which interoperability capabilities are implemented, governed, and monitored and provides the shared infrastructure, technical services, and governance mechanisms required to operationalize the standards and principles defined under the GIF and GEA.

The GIP ensures that government systems interact through standardized interfaces, approved integration patterns, and controlled trust frameworks, enabling coordinated service delivery while maintaining security, accountability, and institutional autonomy.

GIP Federated Architecture

The GIP is not a single application or monolithic platform. It is a federated interoperability environment composed of shared services, approved integration capabilities, and governance controls that collectively support a scalable and resilient digital government ecosystem. This federated approach allows institutions to retain ownership of their systems while participating in a common integration environment that enforces:

- Technical interoperability through standardized protocols and interfaces
- Semantic interoperability through shared data definitions and registries
- Organizational interoperability through coordinated governance
- Security interoperability through shared identity and trust frameworks

GIP operationalizes the legal, organizational, technical semantic and governance requirements defined in the GIF by providing a controlled environment for implementing interoperability. It also accommodates varying levels of institutional maturity, enabling

progressive onboarding while ensuring consistent compliance with defined standards at the national level.

The GIP Reference Architecture in *Figure 19* below provides a logical, governance-oriented view of interoperability capabilities required to support integrated government operations. It defines how integration services are organized, governed, and consumed without prescribing a specific technology stack or deployment model.

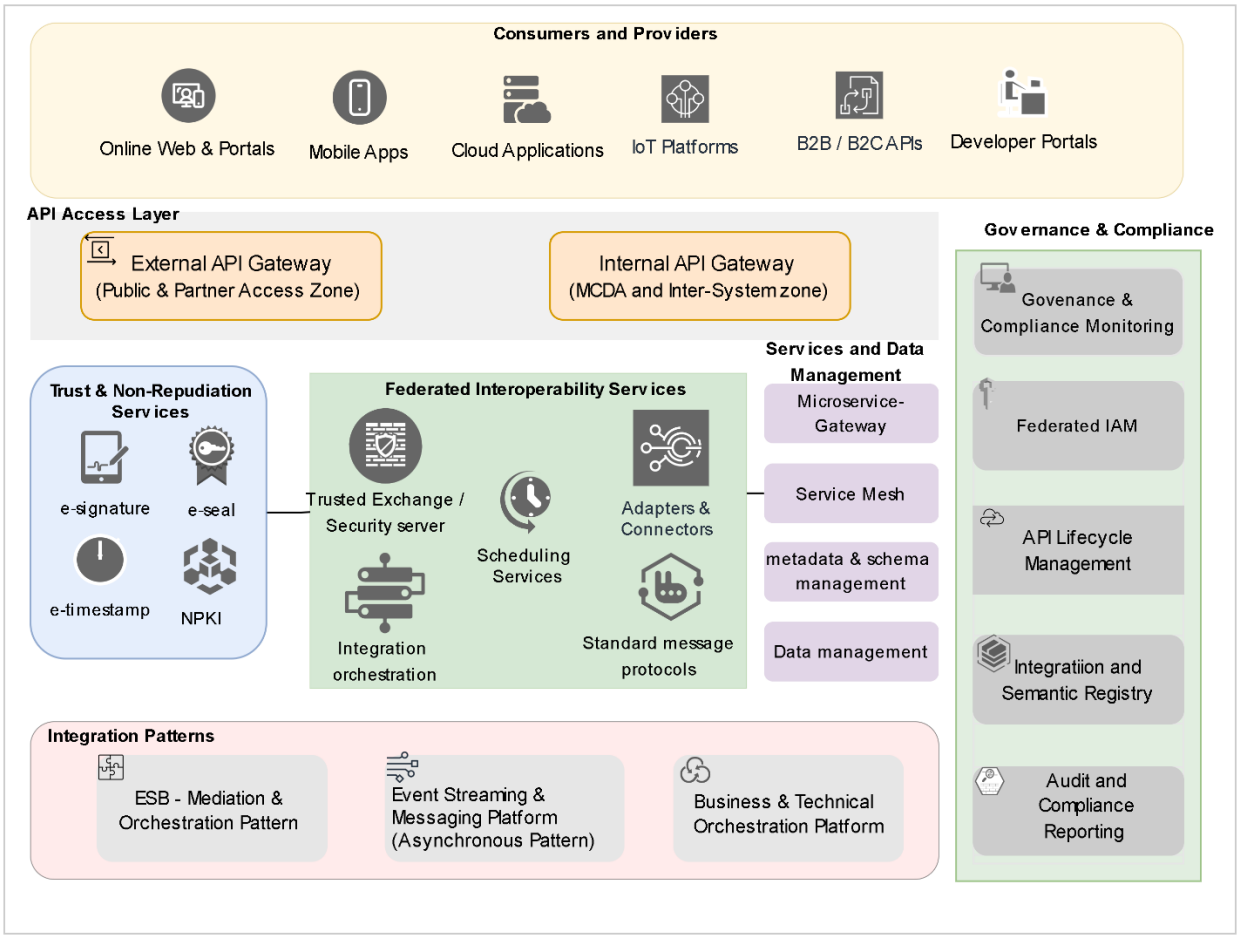

Figure 19- Government Integration Platform (GIP) Reference Architecture

The reference architecture depicts:

- How systems expose and consume services through standardized APIs and messaging interfaces
- How synchronous and asynchronous integration patterns coexist within a governed environment
- How trust, identity, and security controls are applied consistently across integrations

- How semantic consistency is maintained through shared registries and metadata governance
- How interoperability capabilities can be deployed progressively across institutions
- How integration services scale to support national service delivery demands

The model is intended as a guiding framework for implementation and should be applied flexibly based on institutional context, while remaining aligned with national standards and governance processes.

The GIP Reference Architecture is organized into logical capability layers that operate concurrently under centralized governance.

Service Exposure and Consumption Layer	Represents all systems, channels, and platforms that consume or provide government services, including digital portals, mobile applications, partner systems, cloud platforms, and developer ecosystems. Interactions are mediated through secure entry points (external and internal API gateways) to ensure controlled access and monitoring.
Integration and Trust Services Layer	Provides the core capabilities that enable secure, reliable and auditable interactions within the government ecosystem, including: • Trusted exchange services • Service orchestration and mediation • Scheduling and workflow coordination • Adapters and connectors for legacy systems • Standard messaging protocols • Trust services such as digital signatures, seals, and time stamping
Services and Data Management Layer	Supports microservice exposure, service mesh capabilities, metadata management, and data governance to ensure consistency and reliability across service interactions. This enables coordinated management of service definitions, schemas, and operational data flows across the integration environment.
Integration Patterns Layer	Defines approved patterns for implementing interoperability to provide flexibility while maintaining architectural consistency, including:

	• API-led integration • Service mediation and orchestration through ESB capabilities • Event streaming and messaging platforms • Business process orchestration
Governance, Identity, and Compliance Layer	This layer enforces adherence to GIF policies and GEA principles and provides cross-cutting capabilities that ensure integrations operate within defined policy and security boundaries, including: • Federated identity and access management • API lifecycle governance • Integration registries and semantic governance • Monitoring and compliance oversight • Audit and reporting services

NATIONAL DIGITAL PAYMENTS ENABLEMENT

GIP establishes a unified framework for integrating Person-to-Government (P2G) and Business-to-Government (B2G) payment services across the government ecosystem.

In the ongoing review of the ecitizen payment platform, the proposed payments architecture should be designed in such a way that all government revenue transactions are processed through the GIP in a unified, transparent, and auditable platform that strengthens public financial management, improves revenue assurance, enhances citizen convenience, and reduces fragmentation across payment channels.

By providing a centralized orchestration capabilities for connecting service delivery platforms, financial institutions, mobile money providers, payment gateways, and treasury systems, the GIP enables:

- Consolidation of fragmented payment channels into a single governed ecosystem
- Real-time processing and reconciliation of government payments

- Standardized application of fees, policies, and revenue rules
- Improved transparency and auditability of revenue collection
- Reduced operational complexity through shared payment services

As a matter of enforceable policy:

- All payment-enabled government services shall integrate through the GIP payments capability or approved national payment infrastructure.
- Direct integrations between MCDAs and payment providers that bypass GIP governance shall not be permitted unless explicitly authorized by the National Treasury and the GEA Oversight Authority.
- Payment processes shall comply with national public finance laws, Treasury regulations, audit requirements, and applicable financial sector standards.
- Revenue collection shall be traceable end-to-end from payment initiation to reconciliation and reporting.

INTEGRATION OF EXISTING LEGACY APPLICATIONS

Legacy systems remain foundational to the delivery of many critical government services, supporting core administrative, regulatory, and financial functions across MCDAs. While these systems often contain authoritative data and institutional knowledge, they may operate on outdated technologies, rely on proprietary interfaces, or lack native support for modern interoperability standards.

Government modernization efforts shall prioritize their controlled integration into the national digital ecosystem rather than immediate replacement to enable continuity of services, protect institutional investments, and allow progressive modernization while ensuring alignment with national interoperability objectives.

Legacy applications shall not operate as isolated systems, rather such systems shall be integrated into the broader enterprise architecture through approved mechanisms that enable secure data exchange, process coordination, and participation in cross-government service delivery through the GIP.

The integration of legacy applications seeks to achieve the following outcomes:

- Preserve and maximize the value of existing systems by enabling access to authoritative data and core functionality.
- Ensure continuity of essential public services during modernization initiatives.
- Enable interoperability with modern applications, shared platforms, and digital service channels.
- Reduce operational risks associated with abrupt system replacement.
- Support phased modernization through incremental decoupling and capability exposure.
- Improve visibility, governance, and security of legacy system interactions.
- Facilitate eventual migration toward modern, standards-based architectures.

Legacy Integration Approach

Integration of legacy systems shall follow a controlled, non-intrusive strategy that introduces abstraction layers to expose legacy capabilities without modifying core system logic wherever possible. The preferred approach mandates the use of a dedicated Integration Adapter Layer that connects legacy systems to the Government Integration Platform.

The **Integration Adapter Layer** functions as a mediation and translation capability that connects to legacy systems using native protocols such as database interfaces, batch files, message queues, or proprietary APIs, transforms legacy data formats into standards-compliant representation to expose legacy functionality as secure, well-governed APIs or events through GIP.

This enforces security, validation, and monitoring controls and isolates legacy systems from direct external access. This approach enables legacy systems to participate in the interoperability ecosystem while reducing operational risks and preserving system stability.

Integration shall be conducted through a structured lifecycle to ensure consistency and governance as described in the table below.

1.	**Assess Existing Legacy Systems**	Conduct a comprehensive assessment of legacy applications that informs integration design and modernization planning. This covers: • Business criticality • Technical architecture • Data structures and quality • Integration dependencies • Security posture • Operational risks • Vendor support status
2.	**Design the Integration Architecture**	Develop a suitable integration design including interaction patterns, trust boundaries, and performance requirements that aligns with: • GEA principles • IRM layering • GIP onboarding requirements • Security standards • Data governance policies
3.	**Select Integration Tools and Technologies**	Select integration leveraging in GIP capabilities mechanisms such as: • Adapters and connectors • API mediation • ESB orchestration • Event streaming • Data synchronization tools
4.	**Define Interfaces and Data Exchange Protocols**	Establish clear interface specifications using approved standards ensuring: • Clear service contracts • Consistent data models • Version control • Error handling • Auditability

5.	**Implement, Test and Validate the Integration**	Execute the integration plan with rigorous validation including: • Functional testing • Security testing • Performance validation • Compliance review • GIP certification
6.	**Monitoring and Continuous Improvement**	Ensure ongoing oversight through: • Performance monitoring • Operational analytics • Security monitoring • Periodic reviews • Modernization roadmap updates

This Legacy Integration approach allows valuable legacy assets to participate fully in the interoperability ecosystem, decouples them from modern systems to reduce risk, and defers costly 'big bang' modernization projects and the data and processes they hold. It shall support long-term transformation by enabling gradual migration toward:

- API-enabled architectures
- Cloud adoption
- Microservices
- Event-driven systems
- Data platforms
- Digital service channels

KEY INTEGRATION STANDARDS

This section defines the mandatory technical standards for all inter-agency integrations to ensure consistency, security, and interoperability.

Standard	Description	Use Case Example
API Specification:	This is the standard for designing and documenting all RESTful APIs.	When the NTSA develops an API for vehicle lookups, they must

OpenAPI (OAS) 3.0	It creates a machine-readable 'contract' for how an API works, which enables automated testing, code generation, and discoverability.	first publish an OAS 3.0 file that precisely defines the endpoints (e.g., /vehicles/{regno}), the required parameters, and the exact structure of the response JSON.
API Security: OAuth 2.0 & OIDC	These standards provide a secure and standardized way for applications to gain access to resources on behalf of a user, or for systems to access each other, without sharing passwords. This is the global-industry standard for API security. It separates user identity from application authorization, allowing for secure delegated access and preventing credentials from being exposed.	The KRA iTax system needs to access business registration data from the BRS. The KRA system (the client) uses OAuth 2.0 to get a secure access token from the central Identity Service, which it then presents to the BRS API to prove it has permission to access the data.
Data Format: JSON	JSON (JavaScript Object Notation) is the mandatory format for all data payloads (the actual information) exchanged via APIs. JSON is lightweight, human-readable, and easy for machines to parse. Its widespread adoption across the technology industry ensures that nearly all programming languages and tools can work with it natively, reducing development complexity.	When the Ministry of Health requests patient data from a county hospital's system, the hospital's API will return the patient's information formatted as a JSON object, like: {'name': 'Jane Doe', 'patientID': '12345'}.
Messaging Protocol: AMQP	Advanced Message Queuing Protocol is the standard for asynchronous, event-driven communication between systems. **Rationale:** AMQP guarantees message delivery, even if the receiving system is temporarily offline. This is crucial for creating resilient, loosely coupled systems that don't fail when one component is down	When a new business is registered on the eCitizen portal, the BRS system publishes a 'Business Registered' event to a central message broker using AMQP. The KRA and NTSA systems, subscribed to this event, will then independently and automatically receive this message to create their

		respective tax and transport accounts.
Integration Platform: GIP	The centrally managed Government Integration Platform (GIP) is the mandatory technical platform for implementing all inter-agency integrations. **Rationale:** Using a single, central platform prevents the creation of hundreds of insecure, unmanageable point-to-point connections. It provides a single point of control for security, monitoring, and governance, enforcing all other standards.	A county government cannot build a direct, custom connection to the IFMIS system. They must connect their local system to the GIP, which will then manage the secure and standardized communication with IFMIS according to the rules of the GIF.

CASE STUDY: Interoperability with X-Road and Other Patterns

X-Road is an open-source, standards-based data exchange platform originally developed by Estonia and Finland to enable secure, interoperable, and efficient exchange of information between government agencies, private organizations, and citizens. It provides the technical and organizational backbone for digital interoperability, allowing independent information systems to communicate through a trusted, auditable, and decentralized network.

At its core, X-Road functions as a secure data exchange layer whereby each participating organization retains control over its own data and systems, while X-Road ensures that data can be securely requested and transmitted between participants through standardized interfaces.

Within the Kenya's Government Enterprise Architecture (GEA) context, X-Road can serve as the core integration backbone or as the secure data exchange layer under the Government Integration Platform (GIP) as its modular design fits well into the GEA's layered integration model as shown in the figure below (source X-Road):

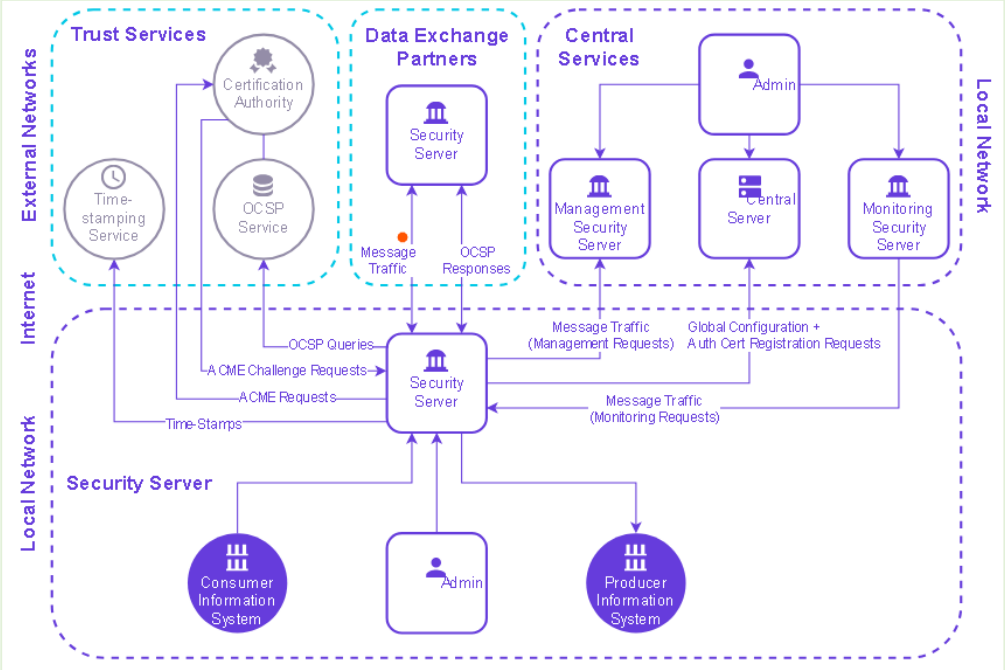

Figure 20 - X-Road Architecture

The X-Road architecture is federated and service-oriented, consisting of national and institutional components that collectively enable secure cross-organization interoperability. Its design principles align closely with the GEA's integration and interoperability objectives.

Integration Architecture Layer	X-Road Role and Implementation
Process Integration Layer	Supports orchestration of services between MCDAs through service calls and standardized workflows defined in the X-Road registry.
Application Integration Layer	Provides the secure connectivity layer between backend systems via Security Servers, acting as an alternative or complement to traditional API gateways or ESBs.

Data Integration Layer	Facilitates real-time, policy-compliant data exchange, ensuring message-level security and auditability.
Infrastructure Integration Layer	Operates as the national integration network, enabling standardized, encrypted connectivity across the public sector's infrastructure.

In this setup, X-Road acts as the transport and trust layer for cross-agency data exchange, while the GIP (Government Integration Platform) provides higher-level services such as API management, service discovery, analytics, and developer lifecycle management.

- X-Road Compatibility: X-Road may be used as the secure, auditable request–response transport for transactional exchanges. X-Road complements the GIP: use X-Road for governed synchronous exchanges and the GIP event streaming layer for asynchronous propagation. Integration adapters and brokers bridge X-Road services and Kafka topics where dual models are required.
- Hybrid Approach: APIs (synchronous), ESB (mediation), and EDA (asynchronous streaming) coexist within GIP; selection is use-case driven (transactional integrity vs. real-time notifications vs. bulk synchronization).

X-Road Server as the Government Integration Platform (GIP)

With some architectural enhancements, X-Road can serve as the core foundation of the GIP, but not as a complete replacement. It is highly suited for secure, standards-based inter-agency data exchange, but requires complementary components for full lifecycle API and service management as envisioned in Kenya's GEA**.**

Proposed Integration Architecture with X-Road as GIP Core

- X-Road as the Secure Data Exchange Layer: Handles encrypted, authenticated, and logged data transfers between MCDAs.
- API Management Layer (WSO2 / Kong): Manages API lifecycle, discovery, and subscription.

- Service Orchestration Layer: Uses workflow engines to coordinate cross-agency processes (e.g., business registration).
- Metadata and Registry Integration: Links X-Road service definitions to the National Metadata Registry for discoverability and governance alignment.
- Monitoring and Audit Layer: Aggregates X-Road transaction logs with system performance data into a unified government observability dashboard.

Integrating X-Road within the GEA Integration Architecture can provide a proven, secure, and scalable foundation for data exchange, aligned with the principles of openness, interoperability, and trust.

As a core component of the Government Integration Platform, X-Road can enable standardized, policy-compliant data exchange across MCDAs while leveraging complementary tools for API management, analytics, and orchestration.

This hybrid implementation would deliver a robust, future-proof digital backbone that would position Kenya to achieve Whole-of-Government interoperability comparable to world-leading digital nations like Estonia and Finland.

SECURITY ARCHITECTURE

Security Architecture represents the enterprise-wide framework of organizational, conceptual, logical, and physical controls that collectively safeguard the confidentiality, integrity, availability, and privacy of government information assets. Within the GEA, Security Architecture is recognized as a first-class architectural domain, on equal footing with business, data, application, integration, and technology architecture, and serves as the foundational trust layer underpinning all digital government services, cross-agency interactions, and national digital infrastructure.

According to the TOGAF definition:

"Security Architecture is a structure of organizational, conceptual, logical, and physical components that interact in a coherent fashion in order to achieve and maintain a state of managed risk and security (or information security). It is both a driver and enabler of secure, safe, resilient, and reliable behavior, as well as for addressing risk areas throughout the enterprise.

Within the Whole-of-Government context, Security Architecture establishes a coordinated and enforceable framework through which MCDAs implement consistent security controls, manage cyber risk, and maintain a unified security posture across the national digital ecosystem.

In modern digital government ecosystems characterized by cloud adoption, API-driven integrations, multi-agency service delivery, mobile access, and pervasive cyber threats, security can no longer function as a reactive or peripheral consideration. Instead, Security Architecture becomes a foundational enabler of national stability, public trust, and resilient digital transformation.

Security Architecture also provides the trust fabric required to support Whole-of-Government interoperability, ensuring that digital services, shared platforms, and cross-agency workflows operate within clearly defined trust boundaries enforced through identity, cryptography, monitoring, and governance mechanisms.

Security Architecture is **cross-cutting**, permeating every other architectural layer. Its scope is enterprise-wide, covering governance, processes, systems, data flows, identities, and technology infrastructures.

It defines the mandatory security baseline, control frameworks, and assurance mechanisms that all government digital initiatives must adhere to, ensuring consistency, auditability, and resilience across the government technology landscape.

GEA Domain	Security Architecture Alignment
Business Architecture	Protects the integrity, availability, and continuity of public services; embeds risk management, compliance, and trust into service delivery models.
Data Architecture	Enforces classification, protection, privacy, and lifecycle governance for government information assets, including personal and sensitive data.
Application Architecture	Ensures secure design, development, deployment, and operation of applications through secure development practices and runtime protections.
Integration Architecture	Protects APIs, event streams, and service exchanges through identity federation, encryption, trust frameworks, and policy enforcement.
Technology Architecture	Secures infrastructure, cloud environments, networks, and endpoints through hardening, monitoring, and resilience mechanisms.

The main objective of the Security Architecture is to establish a proactive, intelligence-driven, and resilient security posture that protects all the digital assets with the MCDAs, shared government platforms, and national digital infrastructure and ensures secure, reliable, and lawful delivery of digital government services while maintaining public trust, protecting national interests, and managing cyber risk across the Whole-of-Government ecosystem.

Objective	Explanation
Strengthen Digital Trust	Uphold citizen privacy and enforce transparent data-handling practices through mandated privacy-by-design, privacy engineering, and citizen-centric consent mechanisms supported by secure digital identity, auditability,

	and strong assurance controls that enable trusted interactions across all government digital channels.
Protect National Assets	Safeguard critical government information and infrastructure against unauthorized access, misuse, disclosure, disruption, modification, or destruction through well-defined security controls and continuous monitoring.
Enable Secure Interoperability	Enforce secure, policy-driven, and privacy-preserving data exchange across MCDAs through GIF-compliant trust frameworks and GIP-aligned API, event, and secure messaging architectures incorporating strong authentication, authorization, encryption, digital signatures, and transaction traceability.
Enable Federated and Secure Identity	Establish federated identity management enabling cross-agency authentication, identity portability, and digital signatures supported by a national PKI, modern identity and access management (IAM), and Zero Trust identity verification mechanisms across users, services, and devices.
Foster a Culture of Security	Embed cybersecurity awareness and accountability at every level of government by embedding security as a shared responsibility across all roles and operations ensuring security is treated as a core operational discipline rather than a technical function
Ensure Resilience	Protect data and systems across their entire lifecycle, from creation and storage to transmission and access, through integrated controls spanning people, processes, and technology, guaranteeing continuity even under cyberattack or system failure ensuring continuity of critical government services during cyber incidents, system failures, or disruptions
Institutionalize Governance and Compliance	Align ICT operations with the Data Protection Act (2019), GIF, ISO 27001, NIST ZTA, and global privacy standards through formal governance structures, continuous assurance, compliance monitoring, and periodic independent audits across government institutions.

GUIDING PRINCIPLES

Principle	Description
Security by Design	Security shall be embedded into every stage of the system and service lifecycle, from policy development, architecture design, procurement,

	and implementation to operations and decommissioning, ensuring that secure configurations and controls are the default state across all government systems.
Privacy-by-Design and Privacy-by-Default	Personal and sensitive data shall be protected throughout its lifecycle through data minimization, purpose limitation, strong encryption, anonymization or pseudonymization where appropriate, and user-centric consent mechanisms consistent with data protection laws.
Zero Trust by Default	All access requests — whether originating internally or externally — shall be continuously authenticated, authorized, validated, and monitored. Trust shall not be implicitly granted based on network location, device ownership, or prior access.
Defense-in-Depth	Security controls shall be implemented in multiple, mutually reinforcing layers across identity, endpoints, networks, applications, data, and infrastructure to reduce the likelihood that a single control failure leads to compromise.
Principle of Least Privilege	Users, systems, services, and applications shall be granted only the minimum level of access required to perform their authorized functions, with privileges regularly reviewed, monitored, and revoked when no longer required.
Proactive Threat Management	MCDAs shall actively identify, assess, and mitigate emerging threats through continuous monitoring, threat intelligence integration, vulnerability management, penetration testing, and adaptive security controls to reduce risk before incidents occur.
Shared Responsibility	Security is a collective responsibility across central government authorities, MCDAs, system owners, service providers, and users, with clearly defined roles, accountability, and governance mechanisms to ensure consistent implementation of security controls.
Continuous Monitoring and Improvement	Security posture shall be continuously evaluated through real-time monitoring, logging, analytics, audits, and periodic reviews to ensure ongoing effectiveness, rapid detection of anomalies, and continuous strengthening of controls.

GEA/GIF AND SECURITY ARCHITECTURE

As governments digitize operations and deliver services through online and mobile platforms, they face escalating cyber threats targeting critical systems, data, and infrastructure. Citizens

and business and users must interact with government systems in a secure, verifiable, and regulation-compliant environment consistent with data protection laws and international cybersecurity standards.

Within the GEA, Security Architecture provides the policy, governance, and technical control framework that ensures digital services and interoperability mechanisms operate within defined trust boundaries across the Whole-of-Government ecosystem

Information shared between government entities must traverse managed, trusted, and monitored networks equipped with strong encryption, mutual authentication, integrity verification, and policy enforcement controls. Data exchanges and service transactions must support electronic identification, digital signatures, secure credential validation, and non-repudiation mechanisms to ensure authenticity, accountability, and traceability.

All cross-agency interactions shall conform GIF, which defines mandatory standards for identity, trust, messaging, data protection, and secure communications across ministries, counties, departments, agencies, and authorized external partners

Robust network and application monitoring must detect anomalies, intrusions, and unauthorized activities in real time, enabling rapid containment, coordinated response, and recovery across government systems.

Security Architecture establishes a federated trust model in which agencies can securely exchange data while maintaining clear accountability, defined trust relationships, and consistent enforcement of security controls.

Security Architecture operates as a cross-cutting discipline (see *Figure 22*), embedded across all the layers of GEA. It is realized through a comprehensive set of policies, standards, architectural views, control frameworks, security services, and operational processes that collectively enable consistent risk management across the government digital environment.

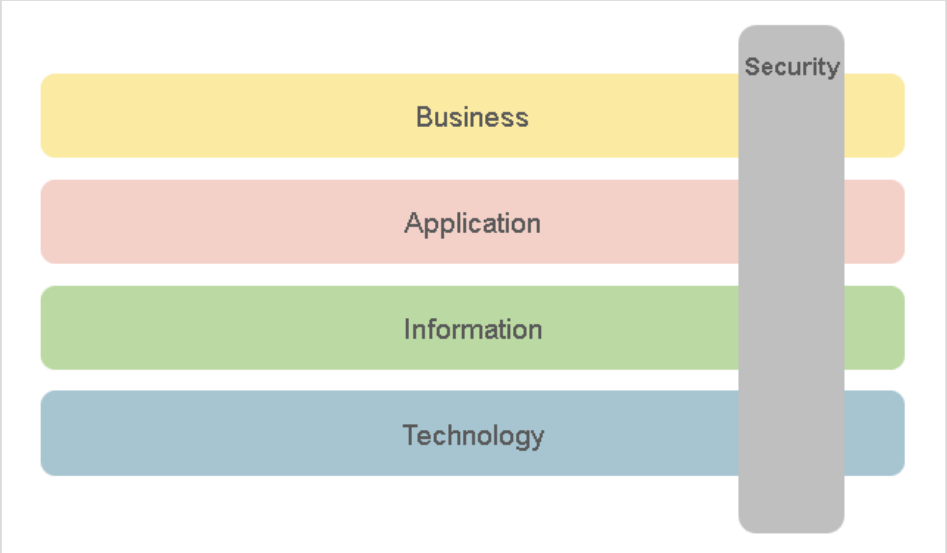

Figure 21 - Security Architecture Layer

It establishes a coherent security model that integrates governance, risk management, technical controls, operational monitoring, and incident response into a unified framework supporting continuous risk management.

Security Architecture is embedded as a foundational component of the GEA including establishment of comprehensive policies, processes, and controls across multiple domain layers:

Domain Layer	Security Focus	Activities
Business Layer	Governance, compliance, and security leadership	• Develop and enforce cybersecurity policies, frameworks, and governance mechanisms. • Define roles, responsibilities, and escalation protocols for incident management. • Integrate risk management into business decision-making.
Infrastructure Layer	Network and physical security	• Secure networks, servers, and data centers through segmentation, firewalls, VPNs, and intrusion detection systems. • Apply hardware hardening, patch management, and redundancy for resilience. • Conduct periodic security configuration audits.

Application Layer	Secure development and access control	• Enforce secure coding practices, OS hardening, and DevSecOps integration. • Use automated vulnerability scanning and code analysis tools. • Implement role-based access control (RBAC), multi-factor authentication (MFA), and logging of all privileged activity.
Data Layer	Data protection and privacy	• Encrypt data at rest and in transit using AES-256 and TLS 1.3 or higher. • Apply strict access policies, data classification, and retention schedules. • Implement anonymization and tokenization where appropriate to protect personal information.

ROLE OF GIF IN SECURITY GOVERNANCE

Security Architecture has been tightly integrated with the GIF and GIP, which together define the operational trust environment for secure cross-government data exchange and service interaction.

GIF establishes the policies, standards, and trust rules governing identity, authentication, authorization, encryption, data protection, and auditability across government systems. Security Architecture translates these policies into enforceable controls, technical standards, and assurance processes implemented across agencies.

The GIP serves as the secure interoperability backbone through which APIs, events, and data exchanges are mediated, monitored, and governed. Security Architecture ensures that all integrations conducted through the GIP adhere to defined trust protocols, including strong authentication, mutual TLS, token-based authorization, digital signatures, transaction logging, and continuous monitoring.

Through this integration, Security Architecture enables a federated trust model where MCDAs can securely share data while maintaining accountability, traceability, and compliance with national laws and policies.

SECURITY REFERENCE MODEL

Security Reference Model (SRM) provides a structured framework for designing, governing, and evolving the current and target state of the government's information security architecture, ensuring alignment of the security posture with organizational business strategies, national cybersecurity objectives, GEA, and GIF.

The SRM establishes a Whole-of-Government security baseline that applies across ministries, counties, departments, agencies (MCDAs), shared digital platforms, and cross-government services, enabling a consistent and coordinated approach to managing cyber risk.

The SRM defines the essential entities, policies, controls, trust relationships, and interdependencies that collectively safeguard the confidentiality, integrity, availability, and privacy of ICT systems, digital services, and data assets across government ecosystem.

It operationalizes a Zero Trust security model in which no user, system, device, or network is implicitly trusted, and all access is continuously verified, authorized, and monitored. It forms the conceptual and governance backbone of the Government's cybersecurity architecture, enabling systematic risk management, policy enforcement, security assurance, and continuous monitoring across all operational domains.

Role of SRM in the GEA Ecosystem

The SRM translates security principles defined within GEA into actionable control frameworks that protect business processes (Business Reference Model), information assets (Data Reference Model), applications (Application Reference Model), integrations (Integration Reference Model), and infrastructure (Technology Reference Model).

It also enforces interoperability trust requirements defined by the GIF and operationalized through the GIP ensuring that all cross-agency interactions occur within a secure, authenticated, encrypted, and auditable environment.

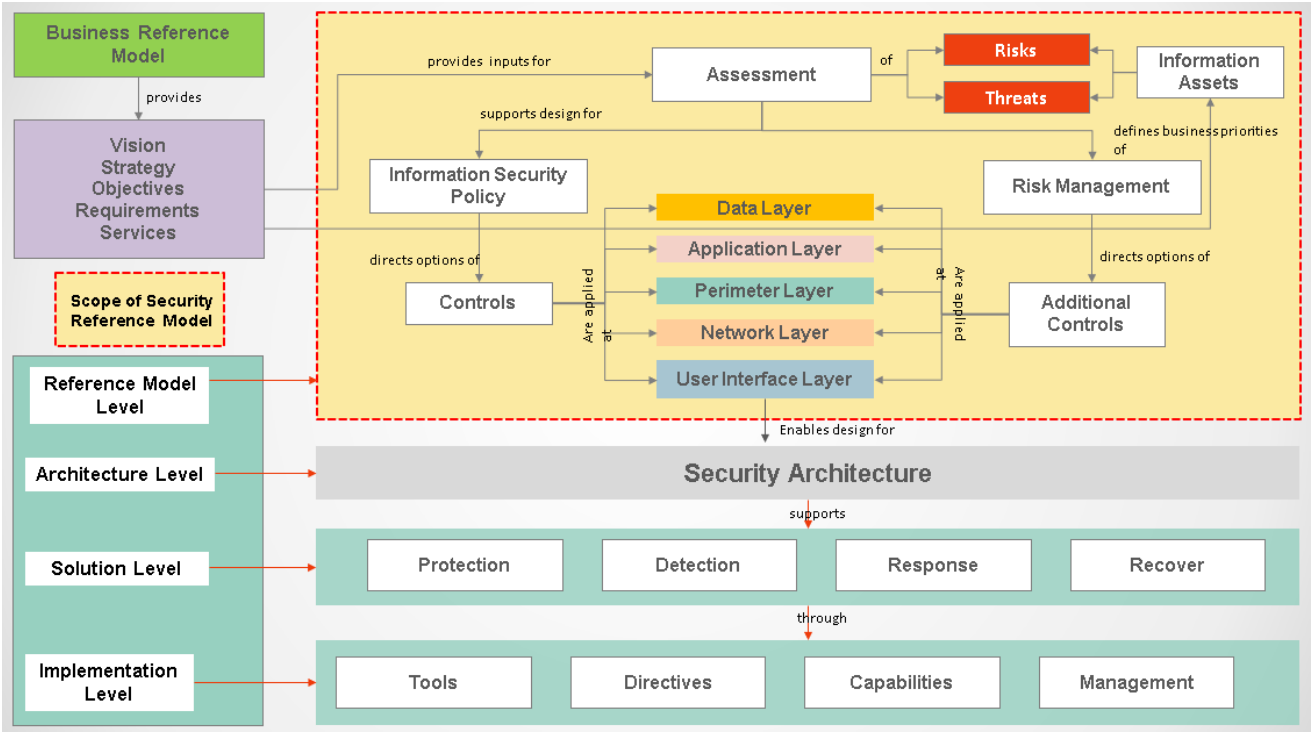

Figure 22 - Security Reference Model (SRM)

Figure 22 illustrates the SRM as a structured representation of how security governance, risk management, policies, and controls interact to protect government information assets and digital services across the enterprise architecture.

The diagram depicts Security Architecture as a Whole-of-Government trust framework that connects business priorities, risk management processes, and technical control layers to ensure consistent protection across MCDAs and shared digital platforms.

The SRM adopts a modern layered model incorporating Identity and Trust, Data, Application, Integration, Network, Endpoint, and Security Operations layers to reflect evolving digital government architectures. This layered approach ensures alignment with business objectives, compliance obligations, and enterprise risk management priorities.

The SRM also provides a defense-in-depth architecture in which each layer reinforces the others, ensuring that failure of one control does not result in systemic compromise. The layered model is implemented in alignment with Zero Trust principles, emphasizing continuous verification, least privilege access, and micro-segmentation.

Security controls are derived from business priorities defined in the Business Reference Model (BRM) and enterprise risk assessments, ensuring that all safeguards support mission delivery, service continuity, and regulatory compliance.

Control selection is informed by threat intelligence, risk analysis, regulatory requirements, and national cybersecurity priorities.

Key elements of the security framework include:

Asset Identification	Determine critical digital and physical assets requiring protection, including citizen data, national registries, shared platforms, applications, and infrastructure.
Risk and Threat Assessment	Identify threats, vulnerabilities, and attack vectors; assess likelihood and impact; and prioritize mitigation strategies.
Policy Definition	Establish enforceable policies, standards, and security baselines aligned with national legislation, GIF requirements, and government cybersecurity frameworks.
Control Design and Implementation	Translate security policies into actionable and measurable controls (technical, administrative, and procedural) across all layers
Compliance and Governance	Ensure all controls align with the Data Protection Act (2019), ICT Authority security guidelines, and relevant IT, privacy, and cybersecurity standards.
Continuous Monitoring	Conduct ongoing assessment, performance tracking, and incident analysis to detect anomalies, strengthen resilience, and maintain compliance.
Incident Detection and Response	Coordinate detection, investigation, containment, and recovery from cybersecurity incidents through centralized monitoring and response capabilities.
Security Assurance	Conduct certification, accreditation, and periodic reviews to validate the effectiveness of implemented controls

SRM operates within a Whole-of-Government governance framework that defines roles, responsibilities, accountability structures, and oversight mechanisms to ensure consistent implementation of security controls across MCDAs.

Central security authorities provide policy direction, monitoring, and coordination, while agencies are responsible for implementing controls in alignment with established standards.

Layered Security Representation

SRM illustrates how security controls are applied across layered domains including Data, Application, Perimeter, Network, and User Interface.

These layers collectively represent the operational environment in which security safeguards are implemented, forming a defense-in-depth architecture that protects systems from multiple threat vectors. While shown as distinct layers, they operate within a unified trust fabric anchored in strong identity, continuous monitoring, and policy enforcement.

The model should be interpreted through a Zero Trust lens, where trust boundaries exist between users, devices, applications, networks, and data regardless of physical location.

The Perimeter Layer: secures the infrastructure that hosts applications, data, and services. It represents the outer defense boundary encompassing physical and virtual infrastructure, data centers, and cloud environments.

The Network Layer: secures all channels through which data is transmitted, whether between internal systems, cloud environments, or external entities. It ensures confidentiality, integrity, and availability of communications.

The Endpoint Layer: focuses on securing all user and device access points—including desktops, laptops, mobile devices, IoT sensors, and biometric authentication hardware. With the expansion of mobile and remote work environments, endpoint protection is critical for preventing data leakage and device compromise.

The Application Layer: defines the controls applied within software systems and application platforms to protect business logic, data processing, and access mechanisms. It ensures applications are securely developed, deployed, and maintained across their lifecycle.

The Data Layer: represents the core of enterprise security, ensuring protection of information across its storage, processing, and exchange lifecycle. Data security spans structured, semi-structured, and unstructured repositories (databases, files, logs, and archives).

SECURITY EMBEDDED IN THE EA LIFECYCLE

Integrating security considerations throughout the Enterprise Architecture lifecycle provides the most cost-effective and sustainable protection strategy. Early adoption of secure design principles minimizes the need for costly redesigns and ensures that all systems are resilient by default.

Security architecture must anticipate abnormal conditions, system failures, and emerging threat vectors throughout all phases of the system lifecycle from planning and procurement to operation, decommissioning, and migration.

Privacy-Preserving Security Patterns

To strengthen the confidentiality, integrity, and lawful processing of citizen information across the Government of Kenya digital ecosystem, the Security Architecture incorporates advanced privacy-enhancing technologies. These capabilities protect sensitive data even in highly integrated service environments, support cross-agency collaboration, and maintain compliance with the Data Protection Act (2019).

Two categories of modern privacy-enhancing technologies are embedded into the GEA Security Architecture:

I. Zero-Knowledge Architecture (ZKA) Patterns
II. Homomorphic Encryption (HE) for secure data processing and exchange

These patterns complement the existing controls (Zero Trust, FIM, Consent Management, PKI, IAM, DLP, etc.) to create a security posture that defends not only against technical threats but also against privacy risks, unauthorized inference, and unlawful secondary use of data.

I. Zero-Knowledge Architecture (ZKA)

Zero-Knowledge Architecture introduces a security approach within GEA in which no entity (including government systems) learns more information than is absolutely necessary to complete a transaction or verify a claim. It allows systems to prove facts without revealing data. ZKA enables:

- Verification of attributes (e.g., age, citizenship, registration validity) without disclosing underlying personal data.
- Compliance with data minimization and purpose-limitation principles.
- Reduced exposure of identifiable data across integrated government services.
- Secure inter-agency collaboration without requiring sensitive datasets to be copied or replicated.

Below are a few examples use cases are listed in the table below:

Use Case	Zero-Knowledge Function
Age verification (e.g., for licensing, permits)	Prove “over 18” without revealing birth date
Tax compliance checks	Prove “tax-compliant” without sharing full tax record
Identity verification	Confirm identity validity without exposing full demographics
Eligibility verification (benefits, subsidies)	Verify eligibility criteria without revealing personal records

ZKA Components Integrated into GEA include:

- **Zero-Knowledge Proof Systems (ZKPs)** – zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge), zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge) for secure validation
- **Attribute-based credentials** - selectively disclosing only the required attributes
- **Selective disclosure protocols** - revealing only what is needed for the service
- **Privacy-preserving validation APIs** - embedded into GIP/API Gateway.

II. Homomorphic Encryption (HE) for Privacy-Preserving Data Sharing

Homomorphic Encryption will enable data to be processed, analyzed, and computed on while still encrypted, ensuring that no system ever sees the raw data. This means that MCDAs can collaborate and perform analytics without exposing citizens’ information, even to internal analysts or external partners.

The purpose in the GEA Context is to allow:

- Secure data-sharing across MCDAs without exposing raw values.
- Advanced analytics for policy, health, education, and finance without violating privacy.
- Compliance with confidentiality requirements even in multi-party processing ecosystems.

The benefits include:

- Elimination of the need to decrypt personal data for analytics or integration.
- Protection against insider threats and unauthorized data access.
- Enable multi-agency analytics without compromising confidentiality.
- Enhance public trust by minimizing data exposure.

GEA Security Architecture integrated these elements into the security layers as cross-cutting privacy-preserving controls

Security Layer	Privacy-Preserving Enhancement
Data Layer	Homomorphic encryption, tokenization, data minimization, secure multiparty computation
Application Layer	APIs enforcing Zero-Knowledge Proofs for attribute verification
Integration Layer (GIP/API Gateway)	Consent enforcement + ZKA validation + encrypted payload pipelines
Identity & Access Layer (FIM + IAM)	Attribute-based credentials, selective disclosure of identity attributes
Security Governance	Updated policies on encrypted analytics, privacy-by-design guidelines, ZK-based assurance models

HUMAN CAPACITY ARCHITECTURE

Human Capacity Architecture domain addresses the most critical success factor for the GEA - **People**. It establishes the government-wide framework for developing, governing, and sustaining the skills, competencies, leadership capabilities, and institutional culture required to deliver Kenya's digital government agenda.

As a core enabling domain of GEA, HCA recognizes that the successful design, implementation, and operation of digital public services depend fundamentally on a capable, accountable, and continuously evolving public service workforce.

HCA provides a structured approach to building and managing the human capabilities necessary to plan, govern, design, implement, secure, and operate digital systems across MCDAs, ensuring alignment with Whole-of-Government principles, the GIF, and national priorities under Kenya's digital transformation strategy.

The architecture defines the policies, competency frameworks, workforce models, institutional arrangements, and governance mechanisms required to ensure that government possesses the right skills at the right levels and in the right places to deliver integrated, secure, citizen-centric, and resilient services. It establishes a common foundation for workforce planning, recruitment, training, performance management, leadership development, and career progression across the public sector, enabling consistent capability development and reducing fragmentation in skills investment.

Beyond workforce development, HCA embeds an architecture-driven culture across government by institutionalizing enterprise architecture practices, promoting cross-government collaboration, strengthening accountability, and ensuring that human capability evolves in tandem with technological and policy changes. It supports the operationalization of key GEA domains including business transformation, data governance, cybersecurity, integration through the GIP and digital service delivery by ensuring that public servants are equipped with the competencies required to execute these functions effectively.

HCA also provides the foundation for workforce governance by defining roles and responsibilities across central oversight institutions, sector ministries, and implementing agencies, and by establishing mechanisms for monitoring capability maturity, enforcing

standards, and measuring workforce readiness. It supports strategic workforce planning through skills forecasting, capability gap analysis, and coordinated investment in capacity building to ensure long-term sustainability of government digital initiatives.

The vision of HCA is to enable a high-performing, digitally competent, and ethically grounded public service that can confidently design and deliver modern public services, manage emerging technologies responsibly, and sustain innovation in support of national development priorities.

Through this architecture, government establishes a coherent and enforceable approach to developing the human capital required to realize a secure, interoperable, data-driven, and citizen-focused digital government ecosystem.

OBJECTIVES

The objectives of the HCA is to establish the strategic direction for developing and sustaining a workforce capable of planning, governing, designing, implementing, and operating digital government systems in a coordinated and secure manner. These objectives ensure that human capability evolves in alignment with enterprise architecture, national priorities, and the operational needs of integrated government.

Objective	Description
Establish a Whole-of-Government Digital Workforce	Build a coordinated and interoperable public sector workforce with standardized roles, skills frameworks, and capability expectations across all MCDAs and counties to support integrated service delivery.
Build Digital Fluency	Ensure all public servants possess baseline digital literacy, data awareness, cybersecurity awareness, and understanding of digital service delivery models required to operate effectively in a modern government environment.
Develop Specialized Talent in Critical Domains	Establish and sustain expert cadres in areas including Enterprise Architecture, cybersecurity, cloud engineering, data governance, digital platforms, interoperability, AI governance, service design,

	and digital operations to reduce reliance on external vendors and strengthen sovereign capability
Institutionalize Architecture-Driven Delivery	Embed enterprise architecture practices into policy development, program design, procurement, and implementation processes to ensure alignment with GEA, GIF, and national standards.
Enable Secure and Trusted Digital Operations	Build workforce competencies required to implement Zero Trust principles, protect government systems and data, manage risks, and uphold security, privacy, and resilience obligations across digital services.
Strengthen Workforce Governance and Accountability	Establish governance mechanisms to oversee capability development, enforce standards, monitor workforce readiness, and ensure alignment with national digital priorities.
Define Clear Career Pathways	Define clear professional pathways, competency progression, and cross-government mobility mechanisms to attract, develop, retain, and effectively deploy digital talent across institutions.
Support Integrated Service Delivery Through Interoperability Skills	Build competencies required to design and operate systems that integrate through the Government Integration Platform (GIP) and comply with the Government Interoperability Framework (GIF).
Enable Continuous Learning and Capability Evolution	Establish mechanisms for continuous upskilling, reskilling, certification, and knowledge sharing to ensure workforce readiness in response to evolving technologies and policy demands.
Implement Workforce Planning and Skills Forecasting	Use data-driven workforce planning to anticipate future capability needs, identify gaps, and guide investment in training and recruitment.
Manage Transformational Change	Ensure successful adoption of digital initiatives through change management programs that build commitment, reduce resistance, and sustain momentum for transformation.

GUIDING PRINCIPLES

The guiding principles define the foundational rules that govern how human capability is developed, managed, and sustained across government. These principles ensure consistency, accountability, and alignment with enterprise architecture and Whole-of-Government delivery.

Principle	Description
Whole-of-Government Capability First	Workforce planning and capability development shall be coordinated at a national level to ensure consistency, avoid duplication, and support integrated service delivery across institutions.
Capability as a Strategic Asset	Human capability shall be managed with the same rigor as financial, information, and technology assets, with formal governance, performance oversight, and long-term investment planning.
Architecture-Led Workforce Development	Skills development and workforce planning shall align with GEA domains, ensuring that competencies support architecture governance, standards adoption, and lifecycle management.
Continuous Learning is a Core Duty	Continuous professional development shall be embedded into workforce management practices, supported by structured training pathways, certification programs, and knowledge sharing mechanisms.
Leadership Drives the Change	Senior leadership shall be responsible for championing digital capability development, ensuring that workforce readiness is integrated into strategic planning and performance oversight.
Collaboration and Cross-Functional Teams	Organizational silos will be broken down by promoting the formation of multi-disciplinary teams that bring together business, technology, and data experts to solve problems.
Talent is Strategically Managed	Manage human capital with the same rigor as financial resources—identifying critical skills, forecasting needs, and strategically developing or sourcing talent.
Sustainability and Resilience	Capability development shall be designed to ensure long-term sustainability, institutional continuity, and resilience against workforce turnover and technological change.

PUBLIC SERVICE COMPETENCY FRAMEWORK

The Public Service Competency Framework establishes the authoritative reference model for defining, governing, and developing the capabilities required to design, deliver, operate, and sustain digital government across all MCDAs. As a foundational component of the HCA, it provides a standardized and enforceable structure for defining workforce competencies aligned with GEA domain and national digital priorities.

The framework ensures that workforce capability development is coordinated across government, enabling institutions to recruit, develop, deploy, and retain personnel with the skills required to support integrated, secure, and citizen-centric services. It establishes a common competency taxonomy, proficiency model, and capability measurement approach that supports workforce planning, performance management, training investments, and continuous improvement.

By aligning competency development with architecture governance, interoperability obligations, cybersecurity requirements, and operational needs, the framework ensures that human capability evolves alongside technological and policy changes. It supports workforce readiness for emerging technologies, strengthens institutional resilience, and reduces reliance on external expertise by building sustainable internal capability.

The framework serves as the foundation for workforce governance, enabling oversight institutions to monitor capability maturity, identify gaps, enforce standards, and guide strategic investment in skills development across government.

Drawing from the *ICT Human Capital and Workforce Development 2023* framework, the competencies for a GEA-ready workforce fall under four clusters:

Competency	Description	Knowledge areas
Strategic Competencies	Capabilities required to guide digital transformation, enforce architecture standards, and align initiatives with national priorities.	Digital leadership and strategy Policy formulation and compliance Enterprise Architecture governance Strategic planning and execution
Technical Competencies	Specialized technical skills required to design, implement, and sustain GEA and GIF.	Cloud architecture and operations Cybersecurity and Zero Trust implementation Data engineering and analytics AI governance and responsible AI API design and lifecycle management Integration patterns (SOA, event-driven) Platform engineering DevSecOps Infrastructure automation

		Digital identity systems
Data and Interoperability Competencies	Capabilities required to manage data as a strategic asset and enable cross-government data sharing.	Data governance and stewardship Metadata management Master data management Data quality management Data sharing agreements Interoperability standards Data lifecycle management Privacy protection
Security and Trust Competencies	Capabilities required to ensure secure and resilient digital operations.	Zero Trust principles Security operations Risk and threat management Incident response Identity and access governance Privacy engineering Insider risk awareness Secure system design Data exchange through GIP
Behavioral Competencies	Skills and attributes that drive adoption, collaboration, and citizen-centric outcomes.	Change management and adaptability Communication and stakeholder engagement Problem-solving and innovation Citizen-first service design thinking
Delivery and Operational Competencies	Capabilities required to deliver reliable digital services.	IT service management Product management Agile delivery Program governance Service monitoring Service continuity Digital service operations Service reliability engineering

The competency framework is actualized through the activities below:

Activity	Description
Workforce Planning	Skills forecasting and capability gap analysis guide recruitment and training priorities.
Recruitment	Roles are defined using competency profiles and proficiency requirements aligned to national standards.
Learning and Development	Structured training pathways, certifications, and communities of practice build capability.
Certification Governance	Critical roles require formal certification and periodic renewal.
Performance Management	Capability development is assessed as part of performance evaluation.
Talent Mobility	Skills registry supports cross-government deployment.
Workforce Analytics	Capability maturity and skills gaps are monitored through dashboards.
Continuous Improvement	Framework is periodically updated to reflect evolving technologies.

KEY DIGITAL ROLES MODEL

The Key Digital Roles Model establishes the authoritative structure for defining, governing, and coordinating the strategic and operational roles required to implement and sustain GEA across all MCDA. It provides clarity on responsibilities, decision rights, reporting relationships, and competency expectations necessary to ensure effective execution of digital government initiatives.

The model ensures that accountability for architecture governance, interoperability compliance, digital service delivery, cybersecurity, data management, and workforce development is clearly defined across institutional levels. By standardizing roles and aligning them with enterprise architecture domains, the model promotes consistency, strengthens governance, and reduces ambiguity in execution.

It supports Whole-of-Government delivery by ensuring that critical capabilities are distributed appropriately between central oversight bodies and implementing institutions, enabling coordinated decision-making, effective oversight, and continuous capability development.

The model also serves as the foundation for workforce planning, recruitment, training, performance management, and succession planning, ensuring that government maintains the leadership and technical expertise required to deliver integrated, secure, and citizen-focused digital services.

National Governance Roles

Role	Core Responsibilities	Required Competencies
Chief Enterprise Architect (National)	Provides strategic EA direction, guides GEA/GIF compliance, chairs EA governance boards	Strategic leadership, policy design, digital transformation, stakeholder engagement
Government Chief Digital Officer	Directs digital transformation delivery, aligns investments with strategy	Digital leadership, portfolio governance
GIP / Integration Architect	Governs integration standards, API lifecycle, interoperability oversight	Integration architecture, API governance
National Cybersecurity Authority Lead	Sets security policy, ensures Zero Trust adoption	Security governance, risk management
National Data Governance Lead	Manages data standards, stewardship frameworks	Data governance, metadata management

Institutional Roles (MCDA Level)

Role	Core Responsibilities	Required Competencies
Domain Architects	Maintain domain architectures	• Deep domain architecture expertise aligned with GEA reference models

		• Standards definition and domain governance enforcement • Domain roadmap development and transition planning • Cross-domain integration coordination • Architecture pattern development and reuse • Data governance and interoperability alignment (where applicable
Digital Transformation Lead	Coordinates transformation initiatives	• Program and transformation governance • Change management strategy development • Benefits realization management • Stakeholder engagement across institutional leadership • Alignment of initiatives with national digital strategies
Service Design Lead	Manages digital transformation delivery, aligns investments with strategy	• Human-centered and citizen-centric service design • Service blueprinting and journey mapping • Digital inclusion and accessibility standards • Service performance measurement • Digital Service Integration
Change Management Lead	Drives organizational adoption, communication, and cultural transformation	Organizational psychology, PROSCI/ADKAR, stakeholder management
ICT Workforce Development Officer	Designs and implements capacity-building programs	Training design, HR planning, digital literacy development
Cybersecurity Specialist	Ensures all architectures embed robust security	CISSP/CISM, risk management, government security standards

Data Stewards/Managers	Manage data governance and quality	Metadata standards, data governance frameworks, analytics
EA Support Analysts	Provide operational support to EA tools and repositories	EA tooling (ArchiMate, Sparx EA), documentation, reporting

ROLE COMPETENCY MAPPING MATRIX

This matrix connects the Key Digital Roles to the Public Service Competency Framework, defining the target proficiency level required for each role. This tool is essential for recruitment, skills gap analysis, and creating targeted development plans.

Key Role	Technical Skills	Business Skills	Architectural Skills	Soft Skills
Chief Enterprise Architect	Advanced	Expert	Expert	Expert
Domain Architect (Data/Security)	Expert	Advanced	Expert	Advanced
Solution Architect	Expert	Advanced	Advanced	Advanced
Business Process Analyst	Intermediate	Advanced	Intermediate	Advanced
Data Steward	Intermediate	Expert	Intermediate	Advanced
Digital Transformation Officer	Advanced	Expert	Advanced	Expert

CHANGE MANAGEMENT FRAMEWORK

This Change Management Framework employs the ADKAR Model to provide a structured, people-centric approach to managing the transition to a new way of working. It recognizes that for any technology or process transformation to succeed, the individuals impacted must be guided through their personal change journey. The framework outlines five sequential, goal-oriented stages that must be achieved for a change to be successfully adopted and sustained.

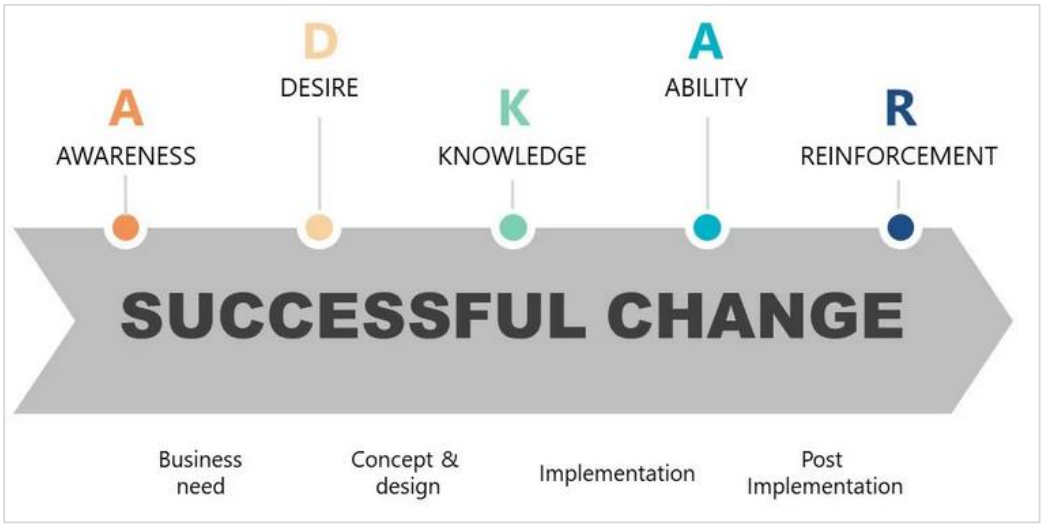

Figure 23 - ADKAT Change Management Model

The ADKAR model is recommended the standard change management methodology for all projects with significant impact. Project teams will be required to develop a formal Change Management Plan based on this framework. This involves identifying impacted stakeholder groups and planning specific activities to guide them through each of the five stages. The Digital Transformation Officer, in collaboration with project leads and HR, will oversee the implementation of these plans.

KEY STANDARDS & FRAMEWORKS

To ensure the Human Capacity Architecture is robust, aligned with best practices, and legally sound, its implementation will be guided by the following key standards and professional frameworks.

Standard / Framework	Description & Application
ICT Human Capital and Workforce Development Standard, 2023	This is the foundational government standard that provides comprehensive guidelines for ICT human resource development. The GEA Human Capacity Architecture is a direct implementation of its principles.
Skills Framework for the Information Age (SFIA)	An internationally recognized framework for describing and managing skills and competencies for the digital world. It will be used to benchmark and standardize the Public Service Competency Framework.

Change Management Body of Knowledge (CMBOK)	Provides best practices and standards for change management. It will inform the government's approach to implementing large-scale transformation projects.

KEY PERFORMANCE INDICATORS (KPIs)

To measure the success and impact of the Human Capacity Architecture, the following key performance indicators will be tracked.

KPI	Description	Target
Digital Literacy Score	An aggregate score from a bi-annual assessment of digital skills across the public service.	Increase the average digital literacy score by 15% within two years.
Critical Roles Fulfillment Rate	The percentage of key digital and architectural roles (as defined in the Key Roles Model) that are filled by qualified individuals.	Achieve a 90% fulfillment rate for all defined critical roles within three years.
Employee Change Readiness Index	A score derived from employee surveys measuring awareness, desire, and knowledge related to major digital transformation initiatives.	Achieve and maintain a Change Readiness Index score of 85% or higher.

GOVERNANCE ARCHITECTURE

The Governance Architecture domain defines the decision-making rights, accountability, structures, and processes required to manage and enforce the Government Enterprise Architecture (GEA) and the Government Interoperability Framework (GIF). It ensures that the GEA is not just a set of documents, but a living, dynamic framework that actively guides technology investment and decision-making across all MCDAs. It answers the critical question of how we manage and control the architecture.

Through the Governance Reference Model (GRM), it establishes the foundational principles for instituting a robust and accountable governance framework to oversee the lifecycle of Enterprise Architecture (EA) within government institutions and ensures that architectural practices are strategically aligned with the Digital Transformation vision, mission, and objectives.

OBJECTIVES OF GOVERNANCE ARCHITECTURE

To main objective is to establish a transparent, agile, and effective governance framework that empowers innovation, drives strategic alignment, enterprise-wide compliance, and the prudent management of the nation's digital investments.

Other objectives can be summarized in the table below

Objective	Explanation
Ensure Strategic Alignment	Verify that all technology initiatives are aligned with the strategic goals of the government as defined in Business Architecture.
Maximize ROI	Ensure that technology investments are cost-effective, reusable, and avoid duplication of effort and resources.
Manage Risk	Provide a formal process for identifying, assessing, and mitigating architectural risks across the enterprise.
Enforce Compliance	Establish the authority and processes required to ensure that all projects adhere to the principles and standards of the GEA.
Facilitate Change	Provide a structured process for evolving the GEA itself, ensuring it remains relevant in the face of new technologies and changing government priorities.

PRINCIPLES OF GOVERNANCE ARCHITECTURE

Below are the principles of Governance Architecture

I. **Transparency**

All architectural decisions, processes, and standards shall be openly documented and accessible to all relevant stakeholders.

II. **Accountability**

All architectural roles and responsibilities shall be clearly defined and assigned to ensure that all decisions will have clear ownership.

III. **Compliance by Default**

Adherence to the GEA is mandatory for all technology projects. Any deviation requires a formal, justified exception process.

IV. **Business-Driven Decisions**

Governance decisions will be primarily driven by the business needs and strategic objectives of the government, not by technology for its own sake.

V. **Pragmatism and Agility**

The governance process will be designed to be as lean and efficient as possible, avoiding unnecessary bureaucracy and enabling rapid, yet controlled, project execution.

VI. **Federated Authority**

While a central body provides oversight, decision-making authority will be delegated to the most appropriate level to ensure that domain-specific expertise is leveraged effectively.

VII. **Stakeholder Engagement**

The governance process will facilitate inclusive decision-making through formal governance bodies and advisory committees.

VIII. **Continuous Oversight and Lifecycle Management**

Implementation of ongoing governance, with mechanisms to monitor implementation, assess architectural impact, and adapt to evolving MCDA needs.

KEY CONCEPTS OF THE GEA GOVERNANCE REFERENCE MODEL

Concept	Mandate Question	Application
IT Governance	Are we doing the right things with IT and getting	The highest level of oversight, ensuring the entire GEA aligns with national strategy. It is embodied by

	value from our investments?	the GEA Steering Committee and guided by frameworks like COBIT and ISO/IEC 38500.
Architecture Governance	Are we managing and controlling the blueprint architecture effectively?	This is the primary function of the Architecture Review Board (ARB), which is responsible for the day-to-day enforcement and lifecycle management of the framework. This is the specific management of the GEA itself.
Compliance	Did we follow the mandatory process?	Refers to the adherence to the formal Architecture Compliance Process. A project is compliant if it submits its architecture to the ARB for review at the designated stages.
Conformance	Does the design adhere to the architectural standards and principles?	It assesses whether a project's design aligns with the GEA's mandated standards and principles. Technical evaluations are performed by the ARB during Compliance Reviews.

GOVERNANCE REFERENCE MODEL (GRM)

The Governance Reference Model (GRM) establishes the structure necessary for effective oversight, coordination, and accountability in the development and implementation of Enterprise Architecture (EA). The model is underpinned by clearly defined institutional roles and a balance of authority across governing bodies. The structural components and guiding principles are outlined as follows:

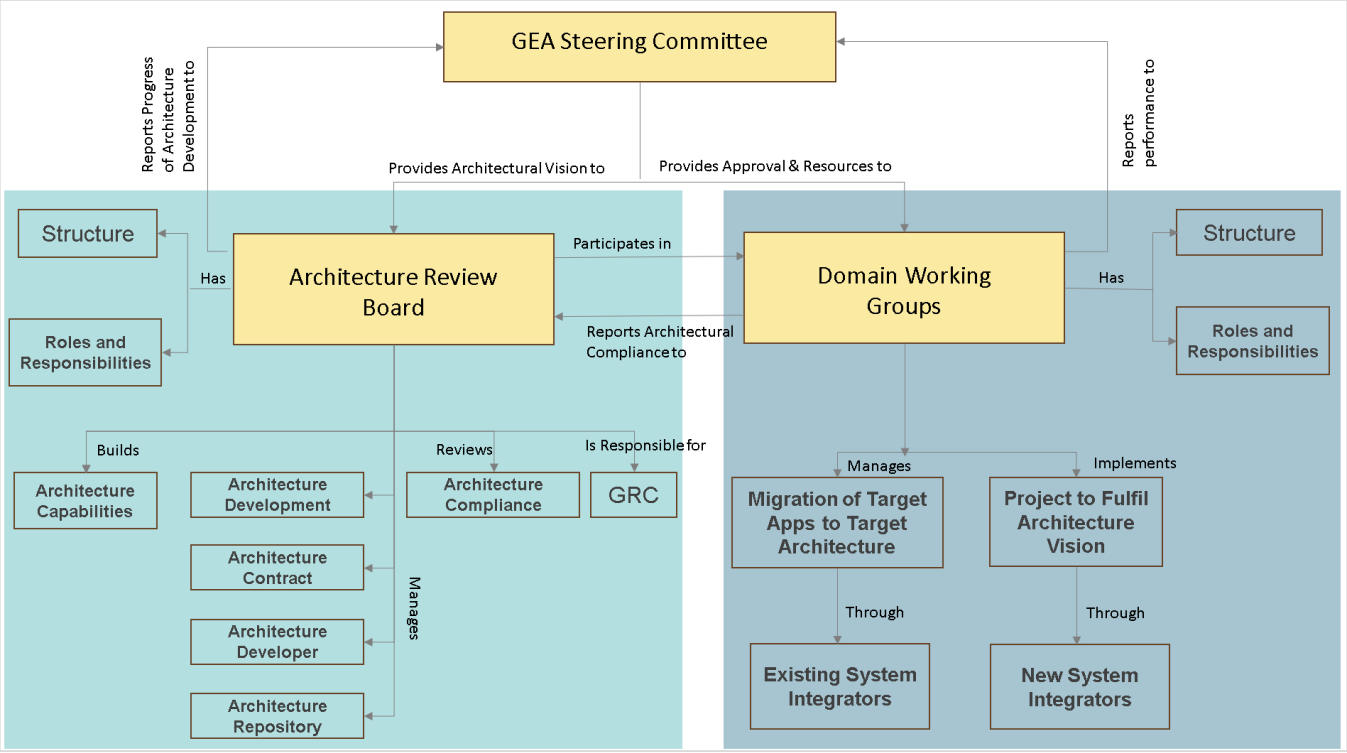

Figure 24 - Governance Reference Model

CORE GOVERNANCE ENTITIES

GRM is built upon three primary entities, each serving a distinct and critical role in the governance ecosystem:

Role	Responsibility	Membership
GEA Steering Committee (Strategic)	Provides strategic direction, high-level oversight, and owns the vision of the EA initiative. This role will be managed under ICTA for the MICTDG.	Cabinet Secretaries, Principal Secretaries (PSs) from key ministries (e.g., ICT, Treasury, Interior), the Director-General of the ICT Authority.
Architecture Review Board (ARB)	The primary working body is responsible for the day-to-day management of GEA. It reviews projects for compliance, approves new standards, and grants exceptions.	Chief Enterprise Architect (Chair), senior architects from key MCDAs, domain leads (Security, Data, Infrastructure).

Domain Working Groups (Technical)	Specialized, often temporary, groups formed to develop and maintain standards within a specific architectural domain (e.g., Cloud Security Working Group, AI Ethics Working Group and provide recommendations to the AGB for adoption.	Technical subject matter experts from across government and consultants.

GRM ROLES AND RESPONSIBILITIES

In as much as specific operational details of architecture governance must be aligned to the unique context and environment of each MCDA, there also exists universally recognized architectural roles critical to the effective development, implementation, and management of GEA. These roles form the core of the governance structure and are typically positioned within the architecture team or board. The key roles include:

Role	Responsibilities
Chief Enterprise Architect (CEA)	• Provides strategic leadership and direction for the EA program • Aligns architecture initiatives with business strategy • Directs architecture governance and artefact lifecycle • Acts as primary liaison between business and architecture teams
Enterprise Business Architect	• Models business strategy, capabilities, and processes • Aligns business goals with IT strategy- • Supports business transformation and future-state planning
Enterprise Application Architect	• Designs and manages the enterprise application portfolio • Establishes application standards and integration strategies • Enhances application interoperability and reduces redundancy
Enterprise Data Architect	• Defines data architecture strategy and standards • Ensures data consistency, quality, and governance • Supports data accessibility and regulatory compliance
Enterprise Technology Architect	• Establishes infrastructure and platform standards • Defines technical reference models and tools • Ensures scalability, sustainability, and compatibility of technologies
Enterprise Security Architect	• Develops and enforces enterprise security architecture • Integrates security controls across all architectural layers

	• Manages data protection, access control, and identity governance

Successful rollout and adoption of the Government Enterprise Architecture requires a strong governance framework to ensure consistency, compliance, accountability, and continuous improvement across MCDAs.

This governance strategy sets out the structures, roles, and mechanisms that will guide the coordinated implementation of GEA and the Government Interoperability Framework (GIF) while providing transparency and accountability.

ARCHITECTURE COMPLIANCE PROCESS

This governance model outlines the detailed, end-to-end process that all major ICT projects must follow to ensure they are compliant with the GEA. This process is the primary operational function of the Architecture Review Board (ARB) and is designed to be both rigorous and agile, providing clear guidance to project teams while safeguarding the integrity of GEA.

Stage	Key Actions	Primary Responsibility	Key Outcome
Project Initiation & Submission	Prepare a standardized 'Architecture Brief' document. Submit the brief to the ARB secretariat via a central management portal.	Project Team	Project is formally logged for review.
ARB Triage & Review Scoping	Conduct an initial assessment of the project's cost, complexity, risk, and impact. Assign a review path (Full or Delegated).	ARB Secretariat	The project team is notified of the review path, timeline, and requirements.
Detailed Compliance Review	Conduct a thorough evaluation of the Architecture Brief for conformance with GEA standards. Involve	ARB (or its delegate) & Domain Working Groups	A comprehensive understanding of the project's architectural conformance is achieved.

	Domain Working Groups for SME input. Hold a formal review meeting.		
ARB Decision & Recommendations	Issue and log a formal, documented decision.	ARB	A clear decision is made: Approved, Approved with Conditions, or Rejected, with actionable feedback provided.
Ongoing Governance	For projects under Full Review, schedule and conduct periodic reviews at key project milestones (e.g., post-procurement, pre-deployment).	ARB	Continued conformance of the implemented solution with the approved architecture is ensured.
Dispensation (Exception) Process	Formally request a temporary exception from a GEA standard, providing business justification, risk assessment, and a mitigation plan.	Project Team (to request), ARB (to approve/deny)	A formal, documented, and risk-assessed deviation from a standard is either granted or denied.

STRATEGIC CONTROL FRAMEWORK

In the context GEA, implementing the digital transformation vision necessitates the execution of large-scale, complex, and often centralized digital transformation projects. These initiatives are increasingly being deployed through Public-Private Partnership (PPP) models, wherein both risk and control are shared between the Government and the Service Provider. Such strategic agreements aim to assign specific risks to the best entity equipped to manage them effectively.

MCDAs while leveraging private sector efficiencies, retains ultimate accountability for ensuring legal and regulatory compliance and protecting citizen data and digital infrastructure.

To uphold this responsibility, it is essential to establish a **Strategic Control Framework** that empowers the Government to oversee and influence critical aspects of the IT ecosystem, even when operational control resides with the Service Provider.

Strategic Control is the set of mechanisms a client organization (MCDA) uses to ensure that a service provider's actions and outputs remain tightly aligned with the client's long-term goals, policies, and risk appetite, without micromanaging the Service Provider's day-to-day internal operations. In context, it refers to the Government's institutionalized authority to design, verify, and ensure that the implemented systems are implemented:

- Align with the Government Enterprise Architecture,
- Fully conform to relevant laws and policies,
- Maintain the integrity and security of core systems and services.

This control is not limited to oversight but includes embedded technical and administrative privileges necessary to enforce compliance throughout the system's lifecycle.

ADOPTING THE STRATEGIC CONTROL FRAMEWORK

A Strategic Control Framework doesn't introduce a new level bureaucracy, rather it is implemented by extending the existing roles and processes defined in the Governance Architecture to oversee external Service Providers.

Key control points are established through:

Control Point	Implementation	Responsibility
Policy and Architectural Standards	All procurement documents and contracts for PPPs or outsourced services must legally mandate conformance with the relevant sections of the GEA. The SP must deliver a service that conforms to the GEA principles	Architecture Review Board (ARB) is responsible for defining which specific GEA standards are applicable to a given project or service.
Contractual Agreements & SLAs	This control mechanism translates the architectural requirements into legally binding obligations by	GEA Steering Committee provides strategic direction, while the ARB provides the

	including specific, measurable Service Level Agreements (SLAs) directly derived from the GEA domains e.g. (security, information, integrations, etc.)	specific technical clauses and KPIs to be embedded in the contracts.
Architectural Review	The government retains the right to approve the provider's technical solution before it is built and deployed through Architecture Compliance Process The provider must submit their design to the ARB. to verify that the provider's design conforms to the GEA's principles and standards.	This directly uses the Architecture Compliance Process model, with the service provider acting as the 'project team' for the purpose of the review.
Continuous Monitoring and Audit Rights	This control provides ongoing assurance that the SP is operating within the agreed-upon architectural and security boundaries. GEA defines a set of KPIs and gains the right to monitor them through AGB. This includes receiving performance reports, security incident logs, and, crucially, the right to conduct its own independent audits to verify the provider's conformance.	AGB (in coordination with Security Operations) KPIs defined in the GEA domains (e.g., MTTD/MTTR from the Security Architecture) become the basis for the monitoring framework

GEA LIFECYCLE MANAGEMENT

The Lifecycle Management model defines the continuous process for keeping the GEA framework itself current, relevant, and effective, ensuring it adapts to technological advances and evolving national priorities. This model is explained in the table below.

Stage	Key Actions	Responsibility	Key Outcome
Monitor	Continuously scan for inputs like new technology trends, legislative changes, and	ARB Secretariat, Domain Working	A curated log of potential architectural drivers and issues.

	feedback from compliance reviews and strategic directives.	Groups, GEA Steering Committee	
Assess	Formally analyze monitored inputs, determine their impact on the GEA, and produce an 'Impact Assessment Report'.	ARB & Domain Working Groups	Change Proposal document that details the identified gaps and the proposed remedy.
Update	Draft specific changes to the GEA, and submit the draft for formal review, debate, and approval/ratification.	Domain Working Groups, ARB, GEA Steering Committee	An updated and version-controlled GEA document.
Communicate & Train	Publish updated GEA documents to a central repository, issue official communications, and organize/deliver training workshops.	ARB Secretariat, Chief Enterprise Architect, Domain Working Groups	A stakeholder community that is aware of and understands the latest architectural standards and equipped to handle EA tasks and deliverables
Enforce	Apply the updated standards as the new baseline within the Architecture Compliance Process for all new and ongoing projects.	ARB	Realized value from the GEA update, with feedback flowing back into the Monitor stage for continuous improvement.

KEY STANDARDS & FRAMEWORKS

To ensure consistency and alignment with global best practices, the GEA Governance model will be guided by and integrate with established international best practice standards and frameworks for IT and architecture governance. The following frameworks will inform the structure and processes of the GEA:

Standard	Description & Application
COBIT	A leading framework for the governance and management of enterprise IT. It will be used to structure the overall IT governance processes within which the GEA operates.

TOGAF	The Open Group Architecture Framework provides a detailed method and set of supporting tools for developing enterprise architecture. GEA is aligned with TOGAF principles.
ISO/IEC 38500	The international standard for the corporate governance of IT. It provides guiding principles for directors on the effective, efficient, and acceptable use of IT.
ITIL	A framework for IT Service Management (ITSM). The GEA governance process will integrate with ITIL processes to ensure that architectural designs are operationally sound.

KEY PERFORMANCE INDICATORS (KPIs)

To measure the effectiveness and adoption of the Governance Architecture, the following KPIs will be tracked and reported on by the ARB. These KPIs provide tangible metrics to assess the success of the governance function.

KPI	Description	Target
Project Compliance Rate	The percentage of new ICT projects reviewed is found to be fully compliant with the GEA.	Achieve a 90% compliance rate for all major projects within two years.
Architecture Review Turnaround Time	The average time taken for the ARB to complete a compliance review and issue a decision for a new project.	An average turnaround time of no more than 15 working days.
Number of Approved Exceptions	The number of projects granted a formal, documented exception to GEA standards per year.	A decreasing trend in exceptions, indicating that architecture is becoming more effective and widely adopted.

GEA RISK MANAGEMENT FRAMEWORK

The implementation of the Government Enterprise Architecture (GEA) is a strategic transformation program of national strategic significance. Its scope, complexity, and interdependencies across MCDAs introduce substantial organizational, technical, and operational risks far higher than conventional ICT or digital projects. Unmanaged or inconsistently managed risks at this scale have the potential to:

- Undermine national digital transformation objectives
- Disrupt essential public services
- Compromise data security, sovereignty, and privacy
- Erode public trust and confidence

Risk as the effect of uncertainty on objectives. Uncertainty is doubt – the possibility of a different outcome, whether more positive or negative, than the expected one. - ISO 31000

A disciplined and structured Enterprise Risk Management (ERM) approach is therefore fundamental to ensure that risks are identified, evaluated, and treated systematically, across all GEA architecture domains and lifecycle phases, to protect public value and sustain transformation outcomes.

OBJECTIVES OF THE RISK MANAGEMENT FRAMEWORK

Risk management refers to coordinated activities to direct and control an organization regarding risks. Simply put, risk management is the method of dealing with possible dangers that threaten an organization's objectives.

The objectives of this framework are to:

- Embed risk-aware decision-making into GEA governance, architecture design, investment planning, and implementation
- Ensure consistent risk identification, classification, and assessment across all MCDAs
- Clarify risk ownership, accountability, and acceptance authority
- Integrate Enterprise Risk Management (ERM) with Enterprise Architecture practice
- Protect public value while enabling controlled innovation and transformation

Risk management within GEA is not a parallel activity; it is a core governance discipline that underpins architecture integrity, interoperability, security, and long-term sustainability.

GEA builds capabilities across people, processes, technology, and information, and these assets are inherently exposed to multiple risk sources, including governance, security, financial, and interoperability factors. The GEA Risk Management Framework attempts to integrate Enterprise Architecture and Risk Management disciplines, ensuring that architects and program leaders proactively manage risk and uncertainty.

SCOPE AND APPLICATION

This Risk Management Framework applies to:

- All GEA architecture domains
- All GEA lifecycle phases, aligned to the Architecture Development Method (ADM)
- All MCDA-led initiatives that adopt, extend, or implement GEA-aligned capabilities
- Shared platforms, national registries, and cross-government digital services

All architecture artefact, solution design, procurement, or implementation milestone will be approved after providing an accompanying documented risk assessment and treatment plan.

RISK MANAGEMENT METHODOLOGY

GEA adopts the ISO 31000 risk management methodology to provide guidelines that enable organizations of any sector or industry to identify, assess, evaluate, and treat risks in a systematic and cost-effective way. The purpose of this standard is to develop a risk management approach and awareness of the importance of monitoring and managing risks among employees and stakeholders.

ISO 31000 provides principles, a framework, and a process to help organizations, of any size or any industry, manage risks in a systematic and cost-effective way. Its principles, framework, and process allow for the management of any type of risk (e.g., information security risks, business continuity risks, financial risks, environmental risks, quality risks, etc.).

Contrary to the widely used financial-based risk management standards and models, ISO 31000 is a standard that can be easily implemented easily by any public, private sector, or non-governmental organization, regardless of its size or field of activity.

This is visually depicted in Figure 23 below. Managing risk starts with establishing the context and continues through sections of risk assessment, risk treatment, recording and reporting, monitoring and reviewing, and communicating and consulting.

Figure 25 - ISO 31000:2018 Risk Management Process

RISK MANAGEMENT FRAMEWORK ALIGNMENT

GEA's Risk Management Framework adopts the principles, framework, and process model of ISO 31000:2018 which promotes integration, structure, inclusivity, and continual improvement, ensuring that risk management supports decision-making and the achievement of government objectives.

ISO 31000:2018 Component	GEA Application
Principles	Establish a value-driven, structured, and inclusive approach to identifying and managing risk across MCDAs.
Framework	Integrate risk management into the GEA governance and decision-making processes, ensuring top management commitment and adequate resources.
Process	Apply a cyclical and adaptive risk management process encompassing context establishment, risk assessment, risk treatment, communication, and monitoring.

RISK MANAGEMENT STRUCTURE

Element	GEA Implementation Focus
Mandate and Commitment	The National GEA Steering Committee and MCDA leadership establish risk policy, assign ownership, and ensure alignment with national cybersecurity and ICT governance frameworks.
Integration into Governance	Risk management is embedded within architecture governance boards, project steering committees, and procurement workflows.
Design of the Framework	Define the risk policy, roles, responsibilities, and escalation matrix. Establish a centralized Risk Register and reporting templates.
Implementation	Integrate risk assessment and treatment into architecture design, project initiation, and solution delivery phases.
Evaluation and Review	Periodically assess framework effectiveness, ensuring alignment with evolving national policies and emerging risks.
Continual Improvement	Update risk methodologies, tools, and metrics based on incident analysis, audits, and post-implementation reviews.

RISK MANAGEMENT PROCESS

The GEA adopts a structured and iterative process that ensures continuous identification, evaluation, and treatment of risks across all domains.

Phase	Key Activities	Outputs

Establish the Context	Define internal and external factors, stakeholder expectations, and scope of risk management across GEA domains (BRM, TRM, ARM, GRM)	Context Statement, Risk Policy, Governance Map.
Risk Identification	Identify threats and opportunities through workshops, interviews, and analysis of historical project data. Use the Standardized GEA Risk Taxonomy	Comprehensive Risk Register.
Risk Scoring Analysis	Assess likelihood and impact using quantitative and qualitative criteria (e.g., 5x5 matrix). Use the Risk Severity and Assessment Model	Risk Analysis Report, Heat Map.
Risk Rating and Evaluation	Rank and prioritize risks as Low, Medium, High, or Critical.	Risk Prioritization Matrix.
Risk Treatment	Select strategies to avoid, transfer, mitigate, or accept risks. Assign ownership and define mitigation plans.	Risk Treatment Plan, Control Implementation Tracker.
Monitoring and Review	Continuously track key risks via dashboards and quarterly reviews by governance boards.	Risk Monitoring Reports, Updated Risk Register.
Communication and Consultation	Maintain transparent, timely communication with stakeholders and escalation channels.	Stakeholder Communication Logs, Governance Briefings.

GEA RISK TAXONOMY

GEA mandates the use of the following standard enterprise risk taxonomy across all risk registers, reports, and assurance activities to eliminate inconsistency and subjectivity. Every identified risk must be assigned one primary risk category and may reference secondary impacts.

Risk Category	Definition
Strategic Risk	Risks that threaten national objectives, policy alignment, funding continuity, or long-term public value
Operational Risk	Risks arising from people, processes, institutional capacity, or execution failures

Risk Category	Definition
Compliance & Legal Risk	Risks of non-compliance with laws, regulations, policies, and mandatory standards
Technology Risk	Risks related to systems, platforms, infrastructure, interoperability, and vendor dependency
Security & Privacy Risk	Risks affecting confidentiality, integrity, availability, privacy, and national digital assets
Reputational Risk	Risks that may damage public trust, credibility, or confidence in government services

RISK FACTORS

Due to its scale and complexity, the risk profile of the entire GEA program exceeds that of a typical ICT project within an MCDA, necessitating robust risk management, therefore foundational to program success. The key risk factors are identified below

Category	Description
Extensive Scope	GEA spans 8 architecture domains and sectoral systems, increasing coordination and planning complexity.
Architectural and Operational Complexity	Implementation requires precise alignment across disparate design layers and integration of legacy systems while maintaining interoperability and standard compliance.
Prolonged Implementation Cycles	Multi-phase deployment introduces long-term dependencies, evolving risks, and coordination challenges.
High Degree of Interdependency	Cross-agency dependencies and varying maturity levels can disrupt uniform adoption of standards and integration schedules.

Enterprise Architects implementing the GEA framework must help MCDAs manage risk through architectures that help avoid, transfer, mitigate, or accept adverse risks, because risks are inherent in any opportunities that the enterprise may embrace. ERM and security are therefore concerns that cut across all GEA domains.

GEA approaches Enterprise Risk Management practices by:

- Understanding various risk categories, the assets exposed to risks in each category, and the relationships between different risks
- Defining risk assessment methods
- Guiding risk management processes
- Integrating ERM into the Enterprise Architecture practice

RISK ASSESSMENT MODEL

The GEA Risk Severity and Assessment Model establishes a uniform, evidence-based mechanism for evaluating risk exposure across all MCDAs.

Its purpose is to eliminate subjective interpretation, ensure comparability of risks, and enable consistent escalation and decision-making at national level. Risk is assessed using two mandatory dimensions:

- Likelihood (probability of occurrence)
- Impact (severity of consequence on government objectives)

The resulting risk score determines governance action, escalation level, and treatment priority.

Level	Description
1 – Rare	Unlikely to occur during the program lifecycle
2 – Unlikely	Possible but not expected
3 – Possible	Could occur under certain conditions
4 – Likely	Expected to occur
5 – Almost Certain	Occurs frequently or repeatedly

IMPACT SCALE

Level	Description
1 – Insignificant	Minimal impact, no service disruption
2 – Minor	Localized and recoverable impact
3 – Moderate	Measurable service or delivery impact
4 – Major	Significant cross-MCDA or political impact
5 – Severe / Critical	National impact, legal breach, or loss of public trust

RISK RATING AND ESCALATION

Score	Risk Level	Governance Action Required
1–4	Low	Managed at project level
5–9	Medium	MCDA senior management oversight
10–16	High	Escalation to GEA governance bodies
17–25	Critical	National GEA Steering Committee decision

RISK SCORING METHOD

Risk Score = Likelihood × Impact

Scores range from **1 to 25** and determine escalation and treatment requirements.

Score Range	Risk Level	Mandatory Governance Action
1–4	Low	Manage at project or solution team level
5–9	Medium	MCDA senior management oversight
10–16	High	Escalation to GEA Architecture & Governance Boards
17–25	Critical	National GEA Steering Committee decision required

MANDATORY EVIDENCE FOR ARCHITECTURE APPROVAL

Risk scoring must be evidence-based, not opinion-based. For every architecture submission, the following risk evidence is required:

- Primary EA domain classification
- Identified dependent domains
- Risk score (inherent and residual)
- Dependency matrix entry
- Named risk owner and acceptance authority
- Treatment plan aligned to ADM phase

Acceptance of residual risk must be explicit, documented, and approved at the correct authority level

Likelihood assessment example in the table below:

Level	Definition	Examples
1 – Rare	May occur only in exceptional circumstances	Failure of a newly commissioned Tier-III government data centre with redundant power and DR
2 – Unlikely	Could occur but not anticipated	Delays due to rare vendor insolvency on a framework contract
3 – Possible	Might occur at some point	MCDA delays adopting new interoperability standards due to skills gaps
4 – Likely	Expected to occur	Integration challenges when onboarding legacy systems to shared platforms
5 – Almost Certain	Occurs frequently or repeatedly	Resistance to change and weak adoption of shared services across agencies

Impact Scale Example

Level	Definition	GEA-Relevant Examples
1 – Insignificant	No material impact on services or objectives	Minor reporting delay with no operational effect
2 – Minor	Localized disruption, quickly recoverable	Short outage of a non-critical internal application
3 – Moderate	Service degradation affecting one or more MCDAs	Delayed rollout of a sector system impacting service turnaround times
4 – Major	Cross-MCDA impact, financial or political implications	Failure of a shared integration platform affecting multiple services
5 – Severe / Critical	National impact, legal breach, or loss of public trust	Breach of a national citizen registry or prolonged outage of a core public service

RISK INDICATORS AND EARLY WARNING SIGNALS

Indicator	Potential Issue / Interpretation
Repeated delays in milestone delivery	Resource bottlenecks or misaligned schedules.
Rising cost variances	Budget estimation or scope management deficiencies.
Conflicting stakeholder inputs	Governance misalignment or unclear accountability.
Non-adoption of standards	Compliance or interoperability breakdown.
Declining stakeholder engagement	Change management or communication gaps.

RISK MANAGEMENT TOOLS AND TEMPLATES

Tool / Template	Purpose
Risk Register	Centralized repository capturing risks, categories, likelihood, impact, mitigation strategies, owners, and status.

Risk Heat Map	Visual representation of prioritized risks to guide focus on high-severity threats.
Impact–Likelihood Matrix	Quantitative and qualitative evaluation of risk exposure.
Risk Response Plan	Structured mitigation strategy outlining risk owner, timeline, and control measures.

Sample High-Level Risk Register Template

ID	Risk Description	Category	Likelihood	Impact	Rating	Mitigation Strategy	Owner	Status
R1	Legacy system cannot integrate with new platform	Technology	High	High	Critical	Develop API bridge; phased integration strategy	CIO	In Progress
R2	Insufficient skilled personnel for EA rollout	Human Capacity	Medium	High	High	Implement accelerated training and mentorship programs	HR Directorate	Ongoing
R3	Data privacy breach in shared environment	Security	Medium	Very High	Critical	Enforce encryption, IAM, and compliance with Data Protection Act	CISO	Controlled

KEY PERFORMANCE INDICATORS (KPIS)

To ensure measurable effectiveness, risk management will be monitored using quantifiable KPIs:

KPI	Target / Threshold
% of critical risks with active mitigation plans	≥ 95 %
Frequency of risk register updates	Quarterly minimum
% of projects aligned with enterprise risk policy	≥ 90 %
Average time to close identified high-risk issues	≤ 30 days
Number of unmitigated audit findings	0 critical, ≤ 2 major per review cycle

By adopting the risk management framework into the GEA governance and architecture lifecycle, MCDAs achieve complete visibility of enterprise risks across all architecture domains, proactive mitigation through structured assessment and continuous monitoring, stronger accountability with clearly defined ownership and escalation and resilient implementation of GEA initiatives that are predictable, transparent, and auditable.

INTEGRATION WITH GEA GOVERNANCE AND ADM

Risk management within GEA is architecturally anchored, not administratively layered meaning that material risk must be understood in terms of where it originates within the Enterprise Architecture, how it propagates across domains, and how it affects downstream delivery, assurance, and service outcomes.

GEA therefore mandates domain-based risk mapping and explicit dependency analysis as part of architecture development, review, and governance.

Mandatory EA Domain Risk Mapping

All identified risks shall be mapped to the following eight canonical EA domains. This mapping is non-optional and forms the foundation for escalation, treatment, and assurance. Each Risk must identify:

- One primary EA domain of origin
- One or more dependent domains impacted

EA Domain	Risk Focus	Risk Triggers
Business	Strategy, policy, services, operating models	Policy misalignment, unclear service ownership, unfunded mandates
Data	Data ownership, quality, standards, sovereignty	Inconsistent master data, unclear stewardship, cross-border data exposure
Application	Functional fit, reuse, lifecycle, coupling	Redundant systems, proprietary platforms, lack of APIs
Technology	Infrastructure, hosting, resilience, scalability	Obsolete platforms, weak DR, single points of failure

EA Domain	Risk Focus	Risk Triggers
Integration	Interoperability, orchestration, dependencies	Non-standard interfaces, tight coupling, brittle integrations
Security	Cybersecurity, privacy, identity, trust	Weak IAM, inadequate encryption, limited monitoring
Governance	Decision rights, compliance, enforcement	Weak architecture enforcement, fragmented oversight
Human Capacity	Skills, roles, institutional capability	Skills gaps, reliance on vendors, resistance to change

GEA DOMAIN DEPENDENCY LOGIC

The dependency logic basically describes how risk propagates through the EA lifecycle. It recognizes that risk is systemic, therefore, the failures in upstream domains inevitably degrade downstream domains.

Canonical Dependency Relationships

The dependency logic below must inform risk scoring and treatment, not just documentation.

Primary Domain	Dependent Domains	Risk Propagation Logic
Business	Data, Application, Human Capacity	Poor service design leads to fragmented systems and weak accountability
Data	Application, Integration, Security	Poor data standards increase integration failures and security exposure
Application	Integration, Technology	Non-modular systems increase coupling and infrastructure load
Technology	Security, Integration, Operations	Weak infrastructure undermines security and availability
Integration	Business, Application	Integration failures disrupt end-to-end services
Security	All Domains	Security breaches disrupt services and erode trust

Primary Domain	Dependent Domains	Risk Propagation Logic
Governance	All Domains	Weak enforcement leads to systemic non-compliance
Human Capacity	All Domains	Skills gaps degrade design, delivery, and operations

INTEGRATION WITH ADM PHASES

Risk assessment is embedded into ADM deliverables, not appended at the end. No ADM phase may be approved without evidence that domain-specific risks have been identified and assessed.

ADM Phase	Primary EA Domains	Mandatory Risk Focus
Preliminary & Architecture Vision (Phase P&A)	Business, Governance	Mandate clarity, funding continuity, policy alignment
Business Architecture and Human Capital Architecture (Phase B1 &B2)	Business, Human Capacity	Operating model feasibility, service ownership
Application Architecture (Phase C1)	Application, Integration	Reuse, modularity, API readiness
Data Architecture (Phase C2)	Data, Security	Data standards, stewardship, privacy
Technology Architecture (Phase C3)	Technology, Security	Resilience, scalability, DR
Opportunities & Solutions (Phase E)	Application, Technology, Governance	Vendor risk, solution viability
Migration Planning	Integration, Human Capacity	Dependency sequencing, change readiness

ADM Phase	Primary EA Domains	Mandatory Risk Focus
(Phase F)		
Implementation Governance (Phase G)	Governance, Security	Control effectiveness, deviation risk
Architecture Change Management (Phase H)	All Domains	Emerging and residual risks

Risk Dependency Matrix (Mandatory Control Artifact)

Every GEA-aligned program or major initiative shall maintain a Risk Dependency Matrix as mandatory control artifact. This matrix makes cross-domain risk visible and prevents isolated mitigation actions.

Any **High** or **Critical** risk with two or more dependent domains automatically escalates to GEA governance bodies.

Sample Risk Dependency Matrix

Risk ID	Primary Domain	Dependent Domains	Risk Description	Risk Level
R-01	Data	Application, Integration, Security	No common data standards across MCDAs	High
R-02	Application	Integration, Technology	Legacy systems lack API capabilities	High
R-03	Human Capacity	Governance, Security	Shortage of cybersecurity skills	Medium
R-04	Governance	All Domains	Weak enforcement of GEA standards	Critical

Integration with GEA Governance Structures

Risk oversight responsibilities are clearly aligned to governance layers. No MCDA should accept cross-domain High or Critical risks independently.

Governance Body	Risk Accountability
National GEA Steering Committee	Strategic and Critical risks, cross-government dependencies
Architecture Review Board (ARB)	Domain alignment and dependency validation
Programme Steering Committees	Delivery, sequencing, and integration risks
MCDA Architecture Teams	Risk identification and mitigation execution

TRANSITION PLAN AND ROADMAP

The Government Enterprise Architecture (GEA) Transition Plan provides a structured, enforceable roadmap to guide Kenya's public sector from today's fragmented digital environment to an integrated, interoperable, and citizen-centric digital government ecosystem.

GEA is not an ICT project; it is a whole-of-government governance and transformation discipline that ensures public investments in digital systems are coherent, reusable, secure, and aligned to national priorities. The successful implementation GEA framework is dependent on a well-defined iterative transition plan with a clear implementation roadmap. The GEA roadmap establishes the rules, platforms, and governance mechanisms required to enable cross-government integration, data sharing, and modern service delivery.

Achieving the target-state architecture requires a phased, structured approach supported by strong governance, capacity building, and institutional alignment. This section outlines the strategy and roadmap for guiding Kenya's public sector from the current fragmented state to an integrated, future-ready digital ecosystem.

STRATEGIC APPROACH

The transition plan for GEA implementation will typically follow and agile iterative, risk-aware, and enforceable approach, drawing from established TOGAF's Architecture Development Method (ADM) enterprise architecture methodology and agile architecture practices. This approach will include:

- Incremental delivery every 6–12 months
- Continuous architecture and delivery feedback loops
- Mandatory compliance integrated into budgeting and procurement
- Strong governance with clear enforcement authority

The plan explicitly recognizes that architecture is not delivered once, but will evolve iteratively through controlled change, continuous learning, and incremental value realization.

The transition will occur across three main phases: Foundational (Year 1–2), Expansion (Year 3–5), and Maturity (Year 6–10).

Guiding Principles for Transition

Principle	Description
Incremental and Iterative	Implementation proceeds in defined increments aligned to ADM cycles, delivering measurable value every 6–12 months
Risk-Aware	Transition plans must factor in legacy dependencies, data sensitivity, and cybersecurity risks to inform sequencing decisions.
Citizen-Focused	Every milestone must prioritize improvements to public service delivery and citizen impact and not modernization alone.
Institutionally Aligned	Architectural decisions must integrate with government budgeting, procurement, and oversight processes.
Data-Driven	Progress and compliance should be continuously measured using GEA maturity models and interoperability maturity indicators.

These guiding principles shall be operationalized through mandatory architecture review gates, ICT investment prioritization criteria, procurement requirements, and periodic GEA and interoperability maturity assessments.

TRANSITION APPROACH

The transition plan adopts an iterative, incremental approach, drawing from:

- TOGAF Standard
  - Architecture Development Method (ADM)
  - Architecture Governance and Implementation Governance
  - Continuous Architecture capability
- Agile Architecture principles
  - Just-enough architecture
  - Incremental delivery of architectural value
  - Continuous feedback between strategy, delivery, and operations

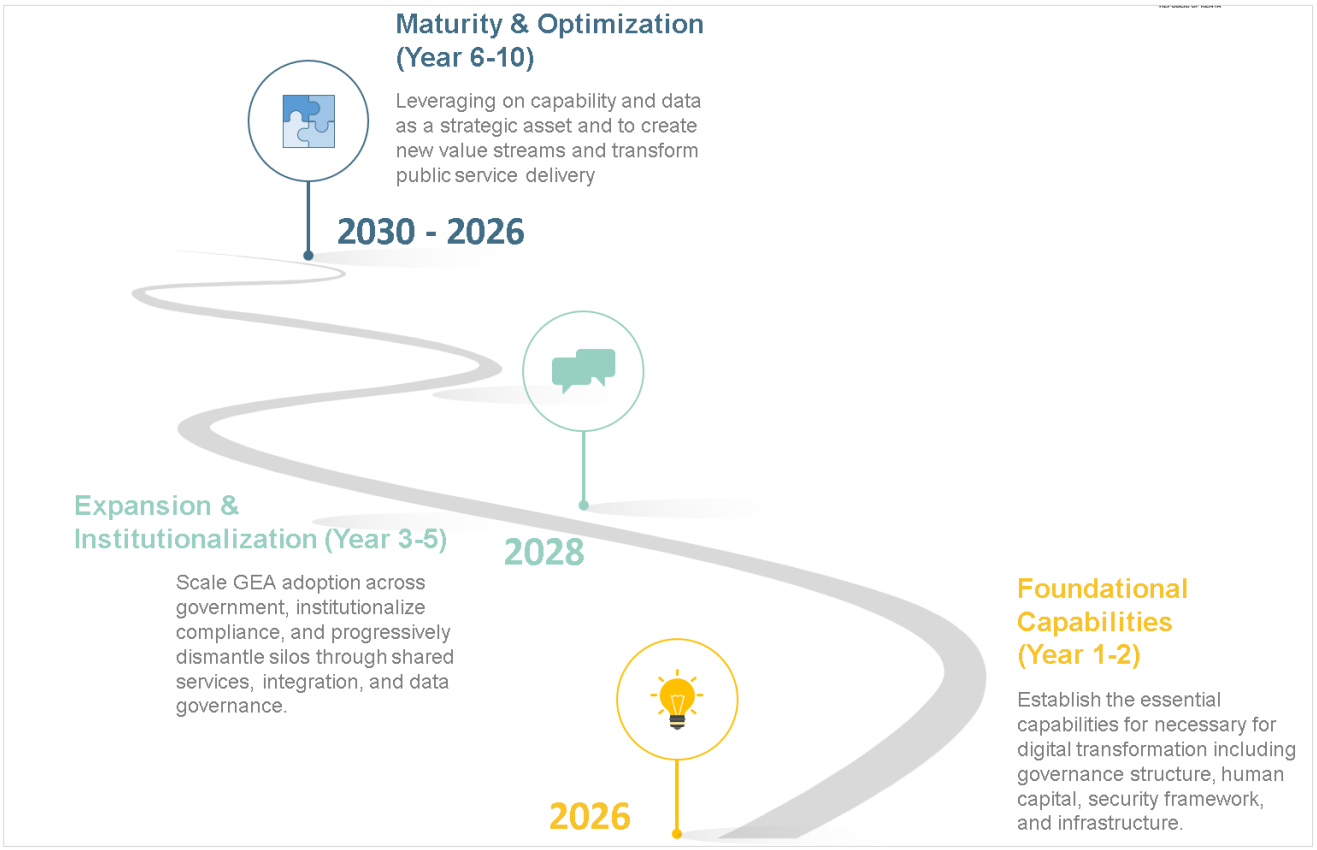

Figure 26 - GEA Maturity Roadmap

Architecture development and implementation will be executed in repeating cycles, not linear phases. Each cycle produces:

- Updated architectures (baseline, transition, target)
- Prioritized implementation increments
- Measurable outcomes and lessons learned

The architecture decisions are thereafter validated through to ensure that GEA remains relevant, adaptive, and enforceable over a multi-year transition plan.

PHASE 1 - FOUNDATIONAL CAPABILITIES (YEAR 1 – 2)

This phase focuses on establishing the essential bedrock for digital transformation. The objective is to set up the legal, governance, architectural, and institutional foundations required to enable consistent adoption of GEA and interoperability across government. Its success lays the groundwork for the subsequent phases and initiatives.

Objectives	Key Activities
Establish the legal, governance, architectural, and institutional foundations required to enable consistent adoption of GEA and interoperability across government.	• Enact GEA/GIF policy, regulations, and governance structures including the Oversight Board • Define architecture principles, standards, and interoperability framework • Conduct baseline EA maturity assessments across MCDAs • Establish EA repository and tooling • Design and implement core Government Integration Platform (GIP) capabilities • Establish national data catalogue, metadata standards, and API registry • Appoint GEA officers across MCDAs • Deliver training and certification programmes • Launch pilot integrations in priority sectors • Establish compliance gates and governance processes

Key outcomes include

- GEA/GIF regulations enacted
- GEA Oversight Board established with enforcement authority
- Baseline architecture and maturity assessments completed
- Government Integration Platform (GIP), data catalog, and API standards established
- Flagship pilots demonstrating early value

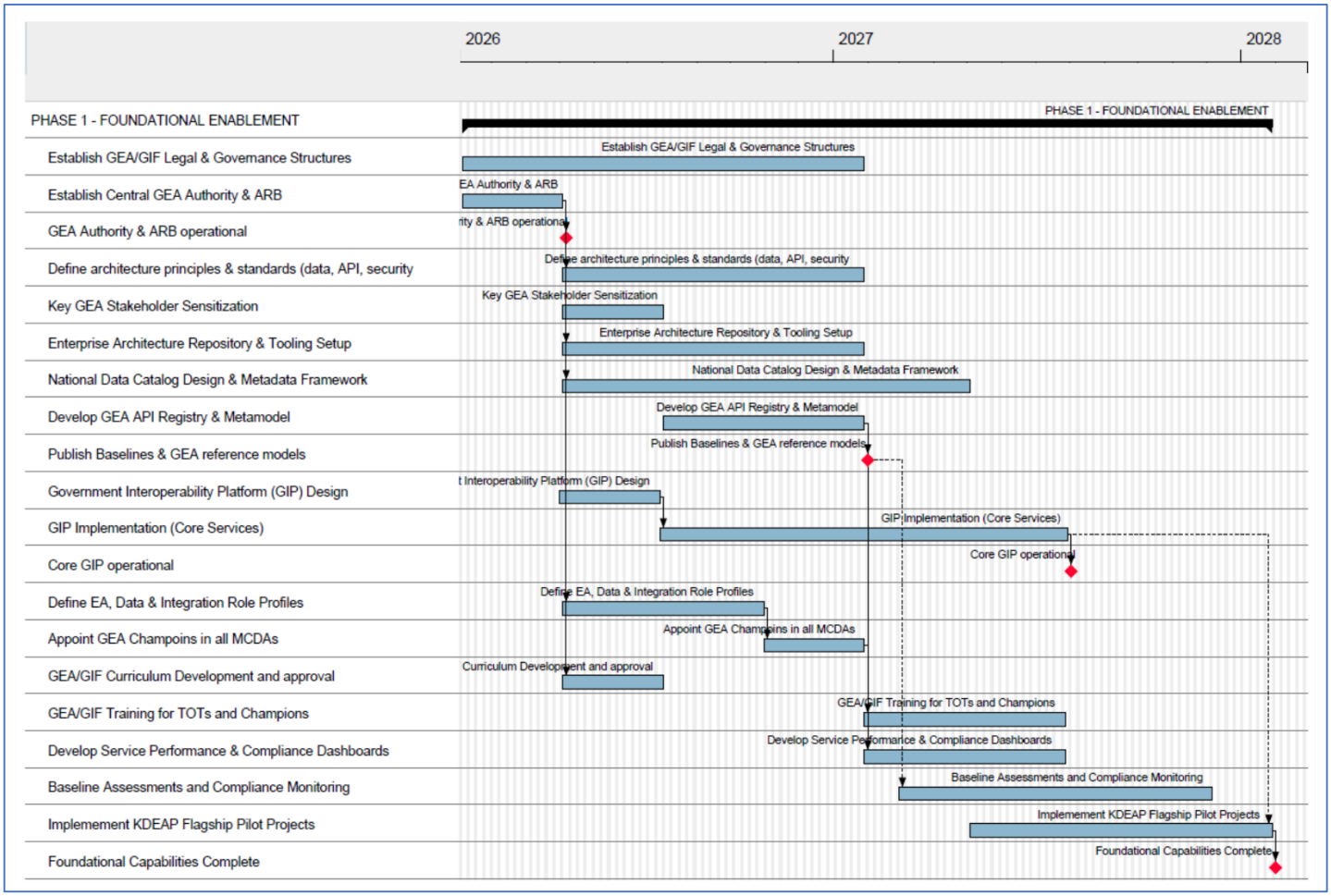

Figure 27 - GEA Phase 1 Gantt Chart

PHASE 2: EXPANSION & INSTITUTIONALIZATION (YEAR 3 – 5)

The objective of this phase is to scale GEA adoption across government, institutionalize compliance, and progressively dismantle silos through shared services, integration, and data governance.

This phase leverages the foundational structures established in Phase 1 to rationalize the existing application portfolio and begin connecting disparate systems and processes to deliver "whole-of-government" services, reduce complexity and begin breaking down silos.

Objectives	Key Activities
Scale adoption of GEA, institutionalize compliance, integrate systems and data	• Mandate GEA compliance for all new ICT investments • Integrate GEA into budgeting, procurement, and approval processes

across government, and rationalize legacy environments.	• Expand GIP integrations across priority MCDAs • Expose key national datasets through standardized APIs • Establish and operationalize Master Data Management for core entities • Rationalize and decommission redundant legacy systems • Implement cloud migration for prioritized workloads • Conduct regular EA compliance audits and performance monitoring • Expand capacity building and GEA champions network • Deliver cross-agency integrated services

Figure 28 below shows the Gantt chart representation of GEA Phase 2 Implementation

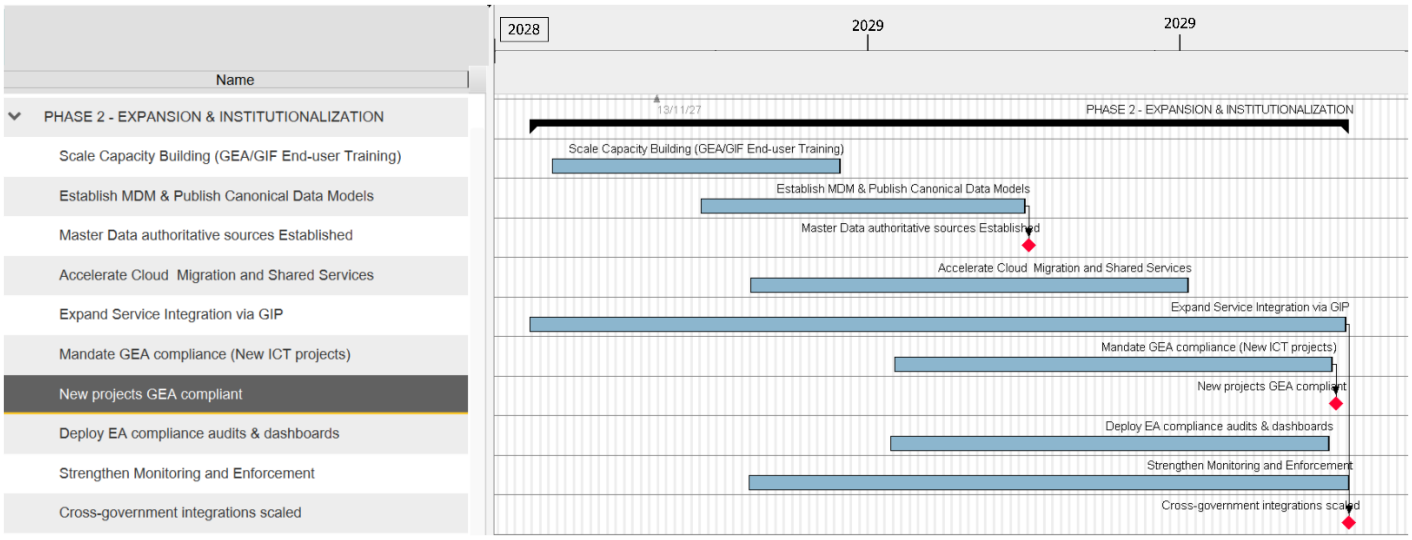

Figure 28 - GEA Phase 2 Gantt Chart

Key Outcomes

- GEA compliance mandatory for all new ICT investments
- Government Integration Platform (GIP) operational across agencies
- Key national datasets exposed through secure, standardized APIs
- Cloud and shared services adoption accelerated
- Master data governance established for citizens, businesses, and land

PHASE 3: MATURITY & OPTIMIZATION (YEAR 6-10)

This phase focuses on leveraging integrated platforms and data as a strategic asset to drive innovation, optimize service delivery, and institutionalize continuous architectural improvement.

Objectives	Key Activities
Optimize architecture, institutionalize continuous improvement, leverage data for innovation, and deliver integrated citizen-centric services at scale.	• Modernize and modularize application landscape • Strengthen enterprise data governance and stewardship • Deliver life-event and end-to-end digital services • Expand API ecosystem and digital platforms • Establish innovation sandboxes for emerging technologies (AI, analytics, automation) • Implement performance analytics and service monitoring dashboards • Conduct continuous architecture optimization and roadmap reviews • Measure outcomes including service quality, efficiency, and user satisfaction

Figure 29 below shows the Gantt chart representation of GEA Phase 3 Implementation

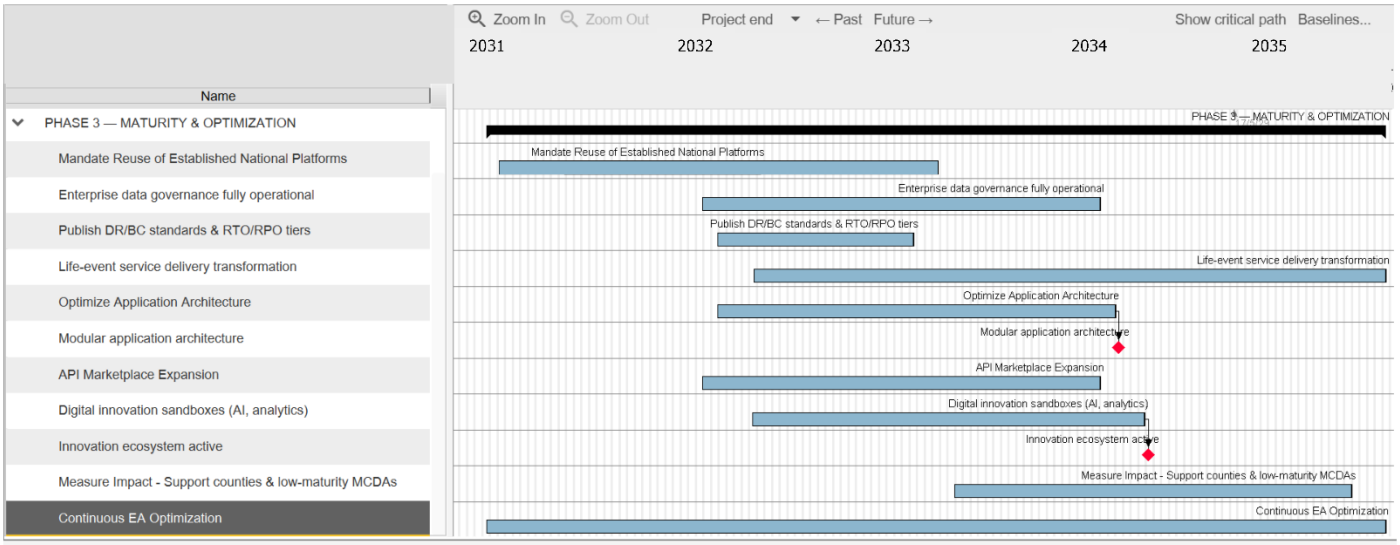

Figure 29 - GEA Phase 3 Gantt Chart

Key outcomes:

- Modular, interoperable application landscape
- Bundled services delivered around citizen life events
- Secure innovation enabled through regulated digital sandboxes
- Data governance fully institutionalized
- Measurable improvements in service quality, cost efficiency, and citizen satisfaction

Architecture roadmaps, transition states, and implementation priorities shall be reviewed at least annually, or earlier where material policy, technology, or service delivery changes occur.

MILESTONES AND KPIS

In addition to structural and compliance indicators, outcome-based KPIs shall be progressively introduced, including service turnaround times, cross-agency service completion rates, cost-to-serve reductions, and measurable improvements in citizen satisfaction.

Year	Key Milestone	Target KPI
Year 1	GEA/GIF regulations enacted	100% of ministries designated GEA focal points
Year 2	National data catalog published	60% of top 50 datasets standardized
Year 3	GIP operational across pilot MCDAs	Minimum 5 cross-agency integrations live
Year 5	GEA compliance institutionalized	80% of MCDAs with approved integration plans
Year 10	Nationwide maturity achieved	>90% EA maturity across all MCDAs

The transition roadmap ensures Kenya builds a connected and efficient digital public service ecosystem and not isolated siloes systems. The Governance and Implementation Strategy are explained in detail in the *GEA Implementation and Adoption Guide.*

INITIATIVE PRIORITIZATION FRAMEWORK

A formal prioritization mechanism is required given the scale, complexity, and interdependencies of GEA initiatives, to ensure that investments deliver maximum strategic value, manage risk, and remain executable within institutional constraints. This framework

establishes clear criteria, a scoring model, and decision rules to guide the sequencing and approval of initiatives within the GEA Transition Plan.

Alignment with Strategic Objectives

All initiatives shall be assessed for alignment with the following national and GEA strategic objectives:

1. **Whole-of-Government Integration** - Enables cross-agency interoperability and data sharing
2. **Citizen-Centric Service Delivery -** Improves service accessibility, turnaround time, or user experience
3. **Policy and Regulatory Compliance -** Supports statutory mandates, data protection, and national ICT policies
4. **Operational Efficiency and Cost Optimization -** Reduces duplication, operational cost, or technical debt
5. **Foundational Enablement -** Establishes reusable platforms, standards, or shared capabilities

Initiatives with weak or indirect alignment to these objectives shall not be prioritized, regardless of technical merit.

Prioritization Matrix: Impact vs. Feasibility

The impact-feasibility matrix helps teams prioritize and ultimately decide which initiatives are worth moving forward, on what timeline and with what effort. By mapping ideas according to how much they are in line with and can achieve set goals (impact) and whether current organizational resources can support them (feasibility), teams can sort ideas between quick wins, major projects, busy work and resource drains. In short, the matrix can help MCDAs prioritize projects/tasks, maximize efficiency and impact and align goals by visualizing how specific tasks or projects advance the set goals.

Impact regards measuring the degree to which an initiative makes attaining a specific strategic objective possible. Feasibility involves measuring the degree to which an action is possible based on an assessment of resources.

Impact Dimension

Measures the strategic and transformational value of an initiative.

Impact Indicators include:

- Contribution to interoperability across MCDAs
- Scale of citizen or business impact
- Enablement of multiple downstream initiatives
- Reduction of systemic risk or duplication
- Strategic importance to national digital priorities

Scoring (1–5):

- 1 = Marginal / localized impact
- 3 = Significant sectoral impact
- 5 = Transformational, cross-government impact

Feasibility Dimension

Measures the practical ability to deliver the initiative successfully. Feasibility Indicators include:

- Institutional readiness and stakeholder alignment
- Availability of skills and capacity
- Legal and regulatory readiness
- Technical complexity and legacy dependencies
- Funding availability and sustainability

Scoring (1–5):

- 1 = High risk / low readiness
- 3 = Moderate complexity and risk
- 5 = High readiness / low execution risk

Scoring and Assessment Guidelines

- Scoring shall be conducted by a multi-disciplinary panel (architecture, policy, ICT, service owners).
- Assumptions, risks, and dependencies must be documented for each initiative.
- Scores must be reviewed and validated by the GEA Oversight Board.
- Initiatives shall be re-scored annually or When material policy, funding, or technical changes occur

Priority Quadrants and Decision Rules

Only initiatives in the top two quadrants may be approved as part of the core GEA transition roadmap.

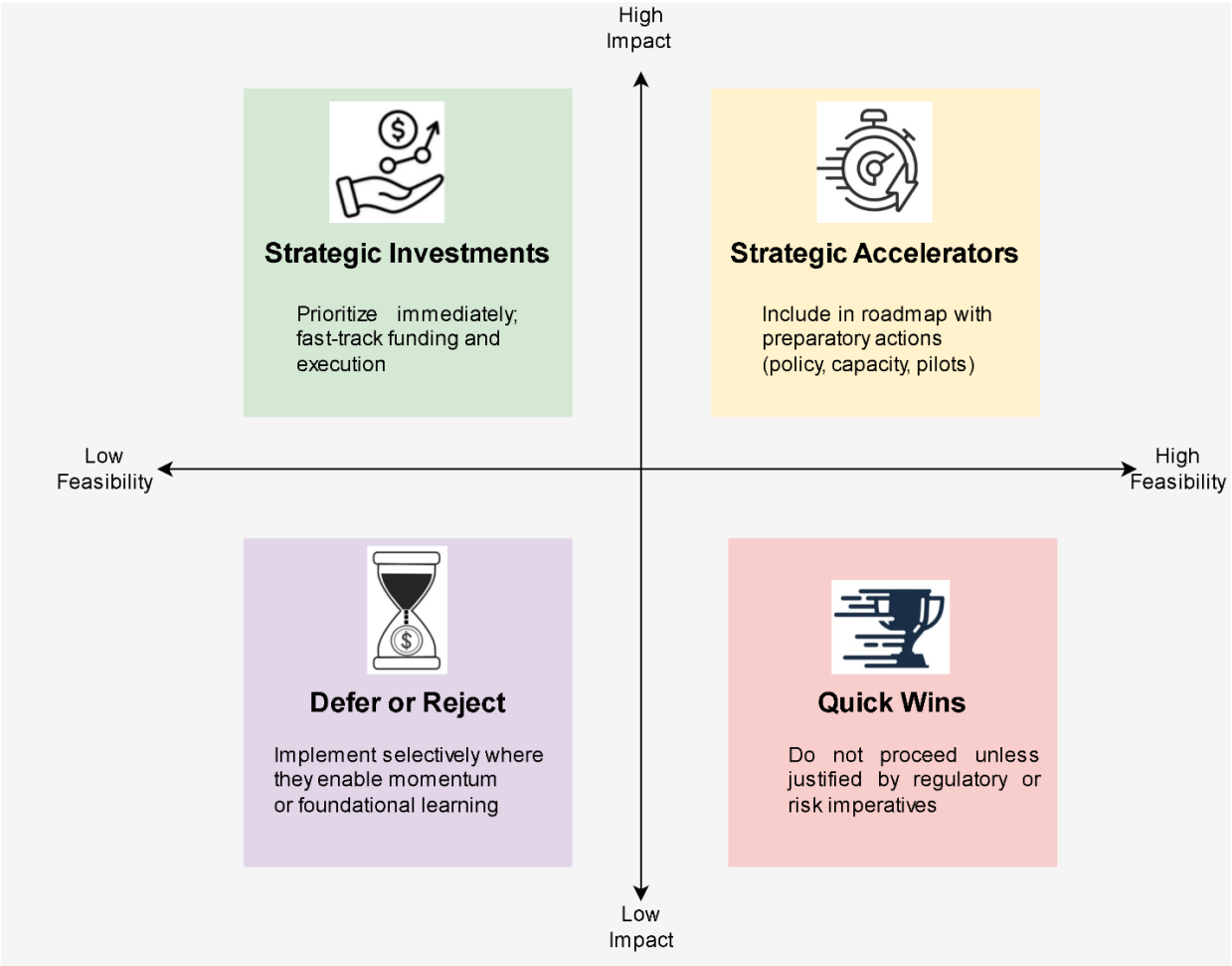

Figure 30- Impact-Feasibility Matrix

GEA GOVERNANCE INTEGRATION

To ensure that GEA priorities translate into enforceable decisions, the outcomes of the initiative prioritization process shall be formally integrated into existing government governance, investment, and oversight mechanisms described in the table below.

Integration with Investment and Budget Decisions	• Prioritization outcomes shall serve as a mandatory input into ICT investment approval processes, ensuring that only initiatives aligned to GEA objectives and whole-of-government priorities proceed to funding consideration. • Annual and multi-year budget allocations for ICT initiatives shall be explicitly informed by approved GEA priority rankings, with higher-ranked initiatives receiving preferential consideration within available fiscal envelopes. • Initiatives that do not meet minimum prioritization thresholds shall not be included in budget submissions, unless justified by statutory, national security, or critical service continuity requirements.
Integration with Procurement and Delivery	• Approved prioritization results shall guide procurement sequencing, ensuring that foundational and high-impact initiatives are implemented ahead of dependent or discretionary projects. • Procurement documentation, including tender specifications and evaluation criteria, shall reference GEA compliance and prioritization status as mandatory requirements. • ICT projects approved for procurement shall be subject to architecture compliance gates at defined stages of the procurement and delivery lifecycle.

Governance, Oversight, and Enforcement	• The GEA Oversight Board shall review and endorse prioritization outcomes and shall have authority to:
	  ○ Recommend approval, deferral, or rejection of ICT initiatives based on prioritization results
	  ○ Require remediation actions where initiatives partially meet GEA criteria.
	• Initiatives that score below agreed prioritization thresholds shall not receive funding approval, except where mandated by law or justified by national security considerations, in which case deviations shall be formally documented and approved at the appropriate executive level.

Transparency, Assurance, and Auditability	• Prioritization results and associated decisions shall be published internally within government to promote transparency, consistency, and institutional learning. • Prioritization records shall form part of the official ICT investment and audit trail, supporting internal audit, external oversight, and accountability where applicable. • Periodic reviews shall assess whether prioritization outcomes are delivering intended strategic and service-level benefits, with findings used to refine criteria and thresholds over time.

This governance integration ensures that GEA is not advisory, but a binding decision framework that shapes how government plans, funds, procures, and delivers digital initiatives protecting public investment and accelerating whole-of-government outcomes.

DEPENDENCY MAPPING AND SEQUENCING

The success of the GEA transition depends on executing strategic initiatives in the correct sequence.

This section establishes how dependencies between initiatives are identified, how the critical path is protected, and how sequencing rules are enforced to prevent fragmented investments and premature system delivery.

GEA initiatives are interlinked components of a single national digital ecosystem. Failure to respect dependencies will result in duplication, wasted investment, and limited service impact The mapping and sequencing mechanism is required to:

- Prevent premature or isolated implementations
- Protect foundational investments
- Ensure coherent, whole-of-government execution

This framework defines initiative dependencies, the critical path, and enforceable sequencing rules that govern roadmap execution.

Dependency Types

All initiatives shall be assessed against six dependency categories. An initiative may only proceed when its critical dependencies are in place.

Dependency Type	Description
Policy & Legal	Requires enabling laws, regulations, or formal mandates
Governance & Institutional	Requires clear authority from governance bodies, decision rights, or operating models to enforce compliance and resolve disputes
Architecture & Standards	Requires approved reference architectures, standards, or principles
Platform & Infrastructure	Depends on shared platforms such as the Government Integration Platform (GIP) or technical foundations
Data & Interoperability	Requires data standards, metadata, master data, and APIs
Capability & Skills	Requires institutional capacity i.e. skilled personnel, operating models, and change readiness

An initiative may have **multiple dependency types**.

Core Initiative Dependency Map

Initiative	Primary Dependencies	Finish to Start
GEA/GIF Regulations	—	—
GEA Oversight Board	GEA/GIF Regulations	Regulations enacted
EA Baseline & Maturity Assessment	Oversight Board	Governance established
National Data Catalog & Metadata Standards	Oversight Board, EA Baseline	Baseline completed
Government Integration Platform (GIP)	Governance, Standards, Data Catalog	Standards and governance in place
API Registry & Standards	GIP Architecture	Integration architecture approved
Master Data Management	Data Catalog, API Standards	Data foundations operational
Cross-Agency Service Integration	GIP, APIs, Master Data	Integration & data foundations live
Government Cloud Migration	Governance, Security Policy, GIP	Integration & security readiness
Life-Event Service Bundling	GIP, Master Data, APIs	Cross-agency integration live
AI / Digital Innovation Sandboxes	Data Governance, Platforms	Data & platform maturity

National Critical Path Identification

The following initiatives form the national GEA critical path. They must be delivered in sequence and cannot be bypassed enable all others.

1. GEA/GIF Legal and Policy Framework
2. GEA Oversight Board and Governance Mechanisms
3. Baseline Architecture & Maturity Assessment
4. National Standards (Data, Metadata, APIs)
5. Government Integration Platform (GIP)
6. Master Data Management
7. Cross-Agency Service Integration
8. Citizen Life-Event Services

Any delay or failure along this path directly impacts national digital transformation outcomes.

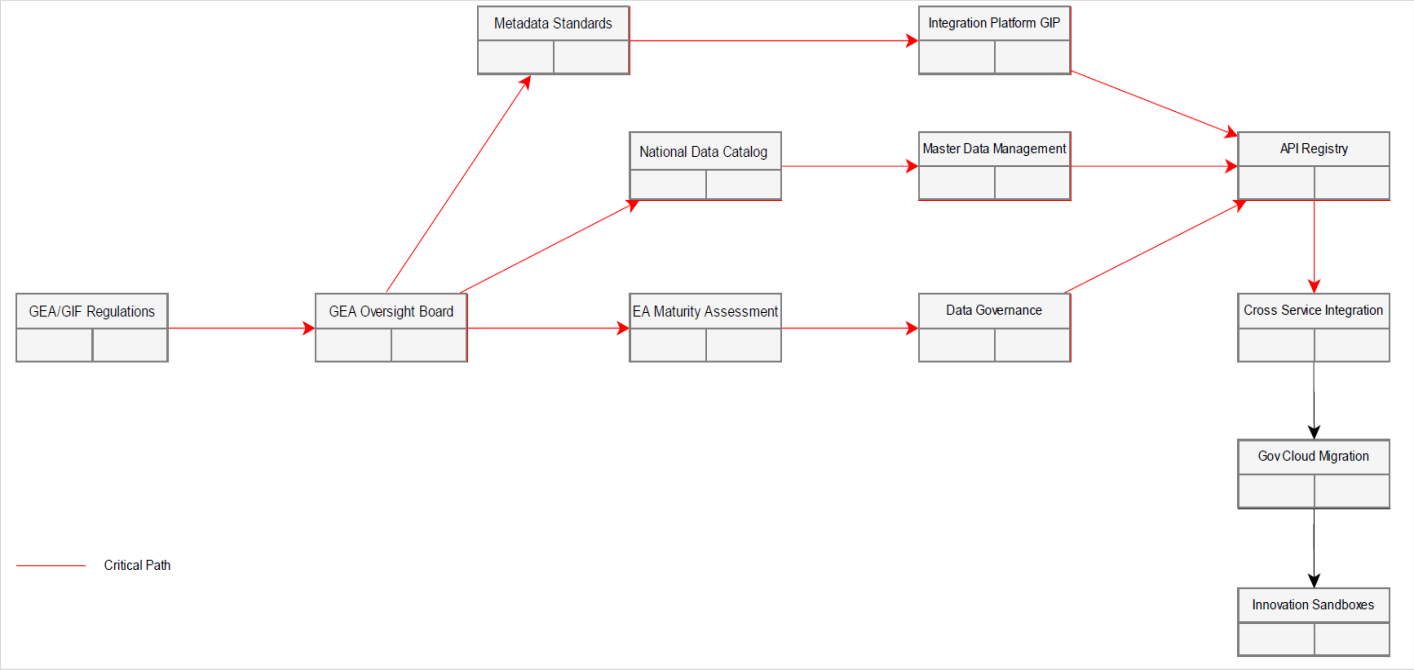

Figure 30 - GEA Dependency Diagram

SEQUENCING RULES

The following sequencing rules shall apply to all initiatives in the GEA roadmap:

Rule	Enforcement Measure
Foundation Before Consumption	No service, platform, or integration initiative may proceed unless its required governance, standards, and platforms are operational.
Integration Before Optimization	Cross-agency integration must precede application optimization, cloud migration at scale, or service bundling.
Data Before Intelligence	Advanced analytics, AI, and innovation initiatives may not proceed without established data governance, metadata, and master data foundations.
Compliance Before Funding	Initiatives that violate dependency sequencing shall not receive funding approval, regardless of urgency or visibility, unless exempted by the relevant governance bodies

Phased Scaling Only	Initiatives may scale nationally only after successful pilots demonstrate architectural compliance and dependency readiness.

GOVERNANCE AND ENFORCEMENT

All initiatives submitted for approval shall include a Dependency Declaration, confirming that the upstream dependencies satisfied and downstream impacts identified.

1. The GEA Oversight Board shall have authority to:

    - Block initiatives that bypass dependencies
    - Re-sequence initiatives to protect the national critical path
    - Resolve cross-agency dependency conflicts

2. Dependency mappings shall be reviewed:

    - Annually as part of roadmap refresh
    - When major policy, funding, or technology changes occur

3. Where dependencies are delayed, affected initiatives shall be Re-sequenced, Phased or formally paused

This dependency framework ensures the GEA roadmap is not a list of projects, but a coherent transformation journey where each initiative builds logically on the last—protecting public investment and preventing fragmentation.

FUNDING STRATEGY AND COST ESTIMATION GUIDELINES

The successful execution of the GEA Transition Plan requires a coherent, multi-year funding strategy supported by transparent, defensible cost estimation practices.

This section defines how GEA initiatives should be funded, sequenced, and sustained, while ensuring value for money, fiscal control, and alignment with national budgeting and public finance processes.

FUNDING PRINCIPLES

GEA funding shall be guided by the following principles:

1. **Foundation First -** Funding shall prioritize shared, reusable capabilities (governance, integration, data, security) before agency-specific solutions.
2. **Incremental and Phased Funding -** Funding shall be released in tranches aligned to transition phases and delivery increments, not as single upfront allocations.
3. **Value-for-Money -** Investments shall demonstrate clear contribution to service outcomes, efficiency gains, or risk reduction.
4. **Reuse Over Duplication -** Initiatives that reuse approved platforms, standards, and shared services shall receive preferential funding consideration.
5. **Sustainability** - Funding decisions shall consider full lifecycle costs, not just initial implementation expenditure.

FUNDING MODEL BY TRANSITION PHASE

Transition Phase	Funding Focus	Strategy
Foundational Capabilities (Years 1–2)	Enablement and national foundations to ensure consistency, neutrality, and enforceability across government.	Primary Funding Sources: • Central government / National Treasury allocations • Development partner and grant funding (where applicable) • Shared services budget lines Cost Categories: • Legal and regulatory development • Governance structures and oversight bodies • EA baseline assessments and maturity reviews • Integration platform design and initial implementation • Capacity building and training programs

Expansion & Institutionalization (Years 3–5)	Scaling, integration, and rationalization. Funding responsibility shall progressively shift toward MCDAs, while central funding continues to support shared and cross-cutting capabilities.	Primary Funding Sources: • Mixed funding model (central + MCDA contributions) • Reallocated savings from decommissioned legacy systems • Program-based budgeting allocations Cost Categories: • Expansion of shared platforms (GIP, data services) • Cloud and shared services migration • Master data management implementation
Phase 3: Maturity & Optimization (Years 6–10)	Optimization, innovation, and value realization. Funding shall emphasize operational sustainability and measurable service outcomes rather than new capital expenditure.	Primary Funding Sources: • MCDA operational budgets • Recurrent ICT and service delivery budgets • Public–private partnerships (where appropriate) Cost Categories: • Application refactoring and optimization • Advanced analytics and innovation sandboxes • Continuous improvement and performance management • Ongoing governance and assurance activities

COST ESTIMATION GUIDELINES

All GEA initiatives shall be costed using a standardized lifecycle-based estimation approach, covering:

A. Cost Dimensions

- Capital Expenditure (CAPEX)
  - Platforms, infrastructure, initial development
- Operational Expenditure (OPEX)
  - Licensing, hosting, support, staffing
- Change and Enablement Costs
  - Training, communication, change management
- Governance and Assurance Costs
  - Architecture reviews, audits, compliance monitoring

B. Estimation Levels

Cost estimates shall be refined progressively as initiatives mature:

Stage	Estimate Type	Purpose
Concept	Rough Order of Magnitude (ROM)	Strategic prioritization
Planning	Indicative Estimate	Budgeting and approvals
Pre-Implementation	Detailed Estimate	Procurement and contracting
Delivery	Revised Forecast	Financial control

C. Cost Drivers to be Explicitly Identified

- Number of participating MCDAs
- Volume of integrations and data exchanges
- Legacy system complexity
- Security and compliance requirements
- Skills availability and sourcing model

FUNDING GOVERNANCE AND CONTROLS

1. All initiatives seeking funding approval shall:

    - Be prioritized using the approved GEA prioritization framework
    - Demonstrate compliance with dependency and sequencing rules
    - Include a lifecycle cost estimate and funding profile

2. Funding releases shall be conditional on passing architecture and compliance gates.
3. The GEA Oversight Board shall advise Treasury and investment committees on:

    - Funding sequencing
    - Readiness to scale initiatives
    - Reallocation of funds where priorities change

BENEFITS REALIZATION AND COST RECOVERY

- Each funded initiative shall define expected benefits, including:
    - Cost avoidance through reuse
    - Reduction in duplication and maintenance
    - Service delivery improvements
- Where applicable:
    - Savings from legacy system decommissioning shall be reinvested into shared platforms.
    - Shared services may adopt cost-recovery or charge-back models over time.

FINANCIAL TRANSPARENCY AND ACCOUNTABILITY

- Funding decisions, cost estimates, and expenditure tracking shall be:
    - Documented
    - Internally published
    - Subject to audit and oversight
- Periodic financial reviews shall assess:
    - Cost variance
    - Benefit realization
    - Alignment with GEA priorities

This funding strategy ensures that the GEA transition is financially disciplined, scalable, and sustainable.

It aligns architecture priorities with national budgeting processes, protects public funds, and ensures that investments deliver measurable, whole-of-government value over time.

CONTINGENCY PLANNING AND RISK-ADJUSTED ROADMAP

The GEA Transition Plan is a complex, multi-year endeavor. This roadmap moves away from "rigid planning" toward Adaptive Governance.

This section, in anticipation, establishes a risk-adjusted roadmap approach that anticipates disruption, embeds flexibility, and defines clear fallback options to ensure continuity of progress even under adverse conditions. The objective is not to eliminate risk, but to prevent systemic failure, sunk costs, and loss of momentum.

Guiding Principles

- **Plan for Disruption, Not Perfection**: Assume environmental shifts; build systems that bend rather than break.
- **Protect the Foundation**: Core governance and integration assets take priority over high-visibility "front-end" apps.
- **Defer Scale, Not Learning:** If resources are cut, reduce the number of sites, but keep the pilot running to capture data.
- **Strategic Pausing:** It is better to resequence a project for six months than to cancel it and lose institutional memory.

Risk responses are therefore embedded within the roadmap, not treated as exceptional afterthoughts.

KEY RISK CATEGORIES AFFECTING GEA ROADMAP

Each initiative within the GEA must be mapped against these six primary risk vectors. Each initiative shall identify its primary risk exposure and associated mitigation path.

Risk Category	Key Scenarios	Strategic Mitigation
Political & Policy	Leadership change, shifting national priorities.	Institutionalize GEA via legislation/policy to outlast political cycles.
Fiscal & Budgetary	Budget cuts, macroeconomic shocks.	Implement "Tranche-Based" funding and modular delivery.
Institutional Readiness	MCDA resistance, skill shortages.	Link funding to compliance; embed "Change Agents" in ministries.
Technical & Legacy	Vendor lock-in, technical debt.	Mandate open standards and modular API-first architecture.
Cyber & Data	Security breaches, privacy constraints.	Security-by-design; "Data Sovereignty" first approach.
Delivery & Capacity	Vendor over-reliance, bottlenecks.	Hybrid teams (Gov + Vendor) with mandatory knowledge transfer.

ANTICIPATED RISK SCENARIOS

Scenario	Impact	Response / Fall Back
Budget Reductions or Delayed Funding	Stalled delivery, incomplete platforms	• Prioritize critical path initiatives only • Defer discretionary or optimization initiatives • Shift focus to standards, governance, and low-cost enablement • Extend timelines rather than fragment scope **Fall Back Rule:** Foundational governance, standards, and integration assets shall not be defunded once initiated

Institutional Resistance (Low Adoption)	Siloed system and fragmented data	• Slow national rollout; Use "Island of Excellence" pilots to prove value. • Pivot to "Gatekeeper Governance." Increase enforcement through funding and procurement gates • Introduce targeted capacity-building interventions • Escalate unresolved resistance to executive governance. **Fall Back Rule:** Adoption shall be enforced through budget and procurement controls rather than voluntary compliance
Technical Complexity or Platform Delays	Dependency blockage, cascading delays	• Implement minimum viable platform capabilities • Use interim integration patterns - lightweight APIs where necessary • Re-sequence dependent initiatives • Protect standards and data foundations while platforms mature **Fall Back Rule:** Standards and governance progress shall continue even if platform delivery is delayed.
Cybersecurity or Data Protection Constraints	Immediate suspension of data sharing, loss of public trust, and potential legal liabilities for MCDAs.	• Narrow scope to low-risk anonymized datasets and use cases • Strengthen security architecture before scaling • Introduce staged access and controlled data exposure • Delay innovation initiatives, not core governance

		Fall Back Rule: Security and Trust over Speed. Innovation initiatives (e.g., AI/Open Data) are paused immediately to protect the integrity of the foundational layers.
Skills and Capacity Shortfalls	Degraded output quality, project "drift," and over-reliance on external consultants without knowledge transfer.	• Reduce parallel initiative load (concurrency) to match headcount. • Standardize on "Low-Code" or "Off-the-Shelf" solutions rather than custom builds to reduce the maintenance burden. • Extend delivery timelines • Prioritize institutional capability building • Introduce targeted expert support with knowledge transfer obligations **Fall Back Rule:** **Architecture over Velocity.** Capability gaps shall trigger timeline extensions rather than the dilution of architectural standards. We will build slower, but we will build correctly

BUILT-IN BUFFER MECHANISMS

To ensure the GEA can absorb shocks without collapsing, three "buffer" layers are integrated into the roadmap:

1. **Time Buffers**

- Each transition phase includes a 15–20% contingency window
- National rollouts occur only after validated pilots
- Annual roadmap refresh allows re-sequencing without re-approval

2. **Scope Buffers**

- Initiatives are defined in modular increments e.g. If the AI Analytics module fails, the Data Collection module remains functional.
- Non-critical features can be deferred without loss of core value. Distinguish between "Must-Have" (Core Integration) and "Nice-to-Have" (Dashboard Visuals).

3. **Funding Buffers**

- Tranche-based funding releases. Funding is unlocked by milestone achievement, reducing sunk cost risk.
- The GEA Board will have the authority to move funds from a 'stalled' initiative to an ongoing none within the same phase.

Fallback Options by Initiative Type

The table below provides the 'Plan B' for specific GEA workstreams to ensure the roadmap remains risk-adjusted

Initiative Type	Primary Fallback Option
Governance & Policy	Utilize interim Executive Directives/Circulars if formal legislation is delayed.
Standards & Architecture	Issue Minimum Mandatory Standards (Top 5) instead of the full Architecture Catalog.
Integration Platforms	Deliver Point-to-Point secure APIs for critical services before the full Enterprise Service Bus.
Data Initiatives	Prioritize Registry Integrity (e.g., Births/Deaths) before attempting complex Master Data Management.
Cloud & Infrastructure	Shift to a Hybrid-Cloud or On-Premise containment strategy if national cloud migration hits a bottleneck.
Cybersecurity	Revert to Air-Gapped or Restricted Access protocols for sensitive datasets while security patches are applied.
Skills & Talent	Deploy a Shared Services technical squad to rotate between MCDAs rather than hiring for every individual department.

GOVERNANCE TRIGGERS FOR CONTINGENCY ACTIVATION

To prevent scope creep the GEA Oversight Board shall activate these contingencies under the following audited conditions:

1. **25% Threshold**: When a critical path milestone is delayed by more than 25% of its allotted phase time.
2. **Capability Gap**: When more than 30% of key technical roles remain vacant for over 90 days.
3. **Fiscal Floor**: If the National Treasury reduces the quarterly disbursement by 15% or more.
4. **Security Red-Line**: If a "High" or "Critical" vulnerability remains unpatched in a production environment for more than 48 hours.

The GEA Oversight Board, in consultation with the National Treasury and Executive leadership, shall:

- Approve re-sequencing or timeline extensions
- Protect the national critical path
- Communicate changes transparently

The contingency plan ensures that the GEA Transition is robust under uncertainty and allows MCDAs to adapt without losing direction, protect foundational investments, and sustain progress even in the face of fiscal, institutional, or technical disruption.

STAKEHOLDER ENGAGEMENT

Effective stakeholder engagement is critical to the successful implementation of Kenya's Government Enterprise Architecture (GEA) and Government Interoperability Framework (GIF). Given the scale and complexity of this transformation, the strategy must involve a broad spectrum of actors, from policymakers and ICT professionals to end-users and private sector players.

The value of the frameworks, standards, and roadmaps defined within the GEA/GIF is only realized when they are understood, adopted, and championed by the people who design, build, and use government services.

This section outlines the formal strategy for managing the human element of the architectural transformation to provide a structured approach to ensure that the GEA is embraced as a shared, business-led vision for a more efficient, integrated, and citizen-centric public service. Effective engagement is the engine that will drive the framework from a set of documents into a living, breathing practice.

OBJECTIVES OF STAKEHOLDER ENGAGEMENT

- Build consensus and shared ownership of the GEA/GIF vision across public institutions.
- Ensure inclusiveness by involving both national and county governments, as well as non-state actors.
- Facilitate the co-creation of standards, frameworks, and best practices that reflect on-the-ground realities.
- Encourage continuous feedback loops for learning, iteration, and adaptation.
- Increase transparency, trust, and public confidence in government digital services.

Guiding Principles

All stakeholder engagement activities will be governed by a set of core principles to ensure that our approach is consistent, respectful, and focused on building a lasting coalition for change.

Principle	Description
Inclusivity and Partnership	All relevant voices are heard, from policy leaders to technical team and end-users. GEA will be developed *with* MCDA, not *for* them, fostering a sense of collective ownership and shared responsibility for its success.
Transparency and Openness	All GEA documentation, architectural decisions, review processes, and roadmaps will be made centrally accessible and communicated in a clear, understandable manner to build trust and ensure that all stakeholders have the information they need to align their efforts.
Value-Driven Communication	Frame all communication in terms of the business value and benefits to each specific stakeholder group while articulating how the GEA enables tangible outcomes.
Proactive and Continuous Engagement	Engagement is continuous two-way dialogue with stakeholders through regular forums, workshops, and feedback channels to ensure that GEA remains relevant and continuously adapts to the evolving needs of the government and its citizens.
Empowerment through Knowledge	Equip stakeholders with the necessary knowledge, training, and resources to participate in the GEA process building digital and architectural literacy across the public service, empowering individuals to become active participants and champions of digital transformation.

STAKEHOLDER ANALYSIS AND ENGAGEMENT MATRIX

This matrix identifies the key groups who will influence or be affected by the GEA. For each group, it defines their primary interests and concerns and outlines the specific strategies that will be used to engage, empower, and coordinate with them throughout the GEA lifecycle.

Stakeholder Group	Key Interests & Concerns	Engagement Strategy (How we'll engage)	Empowerment Method (How we'll enable)	Coordination Channel (Where we'll coordinate)
Political Leadership (Cabinet Secretaries, Principal	**Interests:** Achieving national goals (Vision 2030), demonstrating value for money, enhancing national	Present clear, concise business cases. Report on strategic KPIs (ROI, citizen impact).	Provide dashboards with key metrics to track value realization. Equip them with data-driven insights	**GEA Steering Committee**, Cabinet Meetings, Parliamentary

Secretaries, Parliament)	security, and improving citizen satisfaction. **Concerns:** High cost of digital projects, risk of implementation failure, public perception, pace of change.	Align all proposals with the National Digital Master Plan. Provide regular, high-level progress briefings.	to support policymaking	Committee Briefings.
MCDA Leadership (Directors, Heads of Agencies, CEOs of State Corporations)	**Interests:** Fulfilling their specific mandate, operational efficiency, budget control, improved service delivery. **Concerns:** Loss of departmental autonomy, unfunded mandates, imposed solutions that don't fit their priorities, disruption to current operations.	Focus on the business value for their specific MDA. Involve them in setting priorities. Showcase 'quick wins' and case studies from other MCDA. Offer advisory and solution architecture support.	Grant them representation on the Architecture Review Board (ARB). Provide them with access to shared platforms and services that reduce their operational costs.	**Architecture Review Board (ARB)**, one-on-one strategic reviews, MDA leadership forums.
ICT and Technical Leadership (CIOs, ICT Directors in MDAs)	**Interests:** Technology modernization, standardization, reducing technical debt, improving system security and resilience. **Concerns:** GEA being too theoretical or rigid, lack of budget for new tools, skills gaps in their teams, challenges of integrating legacy systems.	Engage them in the development and review of technical standards. Provide clear reference architectures, patterns, and implementation guides. Facilitate knowledge sharing between MDAs.	Fund and provide access to centralized training programs. Give them a leading role in technical **Domain Working Groups**. Provide access to shared technology platforms (G-Cloud, GIP).	**Architecture Review Board (ARB)**, CIO Council, technical **Domain Working Groups**.
GEA Practitioners	**Interests:** Clear standards and processes, access to	Establish a collaborative community.	Provide certified training (e.g., TOGAF).	**GEA Community of Practice (CoP)**,

(Enterprise Architects, Solution Architects, Security and Data Officers)	professional tools, career development, knowledge sharing, having the authority to enforce architecture. **Concerns:** Lack of clear mandate, being bypassed in projects, skill gaps, resistance to change from project teams.	Provide mentorship and clear career progression paths. Recognize and reward architectural excellence. Involve them in ARB review processes.	Grant access to a central architecture repository and modeling tools. Provide them with delegated authority from the ARB to approve low-impact designs.	**GEA Online Portal**, regular peer review sessions.
Public Servants (End-users of e-government systems)	**Interests:** Systems that are reliable, easy to use, and make their jobs easier. Access to timely information and proper training on new tools. **Concerns:** Fear of automation leading to job losses, complex systems that increase workload, inadequate training and support.	Communicate changes well in advance. Involve them in user testing and feedback sessions. Focus training on selling the productivity benefits (e.g., less paperwork, faster approval, etc.).	Provide comprehensive, role-based training and accessible support materials (videos, guides). Establish responsive helpdesk and super-user programs to provide peer support.	Internal communications (Intranet, newsletters), user acceptance testing (UAT) workshops, training sessions.
Citizens and Businesses (The ultimate consumers of government services)	**Interests:** Simple, accessible, and reliable digital services. Data privacy and security. Not having to provide the same information repeatedly. **Concerns:** Digital divide (accessibility issues), data breaches,	Run public awareness campaigns for new digital services. Provide clear and simple terms of service and data privacy policies. Establish clear channels for feedback and complaints.	Provide easy-to-use, mobile-first digital platforms (e.g., e-Citizen). Offer multi-channel support through Huduma Centres, call centres, and online help.	Official Government Websites, Public Participation Forums, Media Briefings, social media.

	confusing websites, service downtime.			
Private Sector & Academia (Technology partners and innovators)	**Interests:** Partnership opportunities, clear technical standards for integration, fair procurement processes, contributing to national innovation. **Concerns:** Bureaucracy, vendor lock-in to specific technologies, lack of visibility into the government's long-term technology roadmap.	Publish GEA standards and API specifications publicly. Host industry forums, hackathons, and innovation challenges. Establish formal partnerships for research and development.	Create a partner portal and developer sandbox for the Government Integration Platform (GIP). Streamline procurement for innovative solutions that align with the GEA.	Industry engagement forums, GEA Online Portal, hackathons, and joint research programs.

COMMUNICATION PLAN AND ENGAGEMENT PLATFORMS

To ensure consistent, targeted, and effective communication, a multi-channel approach will be used to reach each stakeholder group with the right information at the right time. The following platforms and forums will serve as the primary vehicles for operationalizing the engagement strategy.

a) FORMAL GOVERNANCE BODIES

The established GEA governance structure is the primary channel for formal communication, decision-making, and strategic alignment.

- **GEA Steering Committee:** This body serves as the apex communication channel to Political Leadership. It will translate technical progress and architectural decisions into strategic reports focusing on national impact, ROI, and national objectives such as Vision 2030; and major policy-level communications will be ratified and disseminated from this committee.
- **Architecture Review Board (ARB):** The ARB is the operational heart of GEA communication. It is the formal engagement point for MDA Leadership and

ICT/Technical Leadership. Its decisions, standards approvals, and project reviews will be formally documented and communicated to all relevant agencies, ensuring a clear and authoritative channel for architectural governance.

b) DIGITAL PLATFORMS

Digital platforms will provide a platform to ensure that information is accessible and consistently updated.

- **GEA Online Portal:** A central, web-based portal will be created to serve as the definitive repository for all GEA-related information. It is the single source of truth for all stakeholders, particularly GEA Practitioners and Technical Leadership. The portal will host:
    - All approved architectural principles, policies, and standards.
    - The complete set of reference models and roadmaps.
    - The Application Portfolio Catalog and the Data Asset Catalog.
    - The GEA Glossary and all official documentation.
    - Templates and guides for the Architecture Compliance Process.
- **GEA Newsletter:** A regular (e.g., quarterly) email newsletter distributed to all internal and external stakeholders. This "push" communication channel will provide high-level updates on the transformation roadmap, highlight successful project case studies from various MCDAs, announce newly ratified standards, and promote upcoming training opportunities.

c) DIRECT ENGAGEMENT FORUMS

Direct interactive forums are essential for building a community, fostering collaboration, and gathering feedback.

- **GEA Community of Practitioners:** A regular forum will be established, bringing together GEA Practitioners (architects, security officers, data stewards) from across the government and private sector. The forum will be a practitioner-led community focused on:
    - Sharing best practices and lessons learned.
    - Collaboratively solving common architectural challenges.

- Providing expert, ground-level feedback to the ARB on the evolution of standards.

- **Targeted Workshops and Training Sessions:** A continuous schedule of workshops and training will be implemented, with content tailored to the specific needs of different stakeholder groups:
  - **Leadership Briefings:** Short, high-impact sessions for MCDA leaders on the business value of the GEA.
  - **Technical Deep Dives:** Multi-day, hands-on sessions for developers and architects on new platforms (G-Cloud, GIP) and standards.
  - **User Training:** Role-based training for **Public Servants** on new systems being deployed as part of the GEA roadmap.

d) PUBLIC COMMUNICATION CHANNELS

Engaging the ultimate beneficiaries of the GEA requires leveraging trusted, public-facing channels.

- **Official Government Channels:** Existing government websites (e.g., the main GOK portal, ministry websites) and official social media accounts will be used to inform Citizens and Businesses about new and improved digital services that are direct outcomes of the GEA transformation.
- **Value-Driven Messaging:** All public communication will focus on the tangible benefits to the end-user, such as 'new, simplified process for renewing your license online' or 'a single login for multiple government services,' thereby demonstrating the practical value of the government's digital transformation.

ENGAGEMENT TIMELINE

Phase	Engagement Focus
Initiation (Y1)	Awareness-building, leadership onboarding, GEA orientation workshops.
Design (Y1–2)	Co-creation of standards, feedback on draft frameworks, early pilots.
Rollout (Y3–5)	Scaling engagement to Corporations, vendors, civil society; onboarding new partners.
Maturity (Y6-10)	Institutionalized collaboration via stakeholder compacts, working groups, and open digital governance.

An engaged stakeholder community is foundational to the success and sustainability of Kenya's GEA blueprint. It transforms enterprise architecture from a compliance obligation into a shared national digital transformation agenda.

CONCLUSION AND RECOMMENDATIONS

SUMMARY OF GEA

The design of a GEA framework is not merely a technical undertaking but a strategic imperative for Kenya's national development. The current situational assessment reveals a strong national policy foundation and significant progress in digitization of government services.

However, this also highlights persistent challenges such as siloed operations, data fragmentation, and the critical need for enhanced human and organizational interoperability. The existence of multiple, overlapping digital strategies, while demonstrating commitment, underscores the need for meticulous alignment and governance to prevent fragmentation and ensure synergistic outcomes.

The development and institutionalization of Kenya’s Government Enterprise Architecture (GEA) and Government Interoperability Framework (GIF) represent a bold step toward building a more efficient, citizen-centric, secure, and digitally enabled public sector. This blueprint provides a framework for aligning ICT investments and systems to shared goals, improving coordination across Ministries, Corporations, Departments, and Agencies (MCDAs), and delivering services in a unified and accessible manner.

The architecture domains, principles, standards, and governance mechanisms outlined in this document are designed to support Kenya’s broader aspirations as articulated in Vision 2030, the Digital Economy Blueprint, and the National Digital Master Plan 2022–2032. By adopting an integrated architecture framework that promotes interoperability, reuse, openness, and data-driven innovation, Kenya is positioning itself to lead in delivering transparent, agile, and inclusive digital public services.

However, the transition will not be without challenges. Institutional inertia, legacy systems, fragmented investments, and skills shortages must be addressed through a combination of strong governance, capacity development, and sustained stakeholder engagement. The implementation of the GEA will need to be phased, continuously monitored, and adapted to reflect changing technologies and user needs.

PRIORITIZED RECOMMENDATIONS

GEA is the mechanism by which Kenya converts digital ambition into disciplined execution, public value, and national coherence. Its success depends not on intent, but on enforcement, capability, and sustained leadership.

PRIORITY 1: FOUNDATIONAL ENABLERS (0–12 MONTHS)

Establish the legal authority, governance control, and enforcement mechanisms required to make GEA binding across all public sector digital investments. This priority ensures that architecture moves from guidance to mandated execution, preventing further fragmentation and waste. These are non-negotiable. Without them, GEA will not hold.

Action	Responsible Role	Timeline	Measurable Outcomes
Legally anchor GEA and GIF; link ICT funding to compliance	MICDE / Parliament / NT	0–6 months	Regulations or directives mandating GEA/GIF compliance implemented Linkage ICT funding and procurement approvals to architecture conformance enforced
Establish and empower Central GEA Governance Authority	MICDE / ICTA	0–6 months	ARB, PGB operational; enforcement mandate issued
Mandate interoperability and shared services (APIs, registries, platforms)	GEA Oversight Board	6–12 months	Reduction in duplicated systems; API reuse rate ≥60%
Embed architecture compliance into procurement	National Treasury / PPOA / ICT Authority	6–12 months	EA clauses in all ICT RFPs; zero procurement without ARB sign-off
Establish a formal GEA content metamodel	GEA Oversight Board	0–6 months	Approved National GEA metamodel covering capabilities, services, value streams, data domains, applications, integrations, technology, risks, controls, and dependencies.

Action	Responsible Role	Timeline	Measurable Outcomes
Implement EA tooling	ICT Authority	6-12 months	Procured and configured EA tools aligned to the metamodel (architecture modelling, dependency mapping, compliance tracking
Activate Architecture Review Boards (ARBs)	ICT Authority, GEA Oversight Board	0-12 months	Operationalize ARBs with clear decision rights, compliance checklists, and escalation authority.
Implement Digital Readiness Assessments	GEA Oversight Board	Annual	National EA maturity scorecard published

PRIORITY 2: OPERATIONALIZE INTEROPERABILITY AND DATA FOUNDATIONS (6–24 MONTHS)

Create a secure, scalable, and cost-efficient national digital foundation by modernizing technology platforms, enforcing security-by-design, and rationalizing legacy systems to enable seamless, secure, and reusable data and service exchange across government and with ecosystem partners.

Action	Responsible Role	Timeline	Measurable Outcomes
Implement the Government Interoperability Platform (GIP)	ICT Authority	6-18 months	GIP deployed as the mandatory gateway for APIs, data exchange, and service orchestration.
Enforce canonical data models and semantics	GEA Oversight Board	6-12 months	Finalized and published priority canonical data models and semantic standards under DRM/C2.
Institutionalize external data ingestion controls	ARB, Data Stewards	6–12 months	Enforced staging, cleansing, validation, and licensing checks for all external data sources.
Implement national data archival capability	ICT Authority	6–18 months	Operationalize archival repositories and lifecycle controls aligned to legal ,policy and evidentiary requirements.

Action	Responsible Role	Timeline	Measurable Outcomes
Establish and enforce national data governance framework	ICTA / GEA Oversight Board / ODPC	6–12 months	Authoritative data domains defined; data quality KPIs operational
Enforce TRM, IRM, DRM standards	ARB / Platform Owners	Continuous	Decline in technology variance and integration failures

PRIORITY 3: DRIVE VALUE-LED DELIVERY AND SHARED SERVICES

Shift from project-centric digitization to value-stream-driven service delivery using shared platforms.

Action	Responsible Role	Timeline	Measurable Outcomes
Adopt value streams as the primary planning construct	GEA Oversight Board / ICT Authority / MCDA	12–24 months	Value-stream-aligned portfolios, services, capabilities, investments, and KPIs.
Mandate reuse of national platforms	GEA Oversight Board / ICT Authority / MCDA	12–24 months	Enforced reuse of Digital ID, Payments, e-Citizen, registries, and shared services. Reduced platform duplication
Rationalize application portfolios	ICTA / MCDAs / ARB	6–24 months	Decommissioned redundant systems and consolidated overlapping capabilities. Measurable cost savings

PRIORITY 4: STRENGTHEN RESILIENCE, SECURITY, AND TRUST

Ensure digital government services are secure, resilient, and trusted by citizens and businesses.

Action	Responsible Role	Timeline	Measurable Outcomes
Enforce DR/BC certification	ICTA	6–18 months	Tier 0 and Tier 1 services certified to meet RTO/RPO targets and pass annual DR drills.
Embed security and privacy-by-design	ARB, DPOs	Ongoing	Integrate security architecture and privacy controls into all ADM phases. Reduced security incidents.
Strengthen trust and transparency	ICTA	Ongoing	Published service performance and availability dashboards for citizen confidence. Improved public trust metrics

PRIORITY 5: HUMAN CAPITAL AND ORGANIZATIONAL INTEROPERABILITY

Build and sustain a digitally capable, architecture-literate public service that can govern, deliver, and evolve Whole-of-Government digital services. This priority addresses the people and organizational dimensions that ultimately determine long-term success or failure of GEA.

Action	Responsible Role	Timeline	Measurable Outcomes
Professionalize EA and data roles	ICTA, Public Service Commission	6–18 months	Defined role profiles, certification paths, and career progression for EA, data, integration, and security roles.
Deploy continuous capability maturity assessments	GEA Oversight Board / ARB	Annual	Deployed GEA maturity roadmap and scorecards annually across MCDAs and Counties.
Establish EA and digital architecture certification programs	PSC / ICTA	6–18 months	Certified EA professionals across all key MCDAs
Strengthen cross-agency collaboration and incentives	PSC / ICTA	Ongoing	Increased shared service adoption; reduced duplication
Retain critical digital skills	PSC / MCDA	Ongoing	Reduced reliance on vendors for core capabilities

PRIORITY 6: AGILITY, INNOVATION, AND CONTINUOUS IMPROVEMENT

Ensure that GEA remains a living, adaptive framework capable of responding to technological change, policy shifts, and evolving citizen expectations without compromising interoperability, security, or governance discipline.

Action	Responsible Role	Timeline	Measurable Outcomes
Institutionalize agile, iterative GEA evolution	GEA Oversight Board	Continuous	Annual GEA updates: architecture backlog maintained
Maintain controlled innovation space (AI, IoT, blockchain)	GEA Oversight Board / ARB	Ongoing	Approved pilots transitioned into standards or retired
Publish citizen-facing transparency dashboards	Service Owners	12–24 months	Improved citizen trust and service satisfaction scores

REFERENCES

1. AXELOS. (2019). *ITIL Foundation: ITIL 4 Edition*. TSO (The Stationery Office).
2. Department of Internal Affairs Te Tari Taiwhenua. (2019). *Government Enterprise Architecture for New Zealand*.
3. Government of the Republic of Kenya. (2008). *Kenya Vision 2030: A globally competitive and prosperous Kenya*.
4. ICT Authority. (2023). *ICT Human Capital and Workforce Development Standard*. ICT Authority.
5. International Organization for Standardization. (2015). *Governance of IT for the organization* (ISO/IEC 38500:2015).
6. International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC 27001:2022).
7. ISACA. (2018). *COBIT 2019 Framework: Introduction and Methodology*. ISACA.
8. Ministry of Electronics & Information Technology, Government of India. (2018). *India Enterprise Architecture Framework (IndEA)*.
9. Ministry of Information, Communications, and the Digital Economy. (2025). *Kenya National Artificial Intelligence Strategy 2025-2030*.
10. Ministry of ICT, Innovation and Youth Affairs. (2022). *The Kenya National Digital Master Plan 2022-2032*.
11. National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018
12. Open Web Application Security Project. (2021). *OWASP Top 10:2021*. https://owasp.org/www-project-top-ten/
13. Queensland Government. (2023). *Queensland Government Enterprise Architecture*. Queensland Government Customer and Digital Group.
14. Republic of Kenya. (2018). *Computer Misuse and Cybercrimes Act (No. 5 of 2018)*. Government Printer.
15. Republic of Kenya. (2019). *The Data Protection Act (No. 24 of 2019)*. Government Printer.
16. The Open Group. (2018). *The TOGAF® Standard, Version 10* Van Haren Publishing.

SIGN OFF

Nicoza Africa Limited

MONTE KAJAMAA	**CHIEF EXECUTIVE OFFICER**	**FEBRUARY 25TH, 2026**
Authorized Signatory	Designation	Date

CHRISTINE KIMANI	**DIRECTOR OPERATIONS**	**FEBRUARY 25TH, 2026**
Witness	Designation	Date

GOVERNMENT DIGITAL ENTERPRISE ARCHITECTURE (GEA) DOCUMENT

Kenya Digital Economy Acceleration Project (KDEAP)

3rd Edition

ICTA GEA: 001:2025

Physical Address

Teleposta Towers,12th Flr,

Kenyatta Ave., Nairobi, Kenya

Phone Numbers

(+254)793 879629

(+254)20 6676999

Email Addresses

info@ict.go.ke

Communications@ict.go.ke

ICT Authority KE

ICT Authority KE

ICT Authority KE

REPORT PREPARED BY:

nicoza africa

The ICT Authority is a State Corporation under the State Corporations Act 446

www.icta.go.ke