GOVERNMENT INTEROPERABILITY FRAMEWORK (GIF) DOCUMENT

Standards and Guidance for Data Sharing and System Integration within the Government Ecosystem

3rd Edition
ICTA GIF: 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)**			

EXECUTIVE SUMMARY

This document outlines the Government Interoperability Framework (GIF) for the Government of Kenya, designed to serve as the foundational blueprint for a unified, efficient, and citizen-centric interconnected digital government.

GIF is positioned as a critical, actionable component of the broader Government Enterprise Architecture (GEA), providing the specific standards, models, and governance mechanisms required to achieve seamless, cross-government digital service delivery. By adopting this framework, the Government of Kenya will avoid the implementation of fragmented ad-hoc ICT solutions that lead to isolated data silos and redundant systems.

The framework's core is built upon four interdependent reference models: Legal, Organizational, Semantic and Technical. These models provide a multi-layered approach to interoperability, from the foundational infrastructure and data formats to the legal and procedural agreements necessary for collaboration. The framework defines a robust governance structure, centralizing the Information and Communication Technology Authority (ICTA) as the lead enforcement body, supported by a high-level GEA/GIF Oversight Board. Furthermore, it integrates a comprehensive strategy for security and data protection, aligning with Kenya's Data Protection Act, 2019, and international standards like ISO/IEC 27001.

The proposed implementation roadmap is a phased, multi-year plan aligned with The Open Group Architecture Framework (TOGAF) Architecture Development Method (ADM). This approach will begin with foundational activities and high-impact pilot use cases, such as the GovStack AI Chatbot for eCitizen, before expanding to a nationwide rollout.

GIF's successful adoption will result in substantial benefits, including streamlined public services, enhanced transparency, significant cost savings through the elimination of redundancy, and improved data-driven decision-making. The framework provides a strategic path to operationalize the Kenya National Digital Master Plan 2022-2032 and contribute directly to the national development goals outlined in Kenya Vision 2030. The following sections describe in detail how achievement of these goals will be enabled.

TABLE OF CONTENTS

TABLE OF FIGURES

ABBREVIATIONS AND ACRONYMS

GEA	Government Enterprise Architecture
GIF	Government Interoperability Framework
ICTA	Information and Communication Technology Authority
MCDA	Ministries, Counties, Departments, and Agencies
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
KSDI	Kenya National Spatial Data Infrastructure
AI	Artificial Intelligence
IoT	Internet of Things
TOGAF	The Open Group Architecture Framework
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
EGDI	e-Government Development Index
RBAC	Role-Based Access Control
PKI	Public Key Infrastructure
ABAC	Attribute-Based Access Control

INTRODUCTION

The Government Interoperability Framework (GIF) is the government-wide standard that enables MCDAs, and approved ecosystem partners to securely and consistently exchange data and integrate digital services.

It defines the legal, organizational, semantic, technical, and security rules required to ensure that government systems can work together as one coherent digital ecosystem, supporting seamless service delivery, trusted information sharing, and enforceable compliance across the public sector.

The global landscape of public service is constantly being reshaped through digital transformation with developed economies leveraging enterprise architectures capabilities as blueprints to guide digital transformation and e-government initiatives in a holistic and manageable way.

For developing economies, including Kenya, the challenge lies in moving beyond the ad-hoc, uncoordinated implementation of ICT systems, which has historically resulted in deployment of fragmented ICT systems and applications that are unable to communicate or exchange data with one another. The net effect is the failure to achieve the promise of more efficient and effective public institutions, with MCDAs continuing to develop and implement new systems without adequate focus to the need to connect, share, and reuse data.

The Government Interoperability Framework comes in to serve as a strategic corrective to this systemic fragmentation of ICT systems and digital services by providing a cohesive set of standards, protocols, and architectural guidelines to establish a unified digital ecosystem where government systems can communicate meaningfully and securely, break down and prevent the emergence of digital silos and ensure that future ICT investments are interoperable by design rather than by exception.

In this respect, GIF is not merely a technical specification but is a core enabler of national digital transformation, ensuring that new services, modernized legacy systems, and cross-government initiatives are aligned.

ALIGNMENT WITH THE GOVERNMENT ENTERPRISE ARCHITECTURE (GEA)

GIF is interlinked to the GEA as a core, actionable component of the GEA strategy. While GEA provides the overarching strategic blueprint, aligning business strategy, information assets, applications, technology and security, GIF translates these high-level architectural principles into enforceable technical specifications.

By defining standards for how data is structured, how systems communicate, what terminology they use, and what processes govern their interaction, GIF acts as the mutual enforcement mechanism for the GEA by:

- Translating GEA principles into actionable specifications for integration, data exchange, terminology harmonization, and communication.
- Providing detailed guidance for the Business, Data, Application, and Technology and Security layers to ensure all systems conform to shared protocols.
- Embedding interoperability as a mandatory requirement for all new and modernized ICT systems.

Through this symbiotic relationship, GEA defines ***what*** government seeks to achieve, and the GIF defines ***how*** digital systems must interact to achieve it. Together they establish a harmonized, scalable, and sustainable whole-of-government digital ecosystem.

ROLE IN KENYA'S DIGITAL TRANSFORMATION AGENDA

End-to-end automation and digital service delivery cannot be realized without interoperable systems. GIF actualizes this desired state by ensuring that information flows securely and seamlessly across institutional boundaries through supporting:

- One-stop, citizen-centric government services
- Integrated G2G, G2B, and G2C digital transactions
- Unified government databases
- Real-time data-driven policy and decision-making

GIF is a fundamental enabler of Kenya's strategic initiatives particularly those outlined in the Kenya National Digital Master Plan 2022-2032. The Master Plan's key objectives, such as enhancing service delivery through ICT and automating all government services cannot be achieved without a robust interoperable framework. GIF provides the technical and policy

foundation for achieving these goals by enabling a seamless flow of information and services across government boundaries, which is a key requirement for modern e-government.

By creating a unified digital interoperability platform, GIF enhances transparency, improves the effectiveness and efficiency of public service delivery, building citizen trust in government institutions, enabling digital trade and financial inclusion which are key elements for the success of the national digital transformation objectives.

OBJECTIVES OF GOVERNMENT INTEROPERABILITY FRAMEWORK

The strategic objectives of GIF are designed to address the core challenges of a fragmented digital landscape and align with the national vision for a citizen-centric government.

I. Seamless, Citizen-Centric Service Delivery

GIF enables the delivery of integrated, citizen-centric digital public services by enabling ICT systems in the government ecosystem to securely exchange trusted data and integrate services across MCDAs in real time. This supports the development of "one-stop shop" service channels where citizens and businesses experience government as a unified entity rather than a collection of disconnected services across institutions. By standardizing data exchange, shared service interfaces, and service orchestration patterns, GIF reduces repetitive data collection, shortens processing times, improves service completion rates, and enables end-to-end service journeys that span multiple institutions and jurisdictions and borders.

II. Cost Efficiency, Reuse and Resource Optimization

GIF reduces duplication and fragmented technology investments by enforcing consistent interoperability standards, reusable integration patterns, shared services, and harmonized data models. This promotes systematic reuse of existing government capabilities instead of repeated procurement of similar solutions across MCDA which lowers integration costs, reduces long-term maintenance overheads, improves procurement efficiency, and enables MCDAs to modernize progressively without reintroducing siloed systems.

III. Unified and Trusted View of Government Information

GIF enables secure, accurate, and consistent sharing of government information across MCDAs by enforcing semantic alignment, canonical data models, and governed data exchange agreements. This ensures that government information retains consistent meaning across organizations which strengthens the ability to generate reliable operational and strategic insights, coordinate service delivery, improve inter-agency performance

management, and support effective policymaking through a coherent and trusted view of government data and key national indicators.

IV. Strengthened Security, Privacy, and Regulatory Compliance

GIF mandates a consistent and enforceable security and data protection framework for all interoperability interactions, ensuring that confidentiality, integrity, authenticity, traceability, and non-repudiation are maintained throughout government data exchanges. This includes uniform requirements for secure identity and access management, encryption, audit logging, and controlled data sharing aligned with the Kenya Data Protection Act (2019) and relevant cybersecurity and public service regulations. Embedding these controls into interoperability standards and compliance mechanisms enhances public trust, safeguards national digital assets, and ensures that government integration does not introduce unacceptable privacy, security, or legal risks.

V. Interoperability Extending the Government Ecosystem

GIF enables structured and secure interoperability beyond government ecosystem by providing a consistent framework for trusted information exchange with non-state actors such as approved private sector participants, development partners, service providers, and regional or international digital platform. This objective supports government service delivery models that depend on external procurement, verification, payments, logistics, compliance reporting, and delegated service provision, while ensuring that such exchanges remain legally authorized, semantically consistent, technically standardized, and security-controlled. Through establishment of clear interoperability rules for government-to-ecosystem engagements, GIF increases participation, reduces integration friction, and extends scalability of digital public services beyond the broader national service delivery environment.

VI. Predictable Implementation Governance and Whole-of-Government Accountability

GIF establishes a predictable and enforceable governance model that ensures interoperability initiatives are implemented consistently across MCDAs through mandated standards, defined roles and responsibilities, formal compliance gates, and measurable maturity progression. This ensures that interoperability outcomes are not left to discretionary project decisions but are governed through structured approval processes, architecture compliance reviews,

automated compliance enforcement, and performance reporting. Linking adoption to institutional accountability mechanisms and alignment of implementation requirements to planning, budgeting, procurement, and operational oversight ensures sustained compliance, reduces fragmentation, and enables consistent interoperability maturity across government.

KEY GIF CONCEPTS

Interoperability is the fundamental capability of different systems, in various government and stakeholder organizations, to exchange information, interpret information consistently and use information in their business processes. These are critical prerequisites for a truly integrated digital government to enable seamless flow of information and knowledge to all stakeholders.

Interoperability requires alignment across four dimensions:

1. **Legal Interoperability**

   Legal Interoperability enables system integration and data exchange to be established within a coherent and compliant legal environment within the whole-of-government ecosystem. It harmonizes sector laws, regulations, policies and administrative directives to remove ambiguities and contradictions that obstruct collaboration and defines standardized data-sharing agreements, MoUs, and SLAs that define authority, accountability, and liabilities between institutions. It also embeds compliance with privacy, data protection, records management, and cybersecurity legislation, ensuring that all data exchanges respect existing legal rights and obligations.

2. **Organizational Interoperability**

   The ability of organizations to provide services to other organizations or their clients through harmonized business processes, service-level arrangements in compliance with existing legal agreements.

3. **Semantic Interoperability**

   Defines the ability of different systems / organizations to understand exchanged data consistently through shared terminologies, metadata, code sets, and data definitions.

4. **Technical Interoperability**

   Technical capability of installed software / hardware to exchange data through common data exchange protocols, development of software necessary for management of data connections (APIs), creation of user interfaces to enable communication between different organizations.

SCOPE AND APPLICABILITY

GIF is applicable to any digital system that exchanges, consumes, or provides data or services to any part of the government ecosystem or its partners including:

- Government Ministries, Counties, Departments, and Agencies (MCDAs).
- State corporations, regulators, and sectoral authorities.
- Vendors, data integrators, aggregators and other private-sector partners participating in data exchange.

The GIF scope applies across the entire enterprise architecture lifecycle, cross-cutting all technology constraints, ensuring a cohesive, secure, and integrated digital government ecosystem including:

- Planning and investment
- Acquisition and procurement
- System design and development
- Operations and maintenance
- Integration and data exchange
- Modernization and disposal

The outcome is a standardized interoperability approach taken regardless of whether systems are internally developed, procured from an external vendor, or managed by a third party; based on the purpose and nature of the application and not which department or vendor is responsible for its development.

INTEROPERABILITY GUIDING PRINCIPLES

GIF is governed by a set of core principles that guide the design, development, and implementation of all government digital services. These include:

	Principle	Explanation
1.	**Openness and Open Standards**	GIF mandates the adoption openly published standards, open APIs, and reusable specifications that enable broad, cross-platform interoperability. This principle promotes transparency, better decision-making and fosters development of an innovative and competitive ecosystem for service development and ensures that different systems and institutions, including the private sector, within and beyond borders can easily integrate with government services.

2.	**Transparency**	Transparency ensures that government processes, datasets, and digital interactions are understandable and accessible while maintaining compliance with data protection laws and facilitating accountability.
3.	**Once-Only Principle (OOP)**	The Once-Only Principle (OOP) mandates that citizens and businesses should be required to submit information and documents only once when applying for government and public services. With the user's explicit consent and in accordance with data protection rules, MCDAs can then consume and securely exchange this information with other government entities to serve the user's needs.
4.	**Reusability and Shared Services**	The principle of reuse requires that MCDAs, when faced with a problem, deliberately endeavor to leverage existing solutions capabilities that have proven their value elsewhere in the ecosystem. This reduces fragmentation by encouraging agencies to adopt existing solutions, shared registries, APIs, and common infrastructure instead of building duplicate systems.
5.	**Scalability and Sustainability**	GIF requires designing and implementing solutions that can scale nationwide and evolve alongside changing technological, user demands, and policy environments.
6.	**Technology Neutrality**	The principle of technology neutrality requires that MCDAs prioritize functional needs rather than prescribing specific technologies, ensuring long-term flexibility, competition, and freedom from dependence on proprietary platforms.
7.	**Privacy and Security by Design**	Mandates the embedding data protection, encryption, authentication, and consent management from the earliest stages of system design to guarantee lawful and secure digital interactions. All digital services must be designed to safeguard personal data through employing encryption, robust authentication, and a consent-based approach to data sharing, giving citizens full control over their data.
8.	**Citizen-First Orientation**	All public services should be designed and delivered with the end-user, including citizenry, businesses, and other public administrations, at the

		center. Citizens' needs should be the primary driver for determining which services are provided and how they are delivered. This principle is guided by the following tenets: • Multi-Channel Service Delivery: Public services should be accessible through a variety of channels, including both physical and digital platforms, to accommodate different user needs and preferences. • Single Point of Contact: A single, unified point of contact will be provided for users to hide internal administrative complexity to facilitate seamless access to public services, even when multiple MCDAs are required to work together. • Continuous Improvement through Feedback: User feedback will be systematically collected, assessed, and used as a central mechanism for designing new public services and continually improving existing ones.

CASE STUDY - ESTONIA'S X-ROAD PLATFORM

The development of the GIF draws from internationally proven interoperability architectures, notably Estonia's X-Road platform, which demonstrates how a government can achieve secure, scalable, and resilient data exchange without centralizing data assets. A detailed case study including a comparative analysis of different implantation has been included in the *Annexure Section*

GIF INTEROPERABILITY PILLARS

GIF adopts a globally recognized interoperability structure consisting of **four pillars**, each addressing a distinct requirement to ensure sustainable cross-government data exchange and collaboration. The achievement of GIF objectives hinges on the ability to provide a comprehensive, multi-layered robust blueprint for supporting seamless data and service exchange. The framework is built on four interdependent layers as shown by Figure 2 below:

Figure 1 - Government Interoperability Framework Structure

These layers are not separate constructs but rather a cohesive hierarchical system.

LEGAL INTEROPERABILITY

Legal interoperability creates a harmonized legal environment where data sharing, cross-MCDA collaboration, reuse of ICT assets, and end-to-end digital public services can operate without legal contradictions or institutional barriers. It ensures that data exchange and digital service integrations comply with legal and regulatory frameworks.

OBJECTIVES OF LEGAL INTEROPERABILITY

I. **Enable Lawful and Unrestricted Data Exchange Across MCDAs:** Ensure that all digital interactions between MCDAs comply with applicable law, allowing seamless data sharing for service delivery.

II. **Harmonize Conflicting Legislative and Policy Requirements:** Resolve contradictions or overlaps between sectoral legislation when data is exchanged across domains (e.g., health, agriculture, finance).

III. **Embed Digital-by-Design Legal Requirements:** Drive enactment of new legislation with built-in digital service delivery and interoperability considerations ("digital checks").

IV. **Support Whole-of-Government and Cross-Border Services:** Enable consistent legal agreements that support integrated domestic services and cross-border interoperability.

V. **Strengthen Governance, Compliance, and Accountability:** Establish legal instruments (DSAs, SLAs, MoUs, Compliance Clauses) that enforce compliance to GIF.

KEY ELEMENTS

a) **Alignment with Existing Regulation**: MCDAs shall be required of existing e-government related legal acts and policies. These include:
   - Kenya Information and Communications Act (KICA), 1998
   - ICT Authority Act, 2013
   - Data Protection Act (DPA), 2019

b) **Data Sharing Agreements:** Formal contracts between MCDAs that clearly define the purpose, scope, legal basis, and security measures for data sharing (see Appendix section for sample Data Sharing Agreement).

c) **Sector-Specific Legislation:** Ensuring that any sector-specific regulations are not breached when exchanging information across domains. For example:
   - health data confidentiality
   - financial/securities regulation
   - judicial data privacy
   - national security information
   - child protection data
   - international data transfer rules

d) **Licensing and Intellectual Property Governance:** Ensuring that data and software components have compatible licenses that permit reuse and redistribution. Legal interoperability requires that ICT assets used across government support:
    - Open licensing (e.g. Apache, MIT, GPL-compatible)
    - Reuse and redistribution conditions
    - API consumption rights
    - Data access rights and usage rights
    - Conditions for proprietary software integration
    - Rights to modify, extend, and integrate digital public assets

This protects government from vendor lock-in and supports open ecosystems such as X-Road-style decentralized integration.

Without legal interoperability MCDAs may be prohibited from sharing information, even if systems are technically compatible, impeding the delivery of integrated digital services.

GIF LEGAL VIEW

The Legal View in *Figure 3* below identifies the enablers, policy and legislative elements required to design and run digital public services that work across MCDA and extend borders for end-to-end interoperability.

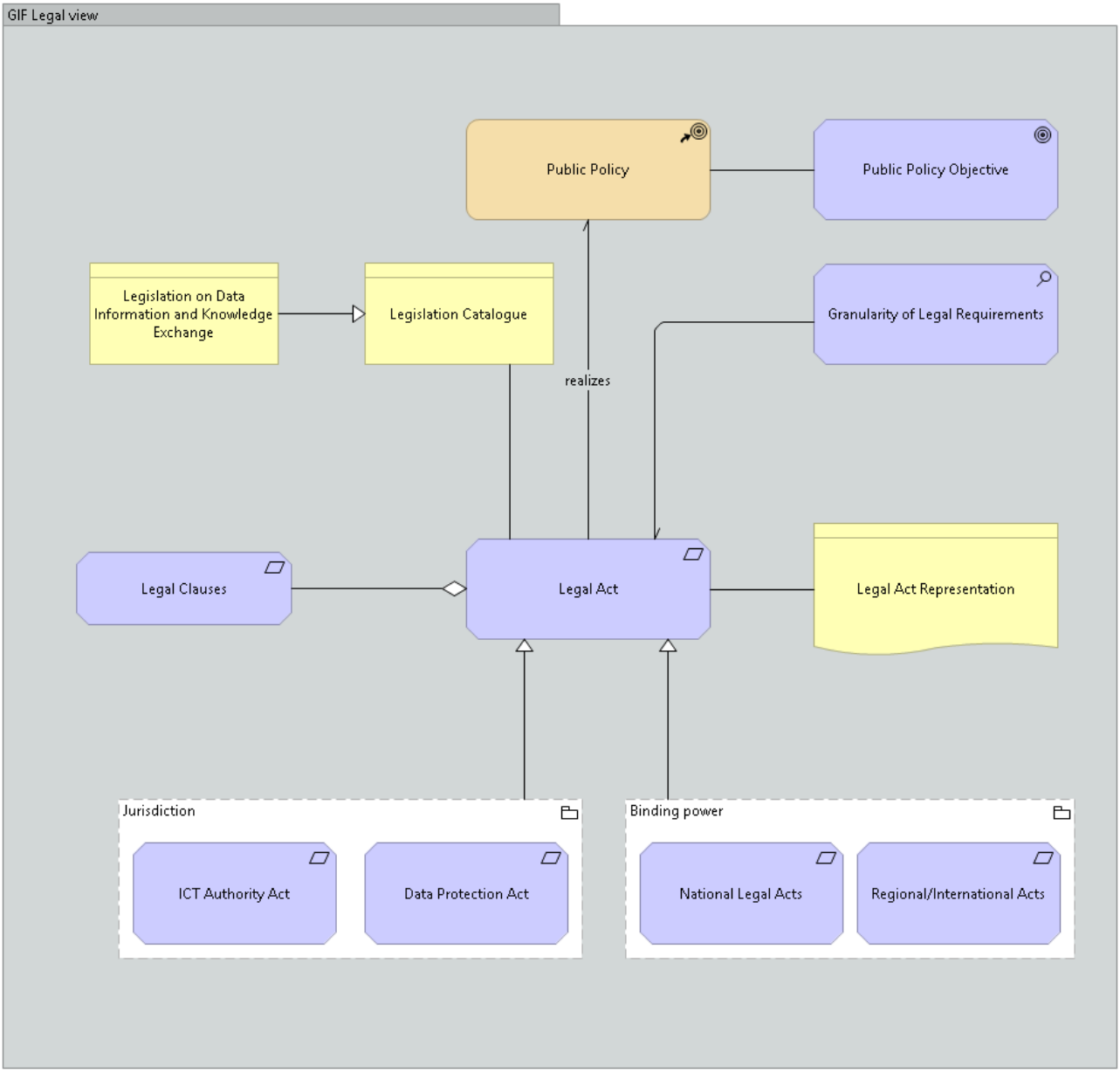

Figure 2 - GIF Legal View

The Legal View defines the laws and policies that enable interoperable digital public services by covering how public policy objectives are turned into legal acts at national or regional / international level.

The **Public Policy** aims at addressing the needs of a group of stakeholders according to the **Public Policy Objective**. The Public Policy is formulated and implemented with the help of **Legal Act** which has two specializations in the form of Binding Instrument or Non-Binding Instrument.

Legislation on Data Information and Knowledge Exchange is key for behavioral interoperability which is a specialization of the **Legislation on Digital Public Services** both contained in Legislation Catalogue.

Key legislation includes rules for digital public services and for data and information exchange, all organized within a **legislation catalogue**.

Governance is supported within legal agreements, especially the Legal Interoperability Agreement, which formalizes cross-border collaboration.

Together, these elements form the **Shared Legal Content**, providing the legal foundation and governance needed for secure, compliant, and interoperable digital services.

STEPS FOR ACHIEVING LEGAL INTEROPERABILITY

Step	Activity	Description
1.	**Legislative and Policy Interoperability Assessment**	Conduct assessments of all relevant legislation to identify: • barriers to data exchange • inconsistent or ambiguous data access rights • conflicting technological mandates • over-restricted licensing constraints • privacy or security contradictions • outdated provisions incompatible with digital services • overlapping responsibilities between MCDAs
2.	**Ensuring Legislative Coherence**	Before new legislation is drafted, conduct: • Interoperability Impact Assessment (IIA) • Cross-MCDA legal impact reviews • Semantic and technical dependency analysis • GEA reference model alignment checks
3.	**Digital Checks on All Proposed Legislation**	All new legislation must undergo a Digital Readiness Check to embed digital-by-design into law-making and ensure future services can be integrated without legislative redesign. It must validate: • Suitability for digital and online service delivery • alignment with GIF, GEA reference models • absence of barriers to API-based or event-driven interoperability

		• compatibility with DPA 2019 and national security directives • alignment with shared government platforms (e.g., identity, payments)
4.	**Creating Inter-Institutional Agreements**	Create the supporting legal frameworks between MCDAs including **Memorandums of Understanding (MoUs)**: Non-binding but formal agreements that outline the intent to cooperate. **Service Level Agreements (SLAs)**: Legally binding contracts that define the quality, uptime, and security responsibilities of the data provider and the data consumer. **Data Sharing Agreements (DSAs)**: Specific documents that detail what data is being shared, why (the legal basis), and how long it can be stored.
5.	**Governance and Enforcement Mechanisms**	Legal rules are only effective if there is a central body to enforce them and a way to resolve disputes. Establish a Lead Governance Authority: Appoint a central body (e.g. a GIF Oversight Board) with the legal power to mediate disputes between MCDAs. Standardized Licensing: Use "Open Government Licenses" so that data can be reused by other MCDAs without negotiating a new contract for every single request. Liability Frameworks e.g. Clearly define who is legally responsible if data is leaked or if incorrect data leads to a wrong administrative decision.
6.	**Continuous Legal Monitoring**	Continually assess for new legislation that might break existing digital connections. • **Interoperability Checks:** Implement a mandatory "Interoperability Impact Assessment" for all new legislation. • **Digital-Ready Rulemaking:** Train legal drafters to write laws in a way that is "machine-readable" or at least

		technology-neutral, avoiding specific mentions of hardware or physical processes.

These steps will facilitate interoperability between public services at the lower levels (semantic and technical) as well, and increase the potential for reusing existing ICT solutions, thereby reducing cost and implementation time.

ORGANIZATIONAL INTEROPERABILITY

Organizational interoperability addresses the institutional, procedural, and human dimensions required to achieve seamless, coordinated digital service delivery across the MCDAs ecosystem. Organizational interoperability ensures institutions can collaborate, aligning their mandates, processes, governance structures, and expectations so that citizens receive integrated, end-to-end services rather than fragmented, agency-centric outputs.

This GIF pillar complements the **GEA**'s **Business Architecture** to translate digital transformation objectives and business capabilities into a coordinated operational delivery model. It provides interoperability guidance to MCDAs on the governance structures they adopt, formal agreements that guarantee compliance, accountability, and shared stewardship of data and digital services.

Organizational interoperability ensures:

- Clear and harmonized responsibilities across participating MCDAs
- Standardized and integrated business processes
- Formalized cooperation through agreements and governance structures
- Cross-functional teams' capabilities to design, implement and operate federated digital services
- An operating environment where technical and data integration is supported by coherent institutional practice

KEY ELEMENTS

Organizational interoperability addresses the procedural and human aspects of interoperability, ensuring that processes and organizations within MCDAs are structured to support seamless digital collaboration. The key elements include:

Element	Description
Governance Structures	How cooperating MCDAs make decisions, resolve disputes, allocate responsibilities, and ensure compliance with interoperability standards. Key components on the governance structure include: • GIF Oversight Board for national-level policy and cross-MCDA coordination • ICT Authority (ICTA) as the standards custodian and compliance authority • MCDA Interoperability Steering Committees to govern agency-level adherence • Joint Service Management Committees for end-to-end service delivery accountability. These organizational structures ensure consistency, discipline, and transparency across all interoperability efforts.
Legal and Policy Frameworks	Formal agreements that operationalize legal mandates to ensure that collaborative processes are legally grounded and enforceable. These include: • Memoranda of Understanding (MoUs) to define roles, responsibilities, and cooperation modalities • Service-Level Agreements (SLAs) to set performance expectations, service windows, and accountability • Data Sharing Agreements (DSAs) defining purpose, scope, lawful basis, retention, and security • Interoperability Policies and Standards mandating compliance with GEA, GIF, and Kenya's legal framework
Business Process Re-engineering	Organizational interoperability requires alignment of business operations across MCDAs to support efficient, predictable, and citizen-centric and integrated digital services. This alignment includes: • End-to-end mapping of cross-agency business processes

	• Identification and elimination of bottlenecks, redundancies, and conflicting workflows • Standardization of activities such as identity validation, document verification, and case management • Adoption of Business Process Management Systems (BPMS) enabling workflow automation across MCDAs
Compliance Governance & Automated Policy Enforcement	Establishment of structures, mechanisms, and automated controls required to ensure continuous conformance with interoperability, security, and data-exchange obligations. These include: **a) Automated Compliance Checking (PaC)** • Encoding interoperability, security, API, and data-governance rules into machine-readable policy sets. • Enforcing compliance in CI/CD pipelines, integration gateways, event brokers, and runtime environments. • Blocking non-compliant deployments and integrations automatically. **b) Continuous Monitoring & Auditability** • Real-time validation of API traffic, data exchanges, rates, schemas, identities, and metadata consistency. • Automated alerts, audit trails, and immutable logs for governance and oversight. **c) Policy Governance** • National GIF policy repository managed by ICTA. • MCDA-level synchronized policy libraries for enforcement. • Architecture Review Board (ARB) oversight of PaC rulesets. **d) Compliance as a Governance Requirement** Compliance automation becomes a mandatory criterion for: • cross-MCDA collaboration • onboarding onto the Government Integration Platform (GIP) • approval of new systems • security audits and refresh cycles

Alignment with GEA Domains	Organizational interoperability provides organizational enforcement for the defined GEA architectural domains • Business Architecture: operating models, roles, processes, and governance necessary for integrated services • Data Architecture: Data stewardship, ownership, and data-sharing responsibilities • Application Architecture: Joint solution requirements and shared service expectations • Technology Architecture: Shared digital infrastructure governance • Integration Architecture: Institutional alignment for data exchange and API orchestration
Practical Application	Organizational interoperability implementation follows a structured TOGAF-aligned process: • Baseline (As-Is) Organizational Assessment: Review existing roles, processes, legal mandates, governance gaps • Target (To-Be) Organizational Operating Model: Define future governance, collaboration structures, and integrated process models • Gap Analysis: Compare As-Is and To-Be to identify changes in mandates, workflows, skills, and governance • Implementation Roadmap: Develop phased transition plans tied to digital transformation priorities and defined architectures • Governance and Change Management

GIF ORGANIZATIONAL VIEW

The Organizational view in *Figure 4* below describes the structures, roles, and agreements needed to design and operate interoperable digital public services across organizations and borders.

The view focuses on how services are delivered, who provides or consumes them, and the governance agreements that ensure interoperability, security, privacy, and data sharing. Together, these elements form the Shared Organizational Content, the foundation for coordinated, cross-agency digital service delivery.

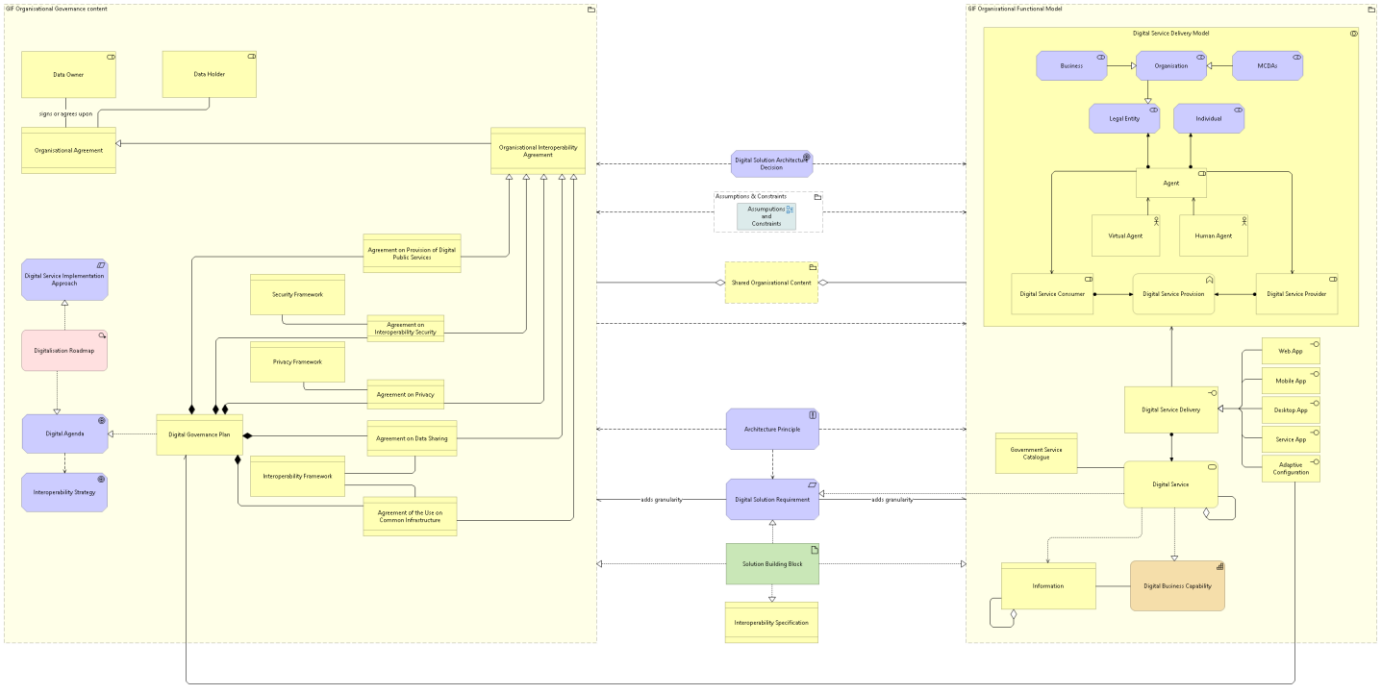

Figure 3 - GIF Organizational View

The view defines the roles, agreements, and governance needed to deliver interoperable digital public services. It covers the following core elements:

Service Design & Delivery Model	Digital Public Services, documented in Service Catalogue, are delivered according to the Digital Public Service Delivery Model which realises Digital Business Capabilities by accessing Information. In the delivery of Digital Services, a business interface is assigned to using various modalities such as Web App, Mobile App, Desktop App, Service App, or Adaptive Configuration. The delivery model is fulfilled through an Agent who can serve in the Digital Public Service Provision function both as Service Consumer and Service Provider
Governance	The Data Owner business role signs the Organizational Agreement which is specialised in Organizational Interoperability Agreement.

	The Digital Governance Plan is composed of contracts (Provision of Digital Public Services, Interoperability Security, Privacy, Data Sharing and Common Infrastructure) each associated with their various frameworks. The Digital Governance Plan realises the Digital Agenda which influences the Interoperability Strategy. Digital Agenda is realised by a Digitalization Roadmap, which develops the constraint Digital Service Implementation Approach.
Strategy Alignment	Corporate and sectoral strategies must align with: • The Digital Agenda • National Interoperability Strategy • MCDA Digitalization Roadmaps • Whole-of-Government service transformation plans

These elements form the Shared Organizational Content, ensuring coordinated, secure, and consistent service delivery across agencies and borders.

GUIDE FOR ACHIEVING ORGANIZATIONAL INTEROPERABILITY

Achieving organizational interoperability requires deliberate action to align all stakeholders around a common digital service strategy. The following steps should be considered while building the necessary institutional and procedural frameworks.

Step	Activity	Description
1.	**User Identification Standardization**	Enable a single, authoritative identity layer for all public services through creation of a single, authoritative digital identity system for citizens, businesses, and government employees. • Mandate use of the Maisha Number for citizen, business, and government authentication • Enforce uniform identity validation processes across MCDAs • Embed digital identity in all cross-agency workflows and service processes This establishes a "presence-less" digital layer that eliminates redundant citizen verification.

2.	**Standardization of Processes**	Seamless cross-agency service delivery requires the standardization of core government processes to reduce friction, eliminate inconsistencies, and support seamless end-to-end services. • Define national-level standard business processes for recurring government functions • Harmonize data capture, verification, and processing activities • Adopt shared workflow patterns for licensing, registration, approvals, payments, etc. • Implement BPM systems that support interagency process automation • This reduces friction, eliminates inconsistencies, and supports seamless end-to-end services.
3.	**Information Ownership Matrix**	A clear data governance model is required to define who owns and is responsible for specific data assets to clarify accountability and ensure lawful processing across organizational boundaries. • Establish MCDA-specific and cross-agency data owners and stewards • Map datasets to custodians in a national Information Ownership Matrix • Define data sharing rules in compliance with the Data Protection Act and GEA Data Architecture • Enforce responsibilities for completeness, accuracy, quality, and lifecycle management
4.	**Process Agreements**	To formalize and enforce the collaboration required for interoperability formal process agreements between MCDAs are necessary to embed interoperability obligations into day-to-day operations. • Develop MoUs, SLAs, DSAs, and Interoperability Agreements • Define shared responsibilities, service levels, escalation paths, and reporting requirements • Validate agreements with legal, ICT, and operational stakeholders

		• Link service-level compliance to performance management

This process involves extensive discussion and validation with stakeholders to ensure all the digital transformation initiatives and projects are aligned with the national strategies and technical solutions are supported by the necessary institutional and legal mandates.

SEMANTIC INTEROPERABILITY

Semantic interoperability refers to the ability of different information systems to exchange data with shared, precise meaning so that the receiving system can interpret and use the data exactly as intended, without ambiguity or loss of context across organizations. Semantic interoperability ensures:

- Common interpretation of exchanged data.
- Consistent meaning across domains, sectors, and jurisdictions.
- Reliable integration of heterogeneous systems.
- Alignment to national data standards and sectoral taxonomies.
- Accurate automation of digital services and workflows.
- Consistent analytics, reporting, and policy decision-making.

By standardizing meaning, semantics close the gap between simple data exchange (technical) and effective business understanding (organizational), semantic interoperability ensures that the meaning of the data being exchanged is understood unambiguously and in a shared way by all systems and organizations. It extends beyond the data formats to focus on its content and context using common data models, shared vocabularies, and ontologies.

Within the GEA context, semantic interoperability operationalizes the Data Architecture domain and provides the shared vocabulary required for integrated public services, cross-agency analytics, automation, and policy formulation.

Semantic layer is essential for enabling Once-Only, data reuse, interoperability-by-default, and whole-of-government digital transformation interoperability principles.

OBJECTIVES OF SEMANTIC INTEROPERABILITY

I. **Common Meaning Across Agencies**

Ensure all MCDAs use shared definitions, taxonomies, and controlled vocabularies for key data entities.

II. **Standardized Metadata and Data Models**

Adopt consistent metadata schemas (e.g., identifiers, formats, units of measure).

III. **Canonical Data Structures for Interchange**

Define cross-government canonical models for common datasets to avoid custom mappings.

IV. **Enable Cross-Agency Analytics & Reporting**

Facilitate large-scale analytics (e.g., social protection, public health, revenue) with unified semantics.

V. **Improve Automation & Integration Quality**

Allow systems to interoperate semantically without custom adapters or duplicative data cleansing.

VI. **Compliance with DRM and GIF Standards**

Enforce alignment with national data standards, API schemas, and information classification rules.

KEY ELEMENTS

The core elements of Semantic interoperability include:

Element	Description
Shared Vocabularies & Controlled Lists	To achieve precise meaning and overcome divergent interpretations of data, the framework will establish common domains of meaning to prevent inconsistent terminology between MCDAs. These include • Person attributes (e.g., name structure, gender codes, identifiers). • Address format standards (aligned with Kenya National Addressing System). • Business classifications (ISIC codes, economic sector codes). • Government service categories (GEA BRM service taxonomy). • Health, education, tax, and justice sector vocabularies.
Metadata Management	Metadata management is the strategic process of collecting, organizing, governing, and analyzing "data about data" to ensure information is discoverable, trustworthy, and compliant.

	Metadata is an abstraction layer that makes up the underlying information of a domain of an application-sector, which can be seamlessly accessed by the users of other domains. Mandatory metadata standards include: • Definitions (semantic meaning). • Data type constraints (integer, date, enumeration, boolean). • Units of measurement and encoding rules. • Allowed values (e.g., "County" list, "Document Type" list). • Relationship constraints (keys and foreign keys). GEA's Data Architecture specifies national metadata and classification standards which all MCDAs must enforce.
Canonical Data Models (CDMs)	Canonical structures define standard cross-government representation of data entities, attributes, and relationships designed to enable seamless integration between disparate systems and eliminate the need for custom transformations between agencies for common datasets such as: • Citizen Canonical Model • Business Entity Canonical Model • Service Request Canonical Model • Payment Canonical Model • Case Management Canonical Model • By providing a common format, it reduces complexity in data exchange, acts as a "single source of truth," and allows systems to interact through a shared language rather than direct, complex point-to-point mappings
Sector-Specific Data Models & Taxonomies	Sector models are structured, standardized frameworks used to classify and organize information within specific sectors. They must align to national-level CDMs and must not conflict with cross-government semantic standards. • Health information models (patient, encounter, diagnosis).

	• Education data models (student, institution, enrollment). • Revenue/tax models (taxpayer, obligation, remittance). • Justice models (case, court event, offender).
Data Dictionaries	The act as centralized, standardized repositories that define the meaning, structure, and usage rules of data elements across disparate systems to ensure consistent interpretation of shared data across different domains or organizations. Each MCDA must maintain a complete enterprise data dictionary which becomes part of the **GEA EA Repository**, ensuring consistent adoption across systems. It should contain: • Attribute names • Definitions • Data types • Business rules • Ownership and stewardship • Security classification
National Identifiers & Reference Data Sets	These act as the "common language" that enables different systems to exchange data while ensuring the precise, unambiguous interpretation of meaning. Semantic interoperability depends on standard identifiers used consistently across all MCDAs else information exchange is limited to simple data transfer (technical interoperability) without shared understanding. These include: • ID Number – citizen/person unique identifier • Business Registration Number (BRN) • KRA PIN • Parcel/land identifiers (LR) • School NEMIS, health facility, police station identifiers (OB Number) • Location codes (county, sub-county, ward) • GIF mandates these identifiers as authoritative master data sources.
Information Classification Standards	Alignment of semantic rules to security classification levels such as • Public • Internal

	• Confidential • Restricted • Highly Restricted Each classification dictates permissible sharing patterns and metadata labelling.

GIF SEMANTIC VIEW

The Semantic View, shown in *Figure 4* below, defines how data is structured, described, and governed to provide the capabilities required for digital public services to share and understand information consistently in the intended context. It categorized into:

- **Data Management**: How data is organized into datasets and catalogues, metadata, and the use of ontologies and controlled vocabularies to create shared meaning.
- **Interoperability Tools**: Data mapping, linked/open data, distributed ledgers, and virtual datasets for seamless data exchange.
- **Governance**: Data owners, service providers, and consumers establish semantic agreements and follow policies on security, privacy, portability, and open data.

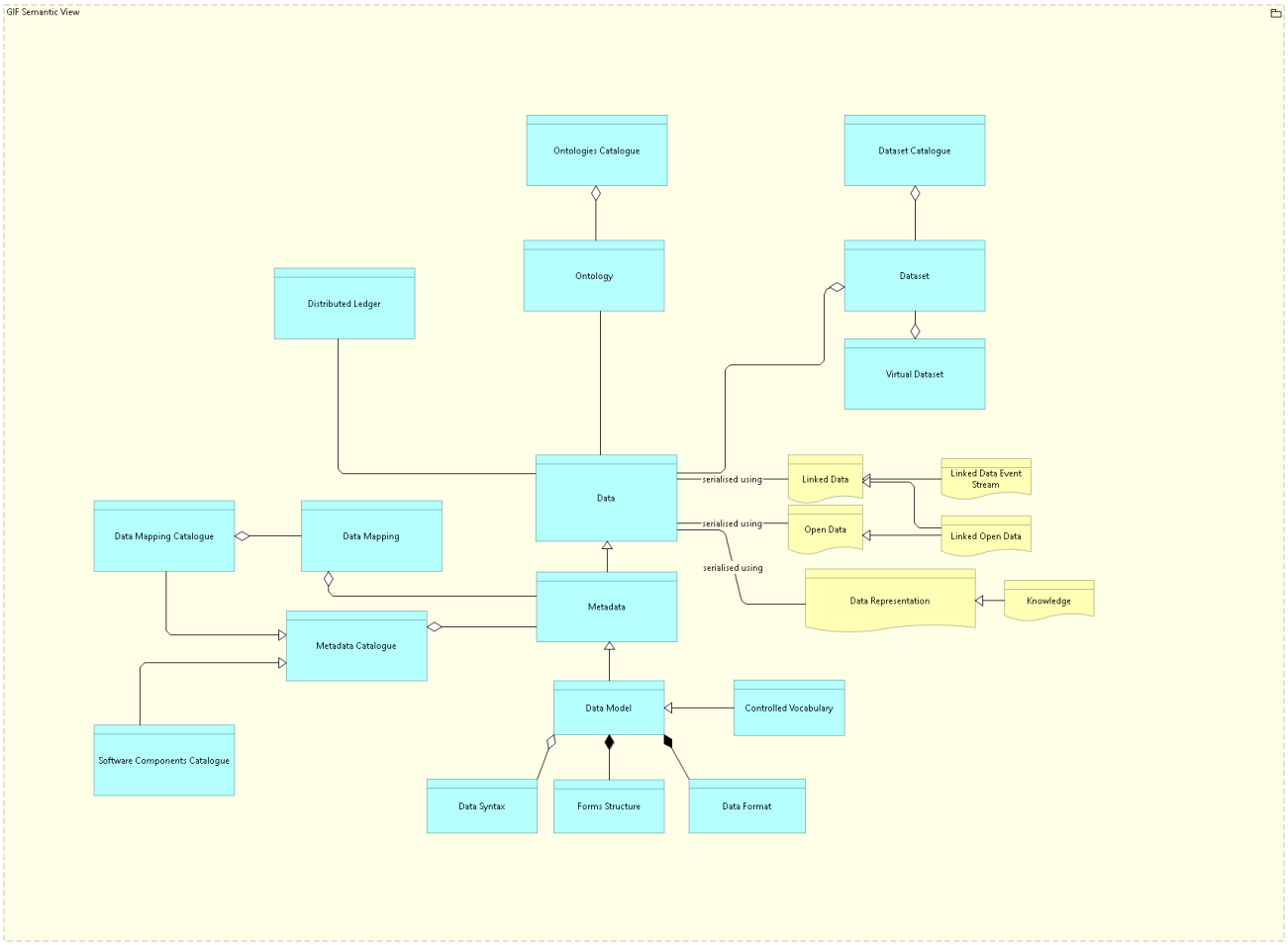

Figure 4 - GIF Semantic View

The GIF Semantic View provides the blueprint for structuring and governing data so that it can be understood and reused consistently across diverse systems and use cases.

The components below form the Semantic Functional Content and Semantic Governance Content, combined as Semantic Knowledge Content to ensure that data exchanged between digital services is accurate, consistent, and meaningful.

Semantic Component	Description
Data to Knowledge	Data & Data Representation: Raw Data is collected, stored and formatted using Data Representation in a specific structure or format. Knowledge Creation: When data is contextualized and properly represented, it becomes useable as Knowledge for decision-making and service delivery.

	Datasets: Data is grouped into Datasets, which are documented in a Dataset Catalogue for discovery and reuse.
Structures and Standards	Ontologies: Define concepts, shared meanings and relationships between data elements in machine readable formats. Ontologies are documented in an Ontologies Catalogue. Data Mapping: Aligns different datasets so they can work together. Mapping details are stored in a Data Mapping Catalogue, which include Metadata, Syntax Mapping, and Software Components. Metadata & Data Models: Metadata describes the context of data and include Data Models (with form structures, data formats, and syntax) and Controlled Vocabularies to ensure consistent terminology.
Data Types	Master and Reference Data: Core, authoritative datasets is stored in a Base Registry. Linked & Open Data: Data that is interlinked or openly accessible; Linked Open Data combines both concepts. Virtual Datasets: Collections of datasets from multiple sources. Distributed Ledger: Enables secure, decentralized sharing of encrypted data across locations. Special Elements: Includes Hash Codes for integrity checks.
Data Governance	Semantic Agreements: Service providers, consumers, and Data Owners agree on how data is defined and used. Policies: Data is managed under Data Policy, which cover Security, Privacy, Master Data, Data Portability, and Open Data policies

STEPS FOR ACHIEVING SEMANTIC INTEROPERABILITY

The development of a 'Kenyan Core Vocabulary' that defines common concepts used across government, such as types of government services, citizen classifications, or geographic administrative boundaries will ensure that information can be correctly routed and understood by different organizations at all levels. These semantic assets will be collaboratively developed across sectors using a structured, standards-based approach.

The following steps will be implemented to build and maintain the necessary semantic assets:

Step	Activity	Description
1.	**Centralized Semantic Repository**	Establish a single, authoritative, centrally governed Semantic Repository will be created and hosted under the national GEA/GIF EA Repository environment. This repository shall: • Serve as the definitive source for all semantic assets (vocabularies, ontologies, taxonomies, canonical data models, code lists, metadata schemas). • Provide open, discoverable, machine-readable formats (e.g. JSON Schema, XML, RDF, CSV). • Support API-based access to metadata, data mapping, dataset catalogues for real-time retrieval of vocabularies and controlled lists. • Integrate with the Government Integration Platform (GIP) to enforce semantic consistency in all API contracts and data exchanges.
2.	**Ontology Development**	Define precise, shared meaning for cross-government entities by: • Identifying concepts (e.g., Citizen, Service, Agency, Payment, Location, etc.). • Defining attributes, permissible values, and constraints. • Documenting business rules, relationships, hierarchies, and semantic relationships (e.g., "Citizen is the subject of Service Request", etc.). See the Appendix section for a sample *GIF Ontology Governance Framework*
3.	**Canonical Data Models (CDMs)**	Create standardized, cross-government data structures for commonly exchanged datasets to ensure consistent meaning and format regardless of agency system design such as: • Citizen CDM, • Business Entity CDM, • Service Request CDM, • Case Management CDM

4.	**Metadata Standards & Schemas**	Develop mandatory metadata schemas which become legally binding in API specifications and DSAs covering: • Field names and definitions • Formats (e.g., ISO 8601 for dates) • Encoding rules • Security classifications • Stewardship and ownership metadata
5.	**Controlled Code Lists & Reference Data Sets**	Develop and maintain versioned and machine-readable authoritative lists for: • County/ward codes, Agency codes, Service category codes • Document types • Sector classifications (e.g., ISIC codes) • Gender, disability, employment, education categories
6.	**Taxonomies and Classification Models**	Define standardized hierarchical classification systems for consistent labelling, routing, analytics, and reporting, including: • Government services • Policy domains • Program categories • Asset types • Public health, education, justice, revenue sector classifications
7.	**Apply a Prescribed Governance and Structural Framework**	All semantic assets must conform to a prescribed data asset structure and modelling standard to guarantee consistency and quality. This structure should align with: • The GEA Data Reference Model (DRM) • The GIF Semantic View • International frameworks (EU-EIF, ISA² Core Vocabularies, NIEM) The governance model will regulate: • Asset creation and modification • Peer review and approval processes • Mandatory stakeholder consultation • Publication and deprecation procedures

8.	**Establish Governance & Maintenance Processes (Lifecycle Management)**	Semantic assets must evolve within a controlled governance environment due to the dynamic nature of government data, legislation, and emerging service needs, **Version Control & Release Management** • Mandatory versioning of all semantic assets. • Clear major/minor versioning conventions (e.g., semantic versioning e.g. Major, Minor, Patch). • Backward compatibility rules for API-based data exchange. **Audit Trails & Historical Tracking** • Full change history for each semantic asset. • Time-stamped edits with author/steward identification. • Documentation of rationale for each change to ensure traceability and accountability. **Automated Alerts & Notifications** Where semantic changes affect systems, the repository must automatically: • Push alerts to registered stakeholders. • Notify API consumers of schema changes. • Trigger CI/CD pipeline checks where semantic validation is enforced. • Warn when deprecated vocabularies or values are still in use. **Annual Semantic Review & Quality Assurance** • Periodic (annual) semantic audits by ICTA and the Semantic Standards Board. • Reconciliation with new legislation, sector reforms, and cross-government service delivery requirements. • Alignment updates to reference models (DRM, ARM, IRM).

Technical interoperability is the foundational layer of GIF that establishes the technical capability of disparate systems to connect and exchange data, invoke services, and operate across MCDAs, regardless of differences in platforms, programming languages, vendors, or deployment environments.

Technical interoperability, however, does not operate in isolation; it implements and enforces the outcomes of legal authority, organizational agreements, and semantic alignment already defined in GIF.

Technical interoperability provides the "plumbing" of digital government, a cohesive collection of integration standards, protocols, interfaces, and specifications that ensure:

- Systems can send and receive data consistently
- Messages conform to shared formats and semantics
- Endpoints are secure and authenticated
- Data exchanges are auditable, traceable, and resilient
- New legacy systems can be integrated without bespoke, ad-hoc solutions

This layer is indispensable for whole-of-government service delivery, the functioning of the Government Integration Platform (GIP), and for enabling the national digital public infrastructure such as digital identity, digital payments, registries, population-scale e-services, and AI-enabled government operations.

OBJECTIVES OF TECHNICAL INTEROPERABILITY

The primary purpose of technical interoperability is to create a unified, reusable, and secure technical integration environment by standardizing the:

- Packaging of data (schemas, payload structures, metadata)
- Transmission of data (protocols, transport layers, encryption)
- Discovery of services (API catalogues, documentation)
- Execution of interactions (API gateways, security servers)
- Validation and governance of technical compliance (PaC, automated policy enforcement)

This is achieved through a catalogue of mandatory technical standards and integration specifications that every MCDA must adopt when developing, modernizing, or integrating digital systems.

Without this technical common ground, even well-designed systems cannot interoperate resulting in fragmentation, redundant solutions, data duplication, and higher operational costs.

KEY PRINCIPLES AND STANDARDS

Elements	Description
API-First Approach	All system integrations within government entities must be designed using an API-first design approach. The use of RESTful APIs (OpenAPI 3.x) will be mandated as the primary integration mechanism due to their simplicity and flexibility, with clear guidelines on their design and security. Event-driven APIs and gRPC interfaces will be permitted for specialized workloads under IRM standards.
Secure Communication Protocols	All data exchanged between MCDAs must be encrypted in transit using TLS 1.3 or equivalent. Authentication and authorization must be enforced through a centralized or federated OAuth2/OIDC system, API gateways, and digital certificates. Only secure, approved cryptographic protocols and cipher suites are allowed.
Service-Oriented Architecture (SOA) and Loose Coupling	GIF adopts a service-oriented, loosely coupled architecture, enabling systems to expose reusable services without interdependencies on internal implementation details. This aligns with international models such as Estonia's X-Road, to provide high levels of resilience, security, and scalability.
Alignment with GEA Domains	Technical interoperability operationalizes the GEA's Technology Architecture, Application Architecture, and Integration Architecture domains by defining the protocols, infrastructure standards, and mechanisms required to ensure systems communicate using approved technical conventions.
Decentralized Security Architecture	GIF advocates for a decentralized security architecture, where each MCDA operates its own security server for secure, auditable, and direct data exchange.

	This model is practical as it avoids the creation of a centralized data hub, which could become a single point of failure and a high-value target for large-scale breaches. The architecture ensures that data flows directly between the sender and receiver, with built-in security features like digital certificates and timestamps for integrity and traceability
Practical Application in Kenya's Context	Kenya should adopt a decentralized interoperability architecture, consistent where: • No central storage of personal data is created • Each MCDA maintains ownership and control of its data • Direct, point-to-point secure exchanges ensure minimal attack surface • Each request is cryptographically signed and logged to provide complete traceability

Technical interoperability is conditional upon semantic interoperability, meaning that system integration, API exposure, or data exchange shall not be implemented unless data definitions, vocabularies, schemas, and reference data are approved under the Semantic Interoperability framework

TECHNICAL INTEROPERABILITY – APPLICATION VIEW

The Application View represents the **application-layer building blocks** (ABBs) required to achieve technical interoperability across government systems. It defines the components and capabilities necessary for applications (new and legacy) to exchange data, collaborate through services, coordinate processes, and enforce consistent technical behavior.

While the infrastructure layer provides connectivity and hosting, the application interoperability layer defines:

- How applications expose and consume services
- How interfaces are standardized
- How processes are coordinated
- How rules and validations are applied
- How application-level security is enforced
- How services are discovered, versioned, governed, and monitored

This layer operationalizes the Government Integration Platform (GIP) and ensures that application systems across MCDAs can function as part of a unified *whole-of-government digital ecosystem*.

OBJECTIVES

The technical interoperability - application view is the functional heart that allows GIF to move beyond technical connectivity toward meaningful, secure, and trusted interactions. The Application View ensures that disparate systems can:

- Interact through standardized APIs
- Coordinate complex workflows and business processes
- Enforce machine-consumable policies
- Maintain technical consistency across distributed systems
- Support cross-border, cross-agency, and cross-platform interoperability
- Remain discoverable, reusable, and governable

The Application View shown in *Figure 5* below depicts the application-level building blocks (ABBs) required to achieve technical interoperability i.e. the ability of different systems to integrate seamlessly and communicate effectively.

These ABBs include:

i) **Interfaces**: Human and machine-to-machine connections
ii) **Process Coordination**: Orchestration, choreography, mediation, and validation
iii) **Operations**: Workflow management, testing, and configuration management
iv) **Security**: Safeguards at the application layer

These building blocks facilitate integrations between applications to operate in a structured, secure, discoverable, and reusable way through APIs, user interfaces, or automated machine interfaces to ensure that digital services in organizations (public or private), including cross-borders, can communicate and cooperate effectively.

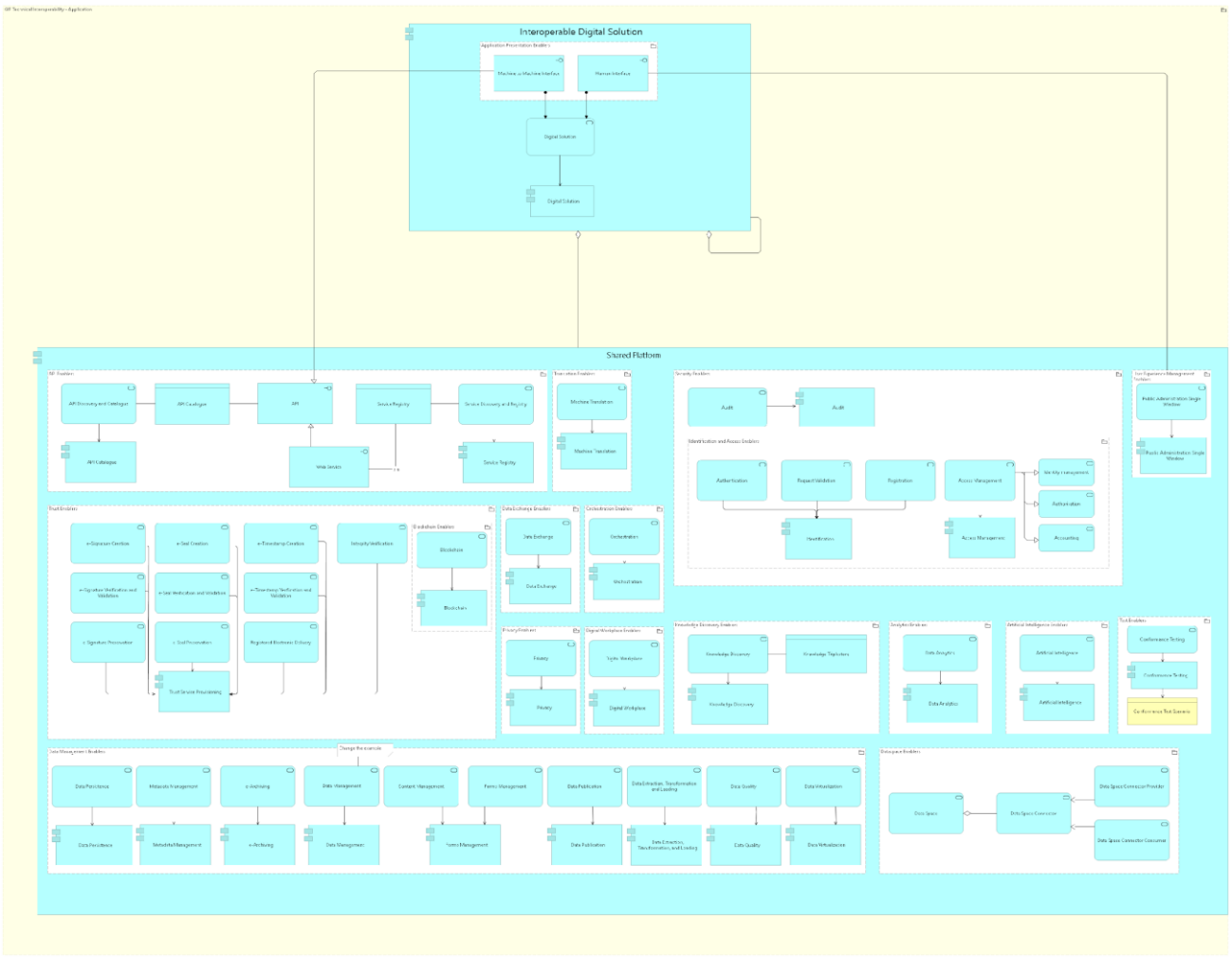

Figure 4 - Technical Interoperability - Application View

The **Interoperable Digital Solution** is the central platform that interfaces people and systems to provide access to digital services and data, supporting the delivery of government and business capabilities to the citizens. It combines a Shared Platform of technical tools and governance agreements to ensure consistent, secure, and reliable operations for machine-to-machine and human interfaces.

At the core is the **Shared Platform**, which provides a wide range of 'enablers' or building blocks. These include API and service management tools for registering and discovering services, orchestration components for coordinating processes, and security features such as authentication, access control, auditing, and blockchain. Testing tools verify compliance, while trust services like e-signatures and e-seals establish secure relationships between systems.

The Shared Platform also contains robust data management capabilities enabling metadata management, storage, archival data quality management, privacy, and analytics and supports

advanced features such as artificial intelligence (AI), machine translation, and knowledge discovery. The dedicated Data Exchange connects data providers and consumers for seamless information sharing.

These elements define the platform's functional and governance content that enable interoperability and technical consistency. The key Architecture Building Block (ABB) are described below at a high level.

Architecture Building Block (ABB)	Description
Human Interface	Web portals, mobile apps, responsive forms, and omni-channel interfaces that provide user-facing access to government services conforming to UX, accessibility, and standard interaction guidelines.
Machine-to-Machine Interface	REST APIs, event streams, service endpoints, SOAP (legacy), and secure message queues. This ABB defines the formal technical contracts, schemas, and interface specifications required for service consumption.
Application Presentation & Access Enablers	API gateways/edge services, front-end delivery. (Maps to API Gateway / Reverse Proxy in SBBs.)
Application Processing Enablers	• Mediation enablers - data translation, validation, transformation) • Decision Support enablers - business rules engines • Maps to ESB/data mapping, validation engines, rules engines.)
Orchestration Service / Choreography Service	Orchestration engines (centralized workflows) vs choreography (event-driven, peer-to-peer interactions).
Functionality Enablers	Application Workflow Enablers, Application Test Enablers, Application Security Enablers Workflow engines, CI/CD and test harnesses, access control and authorization services at the app layer.

TECHNICAL INTEROPERABILITY – INFRASTRUCTURE VIEW

The Technical Interoperability – Infrastructure View defines the physical, virtual, and cloud infrastructure capabilities required to support interoperable, secure, and scalable digital

services across the MCDA ecosystem. It provides a shared, sector-agnostic foundation that ensures systems built can exchange data, invoke services, and participate in whole-of-government workflows reliably and efficiently.

This view translates the GEA Technology Reference Model (TRM) and the GIF technical standards into practical, reusable infrastructure blueprint covering the scope below:

- Compute, storage, hosting, and data platforms
- Network and connectivity infrastructure
- Trust, identity, and cybersecurity foundations
- Integration backbone (API gateways, ESB, event streaming)
- Containers, virtualization, DevSecOps, and automation
- Cross-cutting monitoring, governance, and SLA enforcement

It ensures that all infrastructure supporting systems are interoperable by design, security-hardened, cloud-ready, and aligned with national digital transformation objectives.

The Infrastructure View shown in *Figure 6* below provides a shared, reusable infrastructure that all application layers can reliably be built upon. It enables interoperable digital service delivery through:

- Common hosting environments (GovCloud, hybrid, on-premise DCs, edge)
- Standardized networks (secure WAN, VPN, SD-WAN, firewalls)
- Shared compute and storage services
- Shared identity and trust services
- Integration middleware
- Security and monitoring capabilities
- AI, data, and analytics platforms

It ensures all MCDAs operate on a consistent, secure, standards-driven infrastructure foundation, eliminating silos and incompatible technology stacks.

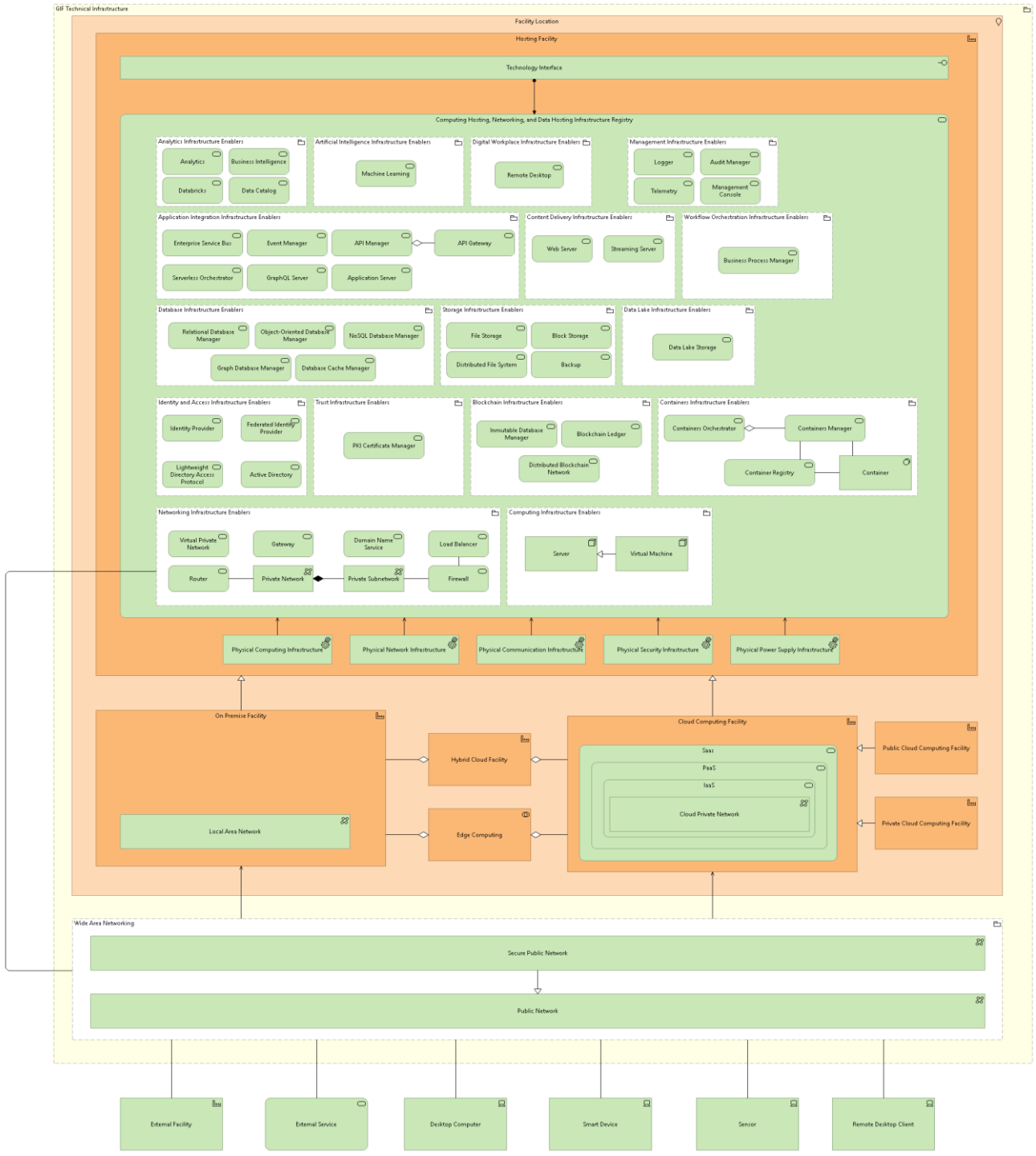

Figure 5 - GIF Technical Interoperability - Infrastructure View

At its core, this view comprises a cohesive set of infrastructure components and enablers that support the development, deployment, and management of modern digital government services. These enablers ensure that capabilities such as data analytics, digital workspaces, integration platforms (ESB, API gateways, microservices), databases, identity management,

storage, networking, and compute resources operate within a standardized, secure, and interoperable environment.

Infrastructure Enabler	Infrastructure Tools
Location Infrastructure	Defines where government systems and data reside across on-premise data centers, regional hosting facilities, and approved cloud environments. It establishes the physical and logical hosting topology required for compliance, sovereignty, resilience, and interoperability. Key elements include: • Government primary and secondary data centers (Tier III or higher) • Regional hosting zones for localized service delivery • Approved public, private, and hybrid cloud environments • Cross-location secure connectivity standards • Hosting policies governing data residency, sovereignty, and classification
Computing Hosting Infrastructure	Provides the standardized processing environment for deploying and scaling government applications across virtualized, containerized, and cloud-native platforms. • Hardened virtual machines running standardized operating system baselines • Container orchestration platforms such as Kubernetes or OpenShift • Secure container registries with digitally signed and verified images • Infrastructure-as-Code tools (Terraform, Ansible, Helm) for automated provisioning • Elastic compute services supporting scaling and high availability
Network Infrastructure	Establishes the secure, high-performance communication backbone for cross-government interoperability which enables systems to exchange data reliably regardless of hosting location. Key capabilities include:

	• Secure Government WAN and GovNet • Network segmentation and micro-segmentation aligned to Zero Trust • Reverse proxies, secure gateways, and controlled ingress/egress • Load balancing for resilient, scalable applications • DNS, DHCP, NTP, and other core networking services • VPNs and encrypted tunnels for cross-agency connectivity • Zero Trust Network Access (ZTNA) for identity-driven access control.
Data Hosting Infrastructure Registry	An authoritative catalog of the government's data assets, including the hosting environments, classifications, and integration endpoints. It must support discoverability, governance, and compliant data sharing. The registry contains: • Lists of all databases, data warehouses, and data lakes • Metadata describing hosting locations, environment types, and sensitivity classifications • Data residency and sovereignty constraints • Registered APIs, connectors, schemas, and integration points • Backup, replication, and disaster recovery configurations
Identity and Access Management (IAM) Infrastructure	Provides a unified authentication, authorization, and credential management across the government ecosystem, enabling secure and standardized access to systems and data. Capabilities include: • Federated identity management (SSO, MFA, SAML, OIDC, OAuth2) • Centralized identity providers for citizens, businesses, and officials • Role-based and attribute-based access control (RBAC/ABAC) • Certificate and credential lifecycle management

	• Privileged Access Management (PAM) • Unified directory services for human and machine identities
Governance & Infrastructure SLAs	All infrastructure must be governed through clear standards, agreements, and compliance mechanisms to ensure quality, reliability, and interoperability. • Interoperability Standards Agreements (ISA) • Formal Service-Level Agreements (SLAs) • Architecture Compliance Reviews (ACRs) • Technical conformance testing • Automated compliance-as-code (OPA/Gatekeeper) Mandatory SLA metrics include: • Uptime (Tier III+ DC or Cloud equivalent) • API latency • Data freshness • Incident response time • Security patching timelines
Storage and Backup Infrastructure	Storage and Backup Infrastructure ensures reliable, scalable, and compliant data persistence and recovery. Key components include: • Primary storage (block, file, object storage) • Archival and long-term compliant storage tiers • Cloud-based elastic storage systems • Automated backup and recovery platforms • DR environments with defined RPO/RTO targets • Synchronous and asynchronous data replication • Immutable storage for logs and regulatory records
Application Integration Infrastructure Enablers	Enables consistent, secure, and scalable data exchange across government systems and operationalizes the GIF's technical and semantic standards. **Enterprise Service Bus (ESB)** Provides routing, transformation, and orchestration of services. Supports: • Protocol mediation

	• Message transformation and validation • Synchronous and asynchronous patterns • Multi-step workflow orchestration • Legacy and modern system integration **API Gateway** Standardizes API exposure, security, and management. Capabilities include: • Central API publishing and lifecycle management • Authentication, authorization, throttling, and rate limiting • API monitoring, analytics, and logging • Enforced compliance with government API standards **Messaging and Event Streaming Bus** Enables real-time, decoupled, event-driven communication. Includes: • Message queues (AMQP, MQTT, RabbitMQ) • Event streaming platforms (Kafka, Pulsar) • Publish/subscribe architectures • High-volume processing for analytics and notifications **Integration Registry** Catalogues all government APIs, endpoints, schemas, and integration metadata, ensuring discoverability and reuse.

GOVERNMENT INTEGRATION PLATFORM (GIP)

The GIP is a federated platform architecture composed of approved integration patterns, shared technical services, and mandatory governance controls that together operationalize the technical, semantic, organizational, and security requirements of the GIF, in alignment with the GEA.

GIP provides the governed interoperability backbone that enables secure, reliable, and semantically consistent data exchange and service interaction across MCDAs and approved external stakeholders.

Role of the GIP in the Interoperability Ecosystem

GIP is not a single system or monolithic platform; it is a **national interoperability enablement capability**, providing shared services that facilitates independently governed systems to exchange data, invoke services, and coordinate processes in a secure, semantically consistent, and legally authorized manner.

By exposing interoperability as a set of governed services, GIP establishes:

- How systems expose and consume services through standardized interfaces
- How multiple integration patterns coexist under governance control
- How semantic consistency and trust are enforced across all exchanges
- How interoperability scales according to MCDA maturity and capacity

It enables consistent and seamless adoption of digital services across varying institutional capacities and technology environments which are consumed by:

- MCDA application systems (new and legacy)
- National shared platforms and digital public infrastructure
- Integration platforms operated by MCDAs under GIF compliance
- Approved external or ecosystem partners where legally permitted

GIP Architectural Principles

The GIP Architecture is governed by the following principles:

I. **Federated by Design** - Data remains with the authoritative source systems. The GIP facilitates exchange without creating a central data repository or transferring ownership.
II. **Governance-First Interoperability** - No technical integration occurs without prior legal authorization, organizational agreement, and semantic approval.
III. **Pattern Coexistence Under Control** - ESB-based, API-based, event-driven, and trusted exchange patterns coexist within a single governed architecture.
IV. **Semantic Interoperability as a Mandatory Prerequisite** - All data exchanges must conform to approved semantic assets, regardless of the technical path used.
V. **Maturity-Driven Adoption** - Advanced capabilities are introduced progressively based on institutional readiness and assessed GIF maturity levels.

GIP REFERENCE ARCHITECTURE

The Reference Architecture in *Figure 7* below shows multiple integration patterns side by side that GIP supports:

- API-based integration for service exposure and consumption
- Trusted exchange (X-Road style) for high-assurance inter-agency data sharing
- ESB-based mediation for complex or legacy integrations
- Event-driven integration for asynchronous, scalable communication

These patterns are complementary, not competing. Pattern selection is governed by use case, maturity, and risk not technology preference and are described in further detail in the sections below.

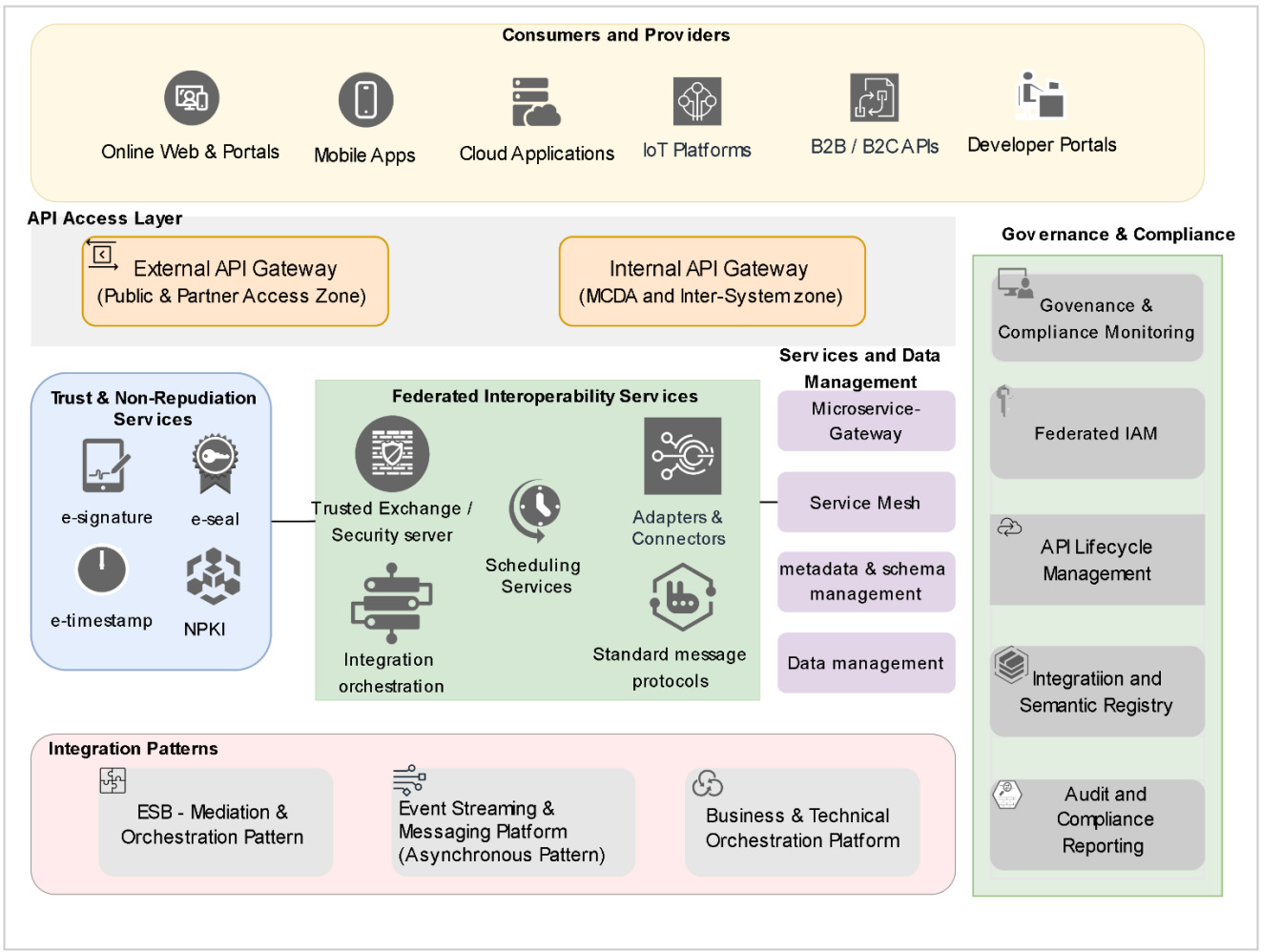

Figure 6- GIP Reference Architecture

The GIP platform has been segmented into six logical layers, each with clearly defined functions as described below.

Layer	Description
Consumers and Providers	Represents entities that consume or provide interoperable services, including MCDAs, national platforms, and approved ecosystem partners. It includes all human and machine actors that consume or provide information and digital services across the government ecosystem. All access passes through this layer mediated through governed interfaces and is subject to GIF security, semantic, and compliance controls provided through the components in the layers below.
API Access Layer	Separate external and internal access zones to enforce security zoning and governance separation: • External API Gateway (Public & Partner Access Zone) Manages access by citizens, businesses, and authorized external systems. It enforces authentication, authorization, rate limiting, and data minimization. • Internal API Gateway (MCDA & Inter-System Zone) Facilitates controlled system-to-system integration across MCDAs and internal platforms. The API gateways enforce: • API lifecycle policies • Semantic validation of payloads • Security standards (TLS, OAuth2/OIDC, certificates) • Monitoring and audit logging
Trust and Non-Repudiation Services	Legally enforceable trust services required for regulated and high-assurance data exchanges. These services ensure Integrity and authenticity of exchanges, non-repudiation and end-to-end traceability. Their application is mandatory where required by law, policy, or data classification.
Federated Interoperability Services Layer	At the GIP core are federated interoperability services, presented as a logical grouping rather than a centralized system. These services may be implemented centrally, regionally, or institutionally depending on organizational maturity and scale. Key capabilities include: • **Trusted Exchange / Security Server** - Implements high-trust, peer-to-peer data exchange consistent with X-Road-style principles, including mutual authentication, digital signatures, and audit logging.

Layer	Description
	• **Integration Orchestration (Pattern-Specific)** – Coordination of multi-step technical interactions where required, without embedding business logic in integration layers. • **Adapters and Connectors** - Enable interoperability with legacy and modern systems while preserving canonical data models. • **Scheduling Services** - Support controlled, time-based data exchanges and batch synchronization, where appropriate. • **Standard Messaging Protocols** - Enforce approved transport and message standards across all integration paths. This layer explicitly does not imply central storage or ownership of data but preserves MCDA autonomy.
Microservices and Data Support Services	This Layer enables modern application interoperability and include the following components: • **Microservices Gateway** for controlled internal service exposure • **Service Mesh** for secure service-to-service communication and observability • **Metadata and Schema Management**, providing technical enforcement point for semantic interoperability • **Data Management Services** for operational data handling (distinct from authoritative data ownership) Semantic assets managed here must be approved and registered before use.
Integration Pattern Layer	The GIP supports multiple, standardized integration patterns, selected based on use case and maturity: • **Enterprise Service Bus (ESB)** - Mediation and Orchestration Pattern Used for legacy integration, protocol transformation, and tightly governed workflows. • **Event Streaming and Messaging Platform (Asynchronous Pattern)** - Enables scalable, decoupled, real-time or near-real-time event propagation across systems. • **Business and Technical Orchestration Platform** - Supports workflow coordination and choreography where process-level integration is required. All patterns are GIF-approved and subject to governance controls. Bespoke, unmanaged point-to-point integrations are prohibited.
Governance, Identity, and Compliance Layer	Cross-cutting layer that provides decision authority and enforcement, not merely tooling. It includes: • **Governance and Compliance Monitoring** - Oversees interoperability governance, approval gates, exception handling, and enforcement actions.

Layer	Description
	• **Federated Identity and Access Management (IAM)** - Provides unified identity, authentication, authorization, and credential management across human and machine actors. • **API Lifecycle Management** - Governs API design, publication, versioning, deprecation, and retirement. • **Integration and Semantic Registry** - Acts as the authoritative catalogue for APIs, schemas, events, semantic assets, and integration endpoints. • **Audit, and Compliance Reporting -** Provides continuous visibility, SLA tracking, audit readiness, and compliance reporting across the GIP.

GIP SERVICE ARCHITECTURE VIEW

The GIP Service Architecture View defines the logical service capabilities provided by the GIP platform to enable, govern, and sustain interoperability across MCDAs, and approved ecosystem participants.

While the GIP Reference Architecture describes the technical composition and deployment patterns of the platform, the Service Architecture View focuses on what services GIP delivers, who consumes them, and how those services collectively operationalize the GIF. This view ensures that GIP is treated as a federated, service-oriented capability, rather than a single monolithic system or technology solution.

The GIP Service Architecture View in *Figure 8* below complements the GIP Reference Architecture by abstracting underlying platforms and components into consumable, governed services. Each service domain may be realised by one or more technical components defined in the Reference Architecture, but the service view remains stable even as technologies evolve.

Together, the two views provide a complete and coherent description of what GIP does, how it is implemented, and how it is governed.

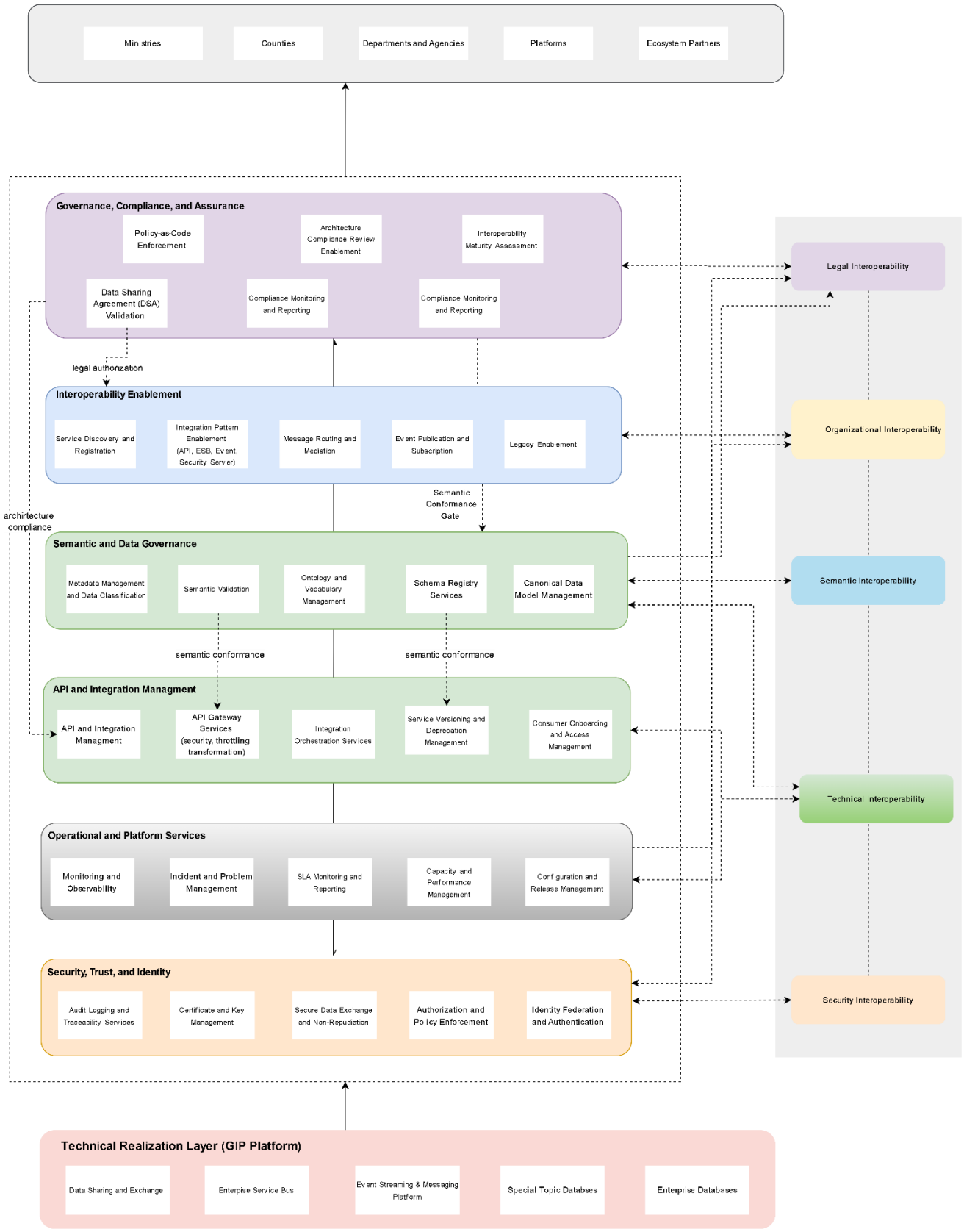

Figure 7 - GIP Service Architecture

The GIP Service Architecture view is not a deployment or vendor diagram its objective is to demonstrate how the GIF interoperability layers are operationalized through GIP services.

Layer	Description
Consumers and Providers	Represents entities that consume or provide interoperable services, including MCDAs, national platforms, and approved ecosystem partners. All interactions must occur through governed GIP services, ensuring uniform enforcement of interoperability rules. No consumer should integrate directly with infrastructure or platforms.
Governance, Compliance, and Assurance Layer	This layer represents the authoritative control plane of the GIP by defining and enforcing the rules under which interoperability is permitted. The DSA Validation capability acts as the Legal Authorization Gate, ensuring that no data exchange occurs without an approved and registered legal basis.
Interoperability Enablement Layer	Provides the core interoperability capabilities that allow systems to connect and exchange information once legal and governance requirements are satisfied. Access to these services is conditionally enabled based on governance approvals. This ensures that interoperability is systematic and standardized, rather than ad-hoc or bespoke.
Semantic and Data Governance Layer	This layer ensures that data exchanged across systems retains consistent meaning and complies with approved standards. The Semantic Conformance Gate enforces that APIs, messages, and events conform to approved schemas and ontologies before they can be published or consumed. This layer operationalizes the principle that semantic interoperability is a prerequisite for technical interoperability.
API and Integration Management Layer	This layer governs how application-level services are exposed, consumed, and evolved across government. This layer is subject to both semantic and architectural compliance gates, ensuring that only compliant interfaces are made available and that changes are controlled and traceable.
Operational and Platform Services Layer	This layer supports the reliable operation of interoperability services but does not define interoperability behavior itself. These services ensure operational stability and performance but do not override governance, semantic, or security constraints.

Layer	Description
Security, Trust, and Identity Layer	The trust layer represents mandatory cross-cutting security controls that apply uniformly across all service domains. Security is not optional or service-specific. All interactions across the GIP are subject to these controls, ensuring confidentiality, integrity, accountability, and trust.
GIP Platform Layer	The GIP layer represents the technical realization of GIP services, including data exchange platforms, enterprise service buses, event streaming platforms, and data stores. This layer is the **Technical Realization Layer**. MCDAs and external systems must not integrate directly with this layer. All access is mediated through the governed service layers above.
Mapping to GIF Interoperability Layers	The right-hand side illustrates how the service architecture components map to the GIF interoperability layers: • Legal Interoperability is enforced through DSA validation and governance services • Organizational Interoperability is supported through onboarding, ownership, and SLA services • Semantic Interoperability is enforced through schema and ontology governance • Technical Interoperability is enabled through APIs, mediation, and event services • Security Interoperability is applied consistently across all interactions The vertical alignment indicates that interoperability layers are hierarchical and interdependent, not independent silos.

GIP GOVERNANCE AND SEMANTIC ENFORCEMENT

Governance and semantic controls apply uniformly across GIP, even where not visually drawn or represented by a connection. The following enforcement rules apply across all layers and patterns:

1. No API, message, or event may be deployed without:
    - Legal and organizational authorization
    - Semantic approval and schema registration
    - Architecture and pattern approval

- Technical and security compliance

2. Mandatory semantic validation occurs at:
    - API gateways
    - ESB mediation points
    - Event schema registries
    - Trusted exchange interfaces

This ensures that interoperability is consistent, lawful, meaningful, and auditable, regardless of technology choices.

GIP Adoption by MCDA Maturity

The GIP architecture is adaptive and allows progressive adoption aligned to the GIF Interoperability Maturity Model using the guidelines below:

- Consume shared gateways and integration services or use simpler integration patterns
- More mature MCDAs to operate independent gateways, event platforms, or trusted exchange nodes
- Progressive adoption aligned to the GIF Interoperability Maturity Model

This reference architecture enables the government to deliver cohesive, secure, and interoperable digital public services across the entire government ecosystem.

GIP INTEGRATION PATTERNS

Integration patterns define architectural mechanisms through which systems exchange data, coordinate processes, and deliver digital services across MCDAs to ensure consistency, resilience, and secure interoperability across digital ecosystems.

Integration patterns operationalize the GEA Integration Architecture by specifying how systems interact synchronously or asynchronously, centrally or in a distributed manner and how data moves between applications while maintaining integrity, availability, and auditability.

GIF mandates the use of approved and standardized integration patterns. Selection of an integration pattern shall be based on service criticality, data sensitivity, institutional maturity, and connectivity context, and shall be subject to architecture governance approval.

Pattern	Description
Enterprise Service Bus (ESB)	ESB acts as the centralized mediation backbone that enables systems to communicate through a shared set of integration services. This pattern is suitable for mature, tightly governed MCDAs with numerous legacy systems requiring transformation, validation, and routing. **Pattern Type:** Centralized, orchestrated, synchronous/asynchronous messaging **Usage Context:** High-governance, structured workflows, legacy system integration, cross-domain orchestration **Key Functions** • Service Orchestration: ESB coordinates multi-step workflows. • Protocol Mediation: Converts SOAP ↔ REST, XML ↔ JSON, HTTP, FTP, SOAP, JMS, SMTP, LDAP, etc. • Message Transformation: XSLT, CSV, SQL, JSON mapping, schema validation, etc. • Centralized Error Handling: Unified retry, reconciliation, and fault logging. • Policy Enforcement: Security, throttling, compliance checks executed at the ESB layer. **GEA/IRM Alignment** • Maps to: SOA/ESB Layer • Supports: Business Process Layer, Service Layer, Messaging Layer • Implements GIF principles: Reusability, Standardization, Security by Design
Message Queuing Pattern (MQ)	Message queuing enables asynchronous communication between systems using durable queues. Messages persist until consumed, ensuring reliability even if the receiver is offline. **Pattern Type:** Asynchronous, decoupled, reliable delivery **Usage Context:** Situations requiring guaranteed delivery, eventual consistency, or decoupling between producers and consumers.

	Key Functions • Guaranteed Delivery: Store-and-forward architecture using persistent queues. • Load Levelling: Prevents overload during high transaction periods. • Producer/Consumer Decoupling: Applications operate independently. • Retry and Dead-Letter Queues: Ensures resilience and robust failure handling. **GEA/IRM Alignment** • Maps to: Messaging Layer under the IRM Integration Architecture • Complements: API Management, SOA, Event-Driven Architecture
Event-Streaming Architecture (EDA)	Event streaming enables systems to publish events that other systems subscribe to and process in real-time. Unlike message queues, events are continuously streamed and often stored long-term. **Pattern Type:** Real-time, high-throughput, publish–subscribe **Usage Context:** Notifications, real-time analytics, policy triggers, cross-agency event propagation. **Key Components** • Event Producers: MCDA systems generating events (e.g., "Tax payment completed"). • Event Brokers: Platforms like Apache Kafka, Redpanda, or RabbitMQ Streams. • Event Consumers: Downstream systems reacting to published events. • Schema Registry: Ensures all event messages follow standardized schemas. • Replay & Audit: Regulatory traceability and forensic investigation capabilities.

Selecting the Appropriate Integration Pattern

The decision tree in *Figure 7* below aims to remove ambiguity and prevent arbitrary or vendor-driven integration decisions. It guides MCDAs to select patterns based on use-case characteristics, not technology preference.

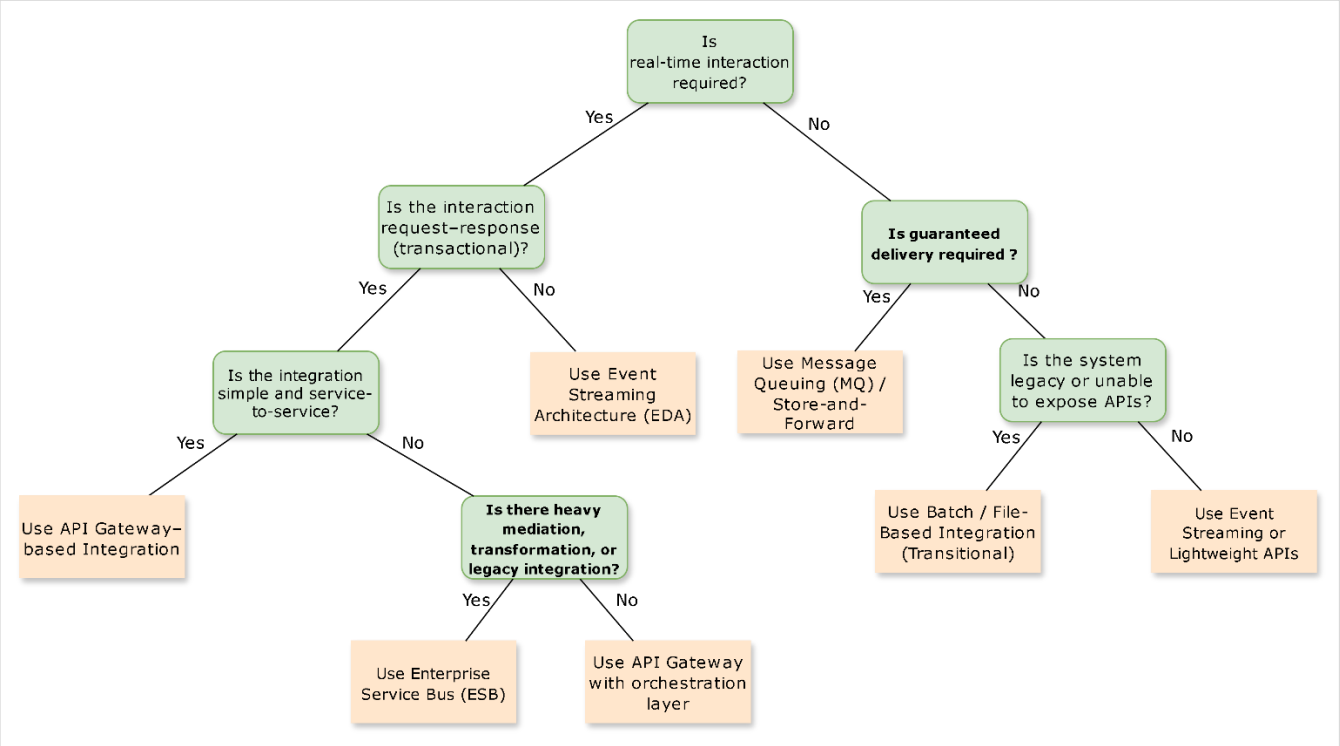

Figure 8 - Integration Pattern Decision Tree

Mandatory Constraints (Governance-Enforced)

The following mandatory constraints should be enforced:

- No integration pattern may be selected without semantic approval
- Advanced patterns (ESB, EDA) shall not be used by MCDAs below Managed (Level 3) maturity
- Bespoke point-to-point integrations are prohibited without governance exception

API LIFECYCLE MANAGEMENT

The API lifecycle governs how APIs are designed, implemented, governed, monitored, evolved, and retired to guarantee quality, semantic correctness, security, and long-term sustainability of interoperability objectives.

API Design Principles

1. **API First**: New digital services must expose APIs as primary integration interfaces.
2. **Reuse Before Build:** MCDAs must prioritize reuse of existing government APIs.
3. **Standardization:** Uniform guidelines must be used for design, documentation, and security.
4. **Security and Privacy by Design:** Mandatory security controls throughout the lifecycle.
5. **Semantic Consistency:** Payloads must use approved data models and taxonomies.
6. **Lifecycle Governance:** APIs must follow a formal lifecycle with clear states.
7. **Discoverability:** All APIs must be listed in the Government API Catalogue.

Key API Capabilities and Components

- **API Gateway:** Central enforcement point for authentication, authorization, routing, rate limiting, analytics, and logging.
- **API Developer Portal**: Supports onboarding, documentation, sandbox testing, and subscription management.
- **Government API Catalogue**: Provides a centralized registry of government APIs, metadata, classifications, and consumption policies.
- **Integration Middleware**: Supports ESB-based orchestration, event-driven communication, and protocol mediation
- **Security Infrastructure**: Includes federated IAM services, token providers, certificate authorities, audit services, and trust frameworks.

Below are the stages of the API lifecycle:

Steps	Descriptions
Design	• Define business capability and interoperability objective. • Align with DRM semantic standards and reference data models. • Model resources, relationships, and naming conventions. • Produce API specifications (OpenAPI, AsyncAPI).
Build & Secure	• Implement API logic using approved development frameworks. • Apply authentication (OIDC/OAuth2), authorization (RBAC/ABAC), and encryption.

	• Conduct vulnerability scans, penetration tests, and conformance tests.
Register & Publish	• Register in the Government API Catalogue. • Publish documentation, usage rules, and required SLAs. • Provide sandbox and testing capabilities in the Developer Portal.
Operate & Monitor	• Monitor performance, latency, usage patterns, and fault rates. • Apply rate limits, quotas, and throttling as required. • Collect security logs, enforce audit trails, and respond to incidents.
Review & Optimize	• Conduct periodic compliance reviews. • Improve APIs with backward-compatible enhancements. • Align evolving semantics with DRM and reference models.
API Retirement	• Follow deprecation procedures with adequate consumer notification. • Remove endpoints from Catalogue and Gateways upon retirement. • Archive metadata and compliance history.

GIF API VIEW

APIs are the primary enabler of government interoperability allowing systems to expose data and services in a standardized, discoverable, and reusable manner. Subsequently APIs must adhere to common design, semantic, legal, and security standards in order to provide the operational backbone for cross-agency interoperability.

The API Interoperability View defines the standards, capabilities, and lifecycle processes required to design, publish, govern, and consume APIs across government. It provides a unified architectural and governance framework that APIs function as consistent, secure, and interoperable interfaces for digital service delivery.

The GIF API View establishes a shared approach for:

- Designing APIs that conform to national interoperability standards
- Ensuring consistency of semantics, naming, data models, and schemas

- Enforcing strong security, identity, and access controls
- Governing API quality, conformance, and lifecycle transitions
- Enabling API publication, discovery, and reuse across the public sector
- Enabling predictable, compliant, and auditable data exchange
- Supporting operational integration patterns such as event-driven, transactional, and real-time services

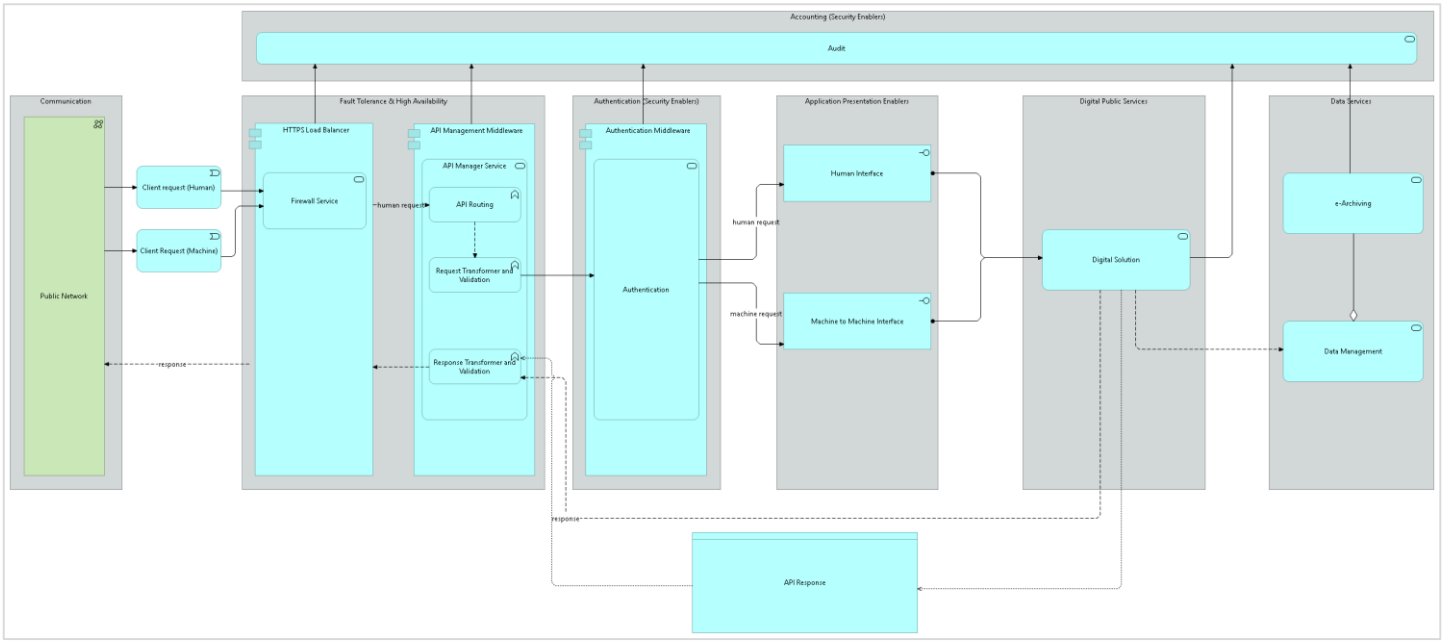

Figure 9 - GIF API View

When a customer or system requests a service, the request first comes in through the Public Network. The GIF system checks:

- Is the request coming from a legitimate, authorized source? (Authentication Service)
- Is the request properly structured and allowed? (Validation)

The request is then sent through a load balancer which directs the request to the correct endpoint responsible for handling the type of service the client requested and handing over the request to the main application service.

The application service passes the request to the application component that contains the business logic (the rules and processing steps), and the component requests the data service to create, retrieve or update information.

Once the required data is retrieved endpoint prepares the response in the format in which it is to be presented (for example, JSON or XML) before sending it back through the system to the requestor and after checking that the response meets the required standards.

ONBOARDING AND MANAGEMENT OF EXISTING APIS

Existing APIs developed prior to the adoption of the GIF framework must be systematically onboarded to ensure alignment with interoperability, security, and semantic standards.

Step	Activity	Description
1.	**Discovery and Registration**	MCDAs must identify their APIs and register them in the Government API Catalogue, including: • Endpoint details • API ownership • Documentation (OpenAPI/Swagger) • Data sensitivity classification • Version information
2.	**Assessment Against GIF Standards**	Each API is evaluated for compliance with: • Security requirements (OAuth2/OIDC, TLS, authorization models) • Semantic standards and DRM-aligned data models • Technical design specifications and naming conventions • Legal and privacy obligations A conformance report identifies gaps and remediation actions.
3.	**Standardization and Remediation**	Non-compliant APIs undergo remediation to: • Update documentation and schemas • Enforce mandated security and authentication controls • Align payloads with standard taxonomy and metadata • Improve naming consistency, error models, and design patterns Controlled exceptions may be granted where temporary deviation is justified.

4.	**Publication and Lifecycle Alignment**	After remediation, APIs are: • Published in the Government API Catalogue • Categorized as Fully Managed, Partially Managed, or Legacy Under Transition • Assigned a lifecycle state (Active, Transitional, Deprecated, Retiring)
5.	**Continuous Monitoring and Governance**	Once onboarded, existing APIs will be governed in the same manner as newly developed APIs through: • SLA monitoring • Security event tracking • Versioning oversight • Periodic Architecture Compliance Reviews
6.	**Migration and Deprecation of Non-Compliant Legacy APIs**	Where APIs cannot meet GIF requirements: • Controlled deprecation timelines are enforced • Migration to government-shared platforms (ESB/API Gateway) is required • Replacement with compliant services may be mandated • This onboarding model ensures older APIs do not compromise interoperability or security.

The GIF API Interoperability View establishes an architectural and governance framework for APIs as strategic integration assets. By incorporating a formal lifecycle management model, including onboarding of existing APIs, GIF ensures uniform, secure, and interoperable API design and operation across the public sector. This view strengthens technical, semantic, organizational, and security interoperability and enables scalable, citizen-centric digital government services.

STEPS FOR ACHIEVING TECHNICAL INTEROPERABILITY

Achieving technical interoperability requires a structured and deliberate approach to ensure that systems can connect and exchange data efficiently.

All technical artefacts including APIs, event schemas, and data payloads shall reference approved semantic assets registered under the GIF semantic governance structures. Technical integrations that do not conform to approved semantic standards shall be deemed non-compliant and shall not be authorized for deployment.

The following minimum steps should be followed during implementation to build a robust technical interoperability foundation.

Step	Activity	Description
1.	**Establish Technical Standards**	Objective: Create the foundation for consistent interoperability where no integration should proceed without standards conformance certification, vendors adhere to open standards and no proprietary protocols allowed. Standards must address: • Open API standards (OpenAPI v3.1, AsyncAPI 3.0) • REST and event-driven interfaces • TLS 1.3, strong encryption • Data serialization formats (JSON, XML, Avro, Protobuf) • Cloud-native standards (OCI, Kubernetes API, Helm)
2.	**Define Infrastructure Conformance Profiles**	Objective: Provide MCDA-specific, reusable interoperability baselines. • Conformance profiles define: • Mandatory cloud/network/security configuration • Canonical data model compliance • Integration protocols • Event schema alignment
3.	**Infrastructure Architecture Blueprinting**	Objective: Ensure all agencies follow a unified reference architecture. This includes: • Standard Network Blueprint • Standard GovCloud Landing Zone • Approved Integration Patterns • Resilience and High-Availability Requirements • DR and Multi-AZ Specifications
4.	**Implement Shared Infrastructure Services**	Objective: Reduce duplication and increase interoperability by default. Shared services must include: • National API Gateway • National Event Bus • National PKI & Trust Framework • Shared Monitoring and Logging Platform • Shared Data Catalog and Metadata Registry

5.	**Compliance, Testing & Certification**	Objective: Ensure infrastructure is interoperable, secure, and operational. Includes: • Automated compliance scans (policy-as-code) • Penetration testing • API conformance checks • Interoperability certification before go-live

All technical artefacts including APIs, event schemas, and data payloads shall reference approved semantic assets registered under the GIF semantic governance structures.

Technical integrations that do not conform to approved semantic standards shall be deemed non-compliant and shall not be authorized for deployment.

GOVERNANCE & COMPLIANCE

Effective implementation of GIF requires robust, enforceable governance and compliance structure. This framework establishes the authority, accountability, and control mechanisms necessary to ensure that interoperability across government is implemented consistently, lawfully, and sustainably.

The governance and compliance framework applies to MCDAs, and authorized external partners participating in government digital services and data-sharing initiatives. Compliance with GIF is mandatory and forms a core component of whole-of-government digital governance.

GOVERNANCE VIEW

The GIF Governance Model defines how policies, agreements, standards, and strategies guide cooperation between organizations and systems. Governance is implemented through clearly defined architectural views and decision-making authorities that together ensure digital services remain interoperable, secure, and consistent across institutions and jurisdictions. Governance under GIF is hierarchical, decision-driven, and enforceable, not advisory.

Elements defined the governance model keeps digital services interoperable, secure, and consistent across organizations and jurisdictions. *Figure 12* below shows the different Architecture Building Blocks that relate to Interoperability Governance from the GIF metamodel.

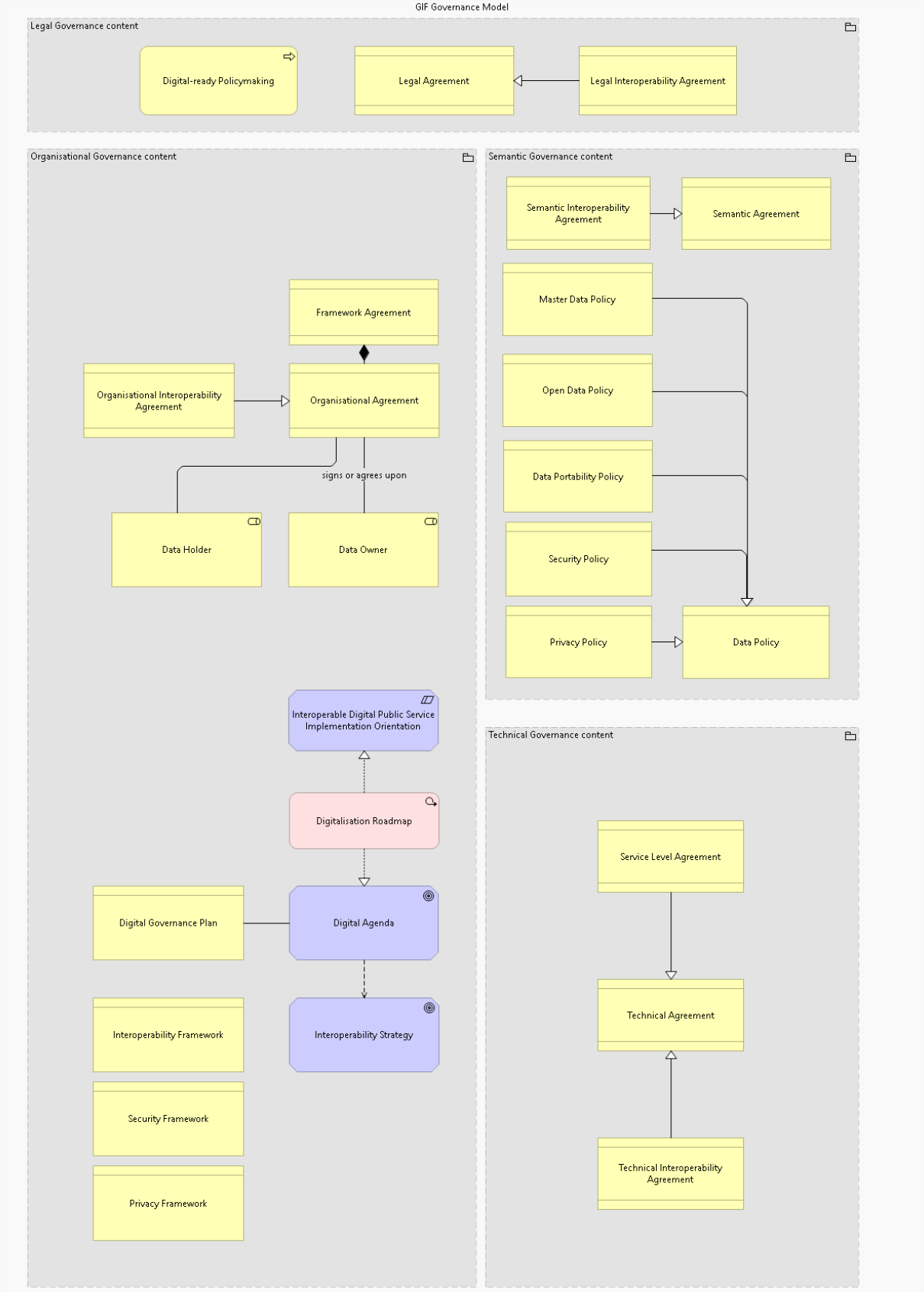

Figure 10 - GIF Governance View

These elements create a unified governance model that keep digital services interoperable, secure, and consistent across organizations and jurisdictions.

1. **Legal Governance Content**

   The Legal Governance View establishes the lawful foundation for interoperability. establishes the legal basis for collaboration between organizations.

   Key elements include:

   - Public policy instruments and the public policy cycle that define strategic direction.
   - Legal Interoperability Agreements that authorize and regulate data sharing.
   - Legal agreements that align with data protection, privacy, records management, and cybersecurity legislation.
   - Clear definition of liability, consent, accountability, and enforcement provisions.

   No interoperability initiative may proceed without explicit legal authorization.

2. **Organizational Governance Content** helps to operationalize legal mandates through institutional alignment. It establishes:
   - Data ownership and stewardship responsibilities formalized through Organizational Agreements.
   - Framework Agreements and Specific Agreements governing service delivery and collaboration.
   - An Interoperability Strategy that implements GIF and aligns with the Security, Privacy, and Skills Frameworks.
   - Delegation of powers for Digital Public Services, realized through the Digitalization Roadmap and the broader Digital Agenda.
   - Oversight by the Interoperability Authority, responsible for coordination and dispute resolution.

Organizational governance ensures that interoperability is executable in practice, not merely permitted in principle.

3. **Semantic Governance Content ensures** that shared data has consistent and agreed meaning. It is governed through:

- A national Data Policy and its specializations that includes
    - Descriptive Metadata Policy
    - Data Portability Policy
    - Open Data Policy
    - Master Data Policy
    - Base Registry Data Policy
    - Reference Data Policy
- Semantic Interoperability Agreements that formalize data definitions, code sets, vocabularies, and metadata standards.

Semantic governance is mandatory before any technical integration is approved.

4. **Technical Governance Content guides** how systems connect and exchange data.
   It is implemented through:
   - Technical Interoperability Agreements defining protocols, interfaces, and integration patterns.
   - Enforcement of approved architectures, platforms, and standards.
   - Alignment with the GEA Technology, Application, Integration, and Security Reference Models.

Technical governance implements the Legal, Organizational, and Semantic governance frameworks and does not operate independently.

GIF COMPLIANCE OVERSIGHT

This is the central governance body mandated by the Ministry of ICT and the Digital Economy (MICDE) for the design, enforcement, and maintenance of the GIF framework under ICTA. The main responsibilities include:

- Setting and enforcing ICT, data, semantic, and interoperability standards.
- Operationalizing GIF requirements across government.
- Conducting architecture compliance reviews and conformance assessments.
- Providing technical guidance and implementation support to MCDAs.

Within the current ICTA setup:

- The Department of Standards enforces technical, data, and semantic standards.

- The Applications and Systems Department issues implementation guidance for digital services and platforms.

GEA/GIF Oversight Board

To provide strategic direction and resolve inter-agency issues, a high-level GEA/GIF Oversight Board will be established. This board will be composed of senior representatives from key Ministries, Counties, Constitutional Commissions, and relevant private sector and civil society stakeholders.

This addresses a major challenge experienced in previous implementations, which observed that the lack of a centralized architecture governance framework often to lower architecture maturity among government institutions.

The key functions of the GEA/GIF Oversight Board are summarized in the table below:

Function Area	Mandate	Key Responsibilities
Strategic Leadership	Provide national political and strategic direction for GEA/GIF adoption	• Set national priorities and sequencing for GEA implementation • Align GEA with national development plans and digital transformation strategy • Champion whole-of-government integration • Resolve inter-ministerial architectural conflicts • Safeguard continuity across political and administrative transitions
Binding Compliance Authority	Serve as the final authority on architecture compliance and policy interpretation	• Issue binding decisions on GEA standards and interoperability mandates • Approve, conditionally approve, or reject ICT initiatives based on compliance • Grant time-bound exceptions under defined conditions • Interpret GEA/GIF policy in cases of dispute

Function Area	Mandate	Key Responsibilities
Strategic Investment Oversight	Ensure ICT investments align with the approved GEA roadmap	• Link compliance with funding approvals • Prevent duplication and fragmented procurement • Oversee rationalization and decommissioning of legacy systems • Enforce dependency sequencing in roadmap execution
Risk and Assurance Oversight	Monitor and manage enterprise-level risks impacting GEA implementation	• Review risk reports across strategic, operational, and technology domains • Ensure cybersecurity and data protection compliance • Escalate systemic risks to Cabinet where required • Direct corrective action for non-compliance or delivery failures
Institutional Alignment	Integrate GEA governance with public sector operational systems	• Align GEA with budgeting, procurement, and audit processes • Require designation of accountable GEA Officers in MCDAs • Mandate adoption of shared platforms (e.g., GIP, data catalog) • Oversee government-wide capacity development
Transparency and Accountability	Ensure decisions are documented, auditable, and transparent	• Publish internal compliance and maturity reports • Maintain formal records of decisions and exceptions • Support oversight by all relevant bodies, levels and arms of government • Require evidence-based decision-making

Function Area	Mandate	Key Responsibilities
Continuous Evolution	Maintain relevance and adaptability of GEA/GIF framework	• Periodically review and update policies and standards • Approve roadmap adjustments based on performance feedback • Ensure controlled adaptation to emerging technologies and regulatory changes

Interoperability Governance Gates and Decision Controls

To prevent fragmented or out-of-sequence implementation, GIF introduces mandatory governance gates aligned with the interoperability dependency model.

All interoperability initiatives must pass the gates in sequence below:

Governance Gate	Description
Legal Authorization Gate	• Verification of legal authority for data sharing. • Approval of data-sharing agreements and legal instruments
Organizational Readiness Gate	• Confirmation of defined roles, responsibilities, workflows, and SLAs. • Validation of institutional ownership and accountability
Semantic Conformance Gate	• Approval of data definitions, schemas, vocabularies, and metadata. • Alignment with national data and semantic standards.
Technical Compliance Gate	• Validation of APIs, integrations, infrastructure, and security controls. • Confirmation of alignment with GEA/GIF technical standards.

Progression to a subsequent gate is prohibited unless the preceding gate is formally approved. For decision authority and escalation:

- Gate approvals are issued by designated authorities aligned to each pillar.
- Failures or disputes are escalated to the GEA/GIF Oversight Board for resolution
- Technical deployment without gate approval constitutes non-compliance.

ACCOUNTABILITY STRUCTURE

Accountability will be ensured through a tiered approach to compliance:

- **Mandatory Reporting**: All MCDAs will be required to submit regular reports to the Oversight Board detailing their progress on the adoption of GIF standards and the status of their digital service integration efforts.
- GIF compliance will be integrated into the ICT planning and budgeting cycle with MCDAs required to submit annual ICT Interoperability Compliance Reports, detailing their adherence to the framework's standards.
- **Regular Audits and Assessments**: ICTA's Directorate of Programmes and Standards will conduct quarterly audits across all MCDAs to determine their level of compliance with the framework. These audits extend beyond checklists and deploy a formal maturity model to track the progress of each MCDA's interoperability
- **Performance Dashboards**: A public-facing performance dashboard will be developed to track key performance indicators (KPIs) related to GIF's implementation, promoting transparency and accountability across government.

GIF COMPLIANCE ENFORCEMENT MECHANISMS

Compliance enforcement will prioritize remediation, correction and enablement but also retain sanction authority. The process for addressing non-compliance will be transparent and structured and for any non-compliant MCDA, a report detailing the extent of the deviation and the prevailing circumstances will be prepared and tabled before the ICTA's Standards Review Board. This board, composed of technical and legal experts, will advise and make recommendations to remedy non-compliance.

The framework will be formally anchored in GIF coordination regulations, providing the necessary legal authority for enforcement. For non-compliance:

- A formal deviation report is prepared.
- The Standards Review Board evaluates technical and legal implications.
- Remediation actions and timelines are mandated.

- Persistent non-compliance is escalated to the GEA / GIF Oversight Board.

ICTA, in line with its statutory mandate will prioritize the formal adoption and enforcement of GEA and interoperability standards, support the establishment and operationalization of the GEA Oversight Board, and provide the necessary oversight, guidance, and institutional support to ensure that all MCDAs achieve and sustain compliance.

AUTOMATED COMPLIANCE GOVERNANCE FRAMEWORK

As systems within the government ecosystem evolve to become modular, API-driven, and decentralized, compliance with GEA and GIF frameworks cannot rely on policy documents, manual reviews, or periodic audits alone. Such approaches are insufficient to manage scale, complexity, and speed of delivery, and they fail to prevent semantic drift, inconsistent interpretations, and fragmented implementations.

Automated Compliance Governance Framework (ACGF) uses AI-driven tools and workflows to automatically discover, classify, monitor, and enforce data policies across an organization. Instead of relying on manual, reactive processes, it provides real-time visibility, consistent compliance, and scalable control as data grows across systems and teams.

Automated Compliance Governance Framework (ACGF) uses AI-driven tools and workflows to automatically discover, classify, monitor, digital assets including APIs, datasets, ontologies, schemas, events, integrations, and infrastructure workloads instead of relying on manual, reactive processes.

It provides real-time visibility, consistent compliance, and scalable control validated against approved GEA and GIF standards before deployment and continuous throughout the lifecycle of digital assets.

This framework operationalizes ontology and semantic governance as executable controls, ensuring that the meaning of data is governed and enforced with the same rigor as security and infrastructure standards.

alignment.

Objectives the Compliance Governance Framework

- Ensure GEA/GIF conformance is consistently enforced to prevent non-compliant architectures, APIs, and data models from being deployed.
- Strengthen interoperability and reduce fragmentation to ensure that all systems adhere to standardized data models, semantics, API protocols, and security controls.
- Establish predictable, audit-ready governance to enable independent auditability and defensibility of digital operations through compliance logs
- Reduce risk, human error, and inconsistency to catch misconfigurations early in design and deployment.
- Improve speed of delivery by providing developers with immediate feedback on CI/CD pipelines, reducing back-and-forth with governance bodies.
- Support ADM Phase G/H governance by providing automated inputs for architecture compliance reviews, change management, and continuous improvement.

Scope and Applicability

The framework applies to all digital assets participating in government interoperability, including:

- APIs, microservices, and events
- Ontologies, vocabularies, schemas, and code lists
- Integration flows and GIP components
- Cloud and on-premises workloads
- CI/CD pipelines and deployment artefacts
- Data pipelines, ETL workflows, and registries
- Procurement specifications and vendor solutions

Compliance is mandatory across design, development, deployment, operation, and change management.

Compliance Governance Principles

The ACGF is built on the following principles:

- **Governance by Design, not Exception -** Compliance is embedded into design, build, deployment, and runtime, not applied after the fact.

- **Semantic Authority as Code -** Approved ontologies, vocabularies, and semantic relationships are enforced through machine-readable rules, not advisory guidance.
- **Shift-Left Enforcement -** Non-compliance is blocked as early as possible, ideally at design or build time.
- **Continuous Assurance -** Approval at one stage does not waive compliance at later stages.

Key Components of Compliance Governance

The ACGF is structured around four key pillars described below:

Pillar	Description
Machine-Readable Standards (MRS)	**All GEA and GIF standards are transformed into authoritative, machine-readable artefacts, including:** • RDF/OWL ontologies defining approved concepts, relationships, and versions • Canonical data models (Avro, JSON Schema, Protobuf) bound to ontology URIs • OpenAPI / AsyncAPI specifications referencing approved semantic assets • YAML catalogues for standards, domains, and ownership metadata • OPA Rego policies encoding governance rules • TRM, DRM, ARM, IRM constraints expressed as validation rules These artefacts form the single source of truth for automated governance.
Policy-as-Code (PaC) Enforcement	Governance rules are expressed as executable policies, enforced automatically using OPA, Gatekeeper, and related engines. PaC enforces, among others: • Use of approved ontologies only (blocking unregistered or conflicting semantic models)

	• Ontology version compliance, including MAJOR/MINOR/PATCH rules • Mandatory binding of APIs, events, and schemas to ontology URIs • Prevention of redefinition of core or base registry concepts • Enforcement of deprecation and sunset timelines • Validation of semantic impact assessment artefacts for breaking changes Semantic governance is therefore not advisory—it is programmatically enforced.
Continuous Compliance Monitoring (CCM)	Compliance is validated continuously across the full system lifecycle: • **Design-Time** EA tools, schema registries, and API design pipelines validate ontology references, version usage, and domain ownership. • **Build-Time** CI/CD pipelines fail builds if: ○ APIs or events lack approved semantic bindings ○ Deprecated ontology versions are used ○ Required mappings or impact artefacts are missing • **Deploy-Time** Kubernetes admission controllers and deployment gates block: ○ Non-compliant manifests ○ Services referencing unauthorized schemas or ontologies • **Run-Time** Continuous monitoring detects: ○ Semantic drift ○ Runtime payload violations ○ Continued use of deprecated ontologies beyond sunset dates
Governance, Accountability & Reporting	All compliance outcomes are logged, aggregated, and reported to governance bodies, including: • Architecture Review Boards (ARB) • Programme Governance Boards (PGB)

	• ICTA standards directorate and central digital governance structures • Internal and external audit • Cabinet-level digital governance dashboards (executive summaries) Semantic compliance metrics include: • Ontology adoption by domain and MCDA • Deprecated ontology usage • Version drift indicators • Outstanding migration obligations

Together, these pillars operationalize GEA principles and GIF interoperability rules into actionable, enforceable code that guarantees whole-of-government consistency and compliance.

SEMANTIC GOVERNANCE ENFORCEMENT ARCHITECTURE

The enforcement architecture operates across the GIF/GEA stack:

GEA Layer	Automated Semantic Enforcement
Business Architecture	Validate service definitions against approved semantic domains
Data Architecture (DRM)	Enforce ontology-backed canonical schemas and classifications
Application Architecture (ARM)	Validate API and event contracts reference approved ontologies
Integration Architecture (IRM)	Enforce schema consistency across ESB, APIs, and event streams
Technology Architecture (TRM)	Ensure infrastructure supports semantic enforcement tooling
Security Architecture (SRM)	Enforce semantic classification in access control and encryption

AUTOMATED COMPLIANCE TOOLS AND COMPONENTS

Component	Description	Role

Semantic Registry	cataloging and managing digital information	Authoritative repository of approved ontologies, versions, and relationships
OPA (Open Policy Agent) / Gatekeeper	Policy engine	Enforce ontology approval, versioning, and binding rules
API Gateway (e.g., Kong, Apigee)	Enforces API standards	Blocks deployment of non-compliant workloads
Schema Registry (Kafka, API Registry)	Stores canonical models	Enforce semantic consistency for events and APIs
CI/CD Integration	Jenkins, GitHub Actions, GitLab	Pre-deployment semantic compliance checks
Compliance Dashboards	Kibana, Grafana	Visibility into ontology adoption and drift
Automated Auditors	OPA plugins, scanners	Detection of post-deployment semantic violations

Integration with Interoperability Pillars

The Automated Compliance Framework enforces compliance across all GIF layers:

Component	Description
Legal	• Ensures data sharing agreements include enforceable metadata classification rules. • Enforces data classification, consent, and sharing constraints via PaC.
Organizational	• Automated checks embedded into MoUs, SLAs, and interoperability agreements. • Compliance dashboards provide inter-agency transparency.
Semantic	• Prevents drift from Kenyan Core Vocabulary. • Enforces ontology approval, versioning, binding, deprecation, and migration automatically
Technical	• Ensures all APIs, events, and integration flows use approved protocols (JSON, REST, OAuth, OpenAPI, etc.). • Enforces protocols, security controls, and infrastructure standards.

Normative Enforcement Rules

1. **No Unapproved Ontologies** - Systems referencing unregistered or conflicting ontologies are automatically blocked.
2. **No Silent Semantic Change** - Breaking changes require approved impact assessments and migration plans.
3. **Deprecation Is Enforced, Not Optional** - Deprecated ontologies are automatically rejected after sunset dates.
4. **Compliance Is Continuous** - Approval at design-time does not exempt runtime enforcement.

The Automated Compliance Governance Framework transforms ontology and semantic governance from policy intent into executable controls, ensuring that shared meaning across government systems is continuously, objectively enforced at scale.

DATA SHARING AGREEMENT (DSA) FRAMEWORK

The Data Sharing Agreement Framework provides the legal certainty, consistency, and enforceability required to enable secure and scalable data sharing across government ecosystem, while ensuring full compliance with the Data Protection Act and national digital governance standards.

DSA Framework transforms data sharing from a legal bottleneck into a standardized, auditable, and DSA instruments for whole-of-government interoperability. The DSA Framework:

- Eliminates repetitive bilateral negotiations
- Reduces legal uncertainty and risk aversion
- Ensures consistent DPA compliance
- Enables faster, safer interoperability
- Strengthens accountability and audit readiness
- Enables scalable, repeatable data sharing across government and beyond

Under GIF, no data exchange may occur without a registered and approved DSA.

STANDARDIZED DSA TEMPLATES

Core DSA Template (Baseline)

A standard government DSA template shall be issued and maintained as part of the GIF legal artefacts. This template is mandatory and may only be extended and not weakened. See the Appendix Section for a *Sample GIF Data Sharing Agreement*

Mandatory Sections (Minimum Legal Requirements)

All DSAs must include, at a minimum:

1. **Purpose Limitation** – Explicit statement of why data is shared, Prohibition of secondary use without approval
2. **Legal Basis for Processing** – Reference to DPA lawful basis (public task, legal obligation, consent where applicable)
3. **Data Description & Classification** – Dataset scope, Classification (public, internal, confidential, sensitive, personal)
4. **Roles and Responsibilities** – Data Controller, Data Processor (if applicable)
5. **Security and Safeguards** – Technical and organizational measures, Encryption, access control, audit logging
6. **Retention and Disposal** – Retention periods, Secure deletion requirements
7. **Rights of Data Subjects** – Access, correction, objection, redress mechanisms
8. **Incident and Breach Management** – Resolution and Notification timelines, Escalation and reporting obligations
9. **Liability and Indemnity** – Allocation of responsibility for misuse or breach
10. **Governance, Review, and Termination** – Review frequency, Termination triggers, post-termination obligations

DSA Approval Workflow

To eliminate ad-hoc negotiations, GIF establishes a clear, time-bound approval workflow as shown in *Figure 13* below

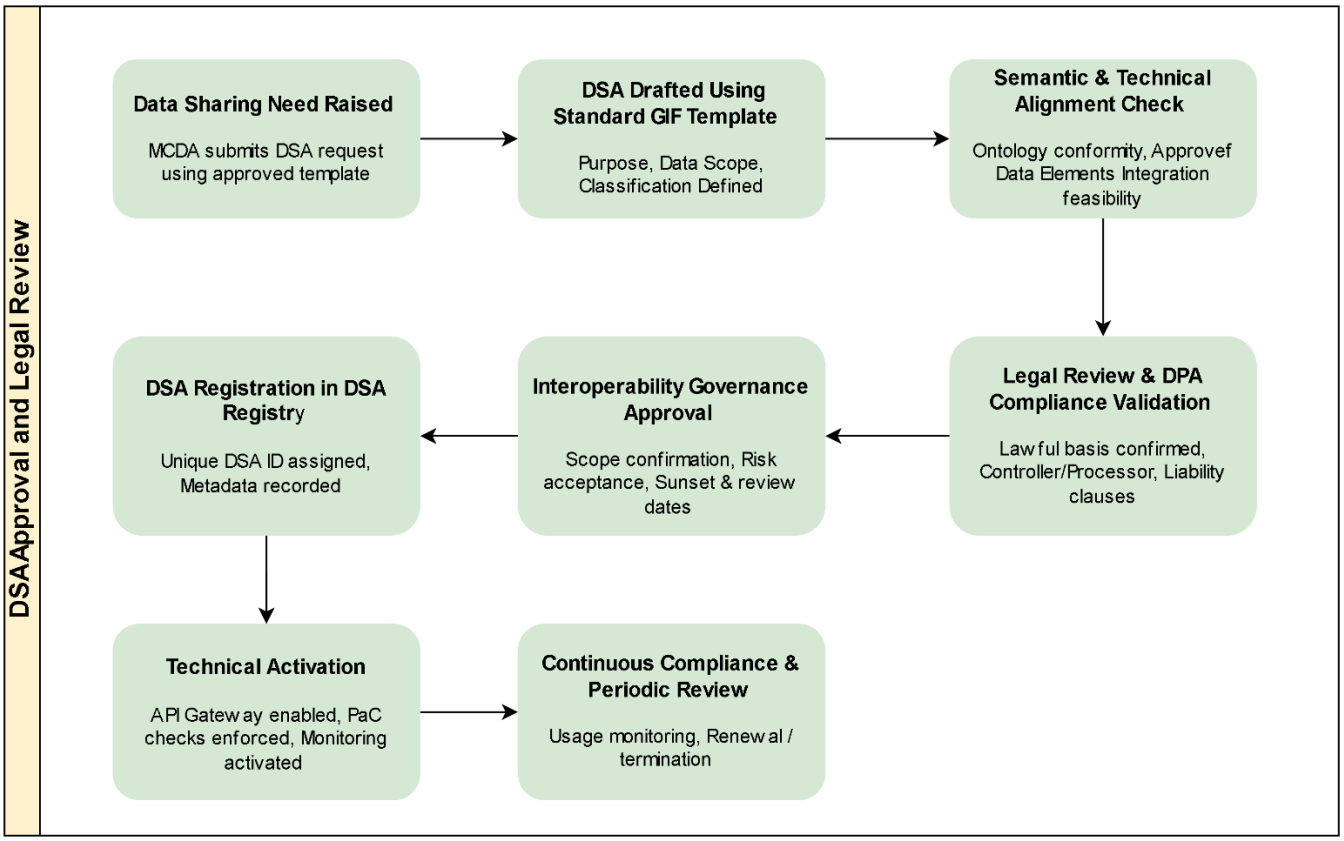

Figure 11 - DSA Approval Workflow

DATA SHARING AGREEMENT REGISTRY

A central DSA Registry shall be maintained to record all active DSAs, track scope, validity, datasets, and parties and provide transparency and auditability

The DSAR will integrate with technical platforms for enforcement and only registered DSAs may enable APIs, data pipelines, or event subscriptions.

Mandatory Registry Metadata

Each DSA record should include:

- Parties to the agreement
- Datasets covered
- Data classification levels
- Legal basis

- Validity period
- Linked APIs and systems
- Security requirements
- Review and expiry dates

The registry integrates with API Gateways to enforce access and Automated Compliance Framework to validate legality.

Sensitive and Personal Data Handling Requirements

For personal, sensitive, or special-category data, DSAs must include enhanced safeguards. Failure to meet these conditions invalidates the DSA:

1. Data Minimization – Share only what is strictly necessary
2. Purpose Binding – Explicit prohibition of reuse or onward sharing
3. Access Controls – Role-based and attribute-based access, Strong authentication (MFA)
4. Encryption – In transit and at rest
5. Audit and Traceability – Immutable access logs, non-repudiation
6. Cross-Border Restrictions – Explicit approval required, Compliance with DPA cross-border rules

Legal Liability and Accountability Allocation

To remove uncertainty, the GIF standardizes liability allocation the Default Liability Model will be used.

- **Data Controller** – Retains primary responsibility for lawful processing and data accuracy
- **Data Recipient / Processor** – Liable for: Misuse, Unauthorized disclosure, Security failures within their control
- **Shared Liability** - Applies where breach results from joint failure

Scenario-Based DSA Templates

To further reduce ambiguity, GIF shall issue pre-approved DSA variants for common scenarios. Each template inherits the core DSA, with scenario-specific extensions. See the *Sample Data Sharing Agreement* in the Annexure Section.

1. **Government-to-Government (G2G)**
    - Internal public service delivery
    - Shared registries and enforcement functions
    - Simplified approval path

2. **Government-to-Business (G2B)**
    - Licensing, compliance, payments
    - Strong commercial confidentiality clauses
    - Clear processor obligations

3. **Government-to-Citizen (G2C)**
    - Consent-based sharing
    - Explicit rights and redress mechanisms
    - Higher transparency requirements

Integration with the Automated Compliance Governance Framework

Under GIF, DSA existence and validity are checked automatically to ensures legal compliance is enforced in real time, not retroactively. No APIs can be exposed without a linked, active DSA.

GIF INTEROPERABILITY MATURITY MODEL

The GIF Interoperability Maturity Model provides a structured, government-wide mechanism for assessing, guiding, and tracking the readiness of MCDAs to implement interoperable digital services. It enables consistent self-assessment, realistic target-setting, and evidence-based prioritization of investments in line with the Government Enterprise Architecture (GEA) framework.

MCDAs currently operate at varying levels of readiness without a common maturity model. While interoperability standards are defined under GIF:

- Agencies may attempt advanced technical integrations prematurely
- Investments may not yield interoperable outcomes
- Fragmentation and duplication may persist

The maturity model ensures sequenced, realistic, and governed progression toward whole-of-government interoperability.

Maturity Model - Key Principles

- Technical interoperability cannot exceed legal, organizational, or semantic readiness
- Each MCDA's overall maturity is capped by its weakest pillar
- Maturity progression is evidence-based and auditable
- The model aligns directly with existing GEA maturity frameworks

Structure of the Maturity Model

The GIF Maturity Model is structured around five progressive maturity levels, assessed consistently across the four interoperability pillars as shown in *Figure 14* below. Each maturity level represents a clearly defined stage of capability, moving from ad hoc and fragmented practices to fully integrated and optimized interoperability.

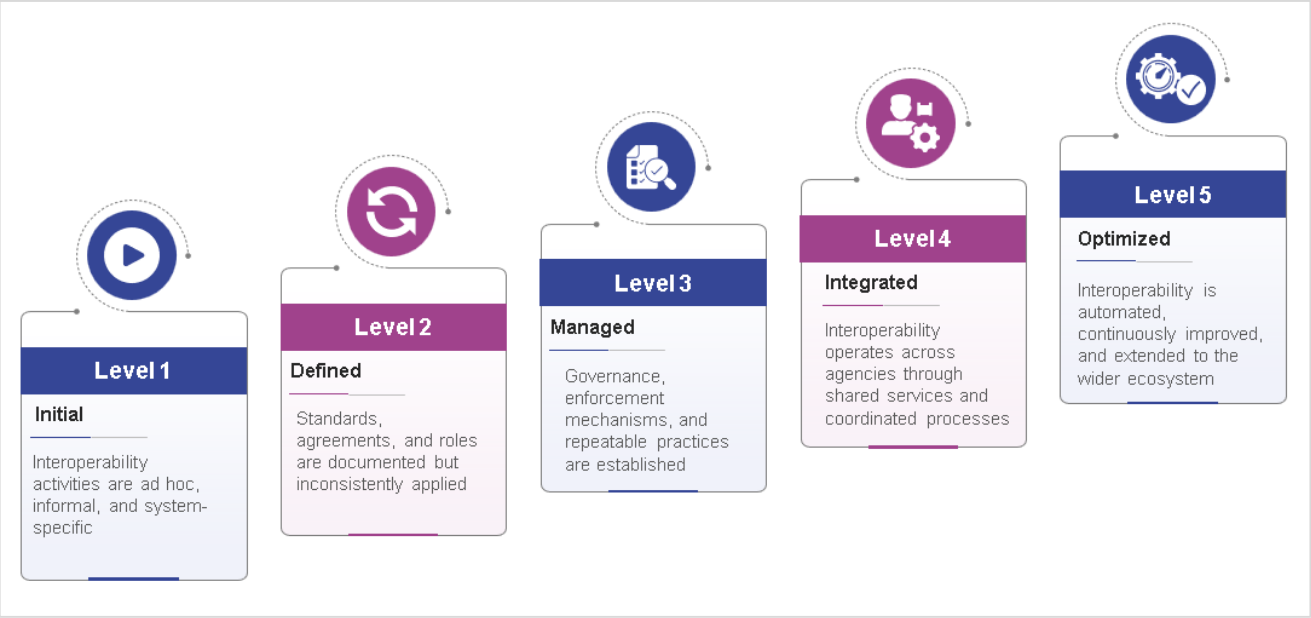

Figure 12 - Interoperability Maturity Structure

Importantly, an institution's overall maturity is constrained by its weakest pillar, ensuring that technical progress does not outpace legal, organizational, or semantic readiness.

Maturity Assessment Criteria by Pillar

Assessment criteria are defined separately for each interoperability pillar to reflect their distinct roles and responsibilities. This ensures that maturity is objectively evaluated and prevents overemphasis on technical integration at the expense of foundational enablers.

Each pillar is assessed independently against level-specific criteria. Advancement to a higher maturity level requires full satisfaction of all criteria at the preceding level, supported by verifiable evidence. Partial compliance does not qualify.

A *GIF Interoperability Maturity Self-Assessment Tool* has been included in the annexure section.

1. Legal Interoperability Maturity

Assesses the existence, enforcement, and harmonization of laws, regulations, and agreements that authorize data sharing and system integration.

Level	Assessment Criteria
1 – Initial	No explicit legal basis for data sharing; ad hoc approvals
2 – Defined	Standard data-sharing agreements exist but applied inconsistently
3 – Managed	Legal interoperability agreements are mandatory and enforced
4 – Integrated	Laws, regulations, and agreements are harmonized across sectors
5 – Optimized	Legal interoperability is proactive, reviewed, and digitally enforced

2. Organizational Interoperability Maturity

Evaluates institutional alignment, governance structures, defined roles, service-level arrangements, and operational coordination.

Level	Assessment Criteria
1 – Initial	No defined interoperability roles or workflows
2 – Defined	Roles and agreements defined per project
3 – Managed	Formal interoperability governance and SLAs in place
4 – Integrated	Shared service models and coordinated workflows across MCDAs

Level	Assessment Criteria
5 – Optimized	Whole-of-government operating model with continuous improvement

3. Semantic Interoperability Maturity

Measures the extent to which shared data meanings, vocabularies, metadata, and reference data are standardized and governed.

Level	Assessment Criteria
1 – Initial	Data definitions are system-specific
2 – Defined	Common vocabularies and schemas documented
3 – Managed	Mandatory use of approved data models and registries
4 – Integrated	Master data and reference data shared across MCDAs
5 – Optimized	Automated semantic governance and change propagation

4. Technical Interoperability Maturity

Assesses the maturity of integration mechanisms, APIs, platforms, security controls, and operational monitoring.

Level	Assessment Criteria
1 – Initial	Point-to-point integrations, manual data exchange
2 – Defined	Standard APIs and protocols defined
3 – Managed	Central API gateways, security enforcement, monitoring
4 – Integrated	Event-driven, reusable, cross-agency integrations
5 – Optimized	Automated compliance, self-healing, analytics-driven optimization

In determination of an MCDA's overall maturity level:

- The overall maturity level is capped by its weakest pillar
- Technical maturity cannot exceed Semantic, Organizational, or Legal maturity
- Self-assessment should be evidence-based (agreements, APIs, schemas, audits)

Interoperability Maturity Progression Roadmap

The maturity progression roadmap shown in *Figure 15* below illustrate common improvement path that MCDAs follow when advancing from one maturity level to the next. This roadmap is

not a rigid prescription but practical guidance that reflects real-world implementation constraints.

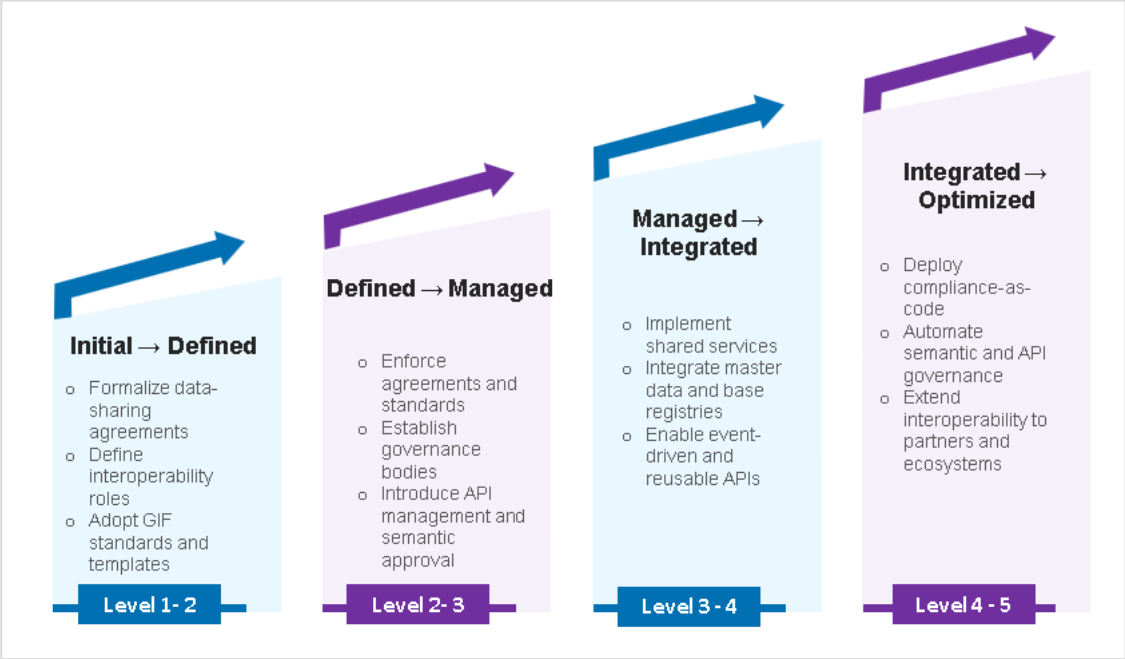

Figure 13 - Maturity Progression Roadmap

Linking GIF Maturity to Funding and Support

The GIF Maturity Model is designed to directly inform funding prioritization and support allocation. Investment decisions should be guided by an institution's demonstrated readiness to absorb and sustain interoperability capabilities.

The maturity model directly informs **investment prioritization and support allocation**:

- Lower-maturity MCDAs receive foundational capacity-building and standardization support
- Mid-maturity MCDAs are prioritized for shared platforms and integration funding
- Higher-maturity MCDAs are enabled to innovate, optimize, and integrate with broader partner ecosystems

Funding is thus linked to **measured readiness and progression**, not ad hoc demand.

By linking funding to maturity levels, government ensures that resources are deployed strategically and equitably, maximizing return on investment while accelerating whole-of-government interoperability.

Alignment with GEA Maturity Models

The GIF Interoperability Maturity Model is fully aligned with the Government Enterprise Architecture (GEA) maturity frameworks to ensure coherence across digital governance initiatives.

Each interoperability pillar maps directly to corresponding GEA domains:

- **Legal Interoperability** aligns with the Governance Reference Model (GRM)
- **Organizational Interoperability** aligns with the Business and Governance Reference Models (BRM, GRM)
- **Semantic Interoperability** aligns with the Data Reference Model (DRM)
- **Technical Interoperability** aligns with the Application, Technology, and Integration Reference Models (ARM, TRM, IRM)

This alignment ensures that interoperability maturity assessments reinforce, not duplicate, enterprise architecture maturity assessments, providing a unified view of institutional digital capability.

Normative Application

All MCDAs shall apply the GIF Interoperability Maturity Model as the official mechanism for assessing interoperability readiness, setting improvement targets, and reporting progress under the GEA and GIF governance framework. The model shall be reviewed periodically to reflect evolving policy, technology, and ecosystem requirements.

LEGACY SYSTEMS INTEGRATION STRATEGY

MCDAs operate mission-critical legacy systems including mainframe platforms, proprietary vendor solutions, and tightly coupled databases that cannot be replaced or modernized immediately without unacceptable operational, financial, or service-delivery risk.

To ensure that such systems are included in the early adoption of the GIF, the Legacy System Integration Strategy defines interim integration approaches, adapter patterns, and controlled modernization pathways.

All legacy system integrations shall be subject to the Interoperability Governance Gates defined under the GIF, including:

- **Legal and Organizational Authorization** to confirm mandate, data-sharing authority, and accountability;
- **Semantic Approval and Registration** to ensure that all exchanged data conforms to approved vocabularies, schemas, and reference data.
- **Architecture and Integration Pattern Approval** to validate the suitability of transitional integration approaches.
- **Technical and Security Compliance Enforcement** prior to deployment.

Legacy integrations approved under this strategy are transitional by design, must be registered within the GIP, and shall be accompanied by a time-bound modernization or retirement roadmap aligned with the GIF Interoperability Maturity Model.

Governing Principles for Legacy Integration

Legacy integration under GIF is governed by the following non-negotiable principles:

- **Participation Before Perfection** - Legacy systems may participate through controlled adapters without full modernization.
- **No Direct Coupling** - Legacy systems shall never be directly coupled with consuming systems. Point-to-point integrations are prohibited.
- **Canonical Mediation Require** - All data exchanged must conform to approved semantic models.
- **Temporary by Design** - Legacy integration patterns are transitional and must have an exit path.
- **Governed and Auditable** - All legacy integrations remain subject to GIF governance gates and compliance checks.

Legacy System Integration Patterns

Pattern	Description	Typical Legacy Systems	Use Cases	Governance Constraints
API Wrapper / Facade	A controlled service layer exposes selected legacy functions or data as governed APIs without modifying the core legacy system.	Mainframes, COBOL applications, proprietary vendor systems	Transaction queries, controlled updates, service exposure	Must pass Legal & Organizational Authorization Semantic Approval, Architecture Pattern Approval Technical & Security Compliance gates
Message Broker / Store-and-Forward Integration	Asynchronous messaging between legacy systems and consumers using queues or brokers to decouple systems and tolerate outages.	Batch systems, systems with intermittent connectivity	Notifications, event propagation, guaranteed delivery scenarios	Message schemas must be approved; retry and audit logging mandatory
Database Replication / Controlled Data Extract	Periodic or near-real-time replication of selected datasets from legacy databases into governed data stores (read-only).	Legacy RDBMS, proprietary databases	Reporting, analytics, reference data dissemination	Write-back prohibited; data minimization, classification, and approval mandatory
File-Based / Batch Integration (Last Resort)	Secure exchange of files on a scheduled basis using canonical formats and schemas.	Very old or vendor-locked platforms	Low-frequency, non-real-time data exchange	Explicit governance exception required; sunset timeline mandatory
Change Data Capture (CDC) Adapter	Captures and publishes data changes from legacy databases as events or messages without altering applications.	Legacy databases supporting logs or triggers	Event-based synchronization, incremental updates	Schema registration and version control mandatory
Screen-Scraping or UI Automation	Automated extraction via user interfaces.	Legacy thick-client systems	Not permitted under GIF	Prohibited due to fragility, security, and audit risks

Strategic Guidance

Context	Recommended Approach
Mission-critical, high risk	Wrap + gradual modernization
Obsolete, low-value system	Replace immediately
Vendor lock-in	Wrap + exit roadmap
Budget constrained	Wrap first, modernize incrementally

Minimum Requirements for Legacy System Participation in GIF

A legacy system may participate in GIF only if it meets the following minimum conditions:

1. **Controlled Interface -** Interaction occurs only through approved adapters.
2. **Semantic Compliance** - Data exchanged conforms to approved schemas and vocabularies.
3. **Security Baseline** - Encryption in transit, identity enforcement, and audit logging are mandatory.
4. **Governance Registration -** System, interfaces, and adapters are registered in GIF registries.
5. **Modernization Roadmap** - A time-bound migration or retirement plan is approved.

Systems that cannot meet these conditions shall not be integrated into the GIP.

GIF INTEROPERABILITY DEPENDENCY MODEL

The GIF interoperability layers do not operate as parallel or independent dimensions. They form a hierarchical dependency chain, where each layer enables or constrains the next. Implementation must follow this order to avoid functional, legal, and semantic conflicts.

The Interoperability Dependency Model establishes a **mandatory hierarchical structure** for implementing interoperability across MCDA and the government ecosystem partners. Its primary objectives are to:

- Ensure lawful, meaningful, and secure data exchange across government and partner systems
- Prevent fragmented or out-of-sequence implementations of interoperability pillars

- Guarantee that technical integrations reflect agreed legal mandates, business responsibilities, and data meaning
- Provide a clear implementation order that MCDAs must follow when designing or integrating systems
- Enable enforceable governance and compliance decisions based on explicit prerequisites

PILLAR ROLES AND DEPENDENCY OBJECTIVES

1. Legal Interoperability

The objective is to establish GIF's authority and legitimacy i.e. the legal mandate, permissions, and constraints for data sharing and system integration.

Without legal authority, data exchange is unlawful, unenforceable, and exposes the entire ecosystem to regulatory and reputational risk. Legal interoperability defines whether data can be shared and under what conditions.

2. Organizational Interoperability

Aligns institutional roles, responsibilities, processes, and service arrangements that operationalize legal mandates.

Organizations can only agree on processes, ownership, or service delivery collaboration on a basis of a legal collaborative framework. Organizational interoperability provides accountability and execution i.e. who does what, how, and when.

3. Semantic Interoperability

Semantic Interoperability ensures that shared data has a consistent, agreed meaning across all participating systems and institutions. It defines what the data means.

It depends on the Legal and Organizational Interoperability pillars to provide clarity on:

- Who owns the data
- Who is authorized to define and change meanings
- How data will be used operationally.

4. Technical Interoperability

Technical Interoperability pillar implements the physical and digital mechanisms that exchange data and integrate systems. It does not define meaning, authority, or responsibility rather it implements only them. APIs, integrations, and networks must reflect:

- Legal permissions
- Organizational workflows
- Semantic definitions

Technical interoperability only defines how data is exchanged but not why or what it means.

NORMATIVE DEPENDENCY RULES

1. **Legal Interoperability and Organizational Interoperability are foundational enablers**.
   Without legal authority and organizational alignment, no data exchange is legitimate or operationally sustainable.
2. **Semantic Interoperability is a mandatory prerequisite for Technical Interoperability.**
   Technical connectivity without agreed meaning results in syntactic exchange but semantic failure.
3. **Technical Interoperability is an implementation layer, not an independent capability.**
   It operationalizes and enforces the outcomes defined by Legal, Organizational, and Semantic interoperability. Therefore, Technical Interoperability must never be implemented in isolation or ahead of the other pillars.

HIERARCHICAL DEPENDENCY STRUCTURE

Interoperability pillars within the GIF are not equal, interchangeable, or independent. They form a dependency-driven hierarchy, where each pillar constrains and enables the next. This hierarchy exists to ensure that:

- Authority precedes exchange
- Responsibility precedes automation

- Meaning precedes connectivity
- Connectivity enforces, not defines, interoperability

The interoperability pillars are sequenced as follows:

1. Legal Interoperability (Foundation Layer)
2. Organizational Interoperability (Operational Enablement Layer)
3. Semantic Interoperability (Meaning and Information Layer)
4. Technical Interoperability (Implementation Layer)

Each layer is dependent on the successful establishment of the layers beneath it (See *Figure 11*); parallel work is allowed only where prerequisites are already satisfied and formally approved. Ignoring this hierarchy during implementation results in technically functional but operationally unusable systems.

INTEROPERABILITY PILLAR DEPENDENCY MATRIX

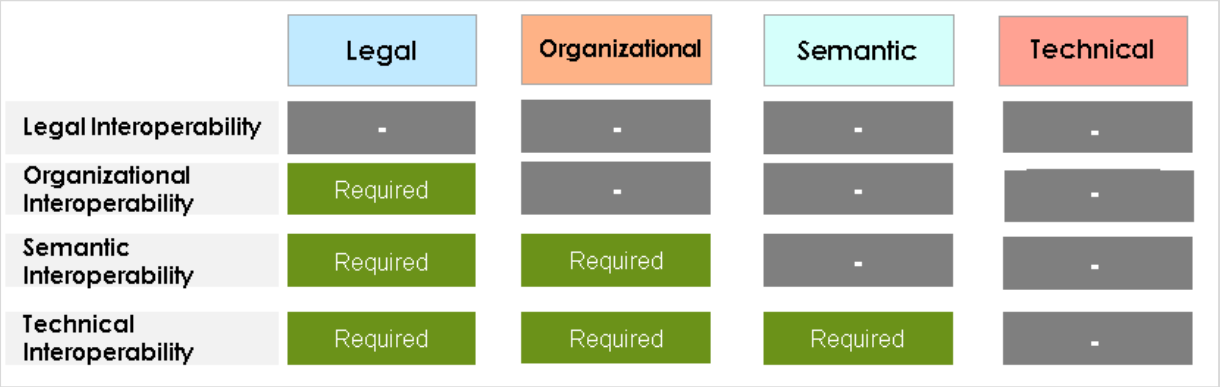

Figure 14- Interoperability Dependency Matrix

- **Legal - Organizational Interdependency**

Legal interoperability establishes authority to share data between organizations. Organizational interoperability defines who does what, how, and under which operational rules. Organizational arrangements cannot exist without legal mandate.

- **Legal & Organizational - Interdependency**

Semantic agreements - data definitions, code sets, metadata are meaningless if data cannot legally be shared, or there is no agreement on business ownership, stewardship, and use

between organizations. Semantic modeling depends on both legal clearance and organizational agreement.

- **Semantic - Technical Interdependency**

Technical interoperability must not proceed unless:

- Data elements are defined
- Meaning is standardized
- Reference data and metadata are agreed

Failure to observe this dependency results in APIs that exchange data correctly but interpret it incorrectly and integration defects that are expensive and difficult to detect. This may lead to lack of trust and operational disputes between institutions leading to poor service implementation.

As control measures the framework should explicitly prohibit the following:

- Implementing APIs or integrations before semantic standards are approved
- Connecting systems to live systems before data-sharing authority is established
- Declaring technical compliance without cross-pillar compliance confirmation

This eliminates the risk of pillar-by-pillar implementation in isolation, which is the root cause of the fragmentation.

INTEROPERABILITY USE CASES – Demonstrating pillar interdependence

The following use cases illustrate how the four interoperability pillars—Legal, Organizational, Semantic, and Technical—operate together as a single, dependent system in real government implementation scenarios. This demonstrates that effective technical integration is only achievable when legal authority, organizational alignment, and shared data meaning are firmly established first. The use cases are intended to provide practical guidance to MCDAs, reinforce the hierarchical nature of the framework, and prevent isolated or out-of-sequence implementations that lead to interoperability failure.

Use Case 1: National Identity Verification for Digital Public Services

Multiple MCDAs require real-time identity verification using the National ID Register to deliver services such as licensing, social benefits, and permits.

Interoperability Pillar	Pillar Role	Objective	Risk Exposure
Legal	Provide authority to share identity data with specific MCDAs	• Legal mandateauthorizes the National ID Authority to share identity attributes with specified MCDAs. • Consent rules, data-sharing agreements, and privacy controls define which attributes may be shared, for what purpose, and under what conditions.	Identity exchange is unlawful regardless of the technical capabilities
Organizational	Defines roles and operational use	• Directorate of Population Registration Services is designated as provider • MCDAs as consumers and define services in their workflows. • SLAs specify response times, availability, and escalation procedures	Disputes over responsibility and service failures occur
Semantic	Ensures consistent interpretation of identity attributes	• Standard definitions and attributes and values for ID number, status, DOB, name • Common metadata specifying attribute sensitivity and usage constraints.	Organizations interpret identity status differently, leading to incorrect service decisions.

Interoperability Pillar	Pillar Role	Objective	Risk Exposure
Technical	Implements secure identity verification	• Secure APIs expose identity verification services. • OAuth2 and mTLS enforce access control. • Responses follow agreed schemas and code sets.	Systems connect but return unusable or misinterpreted data

Use Case 2: Social Protection Eligibility

A social assistance program requires income, employment, and civil registration data from multiple agencies to determine citizen eligibility.

Interoperability Pillar	Pillar Role	Objective	Risk Exposure
Legal	Authorizes sharing of personal and income data	• Legal basis, purpose limitation, retention rules are established. • Purpose limitation restricts use of data to eligibility assessment.	Breach of privacy and legal challenges
Organizational	Aligns agencies and decision processes	• Each MDA's role is defined: data provider, decision authority, appeals handler. • Business processes align eligibility checks with SLAs.	Delays and inconsistent decisions resulting in service quality issues

Interoperability Pillar	Pillar Role	Objective	Risk Exposure
		• Governance body resolves disputes and data quality issues.	
Semantic	Defines eligibility criteria consistently	• Standard definitions for key attributed such as income, household, employment. • Agreed calculation rules and reference periods. • Harmonized code lists for employment categories.	Wrong decisions and eligibility outcomes.
Technical	Automates data exchange and assessment	• APIs and event-driven services exchange eligibility data. • Data is aggregated and evaluated automatically. • Audit logs track every data access and decision.	Manual workarounds and unreliable results

GIF VENDOR EVALUATION CRITERIA

The government procurement process and solution delivery must be aligned to GIF standards from the outset to ensure that GIF is implemented consistently across all MCDAs. Procurement is a primary enforcement lever for interoperability because it determines which technologies, vendors, and delivery approaches are adopted across the public sector.

This section establishes mandatory procurement and solution assurance requirements to ensure that all systems, platforms, and services acquired or developed for government use are interoperable by design, compliant with Kenya's legal and security obligations, and capable of being governed through the GIF compliance framework.

All ICT procurements and system delivery initiatives that involve government data exchange, integration, or digital service delivery shall comply with the GIF and GEA standards. This applies to:

- New systems development and acquisition
- Modernization and enhancement of legacy systems
- Shared platforms (API management, ESB, event streaming, registries)
- Cloud and data platforms
- Managed services and outsourced operations
- Vendor solutions deployed within MCDAs or across government

No solution shall be approved for deployment where it introduces fragmentation, bespoke point-to-point integration, uncontrolled semantic definitions, or vendor lock-in that undermines whole-of-government interoperability.

Mandatory Procurement and Assurance Requirements

All vendor proposals and solutions shall be required to demonstrate, as a condition of procurement and acceptance:

1. **GIF Technical Interoperability Compliance**

The solution must support API-first integration and adopt approved interoperability patterns aligned to the Government Integration Platform (GIP), including secure interface exposure, managed integration, and standard protocols.

2. **Semantic Interoperability and Standard Meaning of Data**

The solution must support alignment to approved government vocabularies, canonical data models, and ontology-governed semantics, ensuring that data exchanged across MCDAs retains consistent meaning.

3. **Security and Trustworthiness by Design**

The solution must implement mandatory security controls including secure authentication and authorization, encryption, audit logging, and traceability, consistent with national cybersecurity and data protection expectations.

4. **Legal and Data Protection Compliance**

The solution must be capable of complying with the Data Protection Act (2019), including purpose limitation, minimization, retention enforcement, incident response readiness, and lawful handling of sensitive data.

5. **Governance and Automated Compliance Readiness**

The solution must support enforcement through automated governance controls, including policy-as-code enforcement, compliance validation in CI/CD pipelines, and audit-ready evidence generation.

6. **Operational Sustainability and Service Assurance**

The solution must support monitoring, incident management integration, resilience, and service-level assurance to ensure that interoperability services remain reliable and measurable in production environments.

7. **Portability and Lock-In Prevention**

The solution must use standards-based interfaces and formats, enable configuration and data export, and provide an exit strategy to preserve government sovereignty and flexibility.

8. **Capability Transfer and Reduced Vendor Dependency**

All procurements shall include enforceable requirements for skills transfer, operational documentation, and local capacity development to ensure long-term sustainability.

Solution Assurance and Acceptance Controls

GIF compliance shall be enforced through standard solution assurance mechanisms, including:

- Architecture Compliance Reviews (ACRs) as a prerequisite for approval and release
- Proof-of-Concept (PoC) demonstrations for high-impact integrations and shared platforms
- Mandatory evidence of interoperability conformance, including governed APIs, registered schemas, and compliance logs
- Integration with the Automated Compliance Governance Framework to ensure continuous enforcement and prevent drift after go-live
- No system shall be operationalized within the government ecosystem without demonstrating compliance at design-time and deploy-time governance gates.

Vendor Evaluation Criteria (Scoring Model)

A detailed evaluation criterion, scoring structure, evidence requirements, and recommended weightings for vendor assessment are defined in the *Detailed GIF Vendor Evaluation Criteria and Scoring Model* in the Annexure Section.

The guidelines shall be applied by all procuring entities as the standard assessment framework to ensure consistent vendor selection decisions across government.

SECURITY & DATA PROTECTION FRAMEWORK

The interoperability security framework establishes standardized rules, policies, and technical controls to ensure secure, trustworthy data exchange between systems in the government ecosystem particularly across organizational or national borders. Key components cross-cut legal, organizational, semantic, and technical interoperability layers, ensuring data integrity, privacy, and mutually recognized security standards

When public institutions and other entities exchange information, it must be based on established security requirements, via a secure, harmonized, managed, and controlled network. Citizens and businesses must be confident that when they interact with public institutions they are interacting in a secure and trustworthy environment and in full compliance with relevant policies and regulations.

Interoperability must never compromise security or data privacy. Appropriate mechanisms must be in place to allow for secure exchange of electronically verified messages, records, forms, and other kinds of information between the different systems; handle specific security requirements and electronic identification and trust services and monitor traffic to detect intrusions, changes of data and other types of attacks.

KEY ELEMENTS

GIF is built on the principle of “Privacy and Security by Design”, ensuring that data sharing is both seamless and secure. These include:

Legal Alignment	The framework's security protocols are fully aligned with the Kenya Data Protection Act, 2019, and relevant global standards such as ISO/IEC 27001
Key Architecture Building Blocks (ABBs)	**Encryption** - All data in transit and at rest will be encrypted using strong, modern cryptographic algorithms. **Authentication and Authorization** - APIs will use robust, token-based authentication (e.g., OAuth 2.0) and granular access control to ensure only authorized entities can access data. **Secure APIs** - All API endpoints will be secured and managed through a central API Gateway, which will handle authentication, throttling, and logging. *(see more details in the Core Architecture Building Blocks section)*

Risk-Based Security Management	MCDAs will be required to conduct Data Protection Impact Assessments (DPIAs) for all new systems that handle personal data and implement a continuous risk management process.

SECURITY INTEROPERABILITY VIEW

The Interoperability Security viewpoint is a collection of the Architecture Building Blocks (ABBs) required to ensure secure, trusted and compliant exchanges between public administrations, businesses and citizens. It spans legal, organizational, semantic and technical layers so security is treated as an end-to-end interoperability requirement.

The security viewpoint models how security and privacy should be built into systems that exchange information across MCDAs, businesses, and citizens to ensure that interactions with government digital services are secure, trustworthy, and compliant with existing regulations as well as the rules on electronic identification and trust services defined in other legislations and policies.

This view operationalizes the GEA Security Reference Model (SRM) and establishes the mechanisms through which interoperability can occur without compromising confidentiality, integrity, availability, authenticity, or accountability.

It provides the structure for:

- Cross-MCDA identity federation
- End-to-end secure data exchange
- Policy-driven access and trust decisions
- Common data classification and handling rules
- Cryptographic trust services (eIDAS-aligned)
- Security monitoring, logging, and audit interoperability
- Zero-trust enforcement, API protection, and infrastructure security

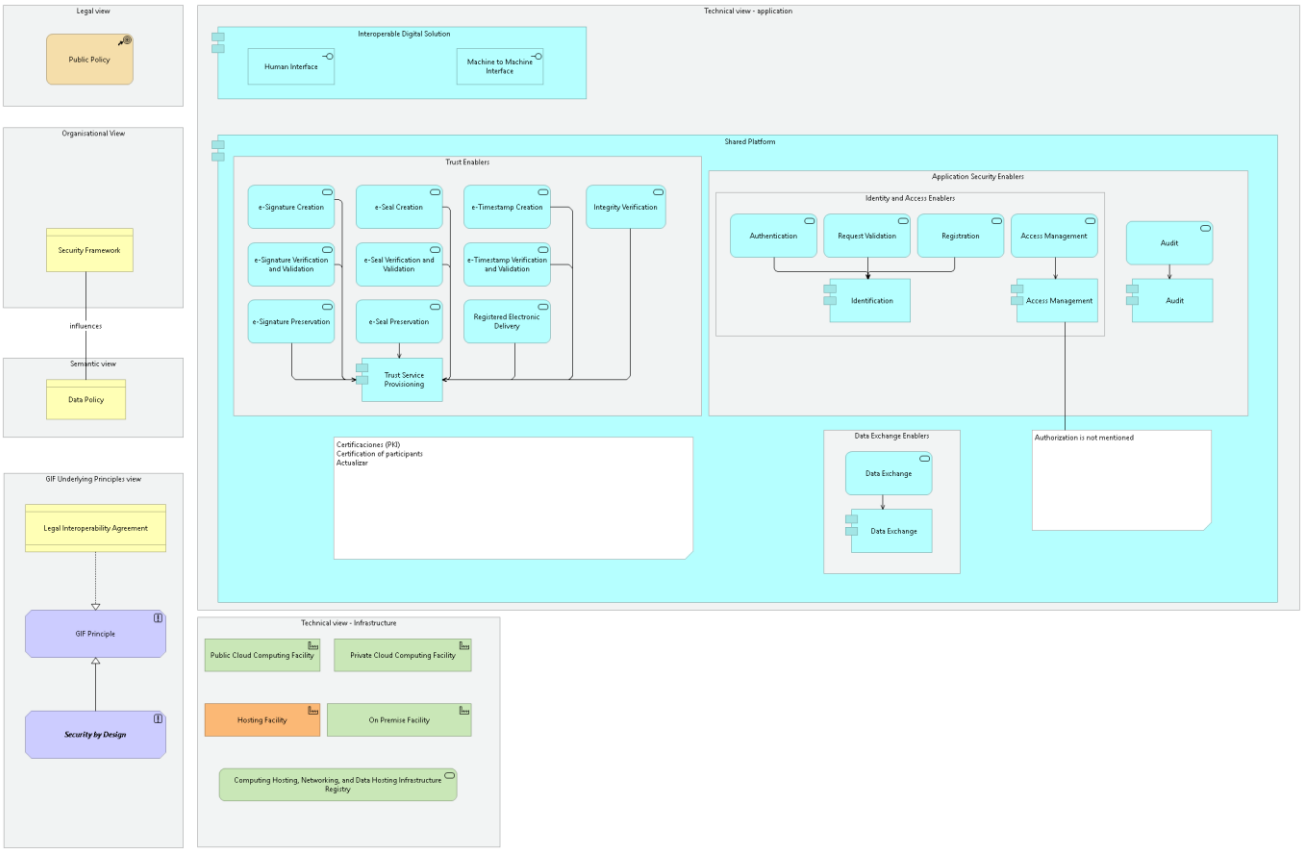

Figure 15 - GIF Security View

The Security View consists of the Architecture Building Blocks (ABBs), shown in *Figure 16* above, required to implement secure cross-agency interactions. These ABBs span the four GIF layers:

GIF Layer	Security Elements Embedded
Legal View	Defines the legal, policy, and regulatory frameworks, ensuring privacy and security compliance for data exchange
Organizational View	Sets up Security frameworks, governance mechanisms, and processes for cross-institutional, governance roles, security SLAs, security obligations in MoUs
Semantic View	Ensures that data exchanged is understood and interpreted consistently, allowing for consistent data classification, metadata schemas labels, controlled vocabularies and security application across systems.

Technical Interoperability	Implementation standardized technology, such as secure protocols and APIs, NPKI, IAM, encryption, encryption, monitoring, secure message buses to facilitate safe machine-to-machine communication.

The combined outcome is a trusted interoperability ecosystem capable of supporting national digital transformation and GovTech initiatives, whole-of-government service delivery and support for boundaryless information flow.

KEY ARCHITECTURE BUILDING BLOCKS

Security interoperability mandates a set of core Architecture Building Blocks (ABBs), which must be adopted uniformly across all MCDAs:

ABB	Elements
Trust Enablers	• Digital signatures, e-seals, certificates (NPKI) • Timestamping verification and validation • E-certificate lifecycle services
Identity and Access Enablers	• National Identity Provider (IdP) • Cross-MCDA Identity Federation (SAML2/OIDC/OAuth2) • Central policy decision points (PDP) • Attribute-based access control (ABAC) • Role-based (RBAC) and consent-based controls • Policy-as-Code enforcement (e.g., OPA/Gatekeeper)
Data Exchange Enablers	• API gateways, rate limiting, throttling • Mutual TLS, JOSE (JWS/JWE/JWT) standards • AS4/REST/JSON-LD secure message exchange • Secure ESB/Message Bus encryption
Monitoring, Logging & Audit	• Unified audit logging • SIEM integration • Cross-agency incident management • Interoperable evidence log
Technical View	• Private Cloud computing facility • Public Cloud computing facility • Network Infrastructure

	• Registry

DATA CLASSIFICATION FRAMEWORK

A Data Classification Framework is a structured approach to categorizing an organization's data assets based on their sensitivity, value, and criticality. It involves identification and assignment of data to predefined categories or impact levels, each with specific security requirements and handling procedures. A standardized national data classification model is essential to ensure that data exchanges across MCDAs are handled in a predictable, governed, and legally compliant manner.

Objectives of Data Classification Framework

Data classification is critical to ensuring effective data management, security, and regulatory compliance. By identifying, categorizing, and labeling data based on its sensitivity, value, and regulatory requirements, MCDAs can implement appropriate security measures, allocate resources efficiently, and reduce the risk of data breaches. Classification of data serves several important purposes listed below:

a) **Data Protection and Security**: Data classification enables organizations to identify and prioritize their valuable and sensitive information and implement appropriate security controls such as encryption, access controls, and data loss prevention mechanisms.

b) **Regulatory Compliance**: Sensitive data classification enables organizations to comply with relevant legislative and industry regulations by identifying and protecting data falling under specific compliance obligations, avoiding regulatory penalties and legal consequences.

c) **Efficient Data Management**: Categorization of data based on its importance, sensitivity, and value enables organization to allocate management and storage resources and efficiently, determine appropriate data retention policies, archiving practices, and secure data disposal methods.

d) **Risk Management**: Understanding the potential risks associated with different classifications of data enables organizations to implement targeted security controls, threat monitoring, and incident response strategies effectively.

e) **Collaboration and Data Sharing**: Data classification allows organizations to define access controls and permissions based on data sensitivity that provide assurance that only authorized individuals or groups can access and share sensitive information and maintain confidentiality and integrity.

The following information should be included as part of a data classification framework:

- **Goal** - why an organization wants to classify data and the benefits it brings.
- **Scope** - the types of data that need to be classified, where the data is stored, and who in the organization will perform the classification and use it.
- **Responsibilities** - specifies which individuals are responsible for which tasks in the data classification workflow.
- **Procedures** - step-by-step processes for accessing, evaluating, and classifying data, considering confidentiality, troubleshooting, and other important issues.
- **Impact level** - mapping out data in the organization and its impact on business processes and compliance requirements. This helps to understand the criticality of data classification for each dataset.
- **Visual data classification guide** - a visual chart showing types of data assets, brief description of these assets, level of impact, and applicable data classification labels.
- **Glossary** - a definition of terms used in the data classification framework, which should be clear to everyone in the organization.

DATA CLASSIFICATION LEVELS

The data classification matrix enables an organization to evaluate various security grades and maintain all data classification information in one repository. An example of a template that describes a data classification framework with 5 security groups ranging is shown below:

Classification Level	Description	Handling & Technical Controls
Public	Information intended for unrestricted release.	No authentication needed; integrity controls required.
Internal	Government-internal data not meant for public release.	Authentication, basic encryption, API gateway mediation.

Confidential	Sensitive operational data; unauthorized disclosure impacts government operations.	Strong authentication (2FA), encryption in transit & at rest, audit logging, access control.
Restricted	Highly sensitive data; unauthorized disclosure causes serious harm.	Zero-trust enforcement, attribute-based access control, HSM-backed key management, privileged access monitoring.
Secret/National Security	Critical data; unauthorized disclosure causes severe harm to national security.	Air-gapped or classified networks, hardware cryptography, multi-person access controls, government-wide risk oversight.

STEPS TO INTEGRATE SECURITY INTO INTEROPERABILITY

To use GIF as the architecture control framework, below is an actionable sequence to be followed:

Step	Activity	Description
1.	**Legal Mapping**	Objective: Establish the formal legal basis for secure cross-agency data exchange. Activities: • Map relevant existing Regulations (DPA 2019, KICA, Records Acts) • Generate "Mandatory Interoperability Security Requirements" • Create legal interoperability specifications
2.	**Governance & Roles**	Objective: Formalize security governance across MCDAs. Activities: • Define Security Governance ABBs • Assign security governance roles: Data Controller, Processor, Security Officers, ARB • Establish Interoperability Security Agreements (ISAs), MoUs, SLAs • Define escalation and compliance workflows
3.	**Data & Privacy Analysis**	Objective: Ensure security requirements derive from data sensitivity and privacy obligations.

		Activities: • Conduct Data Inventory • Define data classification levels • Create data classification matrix • Define lawful bases for processing • Apply data minimization, pseudonymization, and anonymization • Define shared semantic structures for security metadata
4.	**Define Technical Security Specifications**	Objective: Define the technical control stack that enforces the above layers. Activities: • Select ABBs: IAM, PKI, Trust Lists, API Gateway, ESB Security • Align to GIF Technical Specifications (AS4, JSON Schema, XML Encryption) • Define cryptographic controls and message security patterns
5.	**Select or Reuse SBBs**	Objective: Promote reuse of secure components to minimize fragmentation. Activities: • Select SBBs from national repositories • Ensure all SBBs conform to ADMS metadata profile • Enforce reuse before new procurement
6	**Security Design & Integration**	Objective: Embed security into APIs, workflows, and data exchanges. Activities: • Implement authentication/authorization enforcement points • Integrate trust services for document validation • Configure message signing, encryption, timestamping • Produce end-to-end security mapping documentation
7.	**Test & Certify**	Objective: Certify systems for compliance with GIF Security Interoperability requirements. Activities: • Penetration tests • Conformance validation against API schemas

		• Signature and seal validation tests • Security compliance attestation
8.	**Deploy With Operational Controls**	Objective: Ensure sustainable, governed security operations. Activities: Configure SIEM, SOC integration Activate audit logs and monitoring Maintain security SLAs Define incident response collaboration across MCDAs
9.	**Register, Publish & Federate Trust**	Objective: Ensure discoverability and national-level trust interoperability. Activities: • Publish SBB metadata using ADMS • Register trust services in Trusted Lists (TL) • Maintain interoperability registries
10.	**Operate & Periodically Review**	Objective: Sustain compliance and evolve with changing risk, technology, and legislation. Activities: • Continuous monitoring • Re-run security testing after any major change • Update integration security specifications • Conduct annual architecture security reviews

Use the GIF views as the checklist at each step to ensure legal, organizational, semantic and technical traceability.

GIF SECURITY PATTERNS

Security within a modern digital government architecture must be deliberate, pervasive, and engineered into every layer of the enterprise from business processes to data flows, applications, integration channels, and infrastructure. To operationalize the Security Architecture, MCDA ICT ecosystems require codified security patterns - repeatable architectural solutions that consistently apply the mandated controls across all MCDAs.

These security patterns provide authoritative guidance on how trust, identity, encryption, authentication, authorization, monitoring, and compliance must be implemented to achieve a uniform security posture across the whole-of-government landscape.

This section presents the security patterns below in a structured format built upon the following strategic pillars:

Security Pattern	Description
Zero-Trust Architecture (ZTA)	• National Identity Provider (IdP) • Cross-MCDA Identity Federation (SAML2/OIDC/OAuth2) • Digital signatures, seals, certificates (PKI) • Timestamping services • Revocation and certificate lifecycle services
Policy-as-Code (PaC)	Security policies, access rules, data-handling obligations, and compliance requirements are expressed as machine-readable rules (e.g., OPA/Rego), integrated into CI/CD pipelines, API gateways, service meshes, ESB platforms, and message brokers, enabling: • automated policy enforcement • uniform compliance across MCDAs • elimination of human configuration errors • real-time compliance validation • auditable policy history
Automated Compliance and Continuous Assurance	Compliance is embedded into infrastructure and integration layers rather than retroactively audited. Examples include: • schema validation at API gateways • cryptographic enforcement • automated data classification checks • real-time authorization evaluations • key rotation enforcement • mandatory TLS at infrastructure ingress/egress
Strong Cryptography and Trust Services	All data in transit and at rest must be authenticated, encrypted, digitally signed, and auditable using: • National PKI & trusted certificates • FIPS 140-2 validated modules • TLS 1.3 for all transmission • Digital signature & non-repudiation standards • Hardware Security Modules (HSMs) for key custody
Integration-Centric Multi-Layer Security	GIF mandates interoperability therefore, the security patterns focus heavily on securing: • APIs and microservices

	• message queues (MQ) • ESB/SOA messaging • event-driven architecture • data exchange channels • service discovery layers • canonical data models
Reusability and Standardization Across MCDAs	Each pattern represents a national baseline security requirement mapped to GEA reference models to ensure interoperability and prevent inconsistent or incompatible security implementations: • GEA SRM • GIF IRM • GEA ARM (Application) • GEA DRM (Data) • GEA TRM (Technology)

The following patterns constitute the minimum-security baseline for all interoperable systems under the GEA/GIF.

Security Pattern	Purpose	Mandatory Controls	Required ABB/SBB Components
API Security Pattern	Protect APIs by enforcing strong authentication, encryption, schema validation, and centralized governance.	• TLS 1.3 • OAuth 2.1 / OIDC • API Keys (system-to-system) • JSON Schema validation • Rate limiting & throttling • WAF/Threat detection • Digital signatures • Policy-as-Code authorization	• API Gateway • Identity Provider (IdP) • WAF • OPA/Gatekeeper • Service Mesh (optional) • PKI Trust Store
Message Security Pattern (ESB/SOA/MQ)	Secure messages exchanged over ESB, message queues, and service buses.	• Mutual TLS • Message-level encryption • Digital signatures • XML/JSON schema validation • Idempotency controls • Replay protection	• ESB • MQ/Broker (RabbitMQ, ActiveMQ, IBM MQ) • Schema Registry • PKI/HSM

		• Queue/Topic authorization	• OPA-based topic access policies
Event Security Pattern (EDA)	Protect event streams in Kafka/Pulsar/Redpanda by enforcing topic-level access control and cryptographic assurances.	• End-to-end encryption • Role/attribute-based topic ACLs • Signed events • Schema registry enforcement • Partition authorization • Event lineage tracking	• Event Broker (Kafka, Pulsar) • Schema Registry • OPA/Rego topic policies • Audit & Trace Platform
Key Management Pattern	Govern cryptographic keys across certificates, signatures, messages, and API tokens.	• • HSM-secured keys • Automated key rotation • Full certificate lifecycle governance • Segregation of duties • Logging of cryptographic operations	• HSM • PKI Trust Services • Certificate Authority (CA) • Key Vault / Secrets Manager
Zero-Trust Access Pattern	Enforce continuous authentication/authorization for every request. No implicit trust.	• Identity-aware gateways • Continuous session validation • Device posture evaluation • Dynamic risk-based authentication • Attribute-based access control	• IdP (OIDC) • Zero Trust Proxy • Policy Engine (OPA) • SIEM for real-time risk scoring
Policy-as-Code (PaC) Pattern	Automate all security, privacy, and compliance controls as machine-readable policies.	• OPA Gatekeeper at runtime • API Gateway PaC engines • CI/CD PaC compliance tests • Real-time rule evaluation • Automated violation alerts	• OPA/Gatekeeper • Terraform Compliance Engine • GitOps Repository • API Gateway policy module
Data Security & Classification Pattern	Apply data classification, protection, retention, and minimization rules across all systems and integrations.	• Data classification labels • Encryption at rest (AES-256) • Masking/anonymization	• Data Catalog • Metadata Registry • Data Loss Prevention (DLP)

		• Tokenization for sensitive fields • Retention & destruction rules • Data minimization enforcement (PaC)	• Encryption Services • OPA classification rules
Secure DevSecOps Pipeline Pattern	Integrate security scanning, testing, and policy enforcement into CI/CD pipelines.	• SAST/DAST scans • Container image scanning • Infrastructure-as-Code validation • Dependency scanning • Automated compliance gates	• CI/CD platform • SCA/SAST tools • Container Registry • Policy-as-Code engine

IMPLEMENTATION APPROACH & ROADMAP

GIF implementation shall be executed through a phased national programme designed to build interoperability as a binding government capability and not as collection of disconnected ICT projects. Given the scale of the public sector ecosystem and the number of stakeholders involved, implementation must be anchored in a proven enterprise architecture delivery method, reinforced by structured governance, compliance enforcement, and progressive onboarding of MCDAs.

The implementation approach is aligned to the TOGAF's Architecture Development Method (ADM), adapted to government project delivery cycles by incorporating:

- Explicit dependency sequencing across interoperability layers
- Whole-of-government governance gates and decision controls
- Progressive MCDA onboarding based on readiness and maturity
- Structured capability building and institutionalization
- Enforcement through automated compliance mechanisms
- A balanced roadmap combining quick wins with foundational platforms

While GIF has four interoperability layers, implementation will not proceed by treating these layers independently. Instead, rollout will be executed in a hierarchical dependency sequence to prevent common failure patterns where systems integrate technically but fail to exchange meaningful, legally authorized data.

PHASED IMPLEMENTATION APPROACH

The implementation roadmap is structured in three distinct phases, each with clear objectives and activities that correspond to the TOGAF ADM methodology as shown in *Figure 18* below.

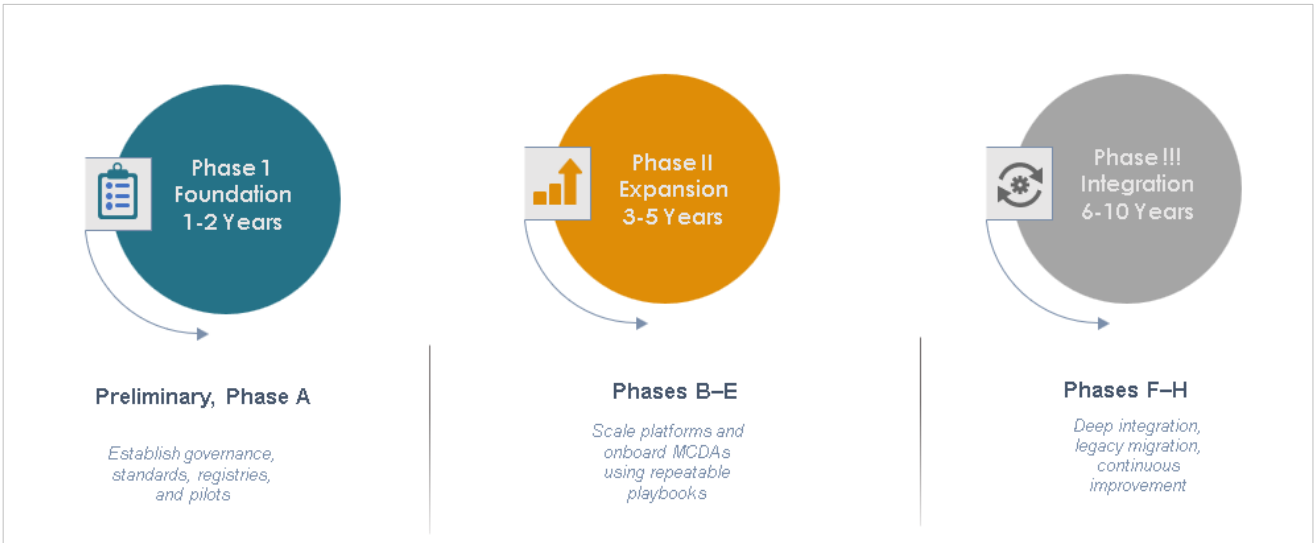

Figure 16 - GIF Phased Implementation Approach

PHASE 1: FOUNDATION (SHORT-TERM, 1-2 YEARS)

This phase is aligned with ADM's Preliminary Phase and Phase A (Architecture Vision)

The main objective is to establish institutional, legal, semantic, and technical foundations that make interoperability enforceable and repeatable. This phase prioritizes establishment of governance structures, standards publication, registry setup, and controlled pilots that validate the approach while building credibility across government.

Interoperability Phase	Key Activities
Legal Interoperability	• Establish standard DSA templates aligned to the Data Protection Act (2019) • Define DSA minimum legal requirements including purpose limitation, lawful basis, retention, breach obligations, liability • Define a formal DSA approval workflow and legal review requirements • Establish the DSA Registry and mandate its use before data exchange activation

Organizational Interoperability	• Establish governance structures including:
	  ○ Oversight Board
	  ○ Interoperability standards review and compliance functions
	• Designate MCDA interoperability focal points and accountable officers

	• Define onboarding procedures and institutional participation obligations • Establish reporting and accountability requirements linked to ICT planning cycles

Semantic Interoperability	• Establish semantic standards catalogue including:
	  ○ Kenyan core vocabulary (where applicable)
	  ○ base registries and reference data standards
	• Establish the ontology governance function and lifecycle controls
	• Stand up semantic asset management capabilities:
	  ○ schema registry
	  ○ ontology registry

Technical Interoperability	• Publish preliminary interoperability technical standards catalogue:
	  ○ API-first standards (OpenAPI 3.x)
	  ○ approved protocols (TLS, OAuth2/OIDC)
	  ○ audit logging requirements
	• Define initial GIP reference architecture
	• Select pilot integration patterns and reference implementations
	• Deliver high-impact, low-complexity pilots (e.g. eCitizen AI Chatbot) as quick wins, ensuring they are GIF-aligned and not standalone

Security (Cross-Cutting)	• Establish minimum security baseline for interoperability: ○ encryption, certificates, IAM integration, audit trails • Define mandatory security controls for all pilots and onboarding systems

Phase 1 Expected Outcomes

- GIF is formally launched with enforceable governance structures in place
- DSAs become standardized and operational through templates and approval workflows
- Standards catalogues and registries exist and are actively used
- Early pilots demonstrate the practicality and value of interoperable delivery
- MCDAs begin structured onboarding guided by governance gates and maturity assessment

PHASE 2: EXPANSION (MEDIUM-TERM, 3-5 YEARS)

Aligned TOGAF ADM Phases: Phases B–D (Business, Information Systems, Technology Architectures), Phase E (Opportunities & Solutions)

The main objective is to scale interoperability beyond pilots by rolling out foundational national shared services and systematically onboarding a broader wave of MCDAs. This phase builds government-wide momentum through repeatable onboarding, service reuse, and increased service integration density.

Legal Interoperability Activities	• Mandate DSA linkage to all active integrations • Establish sector-based DSA patterns and scenario templates (G2G, G2B, G2C) • Integrate DSA enforcement with technical platforms (API gateway access controls) • Operationalize breach reporting procedures tied to governance enforcement
Organizational Interoperability Activities	• Formalize service ownership and accountability models • Establish operational interoperability SLAs and service metrics • Expand inter-agency coordination for shared service rollout • Implement reporting and audit cadence for participating MCDAs

Semantic Interoperability Activities	• Expand canonical data models for priority domains
	• Deploy semantic enforcement mechanisms:
	  ○ schema validation
	  ○ ontology binding requirements for APIs and events
	• Establish semantic change control discipline including versioning and deprecation
	• Resolve cross-domain semantic conflicts through structured governance procedures

Technical Interoperability Activities	• Scale GIP capabilities nationally, enabling coexistence of:
	  ○ API Management
	  ○ ESB mediation
	  ○ Event streaming
	  ○ secure data exchange layer (e.g. X-Road style model)
	• Deploy foundational Digital Public Goods / shared services nationally, including:
	  ○ national digital identity (as applicable)

	○ unified payments platform ○ interoperability layer and registries • Onboard second wave of MCDAs using standard onboarding playbooks • Re-engineer business processes to use shared services rather than silo solutions
Security (Cross-Cutting) Activities	• Establish stronger assurance controls: ○ continuous monitoring ○ vulnerability management ○ audit-ready compliance reporting • Extend security federation across MCDAs for identity and access trust alignment

Phase 2 Expected Outcomes

- Core shared GIP infrastructure is operational at national scale
- A majority of newly developed services integrate using GIF patterns
- DSA enforcement becomes standard practice, not negotiated per case
- Semantic consistency improves measurably through controlled vocabularies and canonical models
- MCDAs realize efficiencies through reuse, reduced duplication, and faster integration

PHASE 3: INTEGRATION (LONG-TERM, 6-10 YEARS)

Aligned TOGAF ADM Phases: Phase F (Migration Planning), Phase G (Implementation Governance), Phase H (Architecture Change Management)

Achieve deep integration and interoperability maturity across government, including systematic legacy migration, enforcement of interoperability-by-default, and establishment of a continuous improvement loop that maintains the GIF as a living framework.

Legal Interoperability Activities	• Strengthen lifecycle governance: ○ DSA expiry, renewal, suspension, and decommissioning • Establish mature risk controls for sensitive data sharing at scale • Expand lawful data-sharing models to broader ecosystem stakeholders where required

Organizational Interoperability Activities	• Institutionalize interoperability governance as standard operating practice • Integrate GIF maturity scores into funding allocation and digital investment approvals • Resolve persistent cross-agency disputes through escalation pathways
Semantic Interoperability Activities	• Fully operationalize ontology lifecycle governance: ○ relationship management, deprecation, migration pathways • Establish semantic assets as a permanent national capability • Ensure all core domains use governed canonical models and ontology-bound APIs

Technical Interoperability Activities	• Full migration of legacy systems via structured playbooks and modernization patterns
	• Enforce GIF compliance for all new projects by default (no exceptions without explicit governance approval)
	• Expand integration capabilities to support:
	  ○ real-time event propagation
	  ○ cross-sector workflows
	  ○ advanced analytics enablement
	  ○ AI Agents and workflows

Security (Cross-Cutting) Activities	• Mature trust and assurance controls:
	  ○ non-repudiation, end-to-end auditability
	  ○ enhanced incident detection and coordinated response
	• Ensure interoperability services remain resilient and continuously protected

Phase 3 Expected Outcomes

- Nationwide scale interoperability is achieved across MCDAs
- Legacy constraints no longer block government-wide integration
- Interoperability becomes a predictable, governed capability embedded in delivery pipelines
- GIF evolves continuously through monitoring, governance, and change management
- Citizen-centric service delivery improves materially through integrated workflows and data reuse

Proposed GIF Implementation Roadmap

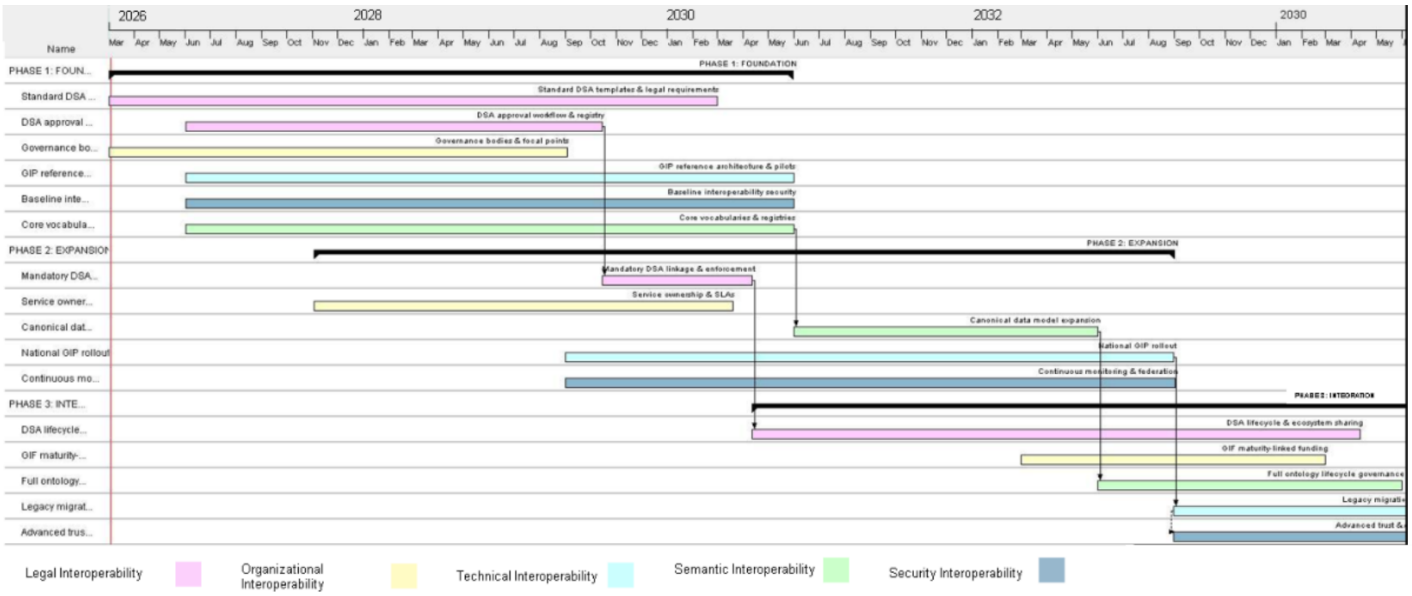

Figure 17 - GIF Implementation Gantt Chart

To prevent premature scaling and unrealistic expectations, the following readiness conditions shall be enforced:

- No cross-MCDA data exchange without an approved and registered DSA
- No technical integration without semantic alignment to approved definitions and schemas
- No onboarding of high-risk systems without security baseline compliance
- No operational deployment without compliance evidence through governance gates
- No major legacy system exemptions without an approved transitional integration plan
- This ensures the GIF programme remains predictable, scalable, and enforceable.

INTEROPERABILITY DEPENDENCY SEQUENCE

Implementation shall adopt the GIF dependency sequence model as described below:

- Legal and Organizational interoperability enable Semantic and Technical interoperability
- Semantic interoperability is a mandatory prerequisite for meaningful technical interoperability

- Technical interoperability implements and operationalizes the outcomes of all other layers

Accordingly, implementation sequence is shown in *Figure 17* below with interoperability security controls embedded cross-cutting all the GIF layers.

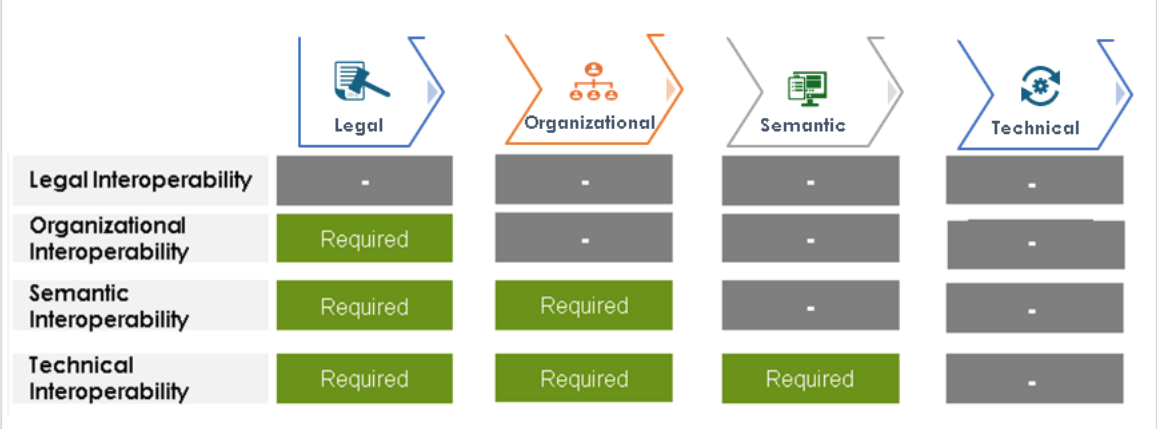

Figure 18 - GIF Implementation Sequencing

GIF PRIORITIZATION FRAMEWORK

GIF rollout should be prioritized using a structured framework that determines *what is implemented first*, *where*, and *under what governance conditions* to manage the dependencies, delivery expectations, based on varying levels of MCDA readiness

Prioritization Criteria

Each candidate initiative, service, or onboarding MCDA shall be prioritized based on the criteria below:

Criteria	Attributes
Public Value and National Impact	• Direct citizen or business service improvement • High transaction volumes and measurable service pain points • Enables multi-agency service integration
Interoperability Dependency Readiness	• DSA readiness and legal basis clarity

	• Organizational willingness and accountability structures • Semantic alignment feasibility (definitions, canonical models) • Technical readiness to expose/consume APIs or events
Delivery Complexity and Risk	• Number of integrating parties (single MCDA vs multi-MCDA) • Legacy dependency severity • Data sensitivity and privacy exposure • Cybersecurity risk rating
Reusability and Platform Leverage	• Potential to become a reusable shared component • Contribution to building national interoperability assets • Ability to be generalized for other MCDAs
MCDA Maturity and Capability	• Current GIF maturity level • Availability of technical and legal capacity • Readiness to comply with governance gates

PRIORITIZATION CATEGORIES

Based on the above prioritization criteria, initiatives shall be classified into the following categories:

Priority Categories	Description
Priority 1: Foundational Enablers	National artefacts and platforms without which scaling is impossible (registries, standards, compliance-as-code, governance).
Priority 2: High-Impact Quick Wins	Citizen-facing services with high visibility but manageable complexity, used to build confidence and adoption momentum.

Priority 3: Cross-Agency Integrations	Multi-MCDA workflows that test legal, semantic, and technical maturity and demonstrate real interoperability value.
Priority 4: Legacy Modernization and Deep Integration	High-risk, high-dependency services requiring structured migration and controlled transitional patterns.

Governance-Based Delivery Expectations

To prevent unrealistic timelines and avoid premature scaling:

- Priority 1 deliverables must be treated as programme prerequisites
- Priority 2 services may proceed only when DSAs and semantic definitions are ready
- Priority 3 and Priority 4 require passing formal interoperability governance gates and readiness thresholds

ONBOARDING IN-FLIGHT INTEROPERABILITY INITIATIVES

Several Government interoperability-related programmes and platform implementations are already underway outside the formal GIF programme structure (for example sector integration platforms, ESB deployments, or independently procured API gateways). While such initiatives may achieve their specific objectives and deliver intended value, unmanaged parallel implementations create fragmentation, inconsistent standards, legal uncertainty, duplicated investment, and long-term integration complexity.

Accordingly, GIF establishes a formal mechanism for onboarding and regularization of in-flight interoperability initiatives to ensure that all such initiatives are progressively brought under the GIF and the GIP reference architecture, without disrupting delivery momentum. This mechanism enables government to preserve investment and delivery progress while ensuring that all interoperability capabilities become legally compliant, semantically consistent, technically standardized, and continuously governed.

This onboarding mechanism applies to any interoperability initiative that:

- Enables or facilitates cross-MCDA data exchange or integration,
- Is positioned as a shared platform or sector integration layer, or
- Provides reusable integration capabilities intended for broad consumption.

Successful onboarding and regularization will ensure that:

- Government retains and benefits from ongoing interoperability investments
- Delivery momentum is preserved without compromising governance
- Data sharing is legally accountable and compliant
- Semantic fragmentation is prevented through controlled vocabularies and ontologies
- Technical interoperability scales predictably through GIP-aligned patterns
- Compliance is continuously enforced through automation and monitoring
- Whole-of-government interoperability progresses as a unified national capability rather than fragmented agency initiatives

CONDITIONAL ACCREDITATION AND CONTROLLED MIGRATION

In-flight interoperability initiatives shall not be treated as permanent exceptions to GIF. Instead, they shall be admitted through a process of Conditional GIF Accreditation, followed by a time-bound migration to full conformance.

Conditional accreditation ensures that:

- Delivery can proceed without unnecessary disruption,
- Critical services are not delayed by governance realignment,
- Interoperability risks are managed through structured controls, and
- Full GIF alignment is achieved through defined sequencing and accountability.

No initiative shall be allowed to operate indefinitely outside GIF governance; there must be a clearly defined migration path onto the framework.

GIF ALIGNMENT ASSESSMENT

All in-flight initiatives shall undergo a formal GIF Alignment Assessment to establish baseline compliance and identify gaps requiring remediation. The assessment shall be conducted across the GIF interoperability layers and aligned to the GEA domains (BRM, DRM, ARM, IRM, TRM, SRM, GRM).

The assessment shall determine:

- The initiative's interoperability scope and target ecosystem (internal MCDA, multi-MCDA, government-wide, external ecosystem)
- The integration patterns used (API, ESB mediation, event streaming, security server model, hybrid)
- The maturity level of legal controls, semantic consistency, and security assurance
- Operational readiness, sustainability, and governance fit

Legal Interoperability Assessment	The assessment shall confirm whether the initiative has: • A valid lawful basis for processing and sharing data • Standardized Data Sharing Agreements (DSAs) for each data exchange relationship • Clear data controller/processor roles and accountability allocation • Defined breach notification and escalation procedures • Alignment with the Kenya Data Protection Act (2019) and applicable sector legislation and policies.
Organizational Interoperability Assessment	The assessment shall confirm whether the initiative has: • Clear service ownership and operational accountability • Defined onboarding processes and service consumption rules • SLAs, service performance commitments, and incident response processes • A dispute resolution pathway for participating entities • Governance structure for decision-making and escalation
Semantic Interoperability Assessment	The assessment shall confirm whether the initiative supports: • Canonical data models and standardized schemas • Ontology binding or approved vocabularies for shared concepts • Schema versioning, change control, and deprecation procedures • Cross-domain semantic alignment and conflict resolution • Registry-based management of semantic assets
Technical Interoperability Assessment	The assessment shall confirm whether the initiative: • Supports API-first principles (OpenAPI 3.x), standard interface specifications, and versioning • Implements approved protocols (TLS, OAuth2/OIDC, certificate-based trust) • Integrates within the GIP architecture patterns (API Gateway, ESB, Event Streaming, Security Server model) • Enables discoverability through API and service registries

	• Avoids bespoke point-to-point integration that cannot scale
Security and Trust Assessment	The assessment shall confirm whether the initiative includes: • Secure authentication and authorization controls • Encryption in transit and at rest where required • Immutable audit logging, traceability, and non-repudiation capabilities • Vulnerability management and incident monitoring procedures • Alignment with Zero Trust principles and national cybersecurity expectations

See the Annexure section for the *GIF ALIGNMENT ASSESSMENT (Baseline Compliance and Gap Remediation Template)*

CONDITIONAL GIF ACCREDITATION MODEL

Following assessment, the initiative shall be issued a Conditional GIF Accreditation, which defines what may proceed immediately and what must be remediated before broader expansion.

Conditional accreditation is granted only where**:**

- The initiative does not introduce unacceptable national, sectoral security or data privacy risks
- Immediate critical services are dependent on the platform
- The implementing entity commits to the GIF migration plan and governance gates

Conditional accreditation shall explicitly define:

- Approved scope of operation (limited or expanded)
- Mandatory remediation activities
- Sequenced compliance deadlines
- Required evidence for each governance gate
- Conditions under which access may be restricted or suspended

Interoperability Governance Gates for Regularization

To operationalize regularization, all in-flight initiatives shall pass through defined Interoperability Governance Gates and Decision Controls. These gates enforce the GIF sequencing model and prevent technical scaling without legal and semantic readiness.

Legal Readiness Gate	Evidence required: • DSA template adoption and execution for each exchange • DSA registration and assignment of unique identifiers • Defined lawful basis and data classification controls • Liability allocation and breach response commitments Data sharing must be lawful and accountable before expansion.
Gate 2: Organizational Readiness Gate	Evidence required: • Designated service owners and accountable officers • Operational SLAs and incident handling procedures • Defined onboarding and participation rules • Governance and dispute resolution arrangements Interoperability must be operationally sustainable and governed.
Gate 4: Technical Conformance Gate	Evidence required: • Published OpenAPI specifications and interface contracts • Conformance to standard protocols and security patterns • Service registration in the API/Integration registry • Alignment to the GIP reference architecture patterns Technical interoperability must be standardized, reusable, and scalable.

Integration into the GIP Architecture

In-flight interoperability initiatives shall be integrated into the GIP architecture through a controlled coexistence model. This ensures that platforms such as X-Road-style security servers, ESB-based mediation, API gateways, and event brokers are treated as complementary patterns within GIP rather than competing architectures. The guidelines below shall be adopted:

- Secure exchange platforms (e.g., X-Road security server model) shall be treated as a secure data exchange pattern
- API gateways shall remain the standard mechanism for API exposure, lifecycle governance, throttling, and consumption control

- ESB mediation shall remain the approved pattern for legacy integration, orchestration, transformation, and structured workflows
- Event streaming platforms shall remain the approved pattern for real-time event propagation and decoupled integration.

All patterns, irrespective of technology choice, shall remain subject to DSA enforcement, Semantic and schema governance Security and auditability requirements and automated compliance monitoring.

Transition and Migration Planning Requirements

Each onboarded initiative shall produce a GIF Regularization and Migration Plan, approved through the required governance controls defined by the GEA/GIF Oversight Board, which include:

- Current state capabilities and gaps
- Target GIF compliance state and required artefacts
- Sequenced remediation activities by interoperability layer
- Timeline with milestones aligned to the governance gates
- Resource requirements and institutional responsibilities
- Risk management actions and fallback options

The migration plan should ensure that ongoing investments/initiatives converge into a unified interoperability ecosystem without duplication or conflict. To prevent uncontrolled proliferation of parallel integration ecosystems the following actions guidelines should be adopted:

- No new MCDA integrations may be added to an in-flight platform unless the platform has passed at minimum **Legal and Semantic Readiness Gates**
- All new services must publish governed APIs and be registered in national registries
- Exceptions must be time-bound, risk-assessed, and approved through formal governance
- Platforms failing to achieve full regularization within agreed timelines may be restricted from onboarding new participants

CAPACITY BUILDING & CHANGE MANAGEMENT

Interoperability at whole-of-government scale cannot be achieved solely through standards, platforms, or regulations. It requires Capacity Building and Change Management as foundational enablers of GIF to build and sustained human capability, institutional readiness, behavioral change, and leadership alignment across MCDAs.

This section establishes a structured, multi-layered approach to building the technical, legal, organizational, and governance capacities required to implement GIF effectively, while actively managing the cultural, institutional, and operational changes that interoperability introduces.

Capacity Building Objectives

The objectives of the GIF Capacity Building Programme are to:

- Assess current MCDAs capabilities for the skills and competencies required to design, implement, govern, operate and sustain interoperable systems
- Reduce dependency on external vendors for core interoperability capabilities
- Enable consistent interpretation and application of GIF standards across government
- Support progressive improvement in GIF maturity levels
- Institutionalize interoperability as a core public service capability, not a project-based skill

TARGET CAPACITY DOMAINS

Capacity building under the GIF shall address multiple, interdependent domains:

1. Leadership and Executive Capacity

Senior leadership capacity is critical to overcome institutional silos and resistance to data sharing. Targeted interventions shall ensure that accounting officers, principal secretaries, chief officers, and senior executives:

- Understand the strategic value of interoperability
- Appreciate legal and accountability implications of data sharing
- Actively sponsor GIF adoption within their institutions

- Align organizational priorities, funding, and performance management with GIF objectives

Leadership capacity building shall be aligned with existing public service leadership programmes and Cabinet-level digital governance engagements.

2. Policy, Legal, and Governance Capacity

Legal officers, policy analysts, and governance practitioners shall be equipped to:

- Interpret and apply GIF's legal and regulatory provisions
- Draft, review, and manage Data Sharing Agreements (DSAs)
- Support compliance with the Data Protection Act and related legislation
- Participate effectively in interoperability governance processes
- Resolve disputes and manage risk associated with cross-agency data sharing

3. Technical and Architectural Capacity

Technical personnel including enterprise architects, solution architects, developers, integration specialists, security engineers, and data professionals, shall be trained to:

- Apply GIF technical, semantic, and security standards
- Design and operate APIs, event streams, and integration patterns
- Implement Policy-as-Code and automated compliance controls
- Integrate legacy systems using approved transitional patterns
- Manage interoperability platforms such as the Government Integration Platform (GIP)

4. Semantic and Data Stewardship Capacity

Semantic interoperability is a common failure point and capacity in this area ensures that shared meaning is governed deliberately and consistently. Dedicated capacity enhancement shall be developed for:

- Data stewardship and ownership roles
- Ontology and vocabulary management
- Metadata, classification, and data quality management

- Impact assessment of semantic changes

STRUCTURED TRAINING AND KNOWLEDGE DEVELOPMENT

Training shall be delivered through a tiered and role-based model, including:

- Executive briefings and governance workshops
- Practitioner-level technical and legal training
- Specialist certification tracks for architects, integration engineers, and data stewards
- Introductory modules for non-technical stakeholders

Training content shall be standardized nationally and updated as GIF evolves.

Knowledge Sharing and Communities of Practice

To avoid fragmentation and duplication, the GIF shall promote:

- Interoperability communities of practice
- Cross-MCDA technical and data forums
- Shared repositories of patterns, templates, and lessons learned
- Case studies of successful interoperability implementations
- These mechanisms support peer learning and institutional memory.

CHANGE MANAGEMENT FRAMEWORK

Interoperability challenges existing organizational norms around data ownership, control, and autonomy. In managing organizational and cultural change under the GIF shall:

- Address cultural resistance to data sharing
- Promote data sharing as a governed responsibility, not a loss of control
- Reinforce trust through legal certainty, security controls, and accountability mechanisms
- Communicate benefits clearly and consistently to all stakeholders. Change management is a continuous process, not a one-off activity.

Stakeholder Engagement and Communication

A structured engagement approach shall be implemented, including:

- Early engagement of affected MCDAs in interoperability initiatives
- Clear communication of roles, expectations, and timelines
- Regular updates on progress, successes, and lessons learned
- Mechanisms for feedback and issue escalation
- This reduces uncertainty and builds institutional confidence.

Alignment with Maturity Progression

Capacity building and change management activities shall be explicitly aligned with the GIF Interoperability Maturity Model.

- Lower-maturity MCDAs shall receive foundational training and targeted support
- Intermediate MCDAs shall focus on advanced integration, governance, and automation capabilities
- Advanced MCDAs shall contribute expertise, mentorship, and innovation
- This ensures that capacity investment is proportionate, targeted, and outcome-driven.

Incentives, Accountability, and Performance Management

Capacity building and change management are reinforced through governance mechanisms:

- GIF maturity and compliance outcomes shall be reflected in performance reviews of accountable officers
- Access to shared platforms, advanced integrations, and funding shall be prioritized for compliant MCDAs
- Persistent lack of progress may trigger governance escalation and remedial interventions
- This ensures that capacity development is not optional, but institutionally embedded.

8. Sustainability and Institutionalization

To ensure long-term sustainability:

- GIF competencies shall be embedded in public service training curricula
- Knowledge artefacts and standards shall be centrally maintained
- Skills transfer shall be mandatory in vendor engagements

- Institutional roles (e.g. architects, data stewards) shall be formally recognized and supported
- Capacity building is thus institutionalized as part of normal government operations, not dependent on individual projects or personalities.

Continuous Improvement of Capacity and Change Interventions

The effectiveness of capacity building and change management interventions should be:

- Monitored through maturity assessments and feedback
- Adjusted based on observed gaps and emerging needs
- Integrated into the broader GIF Monitoring, Evaluation & Continuous Improvement framework
- This ensures that capacity development evolves hand-in-hand alongside GIF.

MONITORING, EVALUATION & CONTINUOUS IMPROVEMENT

Monitoring, Evaluation, and Continuous Improvement is a core governance control function of GIF that ensures that interoperability is measurably implemented, consistently enforced, and continuously improved across MCDAs.

This function provides the evidence base for decision-making, supports accountability at all levels of government, and enables the systematic evolution of GIF in response to operational realities, emerging risks, and changing national priorities. Monitoring and evaluation under GIF is therefore action-oriented, feeding directly into governance decisions, compliance actions, funding prioritization, and framework refinement.

The objectives of the framework include:

- Track adoption, coverage, and depth of interoperability across government
- Measure technical, semantic, legal, and organizational compliance
- Detect fragmentation, duplication, semantic drift, and integration risks early
- Provide objective, audit-ready evidence for governance and oversight
- Link interoperability performance to investment, support, and enforcement decisions
- Enable structured, evidence-driven continuous improvement of the GIF

MONITORING DIMENSIONS AND KPIS

GIF monitoring is structured across three complementary measurement dimensions, ensuring that outcomes are not assessed in isolation from compliance and interoperability health

Dimension	Key Performance Indicator (KPI)
Interoperability Adoption and Coverage Indicators	These indicators measure the extent to which MCDAs are implementing the GIF in practice: • Percentage of government digital services integrated using GIF-approved integration patterns • Percentage of systems exposing or consuming APIs through the Government Integration Platform (GIP) • Percentage of data exchanges covered by registered and active Data Sharing Agreements (DSAs) • Number and proportion of legacy systems participating in GIF-compliant integrations

	• Coverage of shared registries and base datasets across MCDAs
Compliance, Quality, and Interoperability Health Indicators	These indicators assess whether interoperability being implemented correctly and governed sustainably • Percentage of APIs and events passing automated technical and semantic compliance checks • Percentage of systems aligned to approved ontologies and canonical data models • Number of semantic non-compliance incidents detected (e.g. unapproved vocabularies, version drift) • Number of expired, missing, or non-compliant DSAs • Number of integrations operating outside approved patterns or without governance approval • Percentage of legacy integrations beyond approved sunset timelines
Outcome and Public Value Indicators	These indicators measure the impact of interoperability on service delivery and measurable public value: • Reduction in duplicated data collection across services • Cost savings from reduced system duplication and reuse of shared platforms • Average time saved per citizen or business interaction • Reduction in processing time for cross-agency services • Citizen and business satisfaction scores for digital services

PERFORMANCE DASHBOARDS

To support accountability and decision-making, GIF establishes tiered performance dashboards, each serving a defined audience and governance function to support strategic oversight and policy direction.

1. Executive - Level Dashboard

This dashboard provides:

- High-level visibility of GIF adoption and maturity across government
- Key risks and systemic bottlenecks

- Distribution of MCDAs across maturity levels
- Trends in service impact and public value

2. Governance and Oversight Dashboards

Used by ICTA (as the oversight agency) and designated governance bodies, these dashboards provide:

- Detailed compliance metrics
- Semantic drift and ontology usage indicators
- DSA coverage, expiries, and risk flags
- Non-compliance hotspots requiring intervention

3. MCDA Operational Dashboards

To enables self-management, accountability, and continuous improvement, each MCDA shall have access to dashboards showing:

- Its own interoperability maturity score
- Failed or pending compliance checks
- Required remediation actions and timelines
- Benchmarking against peers

AUDITS AND ASSURANCE

Audits under GIF combine automated continuous assurance with periodic human-led reviews.

1. Automated Assurance

Automated compliance tools continuously generate audit evidence to provide near real-time assurance and early detection of deviations including:

- API compliance logs
- Ontology and schema validation results
- DSA enforcement records
- Infrastructure and security conformance data

2. Periodic Audits

Periodic audits conducted by ICTA and authorized bodies to verify that governance is working as intended, not merely documented.

- Validate the effectiveness of automated controls
- Review exceptions and override decisions
- Assess governance processes and outcomes
- Provide independent assurance to oversight bodies

CITIZEN AND STAKEHOLDER FEEDBACK

Citizen and stakeholder feedback is a formal input into GIF improvement, not a peripheral activity. Feedback mechanisms shall:

- Be embedded in digital services
- Capture issues related to data reuse, duplication, and service fragmentation
- Be analyzed centrally to identify systemic interoperability failures
- Inform prioritization of remediation and service redesign
- Feedback is treated as an early warning signal for architectural and data issues.

CONTINUOUS IMPROVEMENT AND CHANGE MANAGEMENT

Monitoring and evaluation feed a closed-loop continuous improvement mechanism aligned with the GEA Architecture Development Method (ADM) Phase H to ensure that GIF remains relevant, effective, and resilient over time.

The continuous improvement process follows the cycle below:

1. **Monitor** – Collect performance, compliance, and feedback data
2. **Evaluate** – Identify gaps, risks, and opportunities
3. **Decide** – Governance bodies determine corrective or improvement actions
4. **Act** – Implement remediation, guidance updates, tooling changes, or enforcement
5. **Evolve** – Update GIF standards, patterns, and controls as required

INSTITUTIONAL ACCOUNTABILITY

Findings arising from monitoring, maturity assessments, audits, and feedback mechanisms constitute formal governance inputs and shall be acted upon by the responsible institutions within defined timelines. Failure to address identified gaps or comply with corrective actions may result in governance escalation, conditional funding, restricted system integration, or suspension of interoperability privileges under GIF. Institutional accountability under this framework is mandatory and non-discretionary.

Clear accountability underpins effective monitoring and evaluation

Responsible Institution	Responsibility
ICTA	• Defining metrics and measurement methods • Operating dashboards and assessment tools • Conducting audits and reporting findings
GIF Governance Bodies	• Acting on findings • Enforcing corrective measures • Aligning investment and policy decisions.
MCDA	• Participating in assessments • Addressing identified gaps • Reporting progress against agreed improvement plans

LEGAL & REGULATORY ALIGNMENT

The Government Interoperability Framework (GIF) derives its authority, enforceability, and sustainability from its formal alignment with Kenya's legal and regulatory framework. Interoperability on a national scale cannot rely on voluntary adoption, technical goodwill, or advisory standards alone. It requires clear legal mandate, binding obligations, and enforceable compliance mechanisms.

This section establishes the legal basis upon which GIF operates, defines its regulatory anchoring, clarifies institutional authority, and sets out enforceable compliance and transition provisions to ensure orderly, lawful, and consistent implementation across all MCDAs.

Formally anchoring the GIF in Kenya's legal and regulatory framework ensures:

- Clear authority for enforcement
- Reduced institutional and personal legal risk
- Predictable compliance expectations
- Confidence for MCDAs to share data lawfully and securely
- Legal certainty is therefore a foundational enabler of interoperability, not an afterthought.

CONSTITUTIONAL AND STATUTORY ALIGNMENT

GIF aligns with and operationalizes Kenya Constitutional principles, including:

- **Article 10** – National values and principles of governance, including transparency, accountability, efficiency, and public participation.
- **Article 35** – Right of access to information, supported through lawful, secure, and interoperable data sharing.
- **Article 47** – Right to fair administrative action, reinforced through integrated and consistent digital service delivery.
- **Article 232** – Values and principles of public service, including responsiveness, efficiency, and effective use of resources.

Interoperability under GIF is therefore not merely a technical objective, but a constitutional enabler of effective public administration.

Alignment with Existing Statutory Frameworks

GIF is designed to operate in harmony with existing legislation, including but not limited to:

- **Data Protection Act, 2019** – Governing lawful processing, data subject rights, security safeguards, and cross-border data flows.
- **Computer Misuse and Cybercrimes Act, 2018** – Supporting security, integrity, and protection of digital systems.
- **Public Finance Management Act, 2012** – Enabling linkage between interoperability compliance and ICT investment, budgeting, and accountability.
- **Access to Information Act, 2016** – Supporting lawful data access while protecting sensitive and personal data.
- **Sector-specific legislation** – Governing data ownership, confidentiality, and statutory mandates of individual MCDAs.

GIF does not override these laws; rather, it provides the operational framework through which they are implemented consistently in digital systems.

GIF ESTABLISHMENT THROUGH REGULATION

GIF shall be formally established through GEA/GIF Coordination Regulations, issued under the appropriate enabling legal instrument, or through an amendment to relevant ICT legislation where necessary.

These regulations shall:

- Declare the GIF a mandatory government standard
- Confer explicit authority on the ICT Authority (ICTA) to:
- Issue interoperability standards, guidelines, and technical specifications
- Enforce compliance across all public service entities
- Conduct audits, assessments, and compliance reviews
- Require all MCDAs to align their systems, integrations, and data exchanges with the GIF

Once gazetted, the GIF shall have the same binding force as other government ICT standards and shall operate as mandatory guidance.

Scope of Applicability

The legal mandate of GIF shall apply to:

- National government ministries and departments
- County governments and their entities
- Constitutional commissions and independent offices
- State corporations and public agencies
- Any third party or service provider processing government data under contract
- This ensures whole-of-government coverage, preventing fragmentation through partial adoption.

COMPLIANCE OBLIGATIONS

Under the regulatory framework, all MCDAs shall be legally required to:

- Adopt GIF-approved interoperability standards, patterns, and protocols
- Register and govern APIs, data exchanges, and integrations
- Execute and register Data Sharing Agreements (DSAs) before any data exchange
- Align data models and schemas to approved semantic standards and ontologies
- Participate in mandatory maturity assessments and audits
- Comply with directives issued under the GIF governance framework
- Non-compliance constitutes a breach of government ICT standards, not a technical preference.

ENFORCEMENT MECHANISMS

1. Graduated Enforcement Model

The regulations shall establish a structured and proportionate enforcement regime, including:

- Formal notices of non-compliance
- Mandatory remediation plans with defined timelines
- Restriction or suspension of system integration or data exchange
- Conditional approval of ICT projects and funding
- Escalation to senior administrative or policy authorities

- Enforcement is designed to be corrective first, but decisive where non-compliance persists.

2. Sanctions

- Where an MCDA or authorized entity fails to comply without reasonable cause, the regulatory framework may provide for:
- Administrative sanctions
- Suspension of interoperability privileges
- Withholding approval for new digital initiatives
- Reporting of persistent non-compliance to oversight bodies
- Sanctions ensure the GIF is enforceable in practice, not merely aspirational.

DISPUTE RESOLUTION AND LEGAL REDRESS

- The legal framework shall provide a clear, structured dispute resolution mechanism, including:
- Internal resolution through designated governance bodies
- Technical and legal review panels for interoperability disputes
- Escalation to appropriate administrative or judicial mechanisms where required
- This ensures disputes are resolved predictably, transparently, and without undermining interoperability objectives.

TRANSITIONAL PROVISIONS FOR LEGACY SYSTEMS

The regulatory framework recognizes that many MCDAs operate critical legacy systems that cannot be immediately replaced. Transitional provisions within the GIF framework provide a lawful and structured pathway for migration without disrupting essential public services including:

- Defined acceptable interim integration approaches (e.g. adapters, wrappers, controlled replication)
- Specific time-bound compliance milestones
- Approved migration and modernization roadmaps
- Prohibition of indefinite reliance on non-compliant integrations

Legacy participation in GIF is therefore conditional, time-limited, and governed, not exempt. All transitional arrangements, however, shall be subject to:

- Defined sunset dates
- Periodic legal and technical review
- Mandatory progression toward full GIF compliance
- This prevents transitional measures from becoming permanent exceptions.

LEGAL EFFECT AND BINDING NATURE

Once established through regulation, GIF shall:

- Be legally binding on all covered entities
- Override conflicting internal ICT standards or practices
- Form part of the compliance baseline for audits, procurement, and funding decisions
- Failure to comply with the GIF constitutes non-compliance with government ICT regulations.

ANNEXES & SUPPORTING MATERIALS

REFERENCES

1. Government of the Republic of Kenya. (2008). *Kenya Vision 2030: A globally competitive and prosperous Kenya*.
2. ICT Authority. (2023). *ICT Human Capital and Workforce Development Standard*. ICT Authority.
3. European Commission, & Interoperable Europe. (2025). European Interoperability Reference Architecture (EIRA) v6.1.0.
4. International Organization for Standardization. (2015). *Governance of IT for the organization* (ISO/IEC 38500:2015).
5. International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC 27001:2022).
6. Ministry of Electronics & Information Technology, Government of India. (2018). *India Enterprise Architecture Framework (IndEA)*.
7. Ministry of Information, Communications, and the Digital Economy. (2025). *Kenya National Artificial Intelligence Strategy 2025-2030*.
8. Ministry of ICT, Innovation and Youth Affairs. (2022). *The Kenya National Digital Master Plan 2022-2032*.
9. 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
10. Open Web Application Security Project. (2021). *OWASP Top 10:2021*. https://owasp.org/www-project-top-ten/
11. Queensland Government. (2023). *Queensland Government Enterprise Architecture*. Queensland Government Customer and Digital Group.
12. Republic of Kenya. (2018). *Computer Misuse and Cybercrimes Act (No. 5 of 2018)*. Government Printer.
13. Republic of Kenya. (2019). *The Data Protection Act (No. 24 of 2019)*. Government Printer.
14. The Open Group. (2018). *The TOGAF® Standard, Version 9.2*. Van Haren Publishing.

GLOSSARY

The following is a comprehensive glossary of key terms and concepts used throughout the Kenya Government Interoperability Framework (GIF) document, organized by architectural domain.

Term	Definition/Context
Government Interoperability Framework (GIF)	A formal, foundational policy and technical blueprint detailing the standards, protocols, and governance mechanisms required to enable seamless data exchange and service integration across all government entities in Kenya.
Government Enterprise Architecture (GEA)	The high-level strategic framework that provides the blueprint for aligning the government's business strategy, ICT systems, information flows, and technology consistently across all Ministries, Counties, Departments and Agencies (MCAs).
Ministry, County, Department, and Agency (MCDA)	The collective term for all public administration bodies—including central government ministries, county governments, state corporations, and independent agencies to which the GIF standards apply.
Digital Public Goods (DPGs)	Reusable software, data standards, or content components (such as digital identity, payment gateways, or APIs) promoted by the framework to eliminate redundant development efforts and accelerate service rollout.
Once-Only Principle (OOP)	A core design principle mandating that citizens and businesses submit information and documents only once to any public authority. Authorities must then retrieve and share that data internally, with user consent, to serve the user's needs.
Technical Interoperability Model	The foundational layer of the GIF that defines the communication protocols, infrastructure standards, and data formatting rules (the "plumbing") that enable systems to physically connect and exchange data seamlessly.
API-First Approach	A strategy mandating that all new system integrations and legacy system access must be designed and exposed through standardized, well-documented Application Programming Interfaces (APIs).
Encapsulation Strategy	A de-risked approach to modernize legacy applications by wrapping their core logic within a new API layer, making the

	system's functionality accessible to modern applications without requiring a costly full rewrite.
Service-Oriented Architecture (SOA)	An architectural style advocating for the creation of independent, loosely coupled, and reusable services that communicate via common standards, promoting interoperability and enterprise-wide data integration.
Microservices	A fine-grained evolution of SOA that breaks down large applications into small, independent services, each focusing on a single function, which significantly enhances system scalability, agility, and resilience.
Master Data Management (MDM)	The processes and standards are implemented to manage the authoritative, non-transactional data entities (e.g., citizens, businesses, locations) to ensure a single, consistent, and trustworthy source of information.
Centralized API Gateway	A unified entry point for all API traffic, responsible for enforcing security, authentication (e.g., OAuth 2.0), throttling, and logging across all integrated government services.
Semantic Interoperability Model	The layer ensuring that the meaning of exchanged data is unambiguous and consistently understood by all participating systems and applications, regardless of the technology used.
Semantic Interoperability Assets (SAs)	Digital resources (schemata, vocabularies, and taxonomies) stored in a central repository that are enriched with metadata to be machine-readable, facilitating common understanding and data federation.
Data Dictionary	A centralized catalogue used to store and communicate metadata and precise, meaningful descriptions for individually named data objects and fields used in government systems.
Metadata	Descriptive data about data (e.g., title, format, update frequency, source) is used to provide context, making information assets self-describing and independent of any specific information system.
Controlled Vocabulary	A standardized list of terms and definitions agreed upon by domain experts and used for data annotation and classification to ensure consistency in data values and meanings across MCDAs.

Ontology	A formal logical model that represents concepts, relationships, and axioms within a specific domain (e.g., land registry, health), facilitating machine-readable understanding and automated reasoning.
Taxonomy	A hierarchical classification scheme used to categorize and organize data, which benefits from the controlled vocabulary to ensure a logical and consistent structure.
Organizational/Process Model	The policy and institutional framework that addresses the procedural and human aspects of interoperability, defining roles, legal mandates, and processes required for cross-agency collaboration and unified service delivery.
Information Ownership Matrix	A clear governance tool that formally maps all critical data assets to the specific MCDA responsible for their custody, quality, maintenance, and compliance with data protection laws.
Process Agreements	Formal institutional agreements, such as Memoranda of Understanding (MoUs) or Service-Level Agreements (SLAs), mandated between MCDAs to define the rules, quality standards, and responsibilities for data sharing and service consumption.
GEA Human Capital Architecture	The strategic component of the GEA focused on aligning workforce planning, skills assessment, training, and change management with the digital transformation goals, ensuring the public sector workforce can effectively implement and manage the new digital ecosystem.
Data Protection Impact Assessment (DPIA)	A mandatory process under the Kenya Data Protection Act, 2019, requiring MCDAs to assess and mitigate the risks to the rights and freedoms of individuals posed by new projects involving personal data processing.
TOGAF Architecture Development Method (ADM)	A phased, iterative methodology used to manage and guide the implementation of the GIF, ensuring a structured approach to architectural planning, standards establishment, and enterprise-wide migration.

CASE STUDY - ESTONIA'S X-ROAD PLATFORM

The development of the GIF draws from internationally proven interoperability architectures, notably Estonia's X-Road platform, which demonstrates how a government can achieve secure, scalable, and resilient data exchange without centralizing data assets.

X-Road exemplifies a decentralized interoperability model (see *Figure 19* below) in which data remains with the authoritative source institution, and interoperability is achieved through a trusted, standardized exchange layer rather than through central data aggregation.

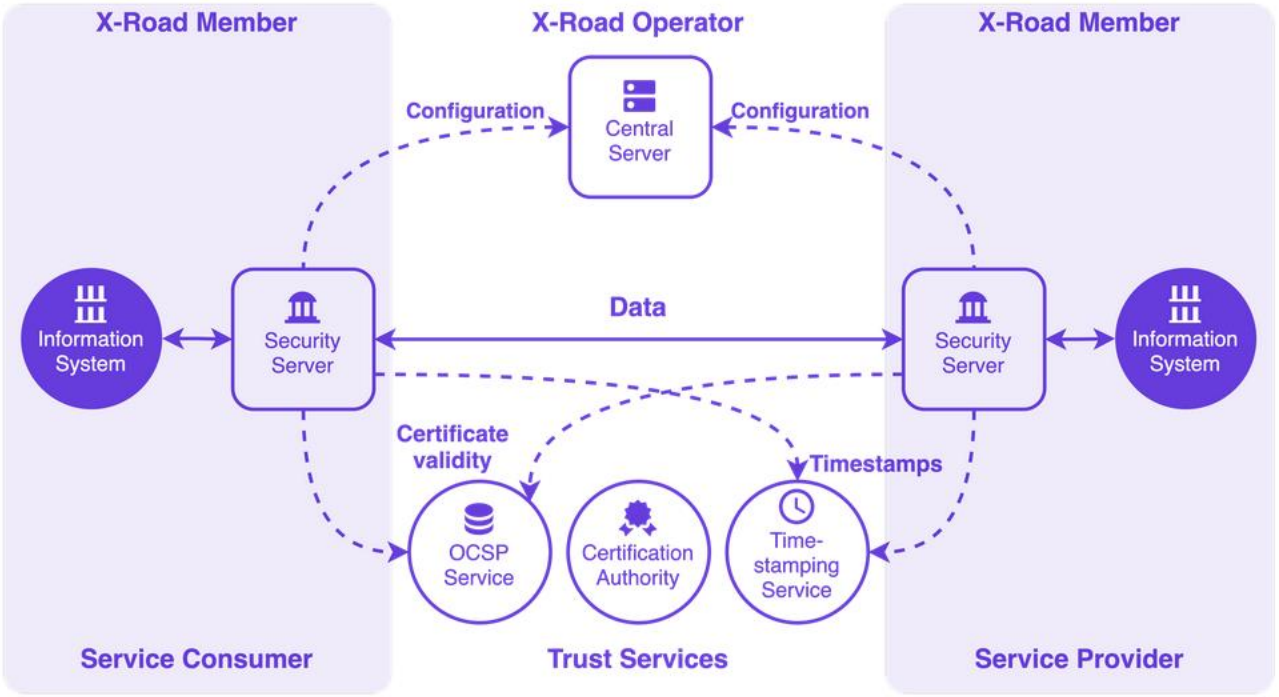

Figure 19 - X-Road Architecture

This architectural principle is directly aligned with GIF's core design objectives of sovereignty, security, resilience, and institutional accountability.

Within the Kenyan context, GIF may adopt and adapt the architectural principles and operating model of X-Road, not as a direct replication, but as a reference implementation pattern, for the following reasons:

I. **Decentralized, secure data exchange**: X-Road is designed so that each participating agency runs its own "security server." Data exchanges are peer-to-peer, not

centralized therefore reducing a single point of failure or a massive data-hub vulnerability. This matches GIF's preference for decentralized security architecture over a monolithic central data store.

II. **Standardized interoperability layer:** X-Road provides a well-defined, proven reference architecture for interoperability including secure messaging, authentication, encryption, logging, and standardized APIs/services. This aligns with GIF's aim to formalize technical interoperability, semantic consistency, and governance.

III. **Cross-agency and cross-border capable:** X-Road supports inter-agency and cross-organizational exchanges under mutual trust frameworks. For a national GEA/GIF deployment, this supports interactions between MCDAs and potentially external bodies (regional, international, private).

IV. **Governance, audit, and compliance built-in:** X-Road embeds logging, non-repudiation, and audit trails aligning with GEA's security, compliance, and governance domains, and the automated compliance/governance frameworks already considered.

V. **Re-usability and standardization:** By adopting a mature data exchange platform rather than rely bespoke middleware-based integrations, government reduces duplication, ensures reuse, enforces common standards, and accelerates onboarding of new service - matching GEA / GIF objectives of efficiency and interoperability.

COMPARATIVE CONTEXT: ESTONIA AND KENYA

While Estonia's X-Road platform provides a proven reference architecture for interoperability, its adoption within the GIF must be informed by contextual differences between Estonia and Kenya, particularly in terms of scale, infrastructure maturity, and governance complexity. A comparison of the 2 countries is shown in the table below.

Dimension	Estonia	Kenya	Implication for GIF Design
Population Size	Small population with high digital penetration	Large, diverse population with uneven digital access	Requires phased, federated rollout rather than uniform deployment

Dimension	Estonia	Kenya	Implication for GIF Design
Government Structure	Highly centralized national administration	Multi-tiered governance: national and county. semi-autonomous MCDAs	Strong governance controls and delegation mechanisms are essential
Digital Identity Coverage	Near-universal, mandatory digital ID	High but variable coverage across services and regions	Interoperability must tolerate partial identity coverage and technology evolution
ICT Infrastructure Maturity	Highly standardized, nationally integrated	Mixed landscape: modern cloud platforms alongside numerous legacy systems.	GIF must support hybrid architectures and incremental modernization
Interoperability Starting Point	Early national decision to standardize interoperability.	Multiple existing integration approaches across MCDAs	GIF must carefully rationalize and govern existing, planned integrations and ongoing integration initiatives
Legal and Policy Alignment	Strong, unified digital governance legislation	Multiple sector laws and evolving data protection regime	Legal interoperability must be explicitly harmonized and enforced
Institutional Capacity	Uniformly high public-sector digital skills	Wide variance in MCDA technical and governance capacity	Centralized support, capacity building and shared services are critical
Security and Trust Model	Long-standing trust in digital government	High sensitivity around data protection and misuse	Security-by-design and auditability must be highly visible
Interoperability Platform Role	National backbone used universally	Reference architecture and shared services platform	X-Road principles adapted, not cloned; flexibility is required

Dimension	Estonia	Kenya	Implication for GIF Design
Change Management Approach	Rapid, top-down enforcement	Gradual, negotiated adoption across government institutions	Governance gates and maturity-based progression are essential

LESSONS FROM COUNTRIES THAT ADAPTED X-ROAD

Several countries have adopted or adapted the X-Road model to suit their own national contexts. Their experiences offer practical lessons for strengthening GIF.

1. Finland

Finland adopted X-Road as a shared interoperability backbone between government agencies and the private sector. Key lessons include:

- Interoperability platforms succeed when anchored in clear legal mandates rather than voluntary participation.
- Strong data ownership and stewardship models are essential to maintain trust between institutions.
- Semantic standardization required more sustained effort than initially anticipated, reinforcing the importance of early semantic governance under GIF.

2. Iceland

Iceland implemented X-Road to modernize public services while preserving institutional autonomy. Key lessons include:

- Decentralized data exchange can coexist with strong national oversight if governance roles are clearly defined.
- Smaller administrations benefited from centralized support services for onboarding and operations. This approach is relevant for supporting lower-capacity MCDAs in Kenya.
- Auditability and non-repudiation were critical in building public and institutional trust.

3. Faroe Islands

Faroe Islands adapted X-Road within a constrained administrative and technical environment to create a secure data exchange environment enabler for further e-governance development. Key lessons include:

- Phased implementation reduced risk and avoided overwhelming institutions with limited capacity.
- Shared infrastructure services lowered costs and simplified compliance.
- Clear separation between policy governance and technical operations improved sustainability.

Cross-Cutting Thematic Lessons Influencing GIF Design

Lesson Area	Observed Lesson	Relevance to GIF	Design Implication for Kenya
Governance First	Interoperability success is driven more by governance than technology	Platforms fail without legal authority and institutional accountability	GIF must enforce legal and organizational readiness before technical integration
Decentralization with Oversight	Decentralized data exchange still requires strong central coordination	Pure decentralization without governance leads to fragmentation	Central governance bodies must define standards, trust, and compliance while data remains distributed. Federated architecture should be considered
Semantic Alignment Complexity	Semantic interoperability consistently takes longer and more effort than expected	Technical connectivity alone does not deliver usable interoperability	GIF must prioritize semantic governance as a mandatory prerequisite to APIs and integrations
Phased Adoption	Incremental onboarding reduces risk and improves sustainability	Big-bang rollouts overwhelm institutions with uneven capacity	GIF implementation should be maturity-driven, phased, and readiness-based
Automation as a Trust Enabler	Built-in logging, audit, and policy	Manual compliance does not scale at national level	GIF must embed automated compliance and auditability as core capabilities

Lesson Area	Observed Lesson	Relevance to GIF	Design Implication for Kenya
	enforcement strengthen trust		
Reuse over Customization	Shared interoperability platforms reduce duplication and cost	Bespoke point-to-point integrations increase long-term complexity	GIF should promote shared services and reusable integration patterns
Clear Separation of Roles	Policy, governance, and technical operations must be distinct	Blurred roles weaken accountability	GIF governance must clearly separate policy authority, standards enforcement, and technical operations
Institutional Capacity Matters	Smaller or less mature institutions require structured support	Uneven capacity slows ecosystem-wide progress	GIF must include central onboarding, tooling, and capacity-building support

These lessons reinforce that GIF must be implemented as a governed system and not merely a technical platform. Successful interoperability requires sequenced adoption, enforced dependencies, and continuous oversight, particularly in a large, federated government environment.

Limitations of the X-Road Model and Viable Alternatives for GIF

Several countries have adopted or adapted the X-Road model to suit their own national contexts. Their experiences offer practical lessons for strengthening GIF.

Constraint Area	X-Road Limitation	Operational Impact	Viable Alternatives
Rural & Intermittent Connectivity	X-Road assumes: • Persistent network availability • Reliable bidirectional connectivity between security servers	• Failed service calls • Incomplete transactions • Operational disruption for frontline services (health, civil registration, agriculture)	• Store-and-forward integration pattern • Offline service design. • Asynchronous Messaging via Intermediaries

Constraint Area	X-Road Limitation	Operational Impact	Viable Alternatives
	• Low-latency, always-on encrypted channels		
Institutional Capacity	X-Road requires each participating institution to: • Operate and maintain a security server • Manage certificates and cryptographic keys • Ensure 24/7 availability and monitoring	For smaller MCDAs or county-level institutions: • Skills and staffing may be insufficient • Operational cost may be prohibitive • Security misconfiguration risk increases operational and skills burden	• Shared security servers model • Managed interoperability services • Tiered Participation Model: - High-capacity institutions operate full nodes while Lower-capacity institutions connect via managed gateways
Real-Time Transaction Overhead	X-Road prioritizes synchronous, request-response transactions with End-to-end encryption and signature validation per call.	In high-volume or latency-sensitive scenarios, Performance overhead may be significant and Real-time user experiences may suffer	**Event-driven integration** for reduced coupling and latency **Data replication** for read-heavy applications GIF must distinguish between: • Transactional interoperability • Event-based interoperability • Data distribution patterns

Constraint Area	X-Road Limitation	Operational Impact	Viable Alternatives
Legacy Systems	Legacy platforms cannot easily expose secure APIs, lack modern authentication mechanisms and are tightly coupled and brittle	Enforcing X-Road-style integration may: • Require costly system rewrites • Delay interoperability benefits • Increase risk of failure	• **Integration Adapters and Wrappers** - Introduce middleware to abstract legacy interfaces • **Batch Integration** - scheduled data exchanges using secure file transfer. • **Hybrid Integration** - Combine real-time APIs with batch and event mechanisms
Data Sensitivity & Over-Exposure	X-Road's openness and discoverability encourages wide service exposure and requires strong data classification discipline	In environments with low data governance maturity there's risk of data over-exposure and misuse leading to trust erosion between institutions	• **Controlled Data Products** - Curated datasets with explicit purpose limitations and access granted per use case • **Federated Query Models** i.e. queries executed at source and results filtered • **Policy-Driven Data Access** using Attribute-based access control enforced centrally
Cross-Border & Partner Integration	X-Road assumes comparable legal regimes, shared trust	• Legal harmonization may lag • Private sector onboarding may be slow	• **API Federation Models** - Standard APIs exposed without

Constraint Area	X-Road Limitation	Operational Impact	Viable Alternatives
	frameworks and mutual recognition of certificates	• Regional interoperability may require lighter-weight mechanisms	full platform coupling, for easy onboarding • **Gateway-to-Gateway Integration** to simplify partner integration by establishing trust at gateway level GIF should allow multiple interoperability modes, not a single backbone
Cost & Time-to-Value	X-Road delivers strong long-term value but requires significant upfront investment has a long maturation timeframe	• Delayed benefits for urgent service delivery needs. • Faster, lighter-weight solutions may be required initially	**Minimum Viable Interoperability** using lightweight API gateways for targeted integration of priority services. **Progressive Platform Adoption** starting with shared gateways evolving toward X-Road-like decentralization over time Interoperability maturity must drive platform choice, not the reverse.

ESTABLISHING A MULTI-LAYERED SECURITY FRAMEWORK

The GIF's Security layer should adopt a robust, multi-layered security framework similar to mature architectures such as X-Road. This framework must ensure confidentiality, integrity, authenticity, traceability, and non-repudiation across all cross-government data exchanges.

The core components of this security model include the following: Digital Certificates: Each participating entity, whether a government agency or a private company, is authenticated using digital certificates issued by a trusted authority.

- Encrypted Channels: All data transferred between systems must travel through encrypted communication channels, protecting it from interception and tampering.
- Digital Signatures and Timestamps: Every transaction is digitally signed and time-stamped to guarantee data integrity
- Trusted audit trails: All interactions must generate immutable and verifiable audit trails

INTEROPERABILITY STANDARDS CATALOGUE

This catalogue below provides a sample of required technical standards, governance, certification and procurement language to ensure systems can discover, authenticate, exchange, interpret, audit and secure information consistently across all MCDAs.

The catalogue will serve as a living document that lists and describes the specific standards adopted by GIF across its four layers

TECHNICAL INTEROPERABILITY STANDARDS

This category defines the foundation that enables systems to connect, exchange data securely, and use shared communication protocols.

Domain Area	Standard/Specification	Compliance Category	Rationale/Applicability
Network & Transport Protocol	TLS 1.2/1.3	Mandatory	Encryption of all data in transit across public networks, ensuring secure communication channels between systems.
	IPv6 Protocol	Recommended	Adoption of the latest Internet Protocol version to ensure scalability and long-term network sustainability.
Data Exchange Format	JSON (JavaScript Object Notation)	Mandatory	Primary lightweight format for structured data exchange via APIs; critical for modern, agile web services.

	XML (extensible Markup Language)	Mandatory (Conditional)	Required for systems that must interface with legacy or specialized platforms that rely on structured document formats.
	CSV (Comma Separated Values)	Recommended	Standard format for transferring tabular data between database and spreadsheet programs for non-real-time exchange.
Web Services & APIs	RESTful API Principles	Mandatory	Mandated approach for building new, reusable web services (API-First approach) to ensure simplicity, scalability, and loose coupling.
	OAuth 2.0 / OpenID Connect	Mandatory	Standard protocol for secure, token-based authentication and authorization of both government applications and external service providers accessing APIs.
System Architecture	Service-Oriented Architecture (SOA)	Mandatory	Principle of structuring major applications as a set of reusables, loosely coupled services to promote reusability and reduce redundancy.
	Microservices Architecture	Recommended	Preferred deployment pattern for new, complex applications requiring high resilience, independent scaling, and continuous deployment.

SEMANTIC INTEROPERABILITY STANDARDS

These standards ensure that the meaning of the exchanged data is consistently understood across all MCDAs, enabling accurate data integration and unified services.

Domain Area	Standard/Specification	Compliance Category	Rationale/Applicability

Data Definition & Metadata	GEA/GIF Data Dictionary Format	Mandatory	Mandatory structure for defining all core data elements (e.g., citizen ID, address, business registration number) to ensure unambiguous meaning.
	Metadata Schema (Dublin Core Extension)	Mandatory	Standardized structure for descriptive metadata, ensuring uniform classification and discoverability of all government data assets.
	Master Data Management (MDM) Protocols	Mandatory	Procedures for managing authoritative data entities (Master Data) to ensure a single, trustworthy source of information is used government-wide.
Controlled Vocabulary	GEA Code Lists & Controlled Values	Mandatory	Standardized lists of pre-defined values (e.g., status codes, location types) for specific data fields to ensure semantic consistency and machine-readability.
	Taxonomy and Ontology	Mandatory  (for Domain Assets)	Development of formal logical models (Ontologies) and hierarchical classification schemes (Taxonomies) for key domain data elements to facilitate automated reasoning and data federation.
Industry Specific (Health)	ICD-11 (International Classification of Diseases, 11th Revision)	Mandatory (for Health Sector)	Global standard for systematically coding health concepts and diagnoses to ensure clinical and statistical data interoperability.

ORGANIZATIONAL STANDARDS

This category defines mandatory compliance standards and policy components necessary to align human capital and institutional processes across the government.

Domain Area	Standard/Specification	Compliance Category	Rationale/Applicability

Process Alignment	GEA Mandate for Process Standardization	Mandatory	Requirement for MCDAs to identify and standardize their unique business processes (e.g., service application, licensing review) to align with national digital workflows.
Human Capital	ICT Human Capital & Workforce Development Standard 2023	Mandatory	Mandates continuous professional development, skills assessment, and training aligned with the GEA's Human Capital Architecture.
Security & Auditing	Information Security Standard 2023	Mandatory	Defines minimum requirements for system security, encryption, and risk management across all MCDA applications and data exchange infrastructure.
Electronic Records	Electronic Records Management Systems Standard 2023	Mandatory	Defines the mandatory protocols for the creation, storage, maintenance, and long-term archival of digital public records.
Accessibility	KS2952 - Kenya Accessibility Standard for ICT Products & Services	Mandatory	Ensures that all public digital services and information are accessible to all citizens, including those with disabilities.

GIF ONTOLOGY GOVERNANCE FRAMEWORK

GIF recognizes ontologies as foundational to semantic interoperability, the absence of explicit governance for ontology lifecycle management presents a material risk to the framework's effectiveness. Without clear authority, approval processes, and change controls, ontology development may become fragmented across domains, leading to duplication, contradiction, and semantic drift.

An **ontology** defines the official meaning of key concepts used across government data and systems. Ontologies are authoritative semantic assets that define shared meaning across government.

To prevent semantic fragmentation, duplication, and conflict, the GIF establishes a formal Ontology Governance Framework that governs the creation, approval, versioning, evolution, and retirement of all ontologies used within government interoperability.
Ontology governance ensures that:

- There is one authoritative definition for shared concepts
- Changes to definitions are controlled, versioned, and approved
- New definitions do not conflict with existing ones
- Agencies know which definitions to use and when to migrate

In effect, ontology governance makes data sharing predictable, trustworthy, and scalable.

Ontology Governance Authority Structure

Governance Role	Description
Interoperability Governance Authority (IGA)	The IGA is the ultimate accountability body for semantic interoperability under GIF. It provides final escalation authority, approves major semantic changes with cross-government impact, and ensures ontology governance is enforced consistently across MCDAs.
Ontology Governance Committee (OGC)	The OGC is the single authoritative body responsible for ontology lifecycle governance. Core responsibilities • Approve new ontologies and major changes • Resolve semantic conflicts across domains • Govern ontology relationships and dependencies • Approve deprecation and migration decisions • Enforce semantic compliance through governance gates

Domain Ontology Leads (DOLs)	Each domain ontology has a designated Domain Ontology Lead who: • Owns domain concepts and definitions • Proposes ontology changes • Defines migration mappings when changes occur
Supporting Roles	• Domain Working Groups (DWGs) provide subject-matter expertise and peer review • Semantic Architecture Team (SAT) provides technical semantic design, validation, and tooling support • ICTA / Standards Secretariat manages registries, publication, and administrative processes • MCDA System Owners implement and comply with approved ontologies

ONTOLOGY GOVERNANCE LIFECYCLE AND RACI MATRIX

Ontology Governance Roles

The roles described below are functional governance roles, not references to new or currently existing statutory bodies. These roles are logical responsibilities required to operationalize the GIF and are intended to be assigned to, or embedded within, existing government institutions, committees, and designated officers in accordance with prevailing legal, administrative, and organizational arrangements.

Specifically:

- **The Interoperability Governance Authority (IGA)** represents the function of overall accountability and escalation and may be fulfilled by an existing inter-ministerial or central digital governance body.
- **The Ontology Governance Committee (OGC)** represents the function of coordinated semantic oversight and may operate as a technical sub-committee under existing standards, architecture, or interoperability governance structure.

- **Domain Ontology Leads (DOLs)** represent designated subject-matter responsibility within MCDAs and do not imply the creation of new posts.

The inclusion of these roles in the framework does not mandate the creation of new institutions, nor does it assume their prior existence. Rather, it provides a clear allocation of responsibilities that can be mapped pragmatically onto existing structures to ensure effective governance, accountability, and enforcement of the GIF.

This approach avoids ambiguity, strengthens oversight, and ensures that semantic interoperability can be governed effectively without introducing additional institutional complexity.

- IGA – Interoperability Governance Authority
- OGC – Ontology Governance Committee
- DOL – Domain Ontology Leads
- DWG – Domain Working Group
- SAT – Semantic Architecture Team
- ICTA-S – ICTA / Standards Secretariat
- MCDA-SO – MCDA System Owners

RACI Matrix

The RACI matrix below operationalizes ontology governance ensuring that semantic authority, accountability, and enforcement are explicit at every architectural decision point.

Ontology Governance Activity	IGA	OGC	DOL	DWG	SAT	ICTA-S	MCDA-SO
Define ontology governance policy & scope	A	R	C	C	C	C	I
Identify semantic domains & dependencies	A	R	C	C	C	I	I
Align business concepts to existing ontologies	A	R	R	C	C	I	I
Propose new ontology or extension	I	C	R	R	C	I	I
Peer review of ontology design	I	C	C	R	R	I	I

Ontology Governance Activity	IGA	OGC	DOL	DWG	SAT	ICTA-S	MCDA-SO
Cross-domain semantic conflict assessment	I	R	C	C	R	I	I
Ontology approval (initial or major change)	A	R	C	I	C	I	I
Ontology registration & publication	I	C	I	I	C	R	I
Assign semantic version (MAJOR/MINOR/PATCH)	I	R	C	I	C	I	I
Bind APIs, schemas, events to ontologies	I	A	C	I	R	I	I
Validate semantic consistency in designs	I	A	C	I	R	I	I
Assess ontology reuse vs new creation	I	A	C	C	R	I	I
Define ontology deprecation decision	A	R	C	I	C	I	I
Define migration mappings & timelines	A	R	R	C	C	I	C
Review semantic impact assessment	A	R	C	C	R	I	C
Enforce ontology compliance at implementation	A	R	I	I	C	C	I
Block non-compliant semantic implementations	A	R	I	I	C	C	I
Review ontology change requests	A	R	C	I	C	I	I
Approve version upgrades or retirement	A	R	C	I	C	I	I
Resolve cross-domain semantic disputes	A	R	C	I	C	I	I

RACI Legend

- **R** – Responsible (executes the work)
- **A** – Accountable (final authority / decision owner)
- **C** – Consulted (provides input)
- **I** – Informed (kept aware)

SEMANTIC VERSIONING AND RELATIONSHIP GOVERNANCE

All ontologies must use semantic versioning **(MAJOR.MINOR. PATCH)**

Ontology relationships (inheritance, alignment, dependency, reference) must be Explicit, documented and approved by the OGC. No redefinition of core or base registry concepts is acceptable.

Version numbers must be explicitly referenced by:

- APIs
- Data schemas
- Event models
- Integration agreements

Version Governance Rules

- MAJOR version changes require:
  - Formal impact assessment
  - Migration plan
  - OGC approval
- MINOR and PATCH changes require:
  - Notification and registry update
  - Backward compatibility assurance

CHANGE CONTROL AND IMPACT ASSESSMENT

Any ontology change must include a Semantic Impact Assessment, covering:

- Affected systems and interfaces
- Cross-domain implications

- Backward compatibility
- Migration cost and effort

Changes without approved **impact** assessments are rejected.

ENFORCEMENT AND COMPLIANCE

- Ontology compliance shall be enforced through:
  - Architecture Compliance Reviews
  - Automated semantic validation (where applicable)
  - Registry-based conformance checks
- Non-compliant ontologies or uncontrolled domain ontologies may be: Rejected, Deprecated or Removed from approved registries

Use of unapproved, deprecated, or conflicting ontologies constitutes GIF non-compliance.

SAMPLE GIF STANDARD DATA SHARING AGREEMENT (DSA)

Below is a Sample Data Sharing Agreement which is a mandatory baseline template under GIF. Extensions to this template are permitted but dilution prohibited

STANDARD DATA SHARING AGREEMENT (DSA)

(Government Interoperability Framework – GIF)

THIS DATA SHARING AGREEMENT

is made on this ___ day of _____ 20__,

BETWEEN

[Name of Data Providing MCDA], a public body established under the laws of Kenya, having its principal office at _____
(hereinafter referred to as the "Data Provider")

AND

[Name of Data Receiving MCDA / Entity], a public body / private entity lawfully authorized to receive data, having its principal office at

_____
(hereinafter referred to as the "Data Recipient")

The Data Provider and the Data Recipient are hereinafter jointly referred to as the **"Parties"** and individually as a **"Party."**

1. PURPOSE AND SCOPE

1.1 The purpose of this Agreement is to establish the legal, operational, and technical conditions under which the Data Provider shall share specified data with the Data Recipient for the following lawful purpose(s):

[Clearly describe the specific public service, statutory function, or approved use case]

1.2 Data shared under this Agreement shall be used solely for the stated purpose and for no other purpose whatsoever unless expressly authorized in writing through an amendment to this Agreement.

2. LEGAL BASIS FOR DATA SHARING

2.1 This Agreement is entered into pursuant to:

- The Constitution of Kenya (as applicable);
- The Data Protection Act, 2019;
- Applicable sector-specific legislation;

The Government Interoperability Framework (GIF).

2.2 The lawful basis for processing personal data under this Agreement is:

☐ Performance of a public task
☐ Legal obligation
☐ Consent (where applicable)
☐ Other lawful basis (specify): _____

3. DATA DESCRIPTION AND CLASSIFICATION

3.1 The data to be shared under this Agreement is described in **Schedule A**.

3.2 Each dataset shall be classified as one or more of the following:

- Public
- Internal
- Confidential
- Personal Data
- Sensitive Personal Data

3.3 No data outside the scope defined in Schedule A shall be shared under this Agreement.

4. ROLES AND RESPONSIBILITIES

4.1 For purposes of the Data Protection Act, 2019:

The **Data Provider** acts as the **Data Controller**.

The **Data Recipient** acts as:
☐ Data Controller
☐ Data Processor (acting on behalf of the Data Provider)

4.2 The Parties shall each comply with their respective obligations under the Data Protection Act, 2019.

5. DATA MINIMISATION AND PURPOSE LIMITATION

5.1 Only data that is **strictly necessary** to achieve the stated purpose shall be shared.

5.2 The Data Recipient shall not:

- Use the data for secondary purposes;
- Share the data with third parties;
- Combine the data with other datasets
  without prior written authorization and, where required, additional legal approval.

6. SECURITY SAFEGUARDS

6.1 The Data Recipient shall implement appropriate **technical and organizational measures** to protect the data, including but not limited to:

- Encryption in transit and at rest;
- Role-based and attribute-based access controls;
- Strong authentication mechanisms;
- Audit logging and monitoring.

6.2 Security controls shall be aligned with GIF security standards and enforced through automated compliance mechanisms where applicable.

7. SEMANTIC AND TECHNICAL COMPLIANCE

7.1 All data exchanged under this Agreement shall:

- Conform to approved data schemas and ontologies;
- Be exchanged through approved integration mechanisms;
- Comply with GIF technical and semantic standards.

7.2 Data exchange shall be technically enabled **only after this Agreement is registered and activated** within the designated DSA Registry.

8. DATA RETENTION AND DISPOSAL

8.1 The Data Recipient shall retain the data only for the duration necessary to fulfil the stated purpose or as required by law.

8.2 Upon expiry or termination of this Agreement, the Data Recipient shall:

- Securely delete or anonymize the data; and
- Certify disposal in writing to the Data Provider.

9. DATA SUBJECT RIGHTS

9.1 The Parties shall ensure that data subjects' rights under the Data Protection Act, 2019—including access, correction, objection, and redress—are respected.

9.2 The Data Recipient shall promptly notify the Data Provider of any request or complaint from a data subject relating to the shared data.

10. DATA BREACH MANAGEMENT

10.1 The Data Recipient shall notify the Data Provider **without undue delay**, and in any event within **seventy-two (72) hours**, of any actual or suspected data breach.

10.2 The Parties shall cooperate fully in breach investigation, mitigation, notification, and reporting obligations.

11. LIABILITY AND INDEMNITY

11.1 Each Party shall be liable for any loss, damage, or penalty arising from its own breach of this Agreement or applicable law.

11.2 The Data Recipient shall indemnify the Data Provider against losses arising from:

- Unauthorized use of data;
- Failure to implement required safeguards;
- Breach of data protection obligations within its control.

11.3 Where a breach arises from joint failure, liability shall be shared proportionately.

12. GOVERNANCE, REVIEW, AND AUDIT

12.1 This Agreement shall be subject to periodic review at intervals of ___ months.

12.2 The Data Provider reserves the right to:

Conduct audits; or

Require compliance evidence
to verify adherence to this Agreement.

13. TERM AND TERMINATION

13.1 This Agreement shall commence on the Effective Date and remain in force until _____, unless terminated earlier.

13.2 Either Party may terminate this Agreement:

For material breach;

For legal or regulatory reasons;

Upon written notice of ___ days.

13.3 Termination shall not relieve either Party of accrued obligations.

14. AMENDMENT

- 14.1 This Agreement may be amended only in writing and with the approval of the authorized representatives of both Parties.

15. GOVERNING LAW AND DISPUTE RESOLUTION

15.1 This Agreement shall be governed by the laws of Kenya.

15.2 Any dispute arising under this Agreement shall be resolved through:
☐ Negotiation
☐ Mediation
☐ Arbitration
☐ Courts of competent jurisdiction in Kenya

16. ENTIRE AGREEMENT

16.1 This Agreement constitutes the entire agreement between the Parties concerning data sharing and supersedes all prior arrangements relating thereto.

SIGNED FOR AND ON BEHALF OF

DATA PROVIDER
Name: _____
Title: _____
Signature: _____
Date: _____

DATA RECIPIENT
Name: _____
Title: _____
Signature: _____
Date: _____

SCHEDULE A – DATA DESCRIPTION

(To be completed for each DSA)

- Dataset Name(s):

- Data Elements:
- Classification:
- Frequency of Sharing:
- Sharing Mechanism (API/Event/File):
- Retention Period:

Below are tailored legal variants of the Standard Data Sharing Agreement (DSA) for the three most common scenarios under GIF. Each variant inherits the core DSA verbatim and adds scenario-specific clauses. To effectively use these variants:

- Core DSA should always be mandatory
- Scenario Addendum should be selected based on context
- Registry records which variant applies
- Automation enforces controls based on variant type

A. GOVERNMENT-TO-GOVERNMENT (G2G) DATA SHARING AGREEMENT

Purpose Context

Internal data sharing between MCDAs for statutory functions, service delivery, enforcement, planning, or coordination. Typical use cases include

- Population registry
- Health systems
- Land registry
- Revenue authority
- Social protection
- Education / Civil registration

G2G-Specific Clauses (Addendum to Standard DSA)

1. Public Task Presumption

1.1 The Parties acknowledge that data sharing under this Agreement is undertaken in the performance of a public task or statutory function, and consent from data subjects is not required where such lawful basis applies under the Data Protection Act, 2019.

2. Simplified Approval and Change Management

2.1 Amendments relating to scope expansion within the same statutory mandate may be approved through the GIF Interoperability Governance process without renegotiation of the entire Agreement.

3. Shared Accountability Model

3.1 Where both Parties act as Data Controllers, responsibility for compliance shall be **joint**, limited to each Party's respective processing activities.

4. Audit and Oversight

4.1 Either Party may request interoperability, security, or data protection audits where reasonable concerns arise.

B. GOVERNMENT-TO-BUSINESS (G2B) DATA SHARING AGREEMENT

Purpose Context

Data sharing with private sector entities for licensing, compliance, payments, verification, or delegated service delivery. Typical use cases include:

- Business licensing and permits
- Credit reference and verification
- Payment service providers
- Outsourced service platforms

G2B-Specific Clauses (Addendum to Standard DSA)

1. Processor Presumption

1.1 Unless expressly stated otherwise, the Business Entity shall act strictly as a **Data Processor** on behalf of the Government Data Provider.

1.2 The Business Entity shall not determine purposes or means of processing.

2. Commercial Confidentiality

2.1 The Business Entity shall treat all non-public government data as confidential and shall not disclose such data to third parties without prior written authorization.

3. Sub-Processing Restrictions

3.1 Sub-processing is prohibited unless:

- Explicitly approved in writing; and
- Subject to equivalent contractual and technical safeguards.

4. Enhanced Liability and Indemnity

4.1 The Business Entity shall indemnify the Government Data Provider against:

- Regulatory penalties;
- Third-party claims;
- Reputational harm

arising from misuse or breach attributable to the Business Entity.

5. Termination for Convenience

5.1 The Government Data Provider may terminate this Agreement **without cause** upon written notice where public interest, security, or policy considerations require.

6. Exit and Data Return

6.1 Upon termination, the Business Entity shall:

- Return all government data; and
- Certify secure deletion from all systems, backups, and logs.

C. GOVERNMENT-TO-CITIZEN (G2C) DATA SHARING AGREEMENT

Purpose Context

Data sharing directly involving citizens, often consent-based, for digital services, benefits, or personalized interactions. Typical use cases include:

- Digital identity services
- Social benefits and grants
- Citizen portals and self-service platforms

G2C-Specific Clauses (Addendum to Standard DSA)

1. Consent-Driven Processing

1.1 Where consent is the lawful basis, such consent shall be:

- Explicit;
- Informed;
- Freely given; and
- Revocable at any time.

1.2 Withdrawal of consent shall result in immediate suspension of processing unless another lawful basis applies.

2. Transparency Obligations

2.1 The Data Provider shall ensure that citizens are informed of:

What data is shared;

- With whom;
- For what purpose;
- For how long.

3. Enhanced Data Subject Rights

3.1 The Data Recipient shall support:

- Real-time access and correction requests;

- Objection and restriction of processing;
- Clear redress and escalation mechanisms.

4. No Onward Sharing

4.1 Data shared under this Agreement shall not be shared onward with any third party without:

- Fresh consent (where applicable); and
- Additional legal authorization.

5. Higher Security Baseline

5.1 The Data Recipient shall apply:

- Strong authentication (MFA);
- Continuous monitoring;
- Enhanced logging and traceability.

DATA SPECIFICATION

A.1 Dataset Description

Dataset Name	Description	Data Classification	Personal Data	Sensitive Personal Data	Source System
Citizen Master Dataset	Core identity record	Confidential	Yes	Yes	National ID System
Business Registry	Legal business entities	Internal	No	No	BRIS
Payments Dataset	G2C/G2B payment transactions	Restricted	Yes	No	ePayments Platform

A.2 Data Elements

Field Name	Description	Data Type	Format	Mandatory	Notes
National_ID	Unique personal identifier	String	########	Yes	Primary Key
Date_of_Birth	Citizen DOB	Date	YYYY-MM-DD	Yes	PII

Business_Registration_No	Unique business ID	String	Alphanumeric	Yes	–

A.3 Frequency & Mode of Data Sharing

- **API:** Real-time
- **Batch:** Hourly / Daily / Weekly
- **Event-streams:** Where applicable (Kafka, MQ)

TECHNICAL SPECIFICATIONS & SLA METRICS

B.1 API Protocols

Specification	Requirement
Transport Layer	HTTPS TLS 1.2+
Authentication	OAuth 2.0 / Mutual TLS
Format	JSON / XML
Schema	OpenAPI 3.0

B.2 API Rate Limits

Tier	Limit
Standard Access	1000 requests/min
High-Volume	10,000 requests/min
Burst	Up to 20,000 requests/min (throttled)

B.3 SLA Metrics

Metric	Target
Availability	99.5% uptime
Response Time	≤ 500 ms (API)
Incident Response	Acknowledgement within 1 hour
Data Freshness	≤ 5 minutes (real-time), ≤ 24 hours (batch)

SECURITY CONTROLS CHECKLIST

C.1 Mandatory Controls

- Encryption: AES-256 at rest, TLS 1.2+ in transit
- MFA for all administrative access
- Zero Trust identity validation
- Role-based access control (RBAC)
- SIEM integration with real-time alerts

- Daily log aggregation and retention (min 1 year)
- Quarterly vulnerability scans
- Annual penetration testing

C.2 Compliance Requirements

- Data Protection Act (2019)
- National Cybersecurity Strategy (2022)
- GEA Security Reference Model
- GIF Integration Standards

APPENDIX D: DATA RETENTION & DESTRUCTION POLICY

D.1 Retention Rules

- Retain only for duration required for Authorized Purpose
- Maximum retention: **5 years**, unless superseded by law
- Audit logs retained **12 months** minimum

D.2 Destruction Requirements

- Secure deletion using NIST-approved methods
- Certificate of Destruction required within 30 days

GIF REFERENCE ARCHITECTURE

GIF provides a **big-picture map** of the key Architecture Building Blocks (ABBs) from all EIRA layers: Legal, Organizational, Semantic, and Technical. It highlights the focal ABBs that connect these views so users can trace relationships and navigate the entire GIF model.

These Building Blocks are not strictly mandatory, but they are critical reference points when designing or assessing any interoperable digital public service.

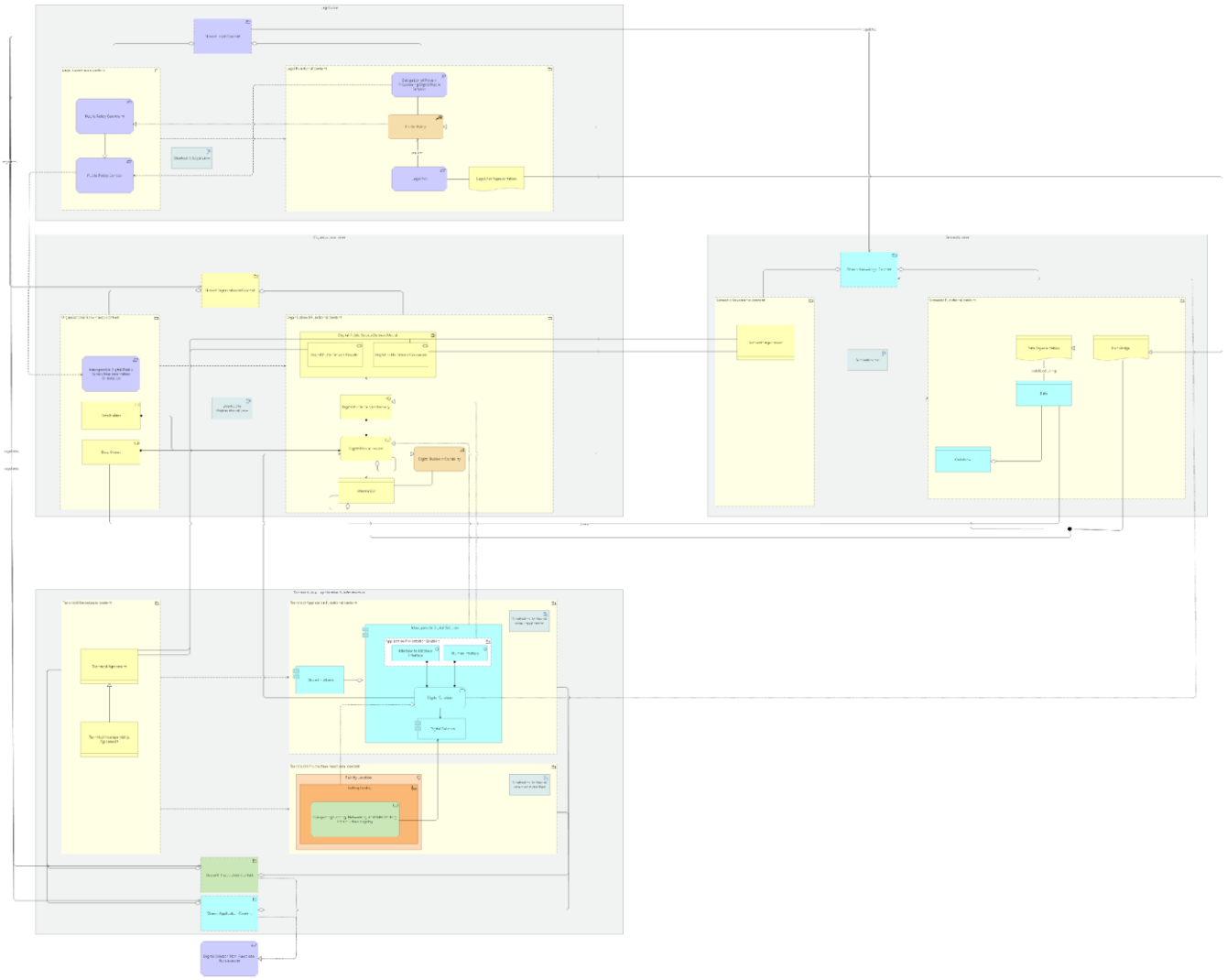

Figure 9 - GIF Reference Architecture

GIF INTEROPERABILITY MATURITY SELF-ASSESSMENT TOOL

How to Use This Tool (Mandatory Guidance)

- Assess each pillar independently using the criteria below
- Select the highest level where ALL criteria are met and evidenced
- Score each pillar from 1 to 5
- Your overall GIF maturity level equals the LOWEST pillar score

Use the improvement guidance to define next-cycle actions

Important: Partial achievement of a level does not qualify for that level.

Scoring Scale

Score	Maturity Level
1	Initial
2	Defined
3	Managed
4	Integrated
5	Optimized

PILLAR 1: LEGAL INTEROPERABILITY

✓	Assessment Criteria	Score
☐	Data sharing occurs informally or on ad-hoc approvals	1
☐	Standard data-sharing agreements exist but are inconsistently applied	2
☐	Legal interoperability agreements are mandatory and enforced	3
☐	Legal instruments are harmonized across sectors and services	4
☐	Legal interoperability is proactively reviewed and digitally enforced	5

1. **Evidence Required:**

☐ Laws / Regulations ☐ MoUs ☐ Data-Sharing Agreements ☐ Legal Opinions ☐ Compliance Logs

2. **Final Legal Score:** ___ / 5

PILLAR 2: ORGANIZATIONAL INTEROPERABILITY

✓	Assessment Criteria	Score
☐	No defined interoperability roles or workflows	1
☐	Roles and agreements exist per project	2

✓	Assessment Criteria	Score
☐	Formal governance, roles, and SLAs are enforced	3
☐	Shared services and coordinated workflows across MCDAs	4
☐	Whole-of-government operating model with continuous optimization	5

3. **Evidence Required:**
   ☐ Organizational Agreements ☐ SLAs ☐ Governance Charters ☐ Process Maps
4. **Final Organizational Score:** ___ / 5

PILLAR 3: SEMANTIC INTEROPERABILITY

✓	Assessment Criteria	Score
☐	Data definitions are system-specific	1
☐	Common vocabularies and schemas documented	2
☐	Mandatory use of approved data models and registries	3
☐	Master and reference data shared across MCDAs	4
☐	Automated semantic governance and change propagation	5

5. **Evidence Required:**
   ☐ Data Dictionaries ☐ Schemas ☐ Metadata Registries ☐ Reference Data Catalogues
6. **Final Semantic Score:** ___ / 5

PILLAR 4: TECHNICAL INTEROPERABILITY

✓	Assessment Criteria	Score
☐	Point-to-point integrations or manual data exchange	1
☐	Standard APIs and protocols defined	2

✓	Assessment Criteria	Score
☐	Central API management, security, and monitoring	3
☐	Event-driven, reusable, cross-agency integrations	4
☐	Automated compliance, optimization, and analytics-driven integration	5

7. **Evidence Required:**
   ☐ API Specs ☐ Gateway Configs ☐ Integration Diagrams ☐ Monitoring Dashboards

8. **Final Technical Score:** ___ / 5

OVERALL GIF MATURITY RESULT

Pillar	Score
Legal	
Organizational	
Semantic	
Technical	

Overall GIF Maturity Level = Lowest Pillar Score

9. **Final GIF Maturity Level: Level** ___

INTERPRETATION OF RESULTS

Overall Level	Meaning
1 – Initial	High risk of failed integrations
2 – Defined	Foundation laid, weak enforcement
3 – Managed	Governed and repeatable
4 – Integrated	Cross-government interoperability operational
5 – Optimized	Automated, scalable, ecosystem-ready

TARGET-SETTING AND IMPROVEMENT PLANNING

Current Level	Recommended Next Target	Focus Area
Level 1	Level 2	Agreements, standards, documentation
Level 2	Level 3	Governance, enforcement, controls
Level 3	Level 4	Shared services, reuse, automation
Level 4	Level 5	Compliance-as-code, optimization

LINK TO FUNDING AND SUPPORT (NORMATIVE)

Maturity Level	Eligible Support
Level 1–2	Capacity building, standards support
Level 3	Shared platforms and integration funding
Level 4	Advanced interoperability investment
Level 5	Innovation and ecosystem enablement

DECLARATION (MANDATORY)

10. *We confirm that this self-assessment is evidence-based and reflects the current interoperability maturity of our institution.*

11. MCDA Name: _____
    Interoperability Lead: _____
    Date: _____
    Signature: _____

GIF VENDOR EVALUATION CRITERIA AND SCORING MODEL

The Vendor Evaluation Criteria provides a standardized, GIF-aligned method for assessing vendors and technology solutions to ensure they meet government interoperability, security, semantic, and governance requirements. It translates the GIF's technical, legal, and operational expectations into measurable evaluation areas, clear assessment indicators, and minimum evidence requirements, enabling MCDAs to select solutions consistently, reduce procurement risk, prevent vendor lock-in, and ensure all acquired systems can integrate effectively within the Government Integration Platform (GIP) and comply with whole-of-government standards.

Criteria Area	GIF Requirement	Assessment Indicators	Minimum Evidence Required
1. Technical Interoperability (API & Integration)	`	• API-first support (REST, OpenAPI 3.x) Supports synchronous + asynchronous patterns • Supports event-driven integration (where required) • Supports integration patterns: API Gateway / ESB / Event Streaming • Legacy integration enablement (wrappers/adapters) • Avoids bespoke point-to-point coupling	• Sample OpenAPI specs • Integration reference architecture • Demo: API onboarding + lifecycle governance • Sample event/message schemas **Scoring Guidance** **5:** Full pattern support + proven GIP alignment **3:** Partial support, customization required **1:** Limited integration capability
2. Semantic Interoperability & Ontology Compliance	Ability to preserve meaning and enforce shared semantics	• Supports canonical schemas + code lists • Ontology binding (URI-based semantics) capability • Schema registry integration • Semantic versioning support • Validation of semantic compliance (design/build/run)	• Examples of schema validation • Canonical model mapping artefacts • Semantic binding documentation • Evidence of versioning controls **Scoring Guidance** **5:** Strong semantic governance + automated validation **3:** Manual mappings only **1:** No semantic controls
3. Security, Trust & Non-Repudiation (SRM-aligned)	Security-by-design to protect cross-agency data exchange	• OAuth2/OIDC integration (default) Encryption in transit & at rest • Certificate lifecycle support • Immutable audit trails / traceability • Least privilege (RBAC/ABAC), PAM support • Security event logging + monitoring integration	• Security architecture documentation • Demo: authentication/authorization flows • Audit log samples + retention settings• Vulnerability management process **Scoring Guidance** **5:** End-to-end security controls + audit-ready evidence

Criteria Area	GIF Requirement	Assessment Indicators	Minimum Evidence Required
			3: Meets baseline but gaps in traceability **1:** Weak security posture
4. Data Protection & Privacy Compliance (DPA 2019)	Ability to comply operationally with Kenya's privacy obligations	• Purpose limitation & minimization controls • Masking/tokenization options • Consent handling (where required) • Retention and disposal enforcement • Breach detection/notification readiness • Cross-border and residency controls	• Privacy compliance mapping to DPA • Data handling controls documentation • Sample DPIA support (where applicable) • Evidence of retention/disposal tooling **Scoring Guidance** **5:** Privacy-by-design embedded + enforceable controls **3:** Policy-only, limited enforcement tools **1:** No practical privacy controls
5. Governance, Compliance & Policy-as-Code (ACGF-aligned)	Vendor supports machine-enforced compliance and governance gates	• OPA/Gatekeeper integration support • CI/CD compliance checks (shift-left) • Runtime enforcement options (gateway policies) • Automated evidence generation for audits • Supports governance workflows and reporting	• Demo: policy enforcement pipeline • Sample PaC rules and outputs • Compliance logs + dashboards samples **Scoring Guidance** **5:** Full PaC lifecycle enforcement + reporting **3:** Partial automation, manual dependence **1:** Governance not automatable
6. Operations, Monitoring & Service Management	Solution can be run reliably across government with measurable SLAs	• Observability (logs/metrics/traces) • SLA monitoring + reporting • Failure handling (retry, DLQ, reconciliation) • Incident integration (ITSM readiness)	• Operational runbooks • SLA templates and supported metrics • HA/DR architecture and RPO/RTO claims • Incident response procedures **Scoring Guidance**

Criteria Area	GIF Requirement	Assessment Indicators	Minimum Evidence Required
		• HA/DR capabilities and tested recovery	**5**: Operationally mature + resilient by design **3**: Operable but limited automation/DR proof **1**: High operational risk
7. Scalability & Resilience	Suitability for Kenya's heterogeneous connectivity and distributed delivery	• Works under intermittent connectivity • Store-and-forward support • Edge/hybrid deployment options • Bandwidth efficiency measures • Local/regional hosting support	• Reference implementation in constrained environments • Architecture showing offline tolerance • Performance/load test results **Scoring Guidance** **5:** Proven resilience + offline-tolerant patterns **3:** Works mainly in stable connectivity contexts **1:** Requires always-on connectivity
8. Vendor Lock-In Risk & Portability	Government retains sovereignty over interfaces, data, and future choices	• Standards-based APIs/formats • Exportable configs, logs, data models • Replaceable components without rewrites • Licensing transparency • Clear exit strategy and transition support	• Exit strategy document • Licensing and TCO breakdown • Portability evidence (containers, standards) **Scoring Guidance** **5:** Low lock-in, portable by design **3:** Moderate lock-in risks **1:** High lock-in / proprietary dependency
9. Implementation Capacity & Track Record	Ability to deliver at national scale with credible plans	• Similar scale deployments • Qualified team availability • Delivery methodology aligned to governance gates • Realistic phased onboarding plan	• Case studies + references• Team CVs and certifications• Delivery plan + milestones **Scoring Guidance** **5:** Strong track record + credible delivery plan **3:** Some experience but limited scale proof **1:** Weak delivery assurance proof.

Criteria Area	GIF Requirement	Assessment Indicators	Minimum Evidence Required
		• Risk and dependency management	
10. Knowledge Transfer & Local Capacity Building	Vendor strengthens government capability rather than creating dependency	• Skills transfer plan (mandatory) • Training materials and certification support • Full documentation + handover • Local support model + escalation paths • **Government**-run operational readiness	• Training plan + curriculum• Handover/runbook samples • Local support commitments **Scoring Guidance** **5:** Strong capacity transfer + sustainable support **3:** Partial training and weak handover **1:** Vendor-dependent operations

Optional Standard Scoring Scale

- 5 = Fully Compliant + Strong evidence + Proven references
- 4 = Fully Compliant + adequate evidence
- 3 = Mostly compliant, minor gaps
- 2 = Material gaps, requires significant remediation
- 1 = Weak compliance
- 0 = Non-compliant / not supported

GIF ALIGNMENT ASSESSMENT

Baseline Compliance and Gap Remediation Template

1. Assessment Purpose and Use

The GIF Alignment Assessment is a mandatory evaluation used to:

- Establish an initiative's baseline alignment to the GIF and GEA standards
- Identify compliance gaps across legal, organizational, semantic, technical, and security layers
- Define remediation actions, ownership, timelines, and governance gates required for onboarding and scaling
- Provide objective evidence to support conditional accreditation, onboarding approvals, or integration restrictions

This assessment applies to:

- New and existing digital systems
- Legacy modernization programmes
- Integration platforms and shared services
- In-flight initiatives operating outside GIF governance
- Vendor-delivered solutions and outsourced platforms

2. Assessment Scope and Identification

- **Assessment ID:** KDEAP_GIF-AA-____
  Date: ____ / ____ / 20__
  Assessing Authority**:** ICTA / Interoperability Governance Function / Architecture Review Board

Initiative / System Details

- **Name of Initiative / System:** _____
- **Owning MCDA:** _____
- **Purpose / Service supported:** _____
- **Acknowledged Data Domains:** (e.g., Identity, Health, Land, Revenue)
  _____
- **Integration Type:**
  ☐ API-based ☐ ESB-mediated ☐ Event-driven ☐ Security-server exchange ☐ Hybrid
- **Deployment Type:**
  ☐ On-prem DC ☐ GovCloud ☐ Public cloud ☐ Hybrid ☐ Edge / regional

Interfaces and Data Exchange

- **Primary Consumers:** _____
- **Primary Providers:** _____
- **Data exchanged:** _____
- **Sensitive data involved?** ☐ Yes ☐ No
- **Cross-agency exchange?** ☐ Yes ☐ No
- **External exchange (private/region/international)?** ☐ Yes ☐ No

3. Assessment Rating Model (Standard)

Each control is rated:

- **0 – Not Present** (no evidence / not implemented)
- **1 – Ad Hoc** (informal, inconsistent, not governed)
- **2 – Defined** (documented and agreed, limited enforcement)
- **3 – Implemented** (operational and measurable)
- **4 – Enforced** (automated enforcement + governance gates)
- **5 – Optimized** (continuous improvement + predictive controls)

Evidence Requirement: Ratings above 2 require tangible evidence (artefacts, logs, dashboards, registry entries).

4. GIF Layer Assessment Matrix (Aligned to GEA Domains)

A) LEGAL INTEROPERABILITY (GEA Alignment: GRM + BRM + DRM)

Objective: Ensure lawful, accountable, and authorized sharing before any technical integration is scaled.

Control Area	Assessment Criteria	Evidence Required	Score (0–5)	Gap / Risk	Remediation Action	Owner	Target Date
Lawful basis for processing	Clear legal basis for collecting and sharing the data (mandate/public task/legal obligation/consent).	Legal basis statement, applicable Acts, policy references					
DSA existence	Data sharing supported by a signed DSA for each exchange	Signed DSA documents					
DSA template compliance	DSA conforms to GIF standard clauses (purpose, retention, breach, liability)	DSA reviewed against template					
DSA Registry entry	DSA registered with metadata and lifecycle status	DSA Registry entry + ID					
Sensitive data handling	DSA includes enhanced controls for personal/sensitive data	Classification, safeguards, DPIA (if required)					
Liability allocation	Roles and liabilities defined	DSA liability clauses					

Control Area	Assessment Criteria	Evidence Required	Score (0–5)	Gap / Risk	Remediation Action	Owner	Target Date
	(Controller/Processor responsibilities)						
Breach notification & escalation	Defined and enforceable breach response procedure	Incident procedure + SLA					

B) ORGANIZATIONAL INTEROPERABILITY (GEA Alignment: BRM + GRM)

Objective: Ensure governance, accountability, operational readiness, and coordinated service delivery across organizations.

Control Area	Assessment Criteria	Evidence Required	Score (0–5)	Gap / Risk	Remediation Action	Owner	Target Date
Service ownership	Named service owner, accountable officer, and operational contact	Role designation letter / org chart					
Operating model	Defined operational responsibilities across MCDAs	RACI / SOPs					
SLA and service expectations	SLAs defined for availability, response, support	SLA document					
Governance participation	Initiative participates in GIF governance structures	Meeting minutes / approvals					
Dispute resolution	Clear dispute resolution mechanism exists	Governance escalation path					
Process alignment	Business processes adapted to reuse shared services	BPMN / process redesign evidence					
Change management	Change plan exists for affected users and agencies	Change plan, comms plan					

C) SEMANTIC INTEROPERABILITY (GEA Alignment: DRM + IRM + ARM)

Objective: Ensure shared meaning, consistent definitions, and controlled evolution of data semantics.

Control Area	Assessment Criteria	Evidence Required	Score (0–5)	Gap / Risk	Remediation Action	Owner	Target Date
Canonical schemas	Uses approved canonical schemas for shared datasets	Schema registry entry					
Ontology binding	Data elements mapped to approved ontology/vocabulary URIs	Ontology mapping artefact					
Schema version control	Semantic versioning applied to schemas	Version history					
Ontology governance adherence	Ontology creation/change follows governance workflow	Approval records					
Semantic conflict management	Mechanism exists to resolve domain conflicts	Resolution logs/decisions					
Metadata & classification	Metadata standards applied (sensitivity, lineage, ownership)	Metadata catalogue entry					
Deprecation and migration	Deprecation timelines and migration paths defined	Deprecation plan					

D) TECHNICAL INTEROPERABILITY (GEA Alignment: ARM + IRM + TRM)

Objective: Ensure standardized connectivity, integration patterns, and scalable interoperability implementation.

Control Area	Assessment Criteria	Evidence Required	Score (0–5)	Gap / Risk	Remediation Action	Owner	Target Date
API-first compliance	APIs defined using OpenAPI 3.x with versioning	OpenAPI specs					
Integration pattern compliance	Uses approved patterns (API Gateway	Architecture diagrams					

Control Area	Assessment Criteria	Evidence Required	Score (0–5)	Gap / Risk	Remediation Action	Owner	Target Date
	/ ESB / Event / Security Server)						
Service discoverability	APIs/services registered and discoverable	API registry entry					
Gateway governance	APIs onboarded to gateway with lifecycle controls	Gateway configs + logs					
Event standardization	Events use standard schemas and registry	AsyncAPI / schema registry					
Legacy enablement	Legacy interfaces wrapped with adapters/strangler guidance	Adapter patterns evidence					
Availability & resilience	HA/DR design supports service continuity	DR plan / RPO-RTO					

E) SECURITY INTEROPERABILITY (GEA Alignment: SRM + TRM + IRM)

Objective: Ensure secure exchange, trust, auditability, and non-repudiation across the ecosystem.

Control Area	Assessment Criteria	Evidence Required	Score (0–5)	Gap / Risk	Remediation Action	Owner	Target Date
Identity and access	OAuth2/OIDC, RBAC/ABAC, SSO as required	IAM configs, auth flows					
Encryption in transit	TLS 1.2+ (TLS 1.3 preferred) enforced	Security configs					
Encryption at rest	Data encrypted at rest for sensitive classes	Storage encryption proof					
Certificates and trust	Certificate lifecycle and trust anchors defined	PKI evidence					
Audit trails	Immutable audit logs for exchanges	Audit logs, SIEM feeds					

Control Area	Assessment Criteria	Evidence Required	Score (0–5)	Gap / Risk	Remediation Action	Owner	Target Date
Non-repudiation controls	Signatures/timestamps where required	Signed transaction proof					
Monitoring and incident response	Security monitoring and incident playbooks	SIEM dashboards, IR plan					

5. Automated Compliance Governance (Cross-Cutting)

Objective: Confirm that compliance is enforceable as code rather than policy-only.

Control Area	Criteria	Evidence Required	Score (0–5)	Gap / Risk	Remediation Action
Machine-readable standards	Standards available as schemas, policies, registries	Registry exports			
Policy-as-Code enforcement	OPA/Gatekeeper policies active in CI/CD or runtime	Policy logs			
Continuous monitoring	Drift detection + compliance dashboards active	Dashboard evidence			
Governance evidence reporting	Audit-ready evidence flows to governance bodies	Reports / logs			

6. Summary Findings and Accreditation Decision

6.1 Baseline Compliance Summary (Layer Ratings)

- Legal: ____ / 5
- Organizational: ____ / 5
- Semantic: ____ / 5
- Technical: ____ / 5
- Security: ____ / 5
- Automated Compliance: ____ / 5

6.2 Risk Classification

- ☐ Low Risk (proceed to scale)
  ☐ Medium Risk (scale allowed with remediation plan)
  ☐ High Risk (restricted onboarding until gaps resolved)

6.3 Accreditation Outcome

- ☐ Full GIF Accreditation
  ☐ Conditional GIF Accreditation (with governance gates and deadlines)
  ☐ Not Accredited (rework required before participation)

7. Governance Gates and Remediation Sequencing

Where Conditional Accreditation applies, remediation shall be sequenced according to GIF dependency hierarchy:

- Legal Readiness Gate (DSAs + lawful basis + registry)
- Organizational Readiness Gate (ownership + SLAs + operating model)
- Semantic Readiness Gate (canonical schemas + ontology binding + registry)
- Technical Conformance Gate (API/gateway/event compliance + GIP alignment)
- Automated Compliance Gate (PaC enforcement + continuous monitoring)

8. Annex: Assessment Evidence Checklist (Minimum Set)

- Signed DSA(s) + DSA Registry entries
- OpenAPI specifications and API registry record(s)
- Canonical schemas + schema registry entry
- Ontology/vocabulary bindings and version history
- Security architecture artefacts and audit log samples
- Monitoring dashboards + incident response plan
- CI/CD compliance evidence (OPA/Gatekeeper logs)

INTERNATIONAL CASE STUDIES & BEST PRACTICES

This section provides detailed summaries of successful international examples that have informed the design of the Kenyan GIF.

ESTONIA'S X-ROAD

X-Road is an open-source platform that enables secure, decentralized data exchange between public and private sector organizations. Its multi-layered security framework, which uses digital certificates and encryption, has allowed Estonia to maintain uninterrupted digital services even in the face of persistent cyber threats. A key lesson for Kenya is its decentralized architecture, which avoids a central data hub, thereby reducing the risk of large-scale data breaches.

INDIA STACK

India Stack is a layered digital infrastructure built on open APIs. Its four layers, Presence-less, Paperless, Cashless, and Consent, enable a unified approach to digital service delivery. The foundation is Aadhaar, a unique biometric identity system, which facilitates paperless and cashless transactions through APIs like e-KYC and the Unified Payments Interface (UPI). The core lesson for Kenya is the power of reusable DPGs for achieving financial and social inclusion at a population scale

EU EIF

The European Interoperability Framework (EIF) is a set of recommendations for communication between administrations, businesses, and citizens across the European Union. It provides a multi-layered model (Legal, Organizational, Semantic, and Technical) that emphasizes the interconnectedness of policy, process, and technology. The lesson for Kenya is the importance of a holistic approach that addresses legal and organizational issues as prerequisites for technical interoperability.

Bahrain NEAF

The Bahrain National Enterprise Architecture Framework (NEAF) is a blueprint for guiding the development of enterprise architecture across government entities. Its implementation was aligned with TOGAF and involved a systematic process of assessing the "As-Is" state, defining a "To-Be" target architecture, and preparing a three-year migration plan. A key lesson for Kenya is the critical need for a formal governance framework to guide and enforce the implementation of the GIF and the value of a phased, roadmap-driven approach.

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 INTEROPERABILITY FRAMEWORK (GIF) DOCUMENT

Kenya Digital Economy Acceleration Project (KDEAP)

3rd Edition

ICTA GIF: 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