GOVERNMENT ENTERPRISE ARCHITECTURE (GEA) AND GOVERNMENT INTEROPERABILITY FRAMEWORK (GIF)

The ICT Authority is a State Corporation under the State Corporations Act 446
www.icta.go.ke

DOCUMENT APPROVAL

Date: _____

Stanley Kamanguya, OGW

Chief Executive Officer ICT Authority

DOCUMENT HISTORY

Version	Revision Date	Revision By	Revision Summary

Table of Contents

GEA & GIF CONCEPT NOTE

EXECUTIVE SUMMARY

The desire to improve the efficiency and effectiveness of communications and information sharing for Government has led to an ever-growing set of platforms and solutions that do not always address operational needs. As a result, MCDAs continue to invest in new products and technologies to improve their services. However, many of these new products and technologies force trade-offs among interoperability, flexibility, security and sustainability, which impacts time to value for any agency.

Typically, the MCDAs must manage a multitude of platforms and systems that don't interoperate and burden the organization with technical complexity and incomplete situational awareness.

Acknowledging the need for government to interoperate, there is need to establish the Government Enterprise Architecture and Interoperability Framework

Making data and systems interoperable and enabling information sharing across platforms is a requirement that spans beyond technical and traditional organizational boundaries. MCDAs should be able to discover, access, and consume any relevant information on a need-to-know basis, regardless of jurisdiction, affiliation, or location.

several dimensions of interoperability shall be considered including common data structures and formats, common messaging protocols, common search and information request service calls, and network and communications interconnectivity. The value proposition of the GIF &GEA

is to provide:

- An interoperable, operational architecture and GEA that can be customized to MCDA use cases and that ensures alignment of people, processes, and technology prior to a major multi-agency, multi-jurisdiction event or investment;
- A roadmap to solving interoperability issues and gaps via architectural blueprints and governance that drives acquisition guidance and alignment Government digitalization agenda
- A guidebook for MCDA acquisition decisions for products and services ensuring that such acquisitions are interoperable, secure, resilient, and enable effective data management;
- A blueprint that informs Government leadership of the complexities and needs for interoperability across multiple MCDAs functions as well as political jurisdictions;
- A framework that incorporates information sharing and Once Only Principle best practices, guidance, and lessons learned; and
- A strategy for GEA and GEA evolution that can be expanded as well as an ongoing embracement of emerging technologies.

1.0 INTRODUCTION

Government Enterprise Architecture (GEA) refers to the strategic framework used by governments to align their technology and business goals. It provides a comprehensive view of the organization's information, processes, systems, and infrastructure, and helps identify opportunities for improvement, modernization, and optimization.

Enterprise architecture, is the glue of the organization, that aligns business goals with all the other aspects of the organization, providing additional effectiveness and efficiencies while also providing guardrails for safety.

In an accelerated path to digitalization, the increasingly important role of enterprise architecture (EA) is one of collaboration across siloes, inside and outside the enterprise, in a configurable way that allows for quick adjustment to new threats and conditions while embracing unprecedented opportunities to scale, stimulating innovation to increase the organization's competitive advantage.

The current need for an accelerated digital transformation elevates the importance of Enterprise Architecture.

The Digital transformation journey brings business and technology increasingly closer.

Because the two become more and more intertwined, the role of Enterprise Architecture increases in importance, aligning the two in providing additional efficiencies.

TOGAF says: **"The Architecture Landscape presents an architectural representation of assets in use, or planned, by the enterprise at particular points in time."**

- Key themes under introduction:
- Interoperability is key
- Reduction of technical complexities
- Establishment of a framework that should be used by all MDAs
- Standardization of the technology principles
- Ease of acquisition

The Government Enterprise architecture (GEA) will be impacted by and will have an increasing role in the following areas

1. **Business agility:** Effective data integration enables the enterprise to build predictive analytics, service orchestration, and other strategies that are enablers for a built-in nimbleness, so that architecture can evolve in ways that increase its competitive advantage.

2. **Tools and automation:** Enterprise Architecture becomes an ever-more important tool in creating the needed handshake between business and IT.

3. **Innovation:** Industries that are currently technology laggers are under tremendous pressure to modernize their ways and reduce costs. We foresee an explosion of industry-specific AI/ ML-powered applications that will bring the need for domain expertise.

4. **Collaborative EA:** EA's collaboration role across siloes. It balances decisions across guilds (business, data, application, infrastructure, integration, security) to achieve cross-domain or enterprise optimization.

It enables collaboration and guidance for programs, platforms, portfolios, projects, DevSecOps, and Operations.

It includes vendor and partner management (e.g. setting up collaboration framework and expectations for suppliers, vendors, and partners).

5. **Security:** Enterprise Architecture can play a role in identifying security threats as well as contributing to a security strategy that anticipates, detects, and mitigates risks. Adequate governance needs to be in place, ensuring that security controls are in line with the governance security policies and compliance requirements.

1.1. Role of Enterprise Architecture in digital transformation

Digital Transformation is becoming increasingly a focus of strategic thinking and planning of many public and private organizations. It is about putting the emphasis on how digital services and applications will change and "transform" citizen's experience and the way we do business in a way that will lead to improvement in quality of life and wellbeing and the attainment of Sustainable Development Goals (SDG)

Digital services need to be personalised, paperless, cashless, presenceless, integrated and consent-based to be transformational. Government needs to develop specific capabilities to be able to deliver such transformational digital services. eight first level building blocks have been identified- digital strategy, digital platform, value delivery ecosystem, digital service attributes, digital enterprise architecture, institutions and governance, citizen insights and delivery capabilities that are required as foundation to ideate, plan, design, deploy and operate citizen-centric transformational digital services. All those building blocks are interrelated and depend on each other. Every building block plays a critical role in the journey towards digital transformation.

A central building block is the digital enterprise architecture, which is the whole-of-government approach to support government ecosystems by transcending boundaries to deliver services in a coordinated, efficient and equitable manner. It is the critical component that translates transformation needs into specific functional and technical requirements that can lead to the deployment of transformation digital services. A digital platform is the result of enterprise architecture. A digital platform is a repository of business, data, application and technology components (reusable building blocks and distinct interfaces) that allow for rapid design, development, deployment and delivery of digital services.

With the use of standard and open interfaces, the digital platform is available to all the key actors in the value delivery ecosystem to build and use components. It will accelerate innovation in integrated and interoperable digital solutions, enabling government to achieve its goals in a more predictable, efficient and cost-effective manner—and with reduced risk.

Digital Transformation Continuum

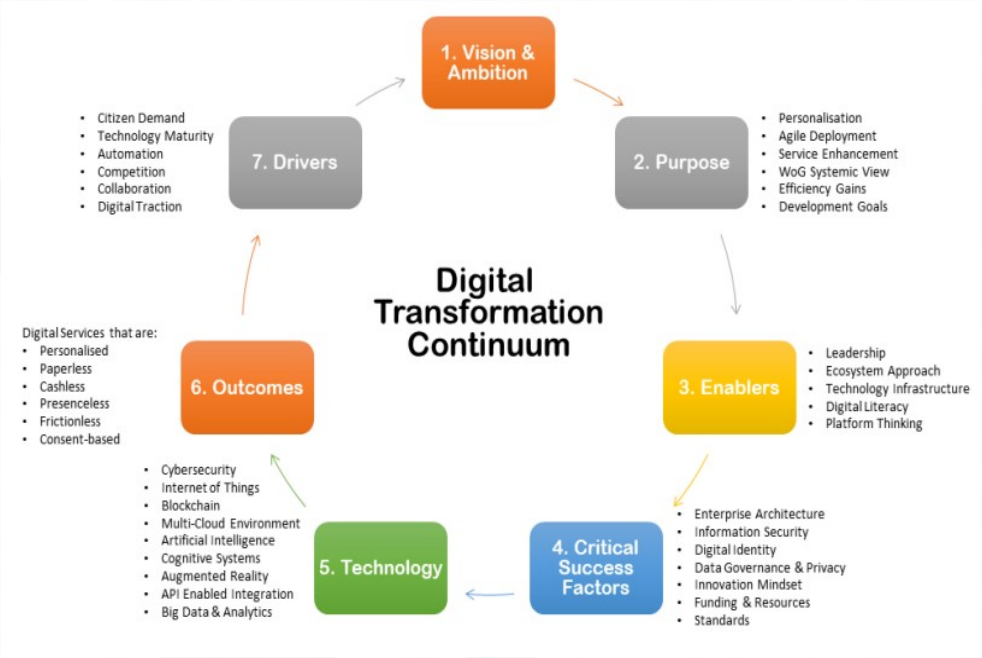


Figure 2: Digital transformation continuum

1.2. Mission & Vision

Mission

The mission of Enterprise Architecture is to provide a process that sets common goals and coordinates the delivery of information technology services to government that are responsible and cost effective.

Vision

"Integrated solutions with focus on agility, digitization and transformation"

1.3. Problem Statement

1. Siloed systems
2. Challenges in integration
3. Duplication of data
4. Spaghetti mess
5. Aging infrastructure

1.4. Description & Rationale

The Government enterprise architecture is the whole-of-government approach to support government ecosystems by transcending boundaries to deliver services in a coordinated, efficient and equitable manner. The aim is to establish best-in-class architectural governance, processes and practices with optimal utilization of ICT infrastructure and applications to offer one government experience to the citizens and businesses through digital services enabled by Boundaryless Information Flow.

The rationale for implementing GEA is to promote collaboration, standardization, and interoperability across different departments and agencies within the government. It helps break down silos, avoid duplication of efforts and resources, and enhance efficiency, effectiveness, and agility.

By creating a shared understanding of the organization's capabilities, data, and systems, GEA helps identify gaps, redundancies, and inefficiencies, and supports evidence-based decision-making, policy development, and service delivery. It also helps the government respond quickly to changing circumstances, new opportunities, and emerging risks.

GEA typically involves developing and maintaining a set of standards, principles, guidelines, and policies that define the organization's technology and business architecture. It also involves establishing a governance structure, roles, and responsibilities, and ensuring compliance with relevant legislation, regulations, and industry standards.

1.5. Goals & Objectives

Goal

To develop an enterprise architecture that aligns the government's technology and business goals by providing a comprehensive view of the government's information, processes, systems, and infrastructure, and helps identify opportunities for improvement, modernization, and optimization.

Objectives

- Agency collaboration
- Data security, confidentiality and compliance
- Re-imagine citizen experience
- Cross-architecture interoperability and standardization
- Transform the infrastructure
- Critical infrastructure resiliency
- Application modernization and optimization
- Secure enterprise network access and orchestration
- Threat detection and incident response
- Connected justice

1.6. Impact/Benefits

The impacts and benefits of Government Enterprise Architecture and Government Interoperability Framework include:

1. Improved Efficiency

GEA helps the government to optimize its operations by identifying and eliminating redundancies in IT systems. It enables the government to standardize its technology infrastructure, promote re-use, reduce duplication and reduce the costs associated with maintaining and supporting disparate systems. This results in improved efficiency and better use of taxpayer funds.

2. Enhanced Service Delivery

GEA helps the government to provide better services to citizens. It enables the government to design and implement IT solutions that are more user-friendly, integrated and accessible. This results in better customer satisfaction and increased trust in government services.

3. Improved Collaboration

GEA promotes collaboration among different departments and agencies. It provides a common language and framework for IT planning and decision-making, which enables different departments to work together towards common goals. This results in better communication, increased knowledge sharing, and improved coordination.

4. Better Risk Management

GEA helps the government to manage IT-related risks. It enables the government to identify and address potential risks associated with IT investments and to develop contingency plans to mitigate those risks. This results in better decision-making and increased confidence in the government's ability to manage IT-related risks.

5. Improved Strategic Planning

GEA helps the government to align its IT investments with its strategic goals and objectives. It enables the government to develop IT solutions that are more closely aligned with its business needs, which results in improved outcomes and better use of resources.

6. Increased Transparency

GEA provides greater transparency in IT investments and operations. It enables the government to track and report on the performance of its IT systems and investments, which increases accountability and transparency.

Overall, GEA has many benefits for the government, including improved efficiency, enhanced service delivery, improved collaboration, better risk management, improved strategic planning, integration and increased transparency. It is an essential tool for any government looking to optimize its IT resources and improve its operations.

1.7. Scope

Development of the GEA and GIF to be adopted by Entire government - including Ministries, Counties, Departments and Agencies **Purpose**

The GEA represents the collective set of knowledge relating to the e-Government architecture, technology standards, interoperability framework, and governance, and performance management.

The purpose of the GEA is to provide the government agencies with adequate reference material in order to:

- Support government agencies that want to develop their enterprise architecture

- Provide the entities with guidelines that allow them to hook up with the central architecture

1.8. Solution Strategy

Implementing a Government Enterprise Architecture (GEA) requires careful planning and execution to ensure that it aligns with the government's goals and objectives. Here are some strategies that will be used to implement GEA:

1.8.1. Develop a roadmap

Developing a roadmap is an essential first step in implementing GEA. The roadmap should outline the government's goals and objectives, as well as the steps that will be taken to achieve those goals. It should also identify the stakeholders and their roles in the implementation process.

1.8.2. Establish a governance structure

Establishing a governance structure is crucial to the success of GEA. The governance structure should define the roles and responsibilities of the different stakeholders, including the enterprise architects, IT managers, and business leaders. It should also establish decision-making processes and policies that will guide the implementation process.

1.8.3. Define the architecture

The architecture should be defined based on the government's goals and objectives. It should be designed to align with the government's business processes, systems, and data. The architecture should also be flexible and scalable, allowing it to adapt to changing business needs and emerging technologies.

1.8.4. Implement the architecture incrementally

GEA should be implemented incrementally, starting with the most critical areas of the government's operations. This approach helps to ensure that the architecture is aligned with the government's goals and objectives and that it can be adapted as needed.

1.8.5. Foster collaboration

Collaboration is essential to the success of GEA. The implementation process should encourage collaboration among the different stakeholders, including the enterprise architects, IT managers, and business leaders. This collaboration will help to ensure that the architecture is aligned with the government's goals and objectives.

1.8.6. Monitor and evaluate progress

The implementation process should be monitored and evaluated regularly to ensure that it is progressing as planned. The evaluation process should include measuring the success of

the architecture in achieving the government's goals and objectives, as well as identifying areas for improvement.

1.8.7. Provide training and support

Training and support are essential to the successful implementation of GEA. The government should provide training and support to the stakeholders to ensure that they have the skills and knowledge needed to implement and maintain the architecture.

2.0 GEA AND (GIF) ROADMAP

2.1 Government Enterprise Architecture (GEA)

A Government Enterprise Architecture (GEA) roadmap outlines a plan of action for developing and implementing a GEA framework within a government organization. The roadmap typically consists of several phases, each with its own set of activities, deliverables, and timelines. Here is a general overview of a GEA roadmap:

1. Current State Assessment

The first phase of the roadmap involves conducting an assessment of the organization's current architecture. This includes gathering information on existing systems, processes, data, and infrastructure. The assessment helps identify gaps, redundancies, and areas for improvement.

2. Future State Vision

In this phase, the organization defines its vision for the future state of its architecture. This includes setting goals, identifying desired outcomes, and establishing principles and standards.

3. Architecture Planning

The third phase involves developing a roadmap for achieving the future state vision. This includes defining the scope of the GEA, prioritizing initiatives, and creating a high-level plan for implementation.

4. Standards and Governance

This phase focuses on developing standards and governance processes to guide the implementation of the GEA. This includes defining roles and responsibilities, establishing policies and procedures, and developing a governance structure.

5. Implementation

The fifth phase is where the actual implementation of the GEA framework begins. This includes developing detailed plans for each initiative, defining project teams and timelines, and executing the plan.

6. Measurement and Evaluation

In this phase, the organization measures and evaluates the effectiveness of the GEA. This includes

monitoring progress, assessing outcomes, and identifying areas for improvement.

7. **Continuous Improvement:**

The final phase involves continuous improvement of the GEA framework. This includes refining the architecture, updating standards and governance processes, and addressing emerging technologies and business needs.

2.2 Context

The desire to improve the efficiency and effectiveness of communications and information sharing for the Government has led to an ever-growing set of platforms and solutions that do not always address operational needs. As a result, MCDAs continue to invest in new products and technologies to improve their services. However, many of these new products and technologies force trade-offs among interoperability, flexibility, security and sustainability, which impacts time to value for any agency.

Typically, the MCDAs must manage a multitude of platforms and systems that don't interoperate and burden the organization with technical complexity and incomplete situational awareness.

Acknowledging the need for government to interoperate, there is need to establish the Government Enterprise Architecture and Interoperability Framework

Making data and systems interoperable and enabling information sharing across platforms is a requirement that spans beyond technical and traditional organizational boundaries. MCDAs should be able to discover, access, and consume any relevant information on a need-to-know basis, regardless of jurisdiction, affiliation, or location.

Several dimensions of interoperability shall be considered including common data structures and formats, common messaging protocols, common search and information request service calls, and network and communications interconnectivity.

2.3 Value proposition

The value proposition of the GIF &GEA is to provide:

- An interoperable, operational architecture and GEA that can be customized to MCDA use cases and that ensures alignment of people, processes, and technology prior to a major multi-agency, multi-jurisdiction event or investment;
- A roadmap to solving interoperability issues and gaps via architectural blueprints and governance that drives acquisition guidance and alignment Government digitalization agenda
- A guidebook for MCDA acquisition decisions for products and services ensuring that such acquisitions are interoperable, secure, resilient, and enable effective data management;
- A blueprint that informs Government leadership of the complexities and needs for interoperability across multiple MCDAs functions as well as political jurisdictions;
- A framework that incorporates information sharing an
- d Once Only Principle best practices, guidance, and lessons learned; and
- A strategy for GEA and GEA evolution that can be expanded as well as an ongoing embracement of emerging technologies.

2.4 GEA Domains

The enterprise architecture consists of eight second level building blocks covering eight architecture domains namely: Business, Information, Solutions, Technology, Integration, Human capacity, Governance and Security.

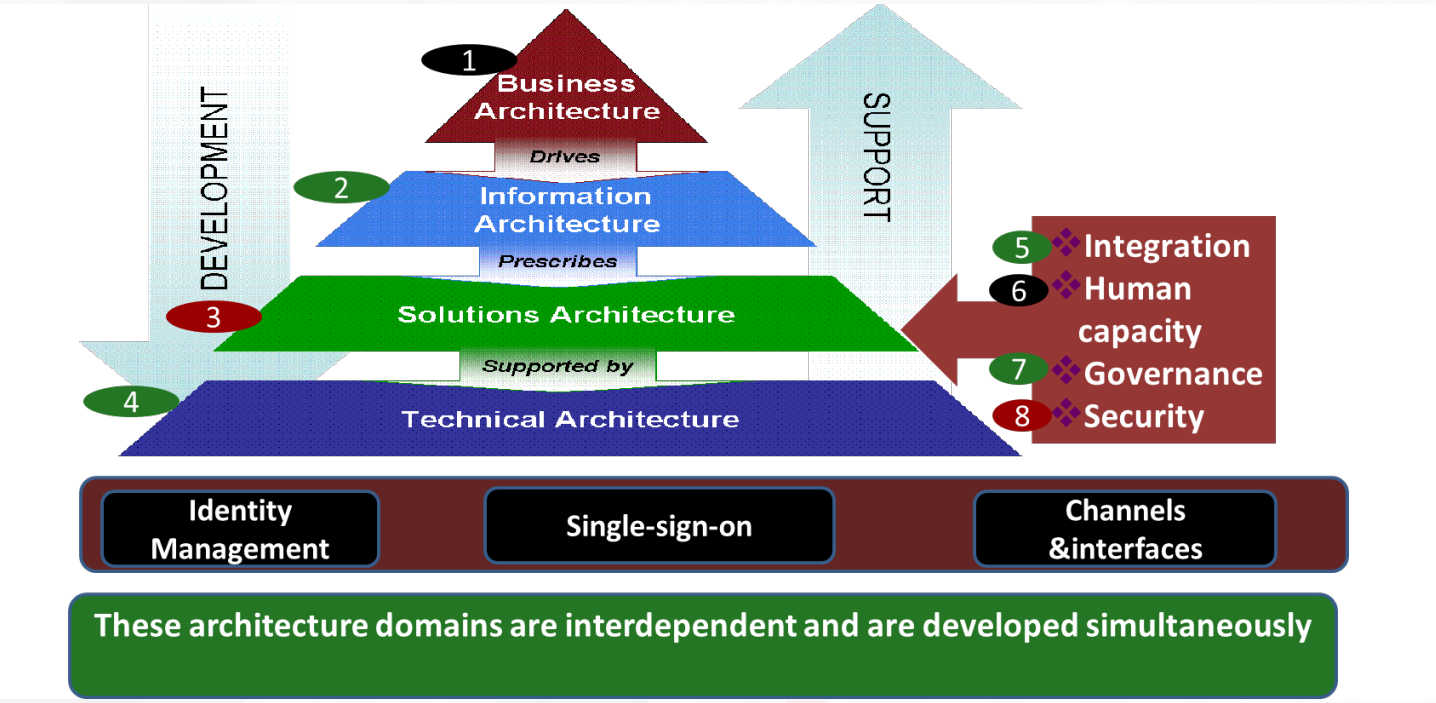


Figure 3: Summary of the GEA components

These domains will subsequently be used to review the MCDAs digital initiatives to ensure their alignment to support strategic outcomes.

2.5 GEA PRINCIPLES

2.5.1 EA Foundation

EA Principles GEA & GIF CONCEPT NOTE

PRINCIPLE	RATIONALE	IMPLICATION
EAP 1:**The government focuses on citizens**	• The government exists to serve the Nepal public who want simpler, faster, better and cheaper access to government services and information.	• Departments will design and apply their business processes and services to benefit citizens. • The Government offers citizens a single, —unified face, reducing duplication, needlessly complex, inconsistent ways of using government services. • Citizens can access government services through various means, devices and

PRINCIPLE	RATIONALE	IMPLICATION
		channels.
EAP 2:The government is a single, unified enterprise	• The government operates as a single enterprise with decision-making flexibility at the MDA level. • A single enterprise with shared strategic objectives, common governance, integrated management processes and consistent policies improves the implementation of government-wide strategies and the coordination of the delivery of department citizen services.	• Government optimizes resource allocations across the enterprise to achieve common goals. • Government optimizes information across the enterprise to support services and processes. • Architectural designs integrate services for efficiency and keep autonomy of operations for effectiveness. • Architectural designs identify and accommodate distinctive (non-homogenous) approaches to maintain important policy objectives.
EAP 3:The Government architecture is mission-driven	• A business-led architecture is more successful in meeting strategic goals, responding to changing mission needs and serving citizens' expectations.	• Architecture is driven by program mission needs and enabling technology. • MDAs will first seek to optimize business processes, and then use performance standards to define automation requirements. • Systems and processes will use an architecture that responds quickly to events. • The government and agencies will use their enterprise architectures to guide their capital planning, budget and investment decisions. • Agencies will manage change in government operations with enough security to keep services flowing. • Government solutions must be agile and flexible to meet business needs.
EAP 4: Security, privacy and protecting information are core government needs	• Security, privacy and protecting information are integral to government operations, and are part of the architecture. • Government must protect information against unauthorized access, denial of service, and both intentional and accidental modification to increase public trust.	• The business context defines security and privacy requirements, which integrate into the entire architecture throughout the business lifecycle. • Architectures must reflect policies to minimize improper use of data and security violations. • Government must apply security and privacy consistently and monitor compliance. • Information security controls need to be clearly defined so cost and risk are balanced and managed.

PRINCIPLE	RATIONALE	IMPLICATION
EAP 5: Information is a national asset	• A well informed citizenry is necessary to our democracy. • Further, accurate information is critical to effective decision making, improved performance, and accurate reporting.	• The government will improve its information sharing environment to better disseminate information to the public. • This requires Government to identify authoritative sources of high quality information, and agencies to provide access to specified data and information. • Authoritative data sources may need to be restructured and catalogued for easy dissemination, access and management. • To realize this principle requires a government strategy • To promote cost effective data sharing with other levels of government.
EAP 6: The architecture simplifies government operations	• The Architecture is designed to reduce complexity and enable integration to the maximum extent possible. • Complex processes and systems with tightly coupled modules are difficult to manage, risk failure, are inflexible to changing agency mission needs, and are expensive to maintain. • Highly modular, loosely coupled systems and processes take advantage of shared services and reusable components within government and available commercially.	• This requires loosely coupled software components shared as services and compatible application development. • Agencies must share their best practices and reusable business and technical components. • Building and integrating reusable components must become a common development method.
EAP 7:Enterprise Architecture is mission-driven	• A business-led architecture is more successful in meeting strategic goals, responding to changing mission needs, and meeting citizens' expectations	• Ensure architectural descriptions demonstrate how the business serves the current Government's priorities and the needs of citizens; • To the extent possible, design artefact type definitions to facilitate integration with descriptive representations of other jurisdictions, thereby allowing MDAs to collaborate with each other ; and • Follow the precept that architecture practice is not an end unto itself.
EAP 8: Enterprise Architecture is aligned with relevant legal framework	• The Legal Framework, as contemplated in the Constitution, Acts and Regulations is designed to ensure good governance, accountability, citizenship and an improved public service delivery. • Compliance to the legal framework reduces the risks of non-conformance	• Laws, regulations, and policies should be considered when developing Enterprise Architecture. • Changes in the law and regulations may drive changes in the Enterprise Architecture of departments and agencies, in particular services, functions, processes and applications.

PRINCIPLE	RATIONALE	IMPLICATION
	and under-performance.	• Business process improvements may lead to changes in the legal framework.
EAP 9: Simplification	• An Enterprise Architecture that is explicit and pragmatic enables transformation of programs and services and minimizes enterprise redundancy.	• Optimize lines of business and business solutions to benefit the enterprise as a whole; • Maintain an EA practice designed to reduce complexity and enable integration to the maximum extent possible; • Make best practices available to ensure architectural representations from all five architecture domains provide a minimal set of information sufficient to describe fully problems, opportunities and solutions.
EAP 10: Reuse	• Reuse minimizes development, complexity, maintenance and support costs through the deployment of common well-understood components	• Define architecture practices in each domain to produce and promote practical mechanisms for reuse; • Ensure reuse is one of the criteria of quality assurance review; • Encourage and reward reuse throughout the enterprise; and • Processes, applications and components are designed to meet reuse objectives
EAP 11: Explicitness	• Explicit architecture facilitates creating and changing an enterprise and its business solutions. • Formally developed and documented enterprise architectures form a baseline and provide an effective foundation for managing change.	• Define architecture practices in each domain to produce and promote pragmatic and useful artefact-type definitions; • Communicate best practices for artefact creation; • Grow and maintain an accessible collection of descriptive representations to provide an evolving picture of the enterprise.
EAP 12: Holistic	• To provide business value over time enterprise architecture contains interrelated information covering all aspects of the enterprise at all levels of abstraction (business; information; application; technology; and security. •	• Establish and mature the architecture practice in the five architecture disciplines; • Ensure artefact type definitions include the means by which transformation and alignment are provable; • Ensure enterprise architecture review requirements include a set of artefacts from • each domain sufficient to contribute

PRINCIPLE	RATIONALE	IMPLICATION
		meaningfully to an enterprise view; and • Include transformation and alignment as criteria for architecture review.
EAP 13: Enterprise Architecture is aligned with relevant legal framework	• Business architecture practice includes the discipline and tools required to enable business strategic and operational planning. •	• Ensure business goals are aligned with enterprise priorities; • Position the business in the context of the broader enterprise; • Develop business model to meet operational objectives and strategic goals; and • Analyse business risk and develop strategies for risk management

2.5.2 BUSINESS ARCHITECTURE

Addresses these in terms of the Business and IT Strategies, Target Operating Model, Vision, Principles, Goals and Objectives. Concerns the people's perspective in the Enterprise answering the 'Who' question. Business Roles and Business Functions (responsibilities), from both an internal (staff, partners) and external (customers, agents) perspective.

Business architecture is a critical aspect for the successful implementation of the GEA. The architectural strategy advocates a whole of government approach where IT is aligned to business services and solutions are based on reusable components implementing business capabilities in order to deliver a cohesive user experience. As such, it is essential that business services, stakeholder needs, opportunities to improve cohesion and opportunities for reuse across government be clearly understood.

It is expected that the IT culture and practices will have to change to make business architecture, in general, and the following elements will be of primary focus.

1. **Design services digitally from end to end to meet the Government of Kenya users and other stakeholders' needs**

- Clearly identify internal and external users and other stakeholders and their needs for each policy, program and business service.
- Include policy requirement applying to specific users and other stakeholder groups, such as accessibility, gender-based plus analysis, and official languages in the creation of the service.

- Perform Algorithmic Impact Assessment (AIA) to support risk mitigation activities when deploying an automated decision system.
- Model end-to-end business service delivery to provide quality, maximize effectiveness and optimize efficiencies across all channels.

2. Architect to be outcome driven and strategically aligned to the department and to the Government

- Identify which departmental/Government business services, outcomes and strategies will be addressed.
- Establish metrics for identified business outcomes throughout the life cycle.
- Translate business outcomes and strategy into business capability implications to establish a common vocabulary between business, development, and operation.

3. Promote horizontal enablement of the enterprise

- Identify opportunities to enable business services horizontally across the government
- enterprise and to provide cohesive experience to users and other stakeholders.

- Reuse common business capabilities, processes and enterprise solutions from across government and private sector.
- Publish all reusable common business capabilities, processes and enterprise solutions for others to develop and leverage cohesive horizontal enterprise services.

Business architecture Principles

PRINCIPLE	RATIONALE	IMPLICATION
BAP 1: Business Planning	• Service Orientation: Identify Deliver Government Services th are Critical, Flexible & Reusable • Compliance with Legislatio Government Regulations a Standards	•
BAP 2: Common vocabulary	• A common business vocabula enhances communication a understanding of the business	• Engage and consult with business stakeholders to ensure mutually agreeable business vocabulary; • Ensure the business vocabulary is explicit
BAP 3: Simple and Flexible	• Opportunities for increasi efficiency, effectiveness, a quality can be identified a realized through simple a flexible business processes.	• Analyse business processes to simplify, integrate, eliminate redundancy, and increase efficiency; • Identify common business processes for reuse; and • Design business processes to enable business agility.
BAP 4: Technology independent	• Business architecture describ the business model independent of supporting technology a provides the foundation f analysis of opportunities f automation.	• Eliminate technology constraints when defini business architecture; and • Ensure automated processes are described at t business process level for analysis and design.
BAP 5: Public and Private collaboration improves public services	• Collaboration between public a private entities, who sha government objectives, improv the efficient use of nation resources; reduces duplication effort and inconsistencies, a optimizes public service delivery •	• The Business Architecture(BA) structures a functions on IT Governance include governan functions (such as direct, evaluate and monit for members of interdepartmental councils a forums. • The BA performance models include shar accountability on programmes as reflected performance scorecards across public servi departments and agencies. • The BA structures and functions includ partnerships across departments and agencie and among public and private sector. • The BA processes reflects that public servi delivery processes traverse across tradition organisational boundaries. • System architecture reflects integratio interoperability and sharing of Information a ICT systems across all spheres of government improve and optimise public service delivery.

PRINCIPLE	RATIONALE	IMPLICATION
		• Architecture reflects the adoption of ope (non-proprietary) standards and industry's be practices.
BAP 6: Operations are optimised and simplified	• Enterprise Architecture facilitates and enables business process effectiveness and efficiency and the reduction of complexity of systems to the maximum extent possible. • Complex business processes and systems with tightly coupled modules are difficult to manage, prone to failure, inflexible to the changing needs of a department, and are expensive to maintain. These complex processes often resulted in diverse solutions and configurations across different department to enable the same or similar business processes.	• Business processes and services are standardised in line with good practice and shared within and across departments. • Business processes are optimized and performance standards defined before automation requirements are defined. • Systems and technology architectures are aligned with business processes and performance models in order to maximize the value of ICT investments. • Systems and software are modular, flexible and loosely coupled. • Information exchange interfaces are simple and based on open standards for all intra- or interdepartmental solutions. • Solutions are implemented based on similar business process building blocks and shared system building blocks.
BAP 7: Systems are designed to ensure Business Continuity	• System failures disrup operations and lead to service delivery failures and therefore we should make sure Critica operations must continue i spite of system failure.	• Mission essential/critical systems are designed according to business continuity and disaster recovery requirements and include the necessary continuity measures (such as redundancy, standby and fail-over components). • Information Systems inventory is established and maintained and each system is classified commensurate their risk of failure profile (e.g. nonessential, essential, critical). • Alternative business processes are followed only when recovery operations take place in the event of system failure. • Essential/Critical systems use technology that is proven to be reliable and maintainable. • Essential/critical systems are monitored and pre-emptively reconfigured to ensure continued operations.
BAP 8: Service Orientation:	• Identify & Deliver Government Services that are Critical, Flexible &Reusable It is key to provide services in a flexible manner. • This supports the target of improving service to citizens	• Reusing services across MDAs eliminate duplicity. Duplicative capability is expensive and contributes to the proliferation of conflicting data

2.5.3 INFORMATION ARCHITECTURE

Information Architecture includes the knowledge, information and data that flows through the business processes and the data that is accessed and stored by applications. Information architecture includes both structured and unstructured data. The best practices and principles aim to support the needs of a business service and business capability orientation.

To facilitate effective sharing of data and information across government, information architectures will be designed to reflect a consistent approach to data, such as the adoption of government and international standards. Information architecture will also reflect responsible data management, information management and governance practices, including the source, quality, interoperability, and associated legal and policy obligations related to the data assets. Information architectures will also distinguish between personal and non-personal data and information as the collection, use, sharing (disclosure), and management of personal information must respect the requirements of the Privacy Act and its related policies.

The following elements will be of primary focus:

1. **Collect data to address the needs of the users and other stakeholders**

- Assess data requirements based on program objectives, as well as users, business and stakeholder needs.
- Collect only the minimum set of data needed to support a policy, program, or service.
- Reuse existing data assets where permissible and only acquire new data if required.
- Ensure data collected, including from third-party sources, are of high quality.

2. **Manage and reuse data strategically and responsibly**

- Define and establish clear roles, responsibilities, and accountabilities for data management
- Identify and document the lineage of data assets.
- Define retention and disposition schedules in accordance with business value as well as applicable privacy and security policy and legislation.
- Ensure data are managed to enable interoperability, reuse and sharing to the greatest extent possible within and across departments in government to avoid duplication and maximize utility, while respecting security and privacy requirements.
- Contribute to and align with enterprise and national data taxonomy and classification structures to manage, store, search and retrieve data.

3. Use and share data openly in an ethical and secure manner

- Share data openly by default while respecting security and privacy requirements; data shared should adhere to existing enterprise, national and international standards, including on data quality and ethics.
- Ensure data formatting aligns to existing enterprise, national and international standards on interoperability; where none exist, we will develop data standards in the open with key subject matter experts.
- Ensure that combined data does not risk identification or reidentification of sensitive or personal information.

4. Design with privacy in mind for the collection, use and management of personal Information

- Ensure alignment with guidance from Office of the Data Protection Commissioner with respect to interpretation and application of the Privacy Act and related policy instruments
- Assess initiatives to determine if personal information will be collected, used, disclosed, retained, shared, and disposed
- Only collect personal information if it directly relates to the operation of the programs or activities
- Notify individuals of the purpose for collection at the point of collection by including a privacy notice
- Personal information should be, wherever possible, collected directly from individuals but can be from other sources where permitted by the Privacy Act
- Personal information must be available to facilitate right of access to and correction of government records
- Design access controls into all processes and across all architectural layers from the earliest stages of design to limit the use and disclosure of personal information
- Design processes so that personal information remains accurate, upto date and as complete as possible, and can be corrected if required and maintain a single-source-of -truth
- The identification techniques should be considered prior to sharing personal information
- In collaboration with Office of the Data Protection Commissioner, determine if a Privacy Impact Assessment (PIA) is required to identify and mitigate privacy risks for new or substantially modified programs that impact the privacy of individuals
- Establish procedures to identify and address privacy breaches so they can be reported quickly and responded to efficiently.

Information Architecture Principles

PRINCIPLE	RATIONALE	IMPLICATION
IAP 1: Formally defined and aligned with business needs	• Well-defined information and data designs contribute to strategic decision- making processes and service delivery. • Well-specified designs maximize alignment and integration of information holdings with business processes.	• Ensure the business information and data needs are clearly communicated; • Organize and document information holdings using information architecture processes, methods and standards; • Document the business information flows and linkages to enable a clear understanding by the data owners/custodians; • Model, design, and develop information holdings using a top-down, enterprise-wide architecture approach.
IAP 2: Information /Data security and permission	• The duty to protect and secure sensitive information must be balanced against the duty to share and release public information. • Laws and Regulations require the safeguarding of sensitive information while permitting free access to public information. • To improve the security of resources, must protect its information from unauthorised access, modification or damage.	• Information System Security capability (people, processes and technology) is in place to determine, monitor and maintain the levels of security of the government information assets (data, applications and technology). • Security architecture is an integral part of business, data, application and technology architectures. • Security architecture is consistently applied throughout departments and systems. • Access control to information and data sources is applied within the data architecture (not in the application architecture).
IAP 3: Data is shared and duplication is reduced	• Data is a strategic resource that requires effective and efficient management across government. Duplicate information and data sources across government systems result in duplicate labour intensive data management processes and frustrated citizens who need to provide same information to multiple departments. Duplication also • leads to public service delivery inconsistency; fragmented data management responsibilities, reduced validity of data, poor data quality, and is open for localised exploitation and potential fraud and corruption.	• Business architecture (processes and functions) of information management includes the roles and responsibilities of "meta-data manager" (person who manages the design of data) and "data governor/steward" (person who manages data quality and integrity on behalf of someone else) as required for data sharing. • System architecture (data exchange and flow models) reflects intra and interdepartmental data exchange and verification models for inclusion in departmental transition plans. • Data sources that are candidates for re-use and sharing across departments are determined in every project in order to reduce the burden of duplicate data collection (e.g. citizen data, geographic data, etc) and to improve the quality and validity of government data. • Shared data sources are consolidated into a shared environment to increase the re- use and sharing. • On-line data exchange and verification interfaces across different data sources are standardized on best practice using data record exchange interfaces, in favor of bulk file transfers (such as

		large "flat-files" or "data dumps").
IAP4: Data is accessible	• Users – public servants and citizens alike – must have access to accurate, relevant and timely data to render or consume an effective government service. • A well informed citizenry is necessary to our constitutional democracy; and accurate information to authorised users is critical to effective decision making, improved performance, and accurate reporting.	• Government wide data catalogue (inventory) is developed and used to identify authoritative sources of high quality information that can be made available for access to empower public servant and citizens alike. • Default Access control to data is set to "open for all" and made available to all through any means, unless security policy requires access restrictions (i.e. application software should not unnecessarily restrict users to access data). • "Search" or "Find" functionality exist for all end-user applications/web portals to improve access to data sources.
IAP 5: Standard, Common vocabulary and data / metadata definitions.	• Data definitions that are consistent and meaningful ensure the effective and efficient development, interoperability and use of data and applications throughout government. • The power of a common vocabulary and data definition also enable effective dialogue to empower user and citizens. Conversely, inconsistent data definitions lead to poor interoperability, misinterpretations and inconsistent reporting.	• Agency and Government have a Dictionary of ICT Terms and Definitions on ICT that is freely shared and collectively owned by ICT practitioners. • A common data reference model (a schema that contains the data entities and their definitions), a meta-data model (a schema that defines relationship between the data entities) and a meta-data store (an electronic repository to store it) are well defined. • Data definitions and ICT Dictionary of terms are available to the whole of government to enable use, integration and common understanding. • Government meta-data management discipline is established, and data standardization initiatives are coordinated throughout government. • Establish business information standards to improve data quality, integrity and reliability; and • Develop clear information and data definitions to enable data sharing, integration, exchange and reuse across the enterprise;
IAP 6: Integrity, Accessibility and Availability	• Information needs to be concise and accurate (integrity), accessible, and available, as required by the business.	• Defines processes that provide for integrity, accessibility and availability of the information and data; • Ensure information owners and custodians are aware of the sensitivity of their information holdings they own/manage; and • Adhere to information architecture modelling standards, best practices, and guidelines.
IAP 7: Data has an owner/ trustee	• Data created once by the owner and the rest re-use	• Creates a single source of truth

2.5.4 APPLICATION ARCHITECTURE

Application architecture practices must evolve significantly for the successful implementation of the GEA. Transitioning from legacy systems based on monolithic architectures to architectures that are oriented around business services and based on reusable components implementing business capabilities, is a major shift. Interoperability becomes a key element, and the number of stakeholders that must be considered increases. The following elements will be of primary focus:

1. **Use open source solutions hosted in public cloud**

- Select existing solutions that can be reused over custom built
- Encourage the use of internally developed or local solutions developed using open source platforms.

2. **Use shared systems across government and package them as software as a service (SaaS) hosted in public cloud**

- Assess the systems that can be shared across government
- Choose SaaS that best fit for purpose based on alignment with SaaS capabilities and that is extendable.

3. **Design for Interoperability**

- Design systems as highly modular and loosely coupled services.
- Expose services, including existing ones, through APIs.
- Make the APIs discoverable to the appropriate stakeholders.

4. **Enable Interoperability**

- Expose data and functionality through service interfaces
- Applications must communicate with each other via those interfaces
- Services interfaces must be published and discoverable

Application Architecture Principles (AAP)

PRINCIPLE	RATIONALE	IMPLICATION
AAP 1: Common applications are shared across government	• Modular and component based • Ease of use and re-use • The sharing of applications that are designed to enable common/transversal business processes/functions of government radically improves the economy of IT investments across government. • Sharing of common/transversal applications reduces the burden of maintaining several configurations of the same type of applications, complexities in support contracts and commensurate licensing fees.	• Information system catalogue (inventory) is developed and used to identify candidates for common and transversal type applications. • Provision is made for departments to (1) dispose or modify some of their unique applications in favour of a common/transversal application standard, and (2) adapt existing business processes to align with the common/transversal business process. • Common/transversal applications use open interfaces to enable development of departmental specific extensions and to enable information exchange with departmental unique application portfolio. • Departments retain data ownership to comply with legal or security requirements. • Priorities and funding for the acquisition of common/transversal type applications are determined collectively by all departments.
AAP 2: Applications are independent of technology infrastructure	• Applications that are independent from the underlying technology infrastructure allows applications to be designed, developed, operated on and migrated to ad variety of front-office (end-user) and back-office (hosting environment) technology platforms to improve flexibility, end-user convenience, cost effectiveness and lower the risk of technology vendor lock-in.	• Application development software that does not support portability or platform independence is avoided. • Commercial Off the Shelf applications that are technology dependent are avoided. • Applications are designed for multi-tier deployment, which separates at least the end-user tier from the back-end tier, and the back-end tier from the database tier. • Application-to-application interfaces are via a common interface bus. • Applications-to-data interfaces comply with data interface standards as prescribed.
AAP 3:Common applications are easy to use	• Common applications (which are intended for broad deployment in government) that have consistent and simple user interfaces reduce the training burden and provide	• User interface design is informed by user location, language, competency, and physical capability. • Applications contain no unnecessary technical options that

	incentive for end-users to use the application.	could reduce productivity and increase the risk of improper use of the application. • Same type applications have a common ''look-and-feel'', support ergonomic requirements and provide context sensitive help. • User friendliness is part of the test and acceptance criteria, which requires sign-off by an end-user representative, before applications are deployed for general use.
AAP 4: Traceability	• Aligns to business; • Build for change; • Facilitates transformation of business architecture; • Enhances traceability to business requirements; • Maximize the effectiveness of the development project; and • Minimizes requirement mismatch	• Need to ensure conformance to EA practice in the creation of artifacts; • Need to follow a Systems Development Life Cycle methodology or applicable standard; and • Need to document stakeholder requirements well
AAP 5: Flexibility	• Application Architecture must be highly modular, multi-tiered, flexible, and loosely coupled. • Optimizes for agility; • Minimizes integration complexity; • Simplifies implementation, deployment and maintenance; • Enhances scalability, upgradeability, supportability; • Enables service and component reusability; • Ensures services are componentized; • Facilitates and improves maintainability; • Enables technology platform changes with minimum effect on business processes; • Enables Component-Based Architecture (CBA) & Services-Oriented Architecture (SOA)	• Need to implement n-tier architecture pattern; • Need to utilize application design patterns; • Need to establish a common approach to integration; • Must consider component- or services-based architectures; and • An enterprise Services-Oriented Architecture strategy may need to be in place
AAP 6: Integrability	• Application Architecture must reduce integration complexity and foster application simplicity. • Reduces costs; • Streamlines business processes; • Facilitates reuse; • Improves integration; • Minimizes application impacts (e.g., potential delays in project	• Need to follow standards (industry, open-standard, technology, security, etc.); • Need to plan for integration; • Need to develop loosely-coupled interfaces; and • Need to publish integration points •

	completion); • Decreases application maintenance and support; • Minimizes duplication and multiple systems; and • Increases application flexibility	
AAP 7: Modularity	• The Application Architecture must follow a service-based approach • Hides the complexity of heterogeneous IT environments from business user; • Allows internal and external business processes to be combined and recombined to support flexibility in business process execution; • Enhances business agility; • Provides an IT architecture that is more flexible, agile, and cost effective; • Helps to ensure better interoperability; • Supports services transformation; • Improves Service Offering; • Potential for cost reductions through IT asset re-use; • Creates opportunities for new business/services integration;	• Use standards-based approach; and • Security and privacy awareness heightened • Better software and faster build (composite applications); and Promotes collaboration
AAP 8: Buy Versus Build	• The Application Architecture must support the concept of reuse before buy and buy before build. • Reduces costs; • Aligns to business requirements; and • Minimizes application development, maintenance and support costs and related resource implications	• Need to conduct a fit/gap and cost-benefit analysis; • Need to comply with ICT directives and operating policies; • Need to be market-aware; • Need to plan for integration; and • Need to follow the acquired solution guidelines for conformance to EA practice
AAP 9: Consolidation	• The Application Architecture must promote consolidation first and integration second. • Reduces cost; • Reduces integration complexity; • Facilitates consolidation of similar functions; • Streamlines similar application into single systems; • Minimizes duplication of solutions; • Increases reuse across the enterprise; and • Simplifies application maintenance and support	• Need to conduct a fit/gap and cost-benefit analysis; • Need to comply with ICT directive; • Need to plan for consolidation; and • Need to follow the acquired solution guidelines for conformance to EA practice

AAP 10: Interoperability	• Supports inter-jurisdictional initiatives; • views the government as a single enterprise; • Facilitates consolidation of similar functions; • Facilitates data sharing between internal and external partners; • Supports streamlining processes; and • Reduces cost	• Need for enforced security standards; • Require open or industry standards; and • Need to use standardized interface
AAP 11: Reusability	• designing applications for reuse. • Reduces cost; • Encourages future reusability of common components/services and applications; • Promotes application assembly and component integration; • Ensures consistency in the development of components/services	• Need to reuse existing application components or services where feasible; • Need to employ Component Based Architecture or Services-Oriented Architecture (SOA)as preferred architecture best practices; and • An enterprise Services-Oriented Architecture strategy may need to be in place
AAP 12: Share ability	• portfolio approach to analyzing, planning, designing, governing, and optimizing enterprise applications. • Optimizes application investment; • Improvers reusability; • Improves application planning; • Enhances IT asset management	• Reduces of the number of applications; • Focuses on application gaps; and • Enables an enterprise-wide application planning and prioritization approach
AAP 13: Upgradability	• must anticipate and plan the replacement and transition of legacy applications. • Minimizes likelihood and risk of developing and deploying applications that are functionally deficient • Reduces likelihood of implementing solutions which are high-cost/high-maintenance • Assists with planning for the replacement of applications - reduces 'crisis' • Replacement and maintenance efforts • Facilitates a responsive enterprise ICT posture that can respond to changing requirements over time	• Need to establish a legacy renewal strategy • Both business and IT must work together in the search for the best possible replacement • Need to develop priorities for the replacement of obsolete, legacy and redundant • systems
AAP 14: Compliance	• Application solutions must be developed using standard, common methodologies. • Increases likelihood of high quality deliverables	• Systems Development Life Cycle standards must be adopted to maximize the effectiveness of the development process; and • Training will be required to support

	• Reduces cost through common methodologies and tools	standard methodologies
AAP 15: Supportability	• The applications must be documented comprehensively to ensure that it: • Aligns to business • Facilitates transformation of business architecture • Enhances traceability to business requirements • Maximizes the effectiveness of the development project • Minimizes requirement mismatch potential • Supports future maintenance of the system	• Need to ensure adherence to EA practice in the creation of artifacts; • Need to ensure the application design reflects the application architecture principles, practices, and standards; • Need to ensure the requirements traceability by cross-referencing the system • requirements with design elements; and • Need to follow a development methodology and/or applicable standard •

2.5.5 TECHNOLOGY ARCHITECTURE

Technology Architecture defines the technologies and infrastructure that support the applications in terms of nodes, networks, devices, system software, communication infrastructure and persistent data storage.

Technology architecture is an important enabler of highly available and adaptable solutions that must be aligned with the chosen application architecture. Cloud adoption provides many potential advantages by mitigating the logistical constraints that often negatively impact legacy solutions hosted "on premises." However, the application architecture must be able to enable these advantages. The following elements will be of primary focus:

1. Use government cloud first

- Adopt the use of the government guidelines to ensure proper security and access controls
- Enforce this order of preference: software as a service (SaaS) first, then platform as a service (PaaS), and lastly infrastructure as a service (IaaS)
- Enforce this order of preference: government cloud first, then hybrid cloud, then private cloud, and lastly non cloud (on premises) solutions
- Design for cloud mobility and develop an exit strategy to avoid vendor lockin

2. Design for performance, availability and scalability

- Ensure response times meet user needs, and critical services are highly available
- Support zero downtime deployments for planned and unplanned maintenance
- Use distributed architectures, assume failure will happen, handle errors gracefully, and monitor performance and behavior actively

- Establish architectures that supports new technology insertion with minimal disruption to existing programs and services
- Control technical diversity; design systems based on modern technologies and platforms already in use

3. DevSecOps (short for development, security, and operations) is a development practice that integrates security initiatives at every stage of the software development lifecycle to deliver robust and secure applications.

- Use continuous integration and continuous deployments
- Ensure automated testing occurs for security and functionality
- Include all users and other stakeholders as part of the DevSecOps process, which refers to the concept of making software security a core part of the overall software delivery process.

Technology Architecture Principles

PRINCIPLE	RATIONALE	IMPLICATION
TAP 1: **Technological diversity is contained**	• Limiting the diversity of technology product mix on a government wide scale will reduce maintenance, supply chain complexities, and reduce the cost of procurement due to leveraging on economy of scale and technology innovation.	• The Technology product portfolio that is utilized for common/transversal systems is reduced to a finite manageable set that will strike a balance between the ease and cost of managing the life-cycle of technology on the one side, and stimulating healthy economic competition and growth of the ICT industry • Growing and evolving the ICT portfolio require that emerging, innovative or cutting-edge ICT products must be monitored on a continued basis; and be subjected to proof-of-concept to test for relevance, compliance and impact to government operations before it is introduced into ICT product portfolio. • The efficacy, efficiency and risk of the existing ICT product portfolio are reviewed on a regular basis to identify candidate products that need to be upgraded or disposed.
• TAP 2: **Technology components are able to interoperate and exchange information**	• Technology components (hardware and software), which cannot exchange information or integrate with each other lead to rampant duplication of data and ICT, increase the number of "islands" and "silos" in government systems introduces	• Government adopts interoperability standards whose specifications are freely available, non-proprietary, have multiple implementations and can easily be maintained; and publish such standards • A government-wide technology product catalogue must be developed and

	inconsistency and complexity. • This is alleviated by introducing interoperability standards that enables products from different vendors to physically connect, integrate and freely exchange information with each other. •	maintained to account for all the types of ICT products and to record their level of compliance. • All prospective ICT products must comply with the standards before it is implemented in Government • The standards are reviewed and updated on a regular basis to keep abreast with technological development through a process of research, consultation and consensus among government stakeholders.

2.5.6 SECURITY ARCHITECTURE

The Security Architecture is a government wide initiative to provide a standardized approach to developing IT security architecture, ensuring that basic security blocks are implemented across the enterprise as the infrastructure is being renewed. The following elements will be of primary focus:

1. **Build security into the system life cycle across all architectural layers**

- Identify and categorize information based on the degree of injury that could be expected to result from a compromise of its confidentiality, integrity and availability.
- Implement a continuous security approach, in alignment with Centre for Cyber Security's, IT Security Risk Management Framework; perform t+hreat modeling to minimize the attack surface by limiting services exposed and information exchanged to the minimum necessary.
- Apply proportionate security measures that address business and user needs while adequately protecting data at rest and data in transit.
- Design systems to be resilient and available in order to support service continuity.

2. **Ensure secure access to systems and services**

- identify and authenticate individuals, processes or devices to an appropriate level of assurance, based on clearly defined roles, before granting access to information and services;
- leverage enterprise services such as trusted digital identity solutions to authorized entities (users and devices), with clearly **defined roles; segment and separate information based on sensitivity of information.**

3. **Management interfaces may require increased levels of protection**

- Implement HTTPS for secure web connections and Domain-based Message Authentication, Reporting and Conformance for enhanced email security.
- Establish secure interconnections between systems through secure APIs or leveraging centrally managed hybrid IT connectivity services.
- Implement the NPKI for secure login.

4. **Maintain secure operations**

- Establish processes to maintain visibility of assets and ensure the prompt application of security related patches and updates in order to reduce exposure to vulnerabilities, in accordance with laid down Guidelines.
- Enable event logging, in accordance with event logging guidance, and perform monitoring of systems and services in order to detect, prevent, and respond to attacks.
- Establish an incident management plan in alignment with the Cyber Security Management Plan and report incidents to the NC3.

Security Architecture Principles (SAP)

PRINCIPLE	RATIONALE	IMPLICATION
SAP 1: Administration - Protection of ICT Assets	• ICT assets and resources will be protected from loss, destruction or unauthorized use or disclosure in accordance with its value, sensitivity and applicable legal requirements. • The appropriate implementation of ICT security measures will be cost-effective and risk- appropriate investments.	• MCAs, ICT Clusters and service providers must effectively assess management and mitigate risks by defining, communicating, developing, improving and implementing.
SAP 2: Administration - Responsive and Cost-Effective	• The design and implementation of security infrastructure (e.g., identification, authentication and authorization services and mechanisms) will be as secure, pluralistic, simple, efficient, cost-effective, reusable and transparent to the end-user as possible. • The impact of security mechanisms and services on business productivity is minimized, encouraging compliance with the security policies and practices by way of a well-considered security model at the MCA, program and ICT Cluster level. •	• Implement solutions in a manner that is consistent with the security tenet of limiting access based on end-user role (e.g., staff members, System Administrators, third party partners, commercial users and private/individual consumers of -offered services). • Develop and implement security mechanisms and ICT infrastructure that are neither intrusive nor invasive. • Develop and implement security mechanisms and ICT infrastructure that conform with government policies and standards regarding identity management, authentication and authorization , including: • Single system sign-on solutions;

		• Multi-factor authentication schemes; and • Authentication and authorization solutions based on smart-card and biometric approaches.
SAP 3: Administration - Auditable Compliance	• The security of ICT systems must be auditable, as required for compliance with statutory, contractual, and policy requirements as well as de facto security standards of care that may apply across jurisdictional boundaries. Audit schedules for ICT systems are consistent with the security models and plans for technology solutions.	• Ensure ongoing security compliance and control; • Ensure security-appropriate standards of care are met regarding safeguarding of ICT assets • Ensure 3rd party service providers comply with GEA ICT security policies, standards and requirements; and
SAP 4: Administration - Commensurate Controls	• All ICT systems will be designed, built and implemented to incorporate the level of assurance, security, privacy controls, auditability and control functions necessary and appropriate to the sensitivity and value of information assets and/or resources that they consume, control, utilize or manage. Target architectures, including those for technology refreshes or upgrades to legacy applications, will be in compliance with security requirements.	• The MCAs must define and communicate: • Security policies, standards and guidelines related to; Information and data sensitivity and classification; Criteria for determining appropriate level of assurance (Confidentiality, • Integrity, Availability) ; Authentication requirements; and Audit trail requirements • Security processes related to: Communications; Compliance; Security testing and evaluation (ST&E); Governance (review, endorsement and approval); and Audit (exceptions and appeals).
SAP 5: Availability - Security Process Support	• ICT enterprise security architecture addresses availability of information assets, ICT- based resources holding and supporting security infrastructure, processes and structures. • The enterprise security architecture will support key security processes such as monitoring and incident response, business continuity and contingency planning (business Impact/Risk Assessment and Analysis), disaster recovery, security configuration and capacity planning and security operations measures.	• The security standards and guidelines and operations processes must address: Monitoring and reporting; Incident response; Business continuity planning; Disaster recovery (DR) and contingency planning; Security design and implementation; Security configuration and capacity planning; Assurance; Forensics; and Security operations planning (e.g., identity and access control, user-id management).
SAP 6: Availability - Controls Consistent	• Safeguards to protect against breaches of security will be implemented to reduce potential risk to ICT assets and resources. The	• The ICT enterprise security architecture policies and procedures must include: • A statement defining what

with Risk & Value	safeguards and level of response to threats will be consistent with the value, vulnerability and sensitivity of protected assets or resources.	constitutes a breach of security and a delineation of which incidents and occurrences are security events rather than security incidents
SAP 7: Assurance – Standards-based Security Services	• The MCAs will adopt and comply with industry-accepted/standard approaches regarding due-diligence and standards of care in order to ensure the secure delivery of ICT-based services and seamless and incident-free information exchange. • Security measures will comply with GEA and industry standards and security will be upheld when parties interact either in a Government-to-Government (G2G), Government-to-Citizen (G2C), or Government-to-Business (G2B) context.	• ICT security architecture must define and improve: • Security processes and structures; • Communication strategies, materials, plans and resources; • Compliance-related information resources and training tools; • Asset control and protection strategies, services and mechanisms; • Monitoring and auditing protocols, processes and techniques; and • Enterprise-wide understanding of the legal ramifications for non-compliance with security-related policies, directives, and statutory/regulatory requirements.
SAP 8: Accountability – Ownership and Sensitivity Determination	• All ICT assets and resources must be accounted for and have an owner, steward and custodian identified, documented and designated. • The value and sensitivity of all ICT assets will be safeguarded in accordance with security directives, policies, standards and guidelines and the applicable statutory frameworks.	• Determine and assign responsibilities, accountabilities, obligation, conditions and rules for designating accountability and authority to parties for securing assets and resources; • Take inventory of all ICT assets and resources and designate person(s) accountable for same; • Design reasonable security measures and ensure they are implemented in order to safeguard the confidentiality, integrity and availability of ICT assets and resources; • Define a threat/risk mitigation process for design and development of enterprise-architecture and ICT systems and infrastructure;
SAP 9: Authorization – Auditable Rule-Based Access	• Access to information and information technology assets and systems must be controlled on the basis of business rules, conditions and obligations. • Access controls for operational systems must be demonstrably auditable	• Enable security, privacy and confidentiality by limiting access to information and ICT assets and resources in accordance with the principles of least privilege and separation of duties.
SAP 10: Authorization	• Access to secure locations will be restricted to those with legitimate	• Ensure that standards are defined, approved, implemented, and

- Restricting Secure Facilities Access	requirements. • Security measures must isolate protected assets and resources from threats, consistent with the value and sensitivity of the information and data holdings. ICT assets must not be vulnerable to security threats or hazards.	enforced for safeguarding access to secure facilities and ICT assets.
SAP 11: Awareness and Training - All Government Employees Responsible	• Awareness of Information and IT security is the responsibility of every government employee and agent. Awareness and training facilitates the consistent execution of ICT security programs and plans across government and an adequate and uniform security posture for the organization.	• Include security and privacy responsibilities in job descriptions and contracts; • Train all employees and agents in security procedures and incident reporting processes; • Include compliance related wording in the conditions of employment as appropriate.
SAP 12: Build security into the system life cycle across all architectural layers	• Identify and categorize information based on the degree of injury that could be expected to result from a compromise of its confidentiality, integrity and availability	• implement a continuous security approach, in alignment with Centre for Cyber Security's, IT Security Risk Management Framework
SAP 13: Ensure secure access to systems and services	• Identify and authenticate individuals, processes or devices to an appropriate level of assurance, based on clearly defined roles, before granting access to information and services; Use of NPKI	•
SAP 14: Protection of interfaces	• implement HTTPS for secure web connections and Domain-based Message Authentication, Reporting and Conformance for enhanced email security • establish secure interconnections between systems through secure APIs or leveraging centrally managed hybrid IT connectivity services	• establish processes to maintain visibility of assets and ensure the prompt application of security-related patches and updates in order to reduce exposure to vulnerabilities, in accordance with laid down Guidelines • enable event logging •

2.5.7 GOVERNANCE ARCHITECTURE

Enterprise Architecture Governance (EAG) is a practice encompassing the fundamental aspects of managing a business.

It involves firm leadership, Change **management** complete knowledge of organizational structure, a confident direction, and the enablement of effective IT processes to promote an enterprise's strategies. The objective of EA Governance is to harmonize the architectural requirements of an

enterprise into an understandable set of policies, processes, procedures, and standards—all of which to ensure an organization's visions and standards are aligned with actual business requirements.

The following outlines the basic principles of corporate governance, :

- Focuses on the rights, roles and equitable treatment of shareholders
- Disclosure and transparency and the responsibilities of the board
- Ensures
  - •Sound strategic guidance of the organization
  - •Effective monitoring of management by the board
  - •Board accountability for the company and to the shareholders
- Board's responsibilities
  - •Reviewing and guiding corporate strategy
  - •Setting and monitoring achievement of management's performance objective

The Characteristics of Governance

- The following characteristics have been adapted from Naidoo (2002) and are positioned here to highlight both the value and necessity for governance as an approach to be adopted within organizations and their dealings with all involved parties:
- **Discipline**
  - •All involved parties will have a commitment to adhere to procedures, processes and authority structures established by the organisation
- **Transparency**
  - •All actions implemented and their decision support will be available for inspection by authorised organisation and provider parties
- **Independence**
  - •All processes, decision-making, and mechanisms used will be established so as to minimize or avoid potential conflicts of interest
- **Accountability**
  - Identifiable groups with the organization, e.g. Governance Boards, who take actions or make decisions are authorised and accountable for their actions
- **Responsibility**
  - Each contracted party is required to act responsibly to the organisation and its stakeholders
- **Fairness**
  - All decisions taken, processes used and their implementation will not be allowed to create unfair advantage to any one particular party.

Project management and governance Principles

PRINCIPLE	RATIONALE	IMPLICATION
GAP 1: Business justification	This means that it is not enough to assess the alignment to organizational objectives only when the project first starts; this should be done all the way through its life. To help, the PRINCE2 processes include activities to check for continued justification periodically	Have continued business justification
GAP 2: Learning from experience	Lessons are sought, recorded and acted upon throughout the life of the project	
GAP 3: Defined roles and responsibilities	Have defined and agreed roles and responsibilities within an organization structure that engages the business, user and supplier stakeholder interests	
GAP 4: Manage by stages	• Projects are planned, monitored and controlled on a stage-by-stage basis. • Breaking a project into a number of management stages provides senior management with control points at major intervals throughout the project. At the end of each stage, the project's status should be assessed, the Business Case and plans reviewed to ensure that the project remains viable, and a decision made as to whether to proceed. In essence it is a stop/ go type of review.	Projects are planned, monitored and controlled on a stage-by-stage basis
GAP 5: Management by exception	• The management by exception principle encompasses: • Delegating authority from one management level to the next by setting tolerances against the target objectives for the respective level of the plan • Setting up controls so that if those tolerances are forecast to be exceeded, they are immediately referred up to the next management layer for a decision on how to proceed • Putting an assurance mechanism in place so that each management layer can be confident that such controls are effective.	Have defined tolerances for each project objective to establish limits of delegated authority
GAP 6: Focus on products	• Focus on the definition and delivery of products, in particular their quality requirements	
GAP 7: tailoring principle	• Be tailored to suit the project's environment size, complexity, importance, capability and risk	
GAP8: Discipline	• All involved parties will have a commitment to adhere to procedures, processes and authority structures established by the organisation	

GAP 9: Transparency	• All actions implemented and their decision support will be available for inspection by authorised organisation and provider parties	
GAP 10:Independence	• All processes, decision-making, and mechanisms used will be established so as to minimize or avoid potential conflicts of interest	
GAP11: Accountability	• Identifiable groups with the organization, e.g Governance Boards, who take actions or make decisions are authorized and accountable for their actions	
GAP12:Responsibility	• Each contracted party is required to act responsibly to the organization and its stakeholders	
GAP13:Fairness	• All decisions taken, processes used and their implementation will not be allowed to create unfair advantage to any one particular party.	

2.5.8 INTEGRATION ARCHITECTURE

Integration Architecture (IA) is a major IT landscape, that simplifies the integration of numerous IT components and enables you to trace data flows between applications. Integration software breaks down silos and enables various software applications to communicate with each other.

In order to connect the different applications with each other, application programming interfaces (APIs) are used, which are specially designed to enable this kind of integration.

Almost all applications are built from separate components and run on different systems. If these applications cannot communicate with each other, they will produce data quality inefficiencies, redundancies, and silos, and decrease satisfaction for the end-user. Therefore, integrations are an important first step to business efficiency and growth.

Integration Architect Principles

PRINCIPLE	RATIONALE	IMPLICATION
IAP 1: **Software and hardware**	• Standards help ensure consistency, thus improving the ability to manage systems and improve user satisfaction, and protect existing IT investments, thus maximizing return on investment and reducing costs. Standards for interoperability additionally help ensure support from multiple vendors for their products, and facilitate supply chain integration. •	• Interoperability standards and industry standards will be followed unless there is a compelling business reason to implement a non-standard solution. • A process for setting standards, reviewing and revising them periodically, and granting exceptions must be established. • The existing IT platforms must be identified and documented. •
IAP 2: **Interoperability**	• Policies defined should reinforce & standards selected should facilitate interoperability • Identify common components (including existing Government policies, standards, application, technology etc. wherever relevant) across the interoperability domain and define policies, standards, and procedures to ensure reusability of artefacts. For e.g. defining data structure, data sets at a national level etc. Choose standards that will enable more choice and reduce the administrative burden. •	• Eliminates patchwork of ICT solutions in different government offices those are unable to ‗talk' or exchange data. Interoperability allows seamless exchange of information, reuse of data models and inter-changeability of data across systems • Brings in the ability to effectively interconnect, collaborate, access and facilitate data • integration in order to communicate between different government organizations (G2G, G2C, and G2B etc.). •
IAP 3: **Confidentiality**	• Guarantee the privacy of information with regard to citizens (e.g. health records), business (e.g. organization statistics) and government (e.g. confidentiality agreements) to help enforce the legally-defined	• This will ensure that the confidential information and data are properly classified and adequately protected. • Privacy cannot be guaranteed by technical standards alone, it has to

PRINCIPLE	RATIONALE	IMPLICATION
	restrictions on access & dissemination of information	have process, inter-organisational agreements, cyber laws etc. in place to enforce it.
IAP 4: Open standards based	• Adherence to open standards should be promoted • Adoption of open standards will facilitate storing of electronic national records and data using open data file formats.	• Adherence to standard that will provide for choice of vendor will promote competitiveness and opportunity to look at cross platforms. • The attributes of open standards such as platform independence, vendor neutrality and ability to use across multiple implementations and the model for establishing open standards are what • will allow for sustainable information exchange, interoperability, flexibility, data preservation & and greater freedom from technology and vendor lock-in
IAP 5: Enterprise Service Bus (ESB) based national service delivery gateway	• The use of ESB promotes loose coupling, support integration of heterogeneous systems, support adherence to open standards • ESB enables rapid development, assembly & deployment of services, ease of • maintenance and improved business visibility	• The Enterprise Service Bus (ESB) should be the public API for the underlying implementation of the enterprise-wide Service Delivery Gateway. As a result it must be available as a resource for any service components in the enterprise. • There should be loose coupling between the service and its underlying layers
IAP 6: Web services for information exchange and granular service.	• By using web services to communicate between the service layers, the enterprise can create the ability to have a rationalized monitoring and security strategy for the Enterprise • Enable compliance with industry standard web service specifications of security, interoperability, reliability etc	• Web Services are to be used between the service layers. Granularity of the services composed in the ESB should not be too fine to promote a huge number of unmanageable services, where change in one, results in a cascaded set of changes in the others. • Governance committee working on the models of consensus, highest common factors and analysis driven frameworks should decide on the request and response payloads of the composed services

2.5.9 HUMAN CAPACITY ARCHITECTURE

Make sure your human capital management plan includes these principles.

PRINCIPLE	RATIONALE
HCAP 1: **Workforce planning**	• HCM makes it possible for businesses to use data to help better predict work patterns and labor needs to make sure that staffing is handled efficiently. • HR managers are no longer forced to guess about possible peak activity times to plan for or having to scramble around the last minute to find temporary workers or add to an existing team. • ability to approach workforce planning more systematically • making all HR professionals breathe a little easier and likely feel more positively about their roles.
HCAP 2: **Performance management**	• tracking employee performance is a crucial component of HR operations • use real data metrics to track employee progress and performance
HCAP 3: Compensation	• Related to performance management, effective HCM allows you to build a strategic compensation approach. This can help boost company morale, as it helps employees know what to expect. If compensation is related to goals, building this strategy out with HCM can lead to more productivity and allow employees to track their progress along with their managers to help better align overall business unit goals.
HCAP 4: Time tracking	• Another important human capital management principle is related to time management, including clocking in and out and submitting paid time off requests. Building time management into your human capital management strategy makes sense because it not only gives HR teams a plethora of data to draw from and use to make employee planning and workforce decisions, but it also can streamline payroll and benefits administration when it's all part of the same system.
HCAP 5: Development and training	• Development is key to employee engagement. When it's built into HCM strategy and highlighted as a human capital management principle, development becomes both more accessible and more relevant. Employee performance reviews, as well as integrated feedback systems, allow for employers to better understand what employees are interested in learning, as well as what the business needs are so that employees can be prepped for career growth and be equipped to carry additional work responsibilities.
HCAP 6: Recruitment and retention	• Recruitment and retention go hand in hand. It's not enough to find and hire great people – it's important that Government find ways to keep them. • Losing employees to turnover is not only time consuming for HR departments to fill the position again, but it's also a loss of productivity for the whole organization. HCM programs have the ability to match employers with better fits for employment earlier in the process, making their hires more likely to succeed. They also enable better employee feedback so that companies can make adjustments to help grow engagement and therefore retention. • HCM systems allow businesses to be both more organized and more flexible. Sanjay Sathe, president, and CEO of RiseSmart told Business News

	Daily that HCM is an important investment to businesses because “Keeping employees happy and engaged in your company now depends very heavily on how you approach the entire employee life cycle.”

2.6 GOVERNMENT INTEROPERABILITY FRAMEWORK

Thisframeworkprovidestechnicalstandardstostreamlineinteroperability.Itprovidesdatastandards to create unique standardized data dictionaries for common data elements across all entities. This will help in removing any confusion regarding the data ownership, type, relationship or structure.

- **It will describe the framework for standardized data exchange between government agencies for cross government services. This covers:**

a) The interoperability charter
b) The interoperability blueprints covering the data standards, technical standards, and metadata standards.

- **Technology standards thatincludes:**

a) SOA architecture principles standards
b) Software development standards

The GIF approach to addressing interoperability is based on a proven approach of defining interfaces and interoperability between enterprises. It includes several architectural views including:

- A logical layered model of data and information that can depict and demonstrate how disparate raw and processed data is transformed into useable information and shared;
- A functional information exchange model that depicts the major types of entities along with the typical function-based information exchanges that are required to happen among the entities in order for them to perform their mandate(s) efficiently and effectively and that are enduring over time; and
- A physical interface model that incorporates the above two models and provides a more tangible description of how the entities need to interface using multiple but related dimensions which include applications, services, devices, networks, and facilities.

The logical, 3-layered model (see Figure ES-1) presumes that existing legacy systems located in the data layer are not necessarily designed for sharing across platforms inside or outside the agency. They are more than likely stove-piped and closely-coupled to proprietary systems and applications. In addition, today's presentation layer tools are increasingly found in applications that reside on wireless smart devices. Thus, interoperability between these legacy data systems and the presentation of that data or

information needed by MCDAs must be addressed by an integration layer where the data is discovered, accessed, transported, processed, aggregated, manipulated, and analyzed into useful information. The resulting information should then be transported/delivered in a standard fashion to the presentation layer so that any MCDA can consume the desired information in the application of their choice and improve their situational awareness.

The interoperability consists of three dimensions that must align: people, process, and technology (see Figure 4).

- The people issues involve consensus across all the stakeholders on the need to share information (and in doing so, address the data interoperability issues).
- The process issues involve having a protocol and governance or other mechanisms to guide the necessary information sharing.
- The technology issues involve infrastructure, software and security considerations that must be addressed.

Data and information sharing success only occurs when the people involved jointly agree to share their data, establish processes to do so, and have a standard, technological approach that enables that agreement.

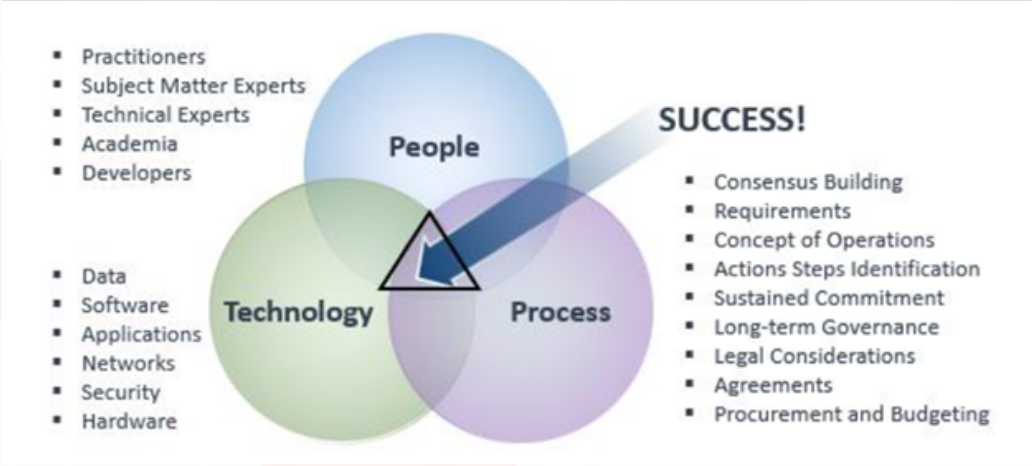


Figure 4: Interoperability Components

Given the scope of the Internet and the rapid increase of devices coming online in the Internet of Things (IoT), discovery and access to such a large amount of information poses significant challenges to avoid overwhelming end users with information beyond what is needed for the decision-making at hand.

When additional information is added for the intended purpose of enhancing situational awareness, consideration must be given to ensuring that the right information is available at the right time to the right individual that is relevant to the current mission.

In addition to enabling the exchange and transport of data and information between content owners (in the data layer) and end users (in the presentation layer), the integration layer needs to provide the analytics critical to ensuring that the information is timely, accurate, relevant, and targeted (see Figure 5).

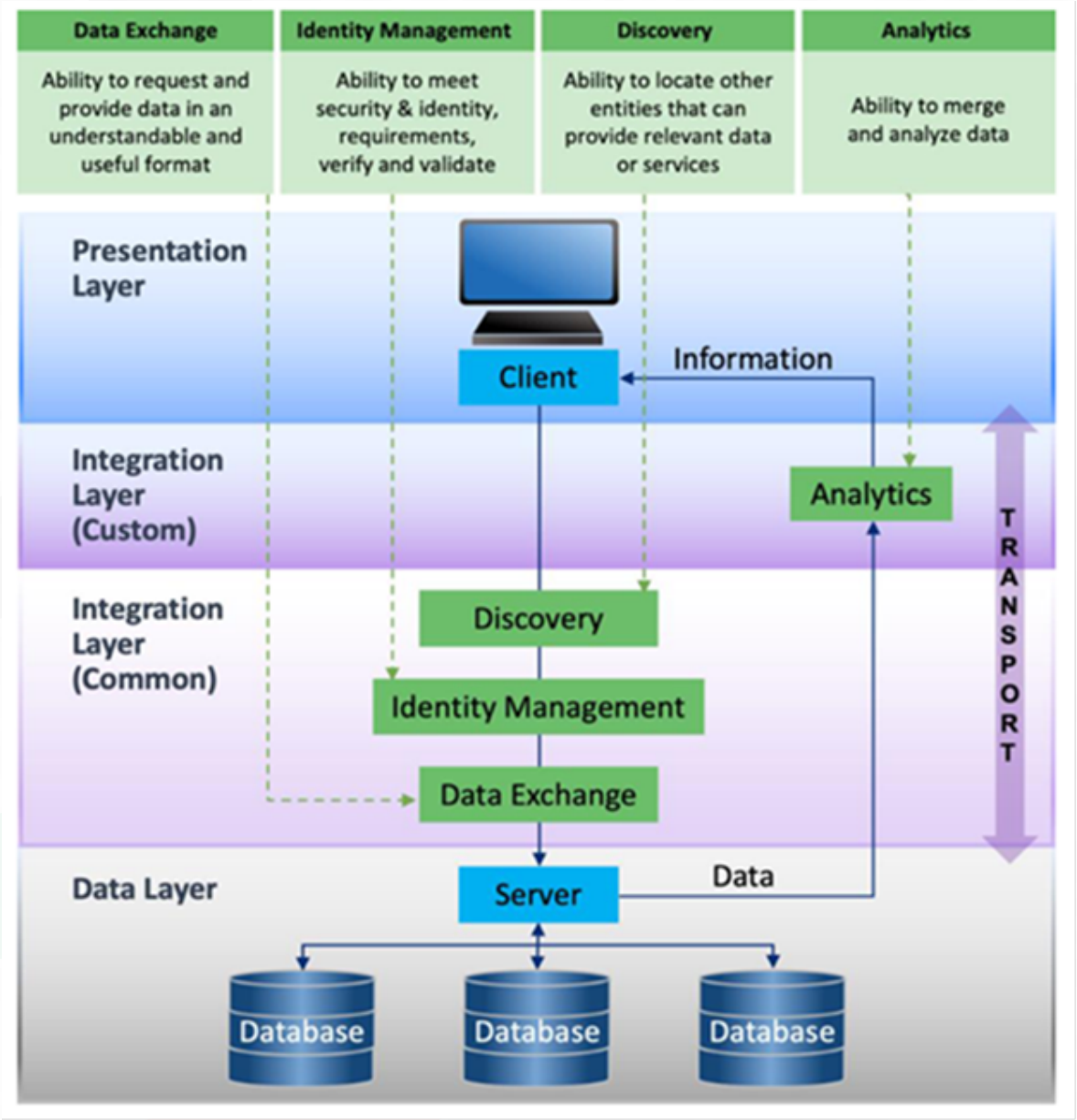


Figure 5: Conceptual Data-Information Model

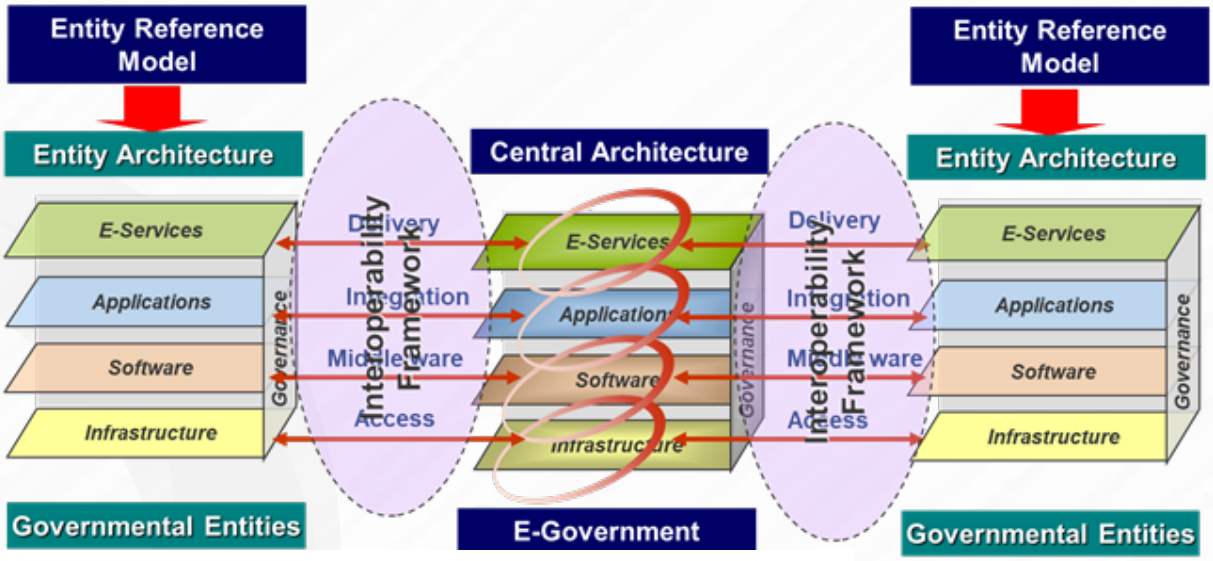
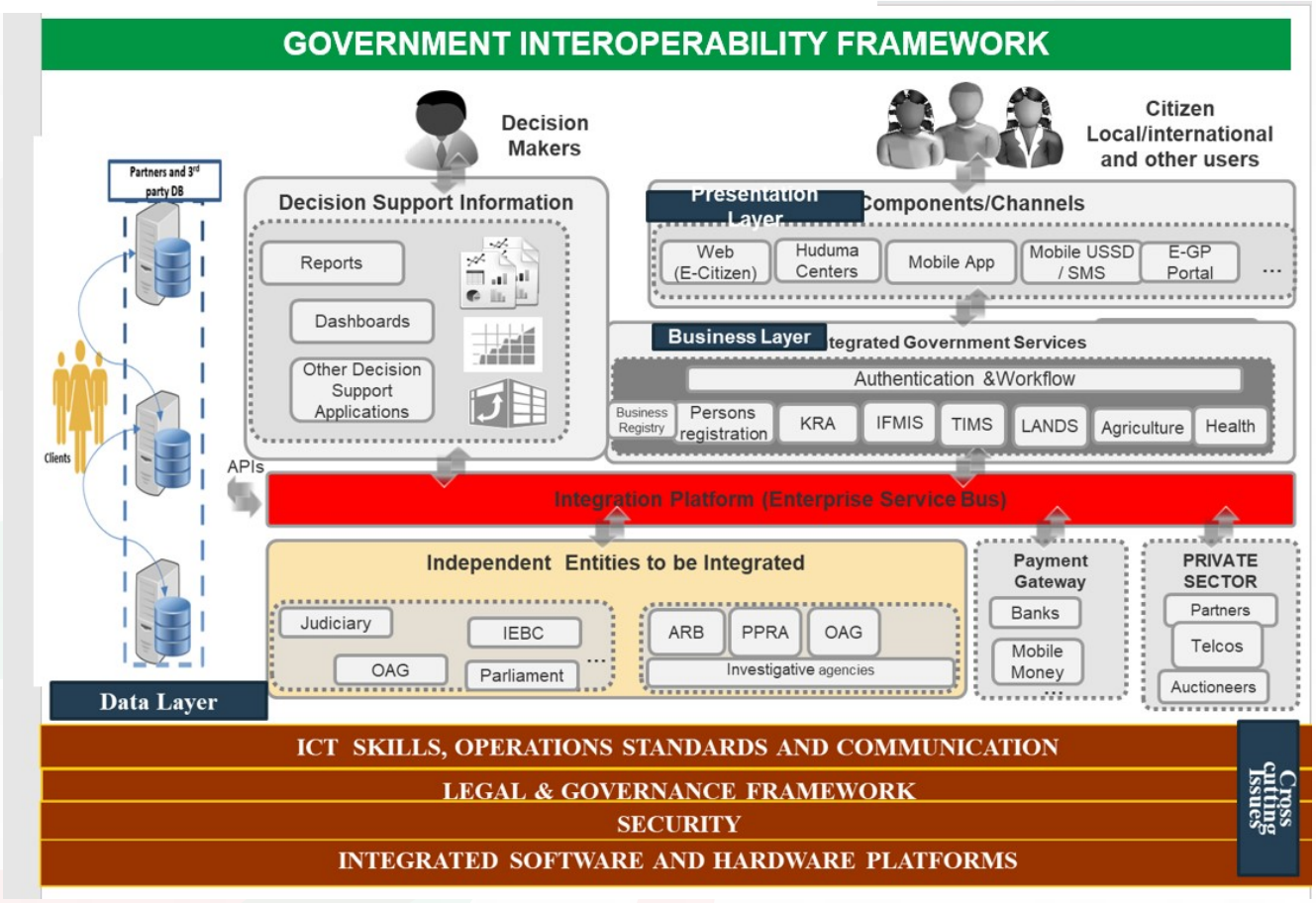
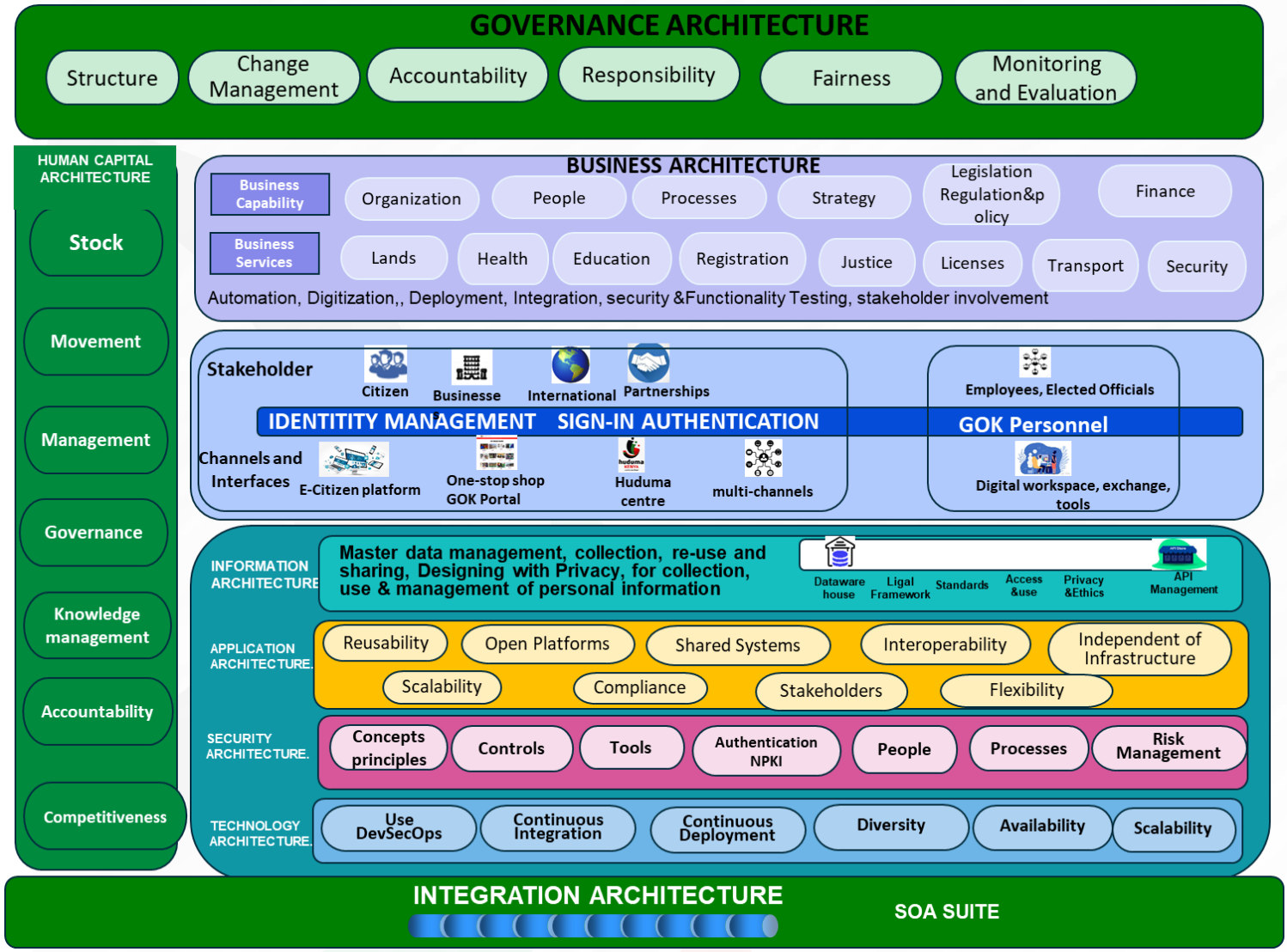


Figure 6: How GEA will work with GIF



DRAFT GEA DIAGRAM



ICT Authority
Telposta Towers, 12th Floor, Kenyatta Ave
P.O. Box 27150 - 00100 Nairobi, Kenya
Telephone: + 254-020-2211960/62
Email: info@ict.go.ke or communications@ict.go.ke
Visit: www.icta.go.ke
Become a fan: www.facebook.com/ICTAuthorityKE
Follow us on twitter: @ICTAuthorityKE


ICT
Authority