

# Rwanda Digital Government Strategy and Governance



**June 2018**

# Contents

<b>1 Executive Summary</b> .....	8
<b>2 Digital Government Strategy</b> .....	11
<b>2.1 Vision and Objectives</b> .....	11
2.1.1 Smart Rwanda Master Plan Context .....	11
2.1.2 The One-Stop-Shop Vision .....	13
2.1.3 Expected Benefits of the Digital Government Platform .....	15
2.1.3.1 Constituency (Citizen, Organization, Intermediary) .....	15
2.1.3.2 Government .....	16
2.1.3.3 Application Developers and Independent Software Vendors .....	16
<b>2.2 Digital Government Platform Architecture</b> .....	17
2.2.1 Architecture Overview .....	17
2.2.2 Integrated Digital Channels .....	18
2.2.2.1 Overview .....	18
2.2.2.2 Government Web Portal .....	19
2.2.2.3 Mobile Services .....	20
2.2.2.4 Social Media Services .....	22
2.2.2.5 E-forms Engine .....	22
2.2.2.6 Service Catalog .....	24
2.2.2.7 Kiosks .....	25
2.2.2.8 Notification Engine .....	25
2.2.2.9 Citizen Experience Management .....	27
2.2.3 Digital Government Enabling Services .....	28
2.2.3.1 Overview .....	28
2.2.3.2 Payment Gateway .....	28
2.2.3.3 Data Services .....	29
2.2.3.4 Government Employee Portal .....	31
2.2.3.5 Government Blockchain .....	31
2.2.3.6 Internet-of-Things Services .....	32
2.2.4 Digital Identity and Security .....	33
2.2.4.1 Overview .....	33

2.2.4.2 Digital Identity.....	34
2.2.4.3 Digital Signature.....	37
2.2.5 Government Service Bus .....	38
2.2.5.1 Overview.....	38
2.2.5.2 Messaging and Routing .....	39
2.2.5.3 Application Integration.....	40
2.2.5.4 Business Process Orchestration.....	41
2.2.6 Secure Infrastructure .....	41
2.2.6.1 Overview.....	41
2.2.6.2 Public / National Cloud.....	42
2.2.6.3 Cyber Security .....	42
2.2.6.4 Communication & Collaboration Services.....	44
<b>2.3 Ownership and Governance .....</b>	<b>44</b>
<b>2.4 Implementation Roadmap.....</b>	<b>47</b>
<b>3 Enterprise Architecture Governance .....</b>	<b>49</b>
<b>3.1 Introduction.....</b>	<b>49</b>
<b>3.2 Background.....</b>	<b>50</b>
<b>3.3 EA Governance Implementation .....</b>	<b>51</b>
3.3.1 GoR Digitization Advisory Committee.....	55
3.3.2 RISA EA Team .....	56
3.3.3 IT Sector Working Group .....	60
3.3.4 IT Committee .....	61
3.3.5 Project Steering Committee (per project).....	63
<b>3.4 Enterprise Architecture Documentation .....</b>	<b>64</b>

## List of Figures

Figure 5 Smart Rwanda Objectives and Outcome .....	12
Figure 6 Rwanda One Stop Shop .....	14
Figure 7 Digital Government Platform in the One-Stop-Shop Context .....	14
Figure 8 Mapping of components to SRMP outcome.....	15
Figure 9 Digital Government Platform Top-Level Components .....	17
Figure 10 Digital Government Architecture .....	18
Figure 11 Integrated Digital Channels .....	18
Figure 12 Interaction of portal with other platform components.....	20
Figure 13 Mobile Services Interaction.....	21
Figure 14 e-Forms Engine .....	23
Figure 15 Notification Services .....	26
Figure 16 Digital Government Enabling Services .....	28
Figure 17 Payment Gateway .....	29
Figure 18 Identity Concepts .....	34
Figure 19 Single Sign-On .....	37
Figure 20 Government Service Bus Components.....	38
Figure 21 Service Bus Integration Patterns .....	40
Figure 22 Secure Infrastructure Components .....	41
Figure 23 RDGP Roadmap .....	48
Figure 1: The Rwanda Government-wide Enterprise Architecture Framework.....	50
Figure 3: EAG Roles and responsibilities .....	54

## List of Tables

Table 2: Roles and Responsibilities for RISA-EA Team .....	59
Table 3: Roles and Responsibilities for IT Sector Working Group .....	61
Table 4: Roles and Responsibilities for IT Committee.....	62

## Acronyms

Acronym	Full Name
BIDAT	Business, Information, Data, Application and Technology Architecture
BU	Business Unit
CIO	Chief Information Officer
DGP	Digital Government Platform
EA	Enterprise Architecture
EAF	Enterprise Architecture Framework
EAG	Enterprise Architecture Governance
GRC	Governance, Risk and Compliance
ICT	Information Communication Technology
IRC	Information Resource Catalogue
IT	Information Technology
ITIL	Information Technology Infrastructure Library
KPI	Key Performance Indicator
NIDA	National Identification Agency
OLA	Operational Level Agreement
PaaS	Platform as a Service
PMO	Project Management Office
RACI	Responsible, Accountable, Consulted, Informed
RDB	Rwanda Development Board
SDLC	System Development Lifecycle
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SRMP	Smart Rwanda Master Plan
TCP	Transmission Control Protocol
TOGAF	The Open Group Architecture Framework

## Terminology

Term	Description
Application Architecture	The architecture models of an application or system that shows interrelationship with other applications within a specified ecosystem. The applications are used in automating some processes within a given environment.
Baseline Architecture	Development of enterprise architecture models that represent the current state of the business operations from the perspective of the architecture domains and their relationship with each other (i.e. Business, Application Data and Technology Architecture Domains).
Business Actor	A user of the system and consumer of the service
Business Architecture	The business direction model which includes the strategy, organisation structure, functions /services, key business processes and information requirements, as well as the relationships between these concepts.
Baseline model	The current or As-Is state of the architecture models in a given environment
Data Architecture	The model of the structure for data sources that applications / systems within an environment uses
Enterprise Architecture	The alignment of the core domains that make up a complete organization. This includes the alignment of the Business, Data, application and technology architectures. This depicts the association between the architecture domains and how they work together to facilitate the achievement of the goals set within the business architecture domain.
Enterprise Architecture Governance	The structure and rules that governs the implementation of enterprise architecture. This sets the standards and policies that enterprise architecture abides by.

# 1 Executive Summary

In October 2015, The Government of Rwanda issued the “*SMART Rwanda Master Plan*” (SRMP), which provides the elements needed to achieve the vision of “a Knowledge Based Society”. The SRMP identified a set of core objectives, including the following:

- Objective #8: Build a secured, shared robust and resilient infrastructure to underpin service delivery and support national ICT initiatives
- Objective #9: Enhance the National ICT Governance Structure for effectiveness implementation of ICT programs
- Objective #10: Transform digital Government through E-Government and effective service delivery

The SRMP also identified three main enablers for Rwanda’s digital transformation which include (1) Effective ICT Governance and Management, (2) ICT Capacity and Capability, and (3) Secured and Shared Infrastructure.

The transformation of digital Government implies the use of technology to automate various processes. This, therefore, requires a setup of backend systems within all entities that need to be integrated for efficient service delivery.

Central to the objectives above is the seamless alignment of IT systems and infrastructure in public entities. To this end, the focus for RISA is the provision of Digital Government Platform (DGP) that will connect all IT systems across public sector entities.

It is, however, acknowledged that to date, the level of technology deployment across public entities in Rwanda is not uniform. For the integration to be effective, there is a need not only to review the current backend systems and to deploy systems within the entities that do not have adequate systems, but also to ensure that standards are well defined to ensure that the deployed solutions meet the set criteria.

It is further acknowledged that all public entities use citizens data in delivering services. As such, the backend systems at the National Identification Agency (NIDA) – where citizens data

from birth to death is captured and maintained – is central to the development of the Digital Government Platform. This is because this is singularly a single source of the truth about all citizens' status.

The automation of processes and integration of systems at NIDA is therefore key for the success of the Digital Government Platform.

This functionality is well served with the implementation of enterprise architecture governance across government of Rwanda. Through this initiative, common standards will be implemented within the public sector through the enforcement of principles and methodology driven by the guidelines set out in the *Government of Rwanda Enterprise Architecture Framework v2.1* and *Blueprint Development Guidelines for Government of Rwanda V1.1* documents.

While the abovementioned documents define both the Enterprise Architecture Framework and Guidelines for developing blueprints, it is necessary to further define the governance structure around enterprise architecture implementation across Rwanda. It was, therefore, necessary for RISA to define governance structure around the setting up of backend systems for public entities driven by enterprise architecture principles to drive seamless alignment. Through this initiative, all public entities are to define their respective architecture blueprints that would outline the IT and business landscape.

The RISA driven initiative seeks to define and enforce common standards across all entities to allow for interoperability and agile systems deployment.

To ensure cohesive architecture models, RISA has defined a framework for Enterprise Architecture as well as the governance that drives its implementation (refer to *Government of Rwanda Enterprise Architecture Framework v2.1*). In addition, a guideline for developing the blueprint has also been defined for all entities (*Blueprint Development Guidelines for Government of Rwanda V1.1*).

The output of the blueprint development initiative will present a clearer view of each entities' readiness to integrate with other public-sector entities through the Digital Government

Platform. In this regard, the blueprints will outline the availability and adequacy of the backend systems for the integration.

The following sections outline two key components that will drive the integration of public entities to meet the abovementioned objectives of the *Smart Rwanda Master Plan*. These components are:

1. The Enterprise Architecture Governance that will drive the development of the blueprints as well as the deployment of adequate backend systems
2. The approach for Digital Government Platform development

## 2 Digital Government Strategy

### 2.1 Vision and Objectives

#### 2.1.1 Smart Rwanda Master Plan Context

In October 2015, The Government of Rwanda issued the “SMART Rwanda Master Plan” (SRMP), which provides the elements needed to achieve the vision of “a Knowledge Based Society”. SRMP identified a set of core objectives, including the following:

- Objective #8: Build a secured, shared robust and resilient infrastructure to underpin service delivery and support national ICT initiatives
- Objective #9: Enhance the National ICT Governance Structure for effectiveness
- implementation of ICT programs
- Objective #10: Transform digital Government through E-Government and effective service delivery

SRMP also identified three main enablers for Rwanda’s digital transformation: Effective ICT Governance and Management, ICT Capacity and Capability, and Secured and Shared Infrastructure.

The following diagram summarizes the expected outcomes from the SRMP in relation the with objectives listed above:



Figure 1 Smart Rwanda Objectives and Outcome

The objectives and outcomes above are to be executed under the SMRP identified policy principles:

- Access:
  - Cloud First
  - Mobile by Default
  - Infrastructure Sharing
  - Bring Your Own Device
  - ICT Affordability
- Security by Design
- Services Data and Innovation
  - Open by Default
  - Efficient Business Processes
  - Privacy Data Protection
  - Innovation and PPP
- ICT Skills and Capacity Building
- Governance

SRMP recognizes the fact that building digital government services requires the establishment of a Government ICT Enterprise Architecture and e-Government framework, that provides shared services needed for service delivery. However, this set of shared services, while critical for digital service delivery, has not yet been fully identified or documented. The objective of this document, and the corresponding Rwanda Digital Government Platform, is to define the framework for these services.

### 2.1.2 The One-Stop-Shop Vision

The Government of Rwanda is actively engaged in a program of evolution into a Smart, Digital Government. The objective is to deliver and manage services electronically and efficiently – both internally and to businesses and citizens.

Better, broader, and more efficient access to the wide diversity of public services is a key driver for these changes. Equally key is the development of more efficient and streamlined internal business processes. Rwanda would like to capitalize on the development of digital channels—such as mobile services and interactive citizen services – to encourage citizens to participate more actively with government. Businesses too can see the benefits: reducing the complexity and bureaucracy of their interactions with Government through the smart application of technology.

The vision is best summarized through the concept of a one-stop-shop, where all government services are presented in an integrated, seamless way that simplifies access to citizens and businesses.



Figure 2 Rwanda One Stop Shop

To enable the One-Stop-Shop concept, a set of critical Information Technology services need to be made available to the entire ecosystem. We refer to these services as the **Digital Government Platform**. On top of this platform, and within the One-Stop-Shop concept, vertical solutions can be built up, including enabling Digital Health, Law, and others.



Figure 3 Digital Government Platform in the One-Stop-Shop Context

**IMPORTANT:** The Digital Government Platform depends on having automation within the government entities. It does not provide the automation of government entity processes but helps in integrating existing automated processes and using them to provide digital services to citizens.

The Digital Government Platform will enable the adherence to the policy principles highlighted in the SMRP as well as the facilitation of the objectives outcomes.

The following diagram shows the mapping between the Digital Government Platform top-level components and the relevant SMRP outcomes:



Figure 4 Mapping of components to SRMP outcome

### 2.1.3 Expected Benefits of the Digital Government Platform

Providing a common infrastructure shared by multiple Digital Government services can produce benefits in several categories:

#### 2.1.3.1 Constituency (Citizen, Organization, Intermediary)

The benefits for the "clients" of Digital Government services include:

- Reductions in cost and time to enable online transactions in a consistent, reliable fashion
- Hidden complexity and multiplicity of back-end systems interactions at the point of delivery, presented as a single online interaction
- Simplified processes for interacting with government across silos, including the potential for "joined-up" services
- Faster access to services

- Single online identity to access multiple government services across multiple channels
- An always-available 24x7 service

### 2.1.3.2 Government

For the Government of Rwanda, the common Digital Government Platform:

- Accelerates the delivery of e-Government services by providing reusable common components needed for online service delivery
- Shares common costs across the Government rather than repeating expenditure multiple times by duplication of identical pieces of core infrastructure for each online service
- Enables innovative, joined-up services
- Provides a common user identity management model for all Government services
- Provides a single, consistent access path for Government services
- Scales to meet the growing demand
- Drives the take-up of Digital Government services

### 2.1.3.3 Application Developers and Independent Software Vendors

For application developers and software vendors building Digital Government solutions, the Digital Government Platform:

- Provides consistent interoperability – consistent standard interfaces expose the functionality, regardless of the services and departments concerned so applications can be built in a consistent way
- Is platform and technology independent
- Complies with open standards

## 2.2 Digital Government Platform Architecture

This section provides an overview of the proposed architecture for the Digital Government Platform.

### 2.2.1 Architecture Overview

The Digital Government Platform is not one single solution, but rather a set of technology components, architecture artefacts, and guidelines, that work together to facilitate all aspects related to building digital government services.

The top-level components are listed below:

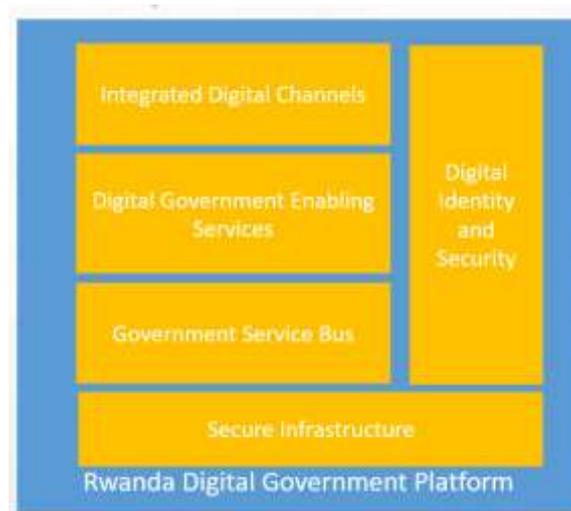


Figure 5 Digital Government Platform Top-Level Components

- **Integrated Digital Channels:** Allows citizens to have a seamless interaction with the government, leveraging latest devices, social media, and other channels to provide unified citizen experiences.
- **Digital Government Enabling Services:** Provide services such as payment, notification, and data management, to facilitate and accelerate the creation of digital services.
- **Digital Identity and Security:** provides technology-based solutions for authenticating citizens and ensuring the security of transactions.

- **Government Service Bus:** Accelerates the creation of new e-services through surfacing government data and processes, simplifying the creation of services that span multiple government entities.
- **Secure Infrastructure:** Provides the backbone of systems, hardware, networking and security that ensures a reliable, secure, and low cost operation of government services.

These components are further broken down in the following diagram:

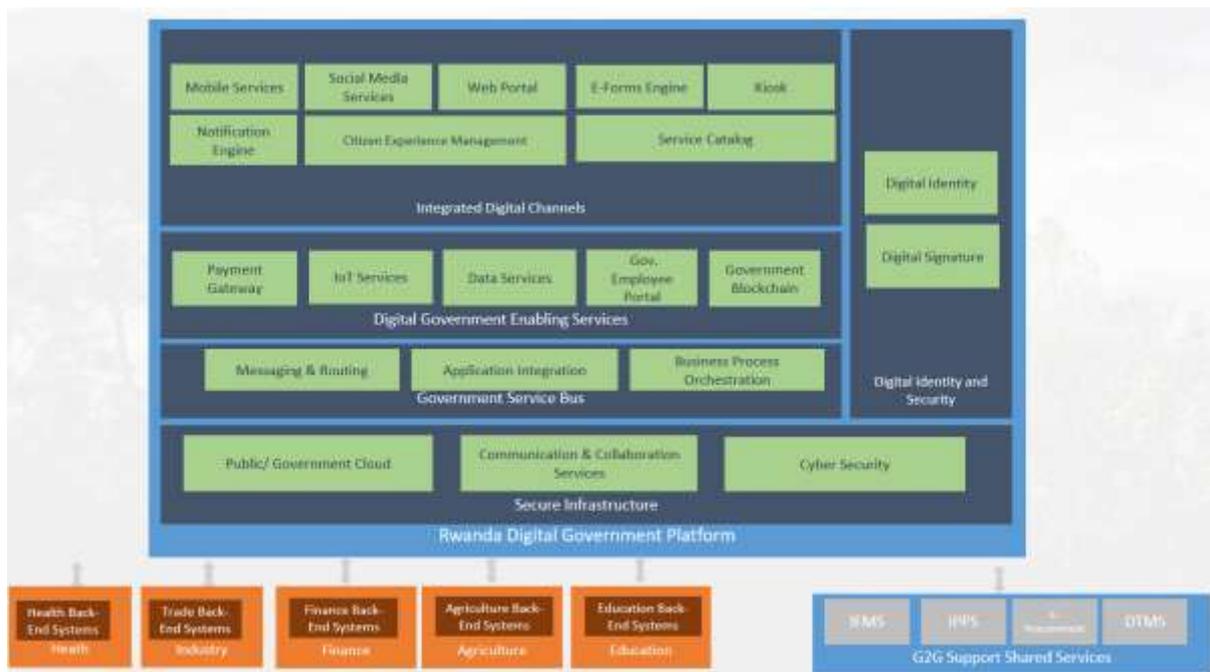


Figure 6 Digital Government Architecture

These components are described below.

## 2.2.2 Integrated Digital Channels

### 2.2.2.1 Overview

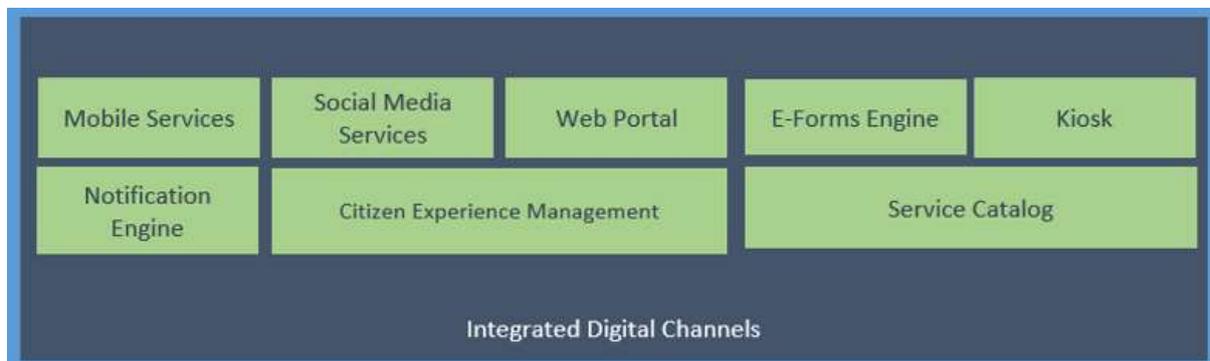


Figure 7 Integrated Digital Channels

Integrated Digital Channels provide the possibility for seamless interaction of citizens with the government using multiple channels. Government services will be accessible from any location, through multiple types of devices, using a consistent user experience that is also context-aware.

### 2.2.2.2 Government Web Portal

The Single Point of Access to Government Services on the web is the Government Web Portal. "Irembo" is the current implementation of the Government Web Portal.

Using the portal, citizens and businesses can:

1. Get information on government and its services
2. Browse the catalog of services and get redirected to the proper location for accessing services (refer to the catalog services section)
3. Communicate directly with government entities
4. Transact with the government services directly using e-services

The web portal would provide some additional features that help in ensuring the best user experience for users:

1. Integrate with Identity management to allow users to login with chosen credentials and leverage single sign-on to access other services
2. Transaction History: Provide users with a history of the transactions that they have conducted with the government
3. Search: ability to search information available on the government portal as well as all government web sites from a central place
4. Chatting / ChatBots: Provide ability to do online chatting with government service representatives, potentially leveraging automated Artificial Intelligence enabled chat bots in appropriate scenarios.

The following diagrams show the interaction of the portal with other components:

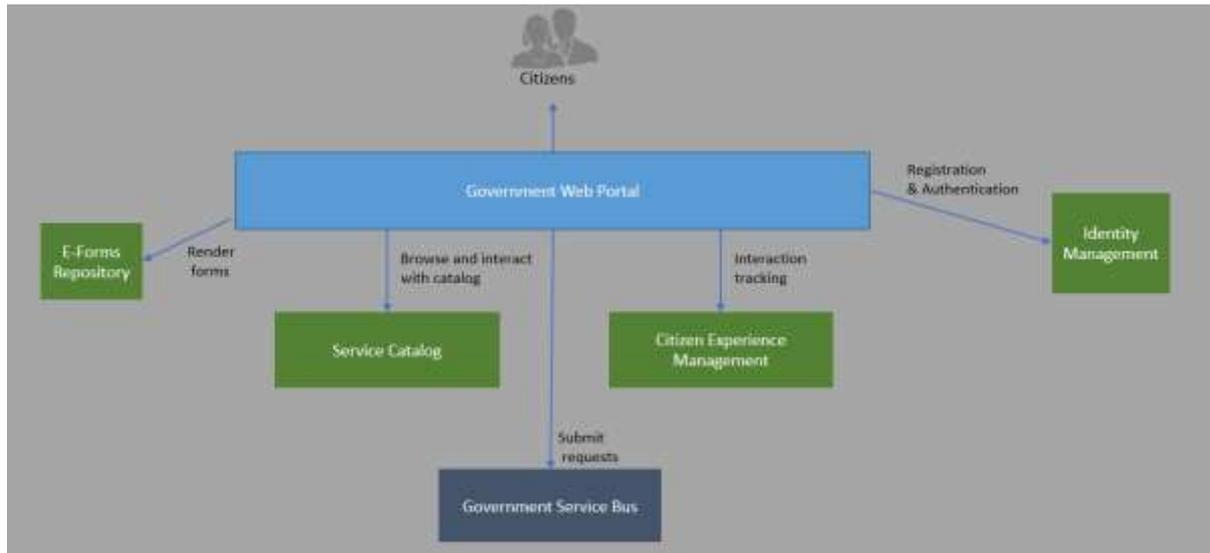


Figure 8 Interaction of portal with other platform components

While Irembo already provides a good entry point to a number of government services, some enhancements are recommended to be put in the roadmap for it to act as a gateway:

- Integration with other government web sites and services, including catalogs, yellow pages, search and sign-sign-on capability across all government web sites and other digital channels
- Omni-Channel Access: The ability to start a transaction on one channel and continue it on another, such as beginning a birth certificate request on a phone app then completing it and submitting it through Irembo.
- Control to Government Entities over web form creation and maintenance, enabling the government entity owning the business to be able to manage the updates to the data and validation it requires from users. Refer to the e-Forms Engine section for details.

### 2.2.2.3 Mobile Services

More than 90% of Rwandans<sup>1</sup> access the Internet on their mobile devices. Therefore, it is natural that the interaction with the government should use mobile as the priority channel. Some Government Services are currently enabled on mobile using USSD. Irembo provides a

<sup>1</sup> Smart Rwanda 2020 Master Plan

responsive-design interface for rendering forms on small screen devices, which helps significantly in making the e-services available on smart phones.

In addition to USSD apps and responsive web design, it is beneficial to create smart phone apps that provide a fluid and responsive mobile service to citizen. Creating one mobile app for government services would be desirable but is not feasible in practice, as it would provide significant challenges in terms of providing useful functionality that is easily accessible to citizens. Therefore, it is expected that multiple mobile apps would be created by the respective owners of services based on the needs.

In that context, centralized government mobile services would have the following objectives:

- Enable standardized mobile-based accessed to services. Standardization would cover security, communication, branding and look-and-feel, among others.
- Ensure integration with other Digital Government Platform components, most notably, Identity Management and Single Sign-On on mobile devices, so that citizens can access mobile services using their assigned credentials.
- Provide a central place (portal) for discovering and accessing mobile apps for government. The portal would be accessible through Irembo and as a mobile app used for launching other government apps.

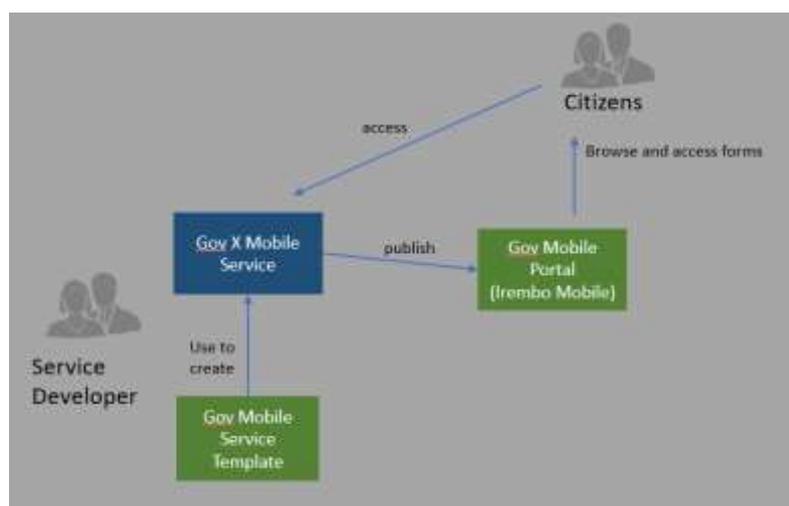


Figure 9 Mobile Services Interaction

- Provide guidance, standards, and templates to government entities and third party developers for building cross-platform mobile services. These would help ensure

consistency even if the development of mobile app is created by multiple developers or vendors, as it is expected.

#### 2.2.2.4 Social Media Services

Social media (Facebook, Twitter, etc.) is increasingly playing a critical role in the digital lives of citizens. They provide a direct, live, and transparent way of reaching out to citizens and encouraging inclusion. The Government of Rwanda needs to leverage this channel to harness the power of social networks to help build relationships and communities with citizens. This will be done in a proactive way with the following objectives:

- **Communicate frequently and announce on events and news:** Social networks provide an opportunity to raise awareness about what's happening with citizens
- **Openly listen and respond to citizen queries and feedback :** Social networks contain a trove of information about citizens and government services. Addressing comments quickly can turn a good or bad citizen experience into long-term satisfaction. It also helps identify the things citizens care about. Social communities can also be a great source of highly detailed feedback and discussion from the people who use government services the most.
- **Analyze general sentiment and context-specific sentiment:** Analyzing social streams allows the government to gather information, intelligence, and insights – leveraging connections with citizens and other organizations at local, national, and international levels.

Within the Digital Government Platform, Social Media Services provide the policies, procedures, and tools for a government agency to achieve the above objectives. It also integrates social media with other components, including the web portal, mobile services, and citizen experience management.

#### 2.2.2.5 E-forms Engine

Automating government paper forms is a common requirement in accelerating the digitization of government business. At the moment, the Irembo team creates online forms for e-services, which requires an extensive programming effort, with the government entities having no

control over form fields and validations. It is desirable to have a way to accelerate the form creation and make it easy to publish and update government forms.

The e-Forms Engine complements the government web portal by providing a system for hosting e-Forms templates, a designer for templates creation and functionality that allows rendering e-Forms in web browsers. The features from the e-Forms engine would be:

- Simplify the creation of online forms following a standardized visual design
- Simplify the submission of forms to web services for processing
- Allow rendering of forms on multiple devices
- Provide a centralized repository of forms

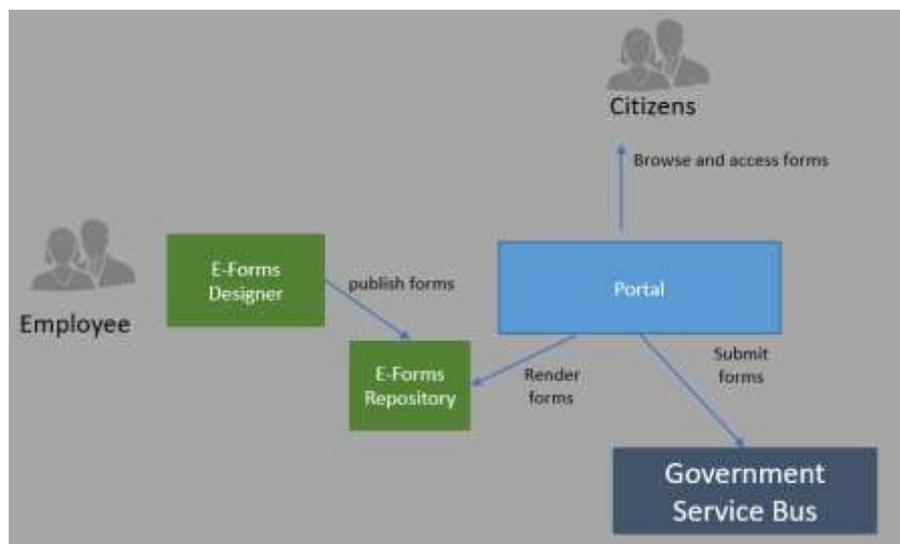


Figure 10 e-Forms Engine

Two main components are there:

- The e-forms Designer: supports easy creation of e-Form
  - It should be possible to create a form which will look like the paper version of the form
  - No deep technical knowledge and programming required
  - Should support multiple languages
  - Allow entry validation
  - Allow complex logic and calculation
  - Ability to call web services during e-Form filling

- The e-forms Repository: provides central repository of published e-Forms templates. Through web services it allows communication with e-Forms Designer and with the portal that is responsible for hosting e-Form Renderer and which are responsible for showing list of templates.

### 2.2.2.6 Service Catalog

Hosted within the government web portal and mobile services, the Service Catalog provides a central place for citizens to learn about and navigate government services. It facilitates three main ways to browse services:

- **E-Services catalog:** the catalog lists all services available to citizens, whether on the central government site or other government sites or channels. For each e-service, the catalog lists the service name, target users, benefits, fees, access mechanisms, government owner. The catalog also allows users to browse the services through different hierarchical categories.
- **Government Yellow Pages:** hosted on the government web site, the government yellow pages allow citizens to navigate the structure of the government, including all departments and local offices, showing information about their web presence, contact information (phone, e-mail, etc.), and the services provided by these government entities.
- **Life Events:** citizens and organizations interact with the government and access different services based on the lifecycle. After birth, citizens require birth registration, birth certificates, vaccination, and others. As he/she progresses in age, he/she will require education services, and others. Similarly, organizations pass through multiple stages throughout their lifecycle. The Life Events feature allows citizens and organizations to access services organized per their lifecycle stages.

Moreover, by integrating with the Citizen Experience Management component, this module allows the government to be able to propose services to citizens proactively based on their own stage in the lifecycle, through integrating with notification services.

### 2.2.2.7 Kiosks

For citizens who are not able to access Internet-connected devices whether permanently or temporarily, the self-service Kiosk channel provides the opportunity for digital engagement with the government. Typically positioned in crowded public places, commonly accessed government offices, or in remote areas, the kiosks would be equipped with:

- Secure computer
- Touch-enabled screen
- A Web Camera
- Bio-metric authentication device
- Printer for receipts and others
- Connects the services with other channels
- Leverages touch screens for seamless experience

Kiosks should enable the customer experience to flow in an omni-channel way with the other channels such as web and mobile, in a way that allows starting one transaction in one of these channels and continuing on the kiosk, such as to print out a receipt.

### 2.2.2.8 Notification Engine

While delivering with services to citizens, the government sends multiple kinds of notifications in the lifecycle of service delivery, including e-mails, mobile text Messages, standard mail notifications, and others. It is important to standardize as well as consolidate and streamline messages sent to citizens, to ensure that messages are sent to citizens are consistent and result in actionable outcome.

Currently the Irembo site delivers SMS and E-mail notification to users of its services, while other government entities have their own separate agreements with service providers to deliver SMS Messages.

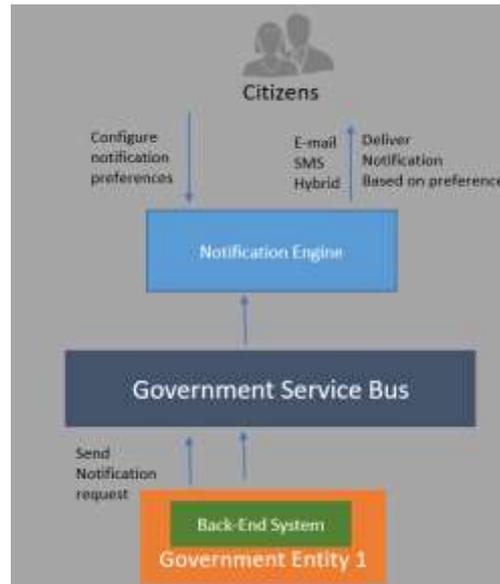


Figure 11 Notification Services

The Notification Engine is a centralized component for streamlining citizen communication in relation with government services by:

- Standardizing the format of messages
- Customizing the delivery mechanism
- Personalization of notification delivery
- Centralization of messaging – such as citizens view all notifications in a single place

The Notification Engine will work as follows:

- Citizens can configure, globally, their preferred notification mechanism (whether by SMS messages, e-mail, or others) and the corresponding contact addresses. They can also customize the type of notification based on service type and urgency. If the citizen changes his address or phone number or any contact mechanism, they only change it from one place (through the government portal), and the new address is used for further notification.
- When a government service wants to deliver a message to a citizen, it sends the message to the Notification Engine, specifying the target citizen, the Notification Engine will then deliver the message that is appropriate to the citizen’s preferences.

- In the back-end, the entity responsible for Notification Engine will ensure the right contractual and technical mechanisms are put in place with vendors (such as SMS vendors) to leverage economies of scale for message transmission.
- The notification engine will also provide the feature of a Hybrid Inbox. This is an advanced notification mechanism that provides:
  - Centralized inbox containing all notifications for a citizen, accessed through web, mobile or other channels.
  - Digital signing of notifications to ensure authenticity and non-repudiation, through integration with the Digital Signature (PKI) infrastructure.
  - Certified proof of delivery, which can be leveraged for legally binding notifications.

### 2.2.2.9 Citizen Experience Management

As citizens get leverage multiple government services, on various channel, it is important to ensure that all these interactions are managed in a coordinated way. The component 'Citizen Experience Management' acts as the unifying place for managing all citizen interactions and providing a 360 degree view of the citizen. Borrowing from the concepts of "Customer Relationship Management", effectively treating citizens as customers, this component delivers the following:

- Records all citizen interactions across all channels, whether they are web or mobile service requests, social media comments, or calls to the call center, and enables them to be viewed per citizen.
- It provides an update to date record on the status of all transactions that can be viewed by the citizen directly on the available channels
- Provides consolidate information, a single version of the truth, about citizens to government employees, enabling them to provide exceptional service
- Connect with data services, feeding information about citizen interactions and getting insights around best actions for servicing the citizen.

## 2.2.3 Digital Government Enabling Services

### 2.2.3.1 Overview

This component provides services to facilitate and accelerate the creation of government digital services. They are used by the digital channels as well as by back-end systems to complete the back-end processing.



Figure 12 Digital Government Enabling Services

### 2.2.3.2 Payment Gateway

Most government transactions require some form of payment. In the digital government, payment for government services is expected to be made as simple and friction-free as possible. While the current government web site, Irembo, already has support for credit card payment through Visa and MasterCard, payment options need to be expanded further and made usable across channels.

The government payment gateway will have the following objectives:

- Payment Gateway should support pluggable payment providers, allowing for flexible payment options that will change over time. These options would include:
  - Credit/debit/prepaid card payment
  - Mobile Payment
  - Payment with NFC
  - Payment through bank transfer
  - Payment through bank direct debit
  - Payment through third party payment providers that operate in Rwanda (such as PayPal)
- That payment gateway should publish standardized API-based integration to allow easy onboarding of government service providers that require using online payment, as well as the integration of new payment providers

- In case the Government Gateway forms global agreements with payment providers on behalf of the government, the Payment Gateway will provide settlement, dispute resolution and reconciliation services on behalf of the respective government entities that utilize the payment services.
- That Payment Gateway would leverage the government PKI to ensure integrity and non-repudiation of transactions

The following diagram describes how the Payment Gateway is used in delivery of an online service:

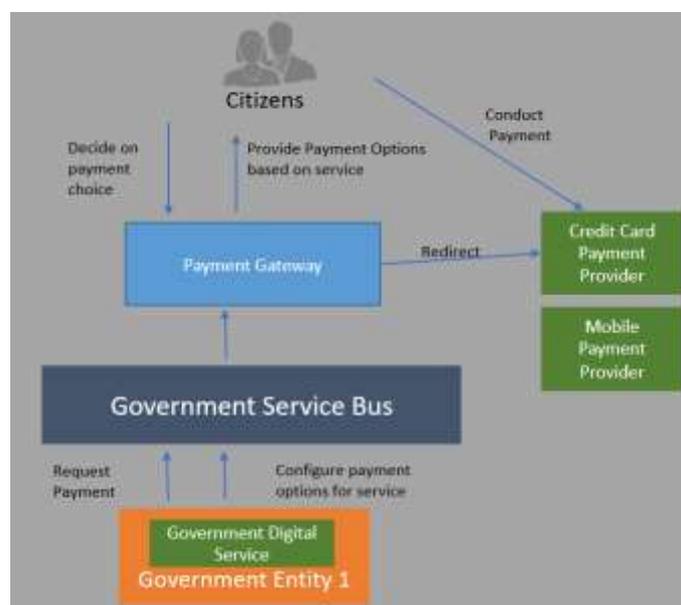


Figure 13 Payment Gateway

### 2.2.3.3 Data Services

It is important for the government to make sense of available data in all aspects of delivery of information and services — from reducing operational costs to enhancing mission efficiency and delivering new and innovative citizen services — all the while preventing fraud/waste and abuses.

Data Services enables the government to leverage the vast amount of data it owns and collects to deliver the highest quality citizen services, leveraging data for insights and decisions. This has 3 components: Master Data Services, Big Data and Analytics, and Open Data Services, described below.

- **Master Data Services:** Master Data is data that represents core business entities that enables consistent use across systems, of the most accurate, timely, and relevant version of truth. Examples are data about citizens, businesses, land registrations, etc. Related to Master Data are Reference Data, which are standardized terms, code values and other unique identifiers, business definitions for each value, business relationships within and across domain value lists. Examples are region codes, city codes, list of government hospitals, schools, etc. Master and Reference Data is used throughout government services, and the objectives of this component include:
  - Standardize codes used for all reference data
  - Ensure consolidation of duplicate records within and across data sources to build and maintain global IDs to enable information integration.
  - Reconciliation across data sources and providing the —golden record or the best version of the truth.
  - Provision of access to the golden data across government applications, either through direct reads (web services through the Government Service Bus), or by replication feeds to databases
- **Big Data and Analytics:** this component provides the tools and processes for storing, processing, and analyzing large amount of structured and un-structured data within the government. This allows monitoring and spotting trends that can help control costs, reduce waste, drive new efficiencies, and streamline overall operations. The objectives for Big Data would be:
  - Enable faster decision speed through greater access to insights
  - Manage government performance by linking collected data to government goals and Key Performance Indicators
  - Improve resource management by identifying areas of inefficiencies
  - Apply predictive analytics to uncover “unintended consequences”, unexpected patterns and associations and evaluate trends.
- **Open Data:** Open Data for the government is a set of policies, process and tools that promotes transparency, accountability, and value creation by making government data available to all. This data can be used to attract nongovernmental sector and community, in general, for participation aiming at strong civic engagement.

The government produces large quantities of data and information, by making this data available, the private, social and government sectors are equipped with strong effective planning tool to institute new, value added, and innovative services for citizens, communities, and the society at large.

This component will provide the elements needed for exposing various types of data, weather structured or unstructured, allowing the ability to define the relevant sets of data catalogues, formats, and enables the rules for managing data publishers, subscribers, and data caching and delivery.

#### 2.2.3.4 Government Employee Portal

The Government Employee Portal is used as a central place for employees to facilitate services to citizens, in addition to being an Intranet for information common to government workers.

The Government Employee Portal also includes the **Task Management Service** that allows employees to participate in long running government processes where no back-end system is present. It would work as follows:

- As part of executing a Government Digital service, a service requires a task to be conducted by a government employee of an entity that has not automated its operations
- The service would send a message to the Task Management Service to log a task for the employee, with the details of the task
- The employee will log on to the Task Management service on the Employee Portal and views all his/her pending tasks
- The employee will complete his task offline, and once done he/she will complete he will mark the task as complete in the portal
- The service will be notified through a message that is sent over the Government Service Bus, and it will resume processing the service request.

#### 2.2.3.5 Government Blockchain

Blockchain is a revolutionary technology that has started to gain grounds in government services after it has initially been used mainly in financial services. Blockchain provides a

distributed ledger, that is secure, shared and immutable. In the government context, Blockchain technology promises greater integrity and transparency through fighting fraud and corruption, reduced cost of operations, and reduced costs of protecting citizens' data while creating the possibility to share data between different entities. While the technology is still in its infancy, and as such presents risks associated with any new technology, it is beneficial to start experimenting with its applications.

Within the Digital Government Blueprint, the approach to blockchain is as follows:

- Ensure that knowledge and expertise about the technology starts to develop within the government
- Explore scenarios where the blockchain can be used to solve existing challenges. For example, the blockchain has been used in other African countries to facilitate distributed secure land registries. This could be one of the high priority scenarios for Rwanda as well.
- Conduct Proof-of-Concepts to apply the usability of the technologies to the above scenarios. Again, the land registry scenario might be the one to start with.
- Use the learnings from the Proof-of-Concepts to do detailed planning for rolling out the technology in production based on its feasibility assessment.

### 2.2.3.6 Internet-of-Things Services

The Digital Government Platform includes smart devices as one key ways to interact with citizens and to capture and utilize data coming from the environment. Some of example of devices that are used in this context are street lights, GPS devices, smart phone cameras, and others.

The Internet of Things (IoT) Services help in the following objective:

- **Connect and Manage Devices:** Connect devices and other assets and capture the data they generate, allowing that data to be managed, analyzed and ultimately presented as usable information.
- **IoT Analytics:** This would allow creation of dashboard that would track practically everything from energy, water, traffic, transportation fleets, personnel, and buildings -

with sensors, analysis tools and key performance indicators. This leverages the Big Data Services already part of this platform.

## 2.2.4 Digital Identity and Security

### 2.2.4.1 Overview

Providing Digital Identity that is secure and ubiquitous is one of the foundations of Digital Government. As described by the World Bank Digital Identity Toolkit:

“Digital Identity (eID) provides technology-based solutions for identification in order to uniquely establish a person’s identity and to credential it, so that the identity can be securely and unambiguously asserted and verified through electronic means for delivery of services across sectors, including healthcare, safety nets, financial services, and transport.”

The following definitions are important in addressing this section:

- **User:** the individual to be identified, authenticated, and authorized to use certain services. It can be one of the following:
  - Individual: a citizen or non-citizen that will use the Gateway.
  - Employee of an Organization: a defined user that is linked to an organization for the purpose of using the e-services
  - Agent Employee: a defined user that is linked to an Agency (defined below) for the purpose of using the e-services on behalf of other users
- **Identity:** represents and identifies a user.
  - A user can choose to maintain several separate identities
- **Credential:** information or other items that is verifiable to assert an identity. Multiple credentials may be associated with the same identity.
- **e-Service (or Service, or Digital Service):** a logical grouping of business functionality offered by a service provider, with consistent rules governing authorization and access for users.
- **e-Service Provider:** A Government Organization that provides online e-Services.
- **Enrolment:** The linkage of an identity to a particular e-Service.
- **Agency:** An organization that is authorized to use the e-Services on behalf of other users or organizations.

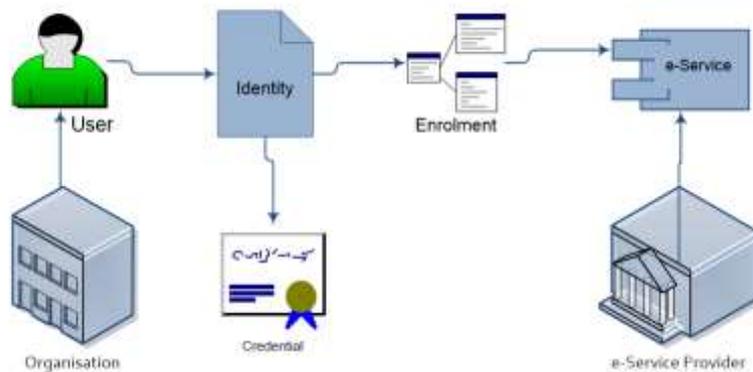


Figure 14 Identity Concepts

### 2.2.4.2 Digital Identity

This component provides technology-based solutions for identification in order to uniquely establish a person's identity and to credential it. The identity has to be:

- Secure : allowing secure and authenticated access to services
- Multi-purpose: supporting multiple ways of authentication for multiple types of services and different security levels
- Mobile – ready : usable for accessing services through mobile channels

The current status for Digital Identity in Rwanda can be summarized as follows:

- The National Population Registry maintained by NIDA forms the authoritative database for citizen identification
- The system also supports storing biometric information
- The citizen records can be tied to mobile phone numbers through collaborating with telco providers
- The government web site, Irembo, currently performs user registration by integrating with NIDA and the Telco providers
- Only user name / password is allowed as credential type in Irembo online services

The Digital Identity component supports the following important features:

- Registration:

- A user must register to access e-Services. The registration component ensures that a user's credentials (e.g., user name and password, certificate) can be unquestionably tied to a real world identity.
- Registration must be efficient, secure and require minimum human interaction
- Registration for specific e-service should be allowed: once a user is registered for the Digital Government Platform, the e-service can specify that the user needs to extend his registration to access the e-service, which could include adding additional service-specific information
  
- Multiple Credentials
  - Multiple credential types should be supported, including:
    - Username/Password authentication
    - Digital Certificates (stored on Smart cards, Tokens, or other secure media)
    - Biometrics (fingerprints, iris scanning, facial recognition, or others)
    - Mobile ID (utilizing mobile SIM cards)
    - One Time Passwords (through SMS, Phone call verification, or others)
    - Other potential credential types in the future
  - Multiple security settings are associated with different e-services and as such corresponding credentials for each e-service should be based on its level of security. For example, a land registration transaction requires a higher level of security than filing a traffic complaint. In this example, the Service Provider for land registration would potentially require Digital Certificates, whereas complaint filing would accept username/password credentials.
  - A user can have multiple credentials and can choose to apply set of credentials based on:
    - Availability: whether it is possible to use the set of credential (e.g if he is carrying his smart card with him).
    - Channel: some credential types are not possible with mobile channels for example.

- The security level for the service itself: different services might require different level of security assurance, as explained above.
- Support for organizations identities and delegation
  - The service should allow identifying and registering organizations and their employees
  - Registration for businesses need to integrate with the central business registry
  - The procedure for adding employees shall be simple, in order to allow the easy expandability of e-services to the organizations.
  - The system should allow delegation for submitting service requests on behalf of other users for specific e-service requests (e.g: for lawyers, other representatives)
- Support for Single Sign-On
- Single sign-on for Government Services allows citizens to be authenticated once on a certain channel (such as the web portal), and be able to access multiple services in the same session, even if these services are hosted on other locations or platforms. Without single sign on, citizens would have to remember multiple user names and passwords for multiple services, causing inconvenience as well as security issues in storing and managing passwords. Moreover, cases where services require going through forms across multiple government entities will not be possible to implement.
- While the vision may be to bring all online services on Irembo, this might not be feasible or practical, and as such the architecture should support multiple government services sites and should allow seamless navigation between them.
- Irembo currently provides a single credential to access many services. However:
  - For the single sign-on to work, services currently need to be hosted on Irembo site.
  - There is no provision for enabling access to other sites with the same credentials
  - Other government sites require users to create and log in with different accounts : example is RISA, RRA
- Federated Identity is the enabler for single sign-on as it enables users from different trust domains to authenticate with their credentials in the home domain, but gain access to resources in other domains, based on established trust relationships between domains.

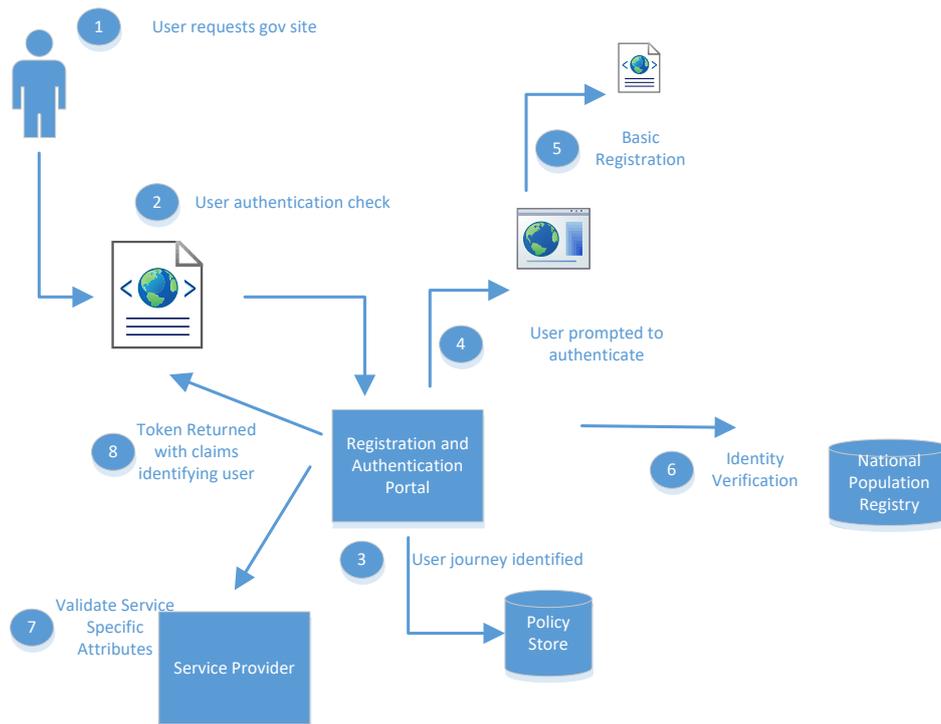


Figure 15 Single Sign-On

- The platform should support the following standards for enabling single sign-on though identity federation:
  - WS-Federation
  - SAML 2.0
  - OAuth 2.0
  - OpenID Connect
- All channels need to integrate with Single Sign-On using the agreed upon federated authentication protocol

### 2.2.4.3 Digital Signature

With the objective of paper-free digital government, it is essential to provide the facility for digital signature, and secure digital document exchange. Digital signature facilitates the transition to digital government whereby documents and transactions can be electronically signed. The objectives of this component are:

- **Confidentiality:** ensure that transactions passing between government entities as well as external entities are secured and confidential

- **Integrity:** ensure that no unauthorized modification to transaction is taking place through digital signature
- **Authentication:** ensure that parties can securely identify themselves through digital certificates
- **Non-repudiation:** ensure that transactions cannot be disputed and can be traced back to the originating entity

Currently, the Rwanda Electronic Transactions Law supports digital signature and makes it equivalent to hand-written signature. RISA has started the implementation of a National Public Key Infrastructure, which is currently used to issue certificate for government and private institutions for document signing purposes.

This infrastructure needs to be accredited so that its certificates are recognizable by common browsers and devices.

## 2.2.5 Government Service Bus

### 2.2.5.1 Overview

The Government Service Bus is a core component in the Digital Government Platform. It has the following main objectives:

- Accelerate the creation of new e-services through surfacing government data and processes
- Simplify the creation of services that span multiple government entities
- Reduce costs through removal of duplication of integration efforts
- Enforce security and privacy of message exchanges
- Standardize data integration and ensure interoperability
- Enable management and control over integration



Figure 16 Government Service Bus Components

It consists of the following main services:

- **Messaging & Routing Services** - responsible for managing messages that pass through the Bus: accepting, validating, and passing messages to the appropriate locations.
- **Application Integration Services** - connect to the target government organization services and routes messages and documents to and from them, handle the secure and reliable delivery of messages
- **Business Process Orchestration** – allows the aggregation of messages across multiple government entities to deliver combined processes

### 2.2.5.2 Messaging and Routing

Transactions which are initiated by government entities shall typically be submitted through either the Portal or by automated system interfaces. While the Portal provides a web-based interface allowing users to interact with the Gateway in a user friendly manner, automated system interfaces are required to allow external systems, inside and outside the Government, to submit transaction requests to the Bus without human intervention.

To support the above, the transaction and messaging services shall contain a transaction engine providing the following functionality:

- **Service identification:** In order to route a transaction request, the transaction engine must be able to determine which system(s) to route the transaction to. The target is typically based on the format of the transaction; however, it could be based on the data contained within the transaction itself.
- **Transaction routing:** The transaction engine shall be able to route a request to the proper recipient. Transactions may have multiple destinations or may come from multiple sources, depending on the specific process to be executed. The Gateway shall be able to route transactions between all supported sources and destinations.
- **Auditing and Tracking:** The transaction engine shall provide information on the transactions, which have been processed, for auditing and tracking purposes.
- **Asynchronous Messaging:** preferred to ensure reliability and scalability
- **Synchronous Messaging:** used to deliver near real-time services

- Publish/Subscribe Messaging: used to broadcast certain types of messages to subscribers

The Bus should support international open standards for messaging including:

- Message Formats : XML or JSON
- Transport: HTTP / SOAP / REST
- Security: SSL, SAML, WS-Federation, Oauth, OpenID Connect

### 2.2.5.3 Application Integration

Integrating with the existing back-end systems, through the different protocols and access methods currently supported by these systems, is an important component that shall be implemented by the Government Service Bus. This component shall enable application integration by providing a standard and customized set of adapters for existing back-end systems.

The following integration patterns can be supported by the bus:

- Back-end systems should provide a Web Service interface (SOAP or REST)
- Using local integration servers (remote adapters) that connect to the bus
- Using adapters that can translate between canonical message formats and back-end systems in case a web service is not available

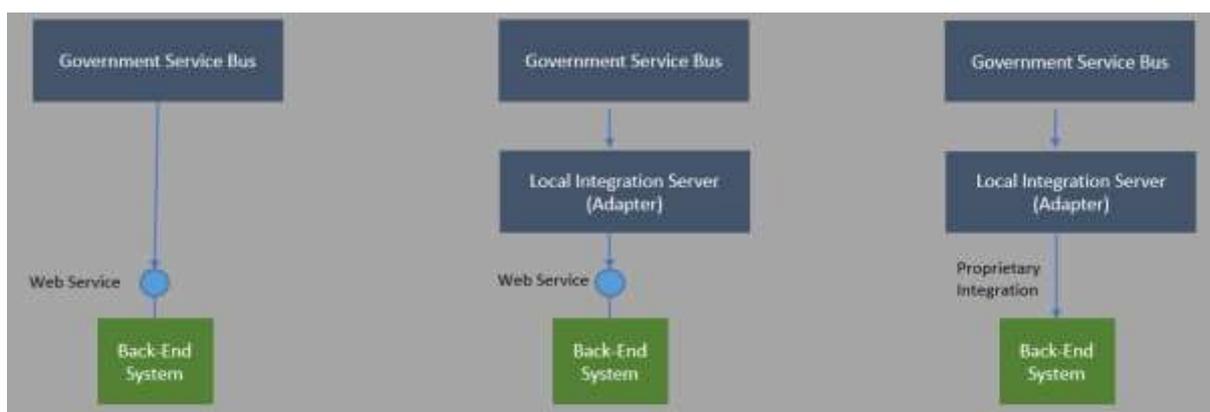


Figure 17 Service Bus Integration Patterns

As the government is already in the process of building back-end systems to automate government functions, it would be useful to ensure that, as these systems are built, they facilitate future integration needs. Typical requirements for back-end systems for integration include:

- Systems should provide secure, well-documented Open APIs that are made available through standard interfaces that are accessible through REST or SOAP.
- The Open APIs should expose system data, provide the ability to initiate transactions and workflows, retrieve the status of transactions and workflows.
- Systems should support federated authentication and authorization through integration with Identity Management using OpenID Connect or WS-Federation. This would allow users to authenticate with single credentials on multiple systems.

#### 2.2.5.4 Business Process Orchestration

The Government Service Bus should provide the ability to model and execute customized business processes and rules that coordinate (through appropriate workflow) the execution of an e-Service with back-end systems.

While orchestration is a desired component of integration, it should be reviewed carefully due to the issue of ownership of the orchestration logic. The GSB as a central government component is not preferred to host and manage business logic related to other entities due to ownership and maintainability issues. It should allow the creation of orchestration logic that is created and maintained in the individual government entity, integrating with the GSB but not living in the central government GSB.

### 2.2.6 Secure Infrastructure

#### 2.2.6.1 Overview

The Secure Infrastructure component provides the backbone of systems, hardware, networking and security that ensures a reliable, secure, and low cost operation of government services.



Figure 18 Secure Infrastructure Components

### 2.2.6.2 Public / National Cloud

The Smart Rwanda Master Plan advocates for a “Cloud-First” approach, stating that, while setting up new systems and applications, public sector organizations shall prioritize business models and solutions that are cloud-based over stand-alone or individually hosted services. Cloud Services provide the capability to quickly deploy IT infrastructure and software to deliver government services. It provides:

- Fast time to market for services, due to the readily available virtualized resources that can quickly be deployed, the government can accelerate the pace it delivers services to citizens.
- Cost efficiency through economies of scale as multiple government entities are able to host their services on consolidated hardware, software, and infrastructure.
- Enabling innovation and modernization of services: through making
- Scalability on demand: to match demand, especially in seasonal scenarios, the cloud provides the capability to increase available resources to scale the service.
- Public Cloud Operators utilize advanced security mechanisms to ensure the privacy and security of data, and as such can provide better security commitments than data hosted within the government entity data centers.

The Government of Rwanda has the option to leverage existing Public Cloud offerings as well as the expanding a National Cloud based on the existing national data center. While the National Cloud provides the ability to store data within the borders of the country, the Public Cloud provides significant benefits leveraging the innovation and scale of international technology vendors.

### 2.2.6.3 Cyber Security

With the Government of Rwanda going Digital, more and more government systems and services are open on the Internet. The Government of Rwanda has openly recognized the importance of Cyber Security in ensuring that all Digital Services and connected systems are properly protected. It has identified the following related objectives (based on Rwanda Cyber Security Policy):

- Build **cyber security capabilities** for detection, prevention and response to cyber security incidents and threats
- Establish an **institutional framework** to foster cyber-security governance and coordination;
- Strengthen **legal and regulatory frameworks**, as well as promote compliance with appropriate technical and operational security standards
- Promote **Research and Development** in the field of cyber security
- Promote **Cyber Security Awareness** in all sectors and at levels in order to build a culture of security within country
- Promote National, Regional and International Cooperation in the field of cyber security.

As the government seeks to build **cyber security capabilities** for detection, prevention and response to cyber security incidents and threats, it can leverage the following services within the cyber security component:

- Security Risk Assessment
  - Regularly review cyber security people, processes, technology covering four categories of assets:
    - **Identities** – Critical element to security as all assurances are based on authentication and authorization provided by identity systems
    - **Applications and Data** – The stores of business value whose confidentiality, integrity, and availability must be protected.
    - **Infrastructure** – A critical security dependency for most apps and data that adversaries are exploiting to get at them
    - **Devices** – the front line of the security battle that collectively protects access to all assets
- Continuous infrastructure protection, hardening and remediation.
- Conduct continuous Cyber Security Threat Detection and Analytics and response.

#### 2.2.6.4 Communication & Collaboration Services

In order to be able to deliver on digital government needs, government employees need to be able to collaborate and communicate efficiently. Currently, most government entities maintain mail servers at their premises, while some government entities utilize the services of the Government Data Center for mail hosting. While some government entities utilize video conferencing technology mainly for conferencing with remote offices, there is no unified communication platform (mail, voice, video, instant messaging) in most government entities.

The Communication and Collaboration Services in the Digital Government Platform:

- Provide a scalable government-wide communication and collaboration platform that facilitates employee-employee interactions
- Support unified real-time communication within and across entities covering:
  - E-mail
  - Instant messaging
  - Audio conferencing
  - Video conferencing
  - Collaboration and Information sharing
  - Community and forum discussions
- Integrates with the Digital Government Notification Services to facilitate citizen interactions

### 2.3 Ownership and Governance

As described earlier, the Rwanda Digital Government Platform (RDGP) should not be considered as one monolithic solution that can be deployed at once. It is rather a set of technology systems, components, architecture artefacts, and guidelines that are most likely going to be deployed and operated by separate organizations at various points of time. The most critical success factor of this Platform is ensuring that all components integrate and work together towards the common vision.

This section lists the recommended ownership and governance framework for the platform. The key principles related to governance of the platform are listed below:

### 1. RDGP Global Ownership

- The overall ownership of the Rwanda Digital Platform belongs to the GoR.
- MiTEC has the responsibility of overall oversight, setting policies around information sharing and protection as well as overseeing the implementation of different components.
- RISA has the responsibility to ensure that the architecture is maintained and evolved. Also to ensure interoperability of all components under it, and coordinating all the initiatives stemming from it as well as compliance.

### 2. RDGP Component Ownership

Each component of the Platform must have one single accountable government entity as owner but still ensure that the implementation of the Component is aligned to the global strategy and quality requirements of the overall RDGP.

### 3. Public-Private-Partnership

Whenever possible, implementation and operation of RDGP components will prioritise a PPP model, while keeping the ownership structure as articulated in points 1, and 2 above.

The following table provides the recommended ownership model. This is presented for discussion only.

Top-Level Component	Sub-Component(s)	Ownership	Implementation	Operation
RDGP Global Ownership		GOR (MiTEC/RISA)	RISA (Coordination)	RISA (Coordination)
Integrated Digital Channels	Web portal e-forms engine Life evens Gov. yellow pages Service catalog Appointment scheduling Kiosks	RISA	RISA/ROL	RISA/ROL

	Online chat engine Map/location services Search			
	Mobile services	RISA	<ul style="list-style-type: none"> <li>• Creation of guidelines and templates by RISA</li> <li>• Mobile App implementation will be done by various private or public-sector organizations depending on the service to be provided</li> </ul>	RISA/ROL
	Social Media Services	OGS	GOR's entities	GOR's entities
	Call Center	RISA	To be outsourced	To be outsourced
	Citizen Experience Management	MINALOC	RGB	RGB
	IoT Services	RISA	RISA	RISA
Digital Government Enabling Services	Payment Gateway	BNR	BNR/RISA/RURA	BNR
	Notification Gateway	RISA	RISA/ROL	RISA/ROL
	Data Services	RISA	RISA/ROL	RISA/ROL
	Employee Portal	RISA	RISA	RISA
Government Services Bus	Government Services Bus	RISA	RISA	RISA
Secure Infrastructure	Communication & Collaboration Services	RISA	RISA	RISA
	Cyber Security	RISA	RISA	RISA

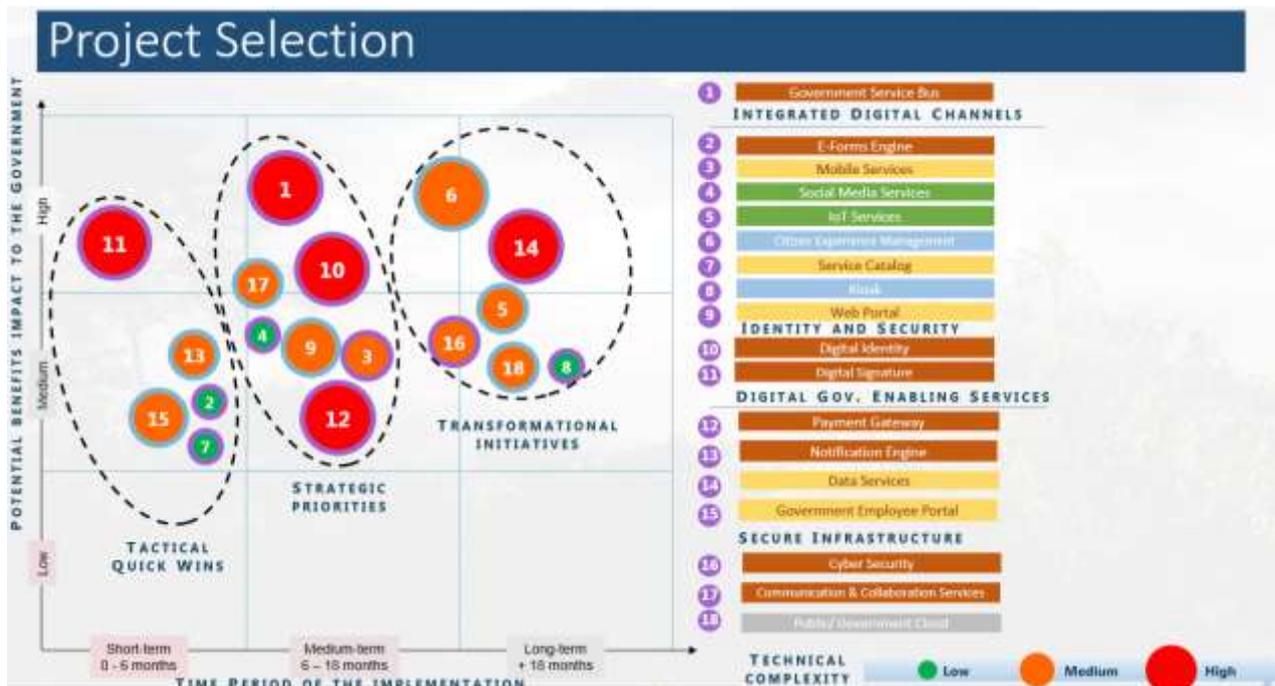
	Operation management	RISA	RISA	RISA
Digital Identity and Security	Digital Identity, Single Sign-On	RISA	RISA	RISA
	Digital Signature	RISA	RISA	RISA

## 2.4 Implementation Roadmap

Considering the gap between the current status and the expected future status, the RDGP's components are further classified into three categories:

- Tactical quick wins
- Strategic priorities
- Transformational initiatives.

The matrix below is a summary of the project prioritization process.



For implementation, the roadmap focuses first on high value items. Components that already exist in some form are shifted forward as per the diagram below:

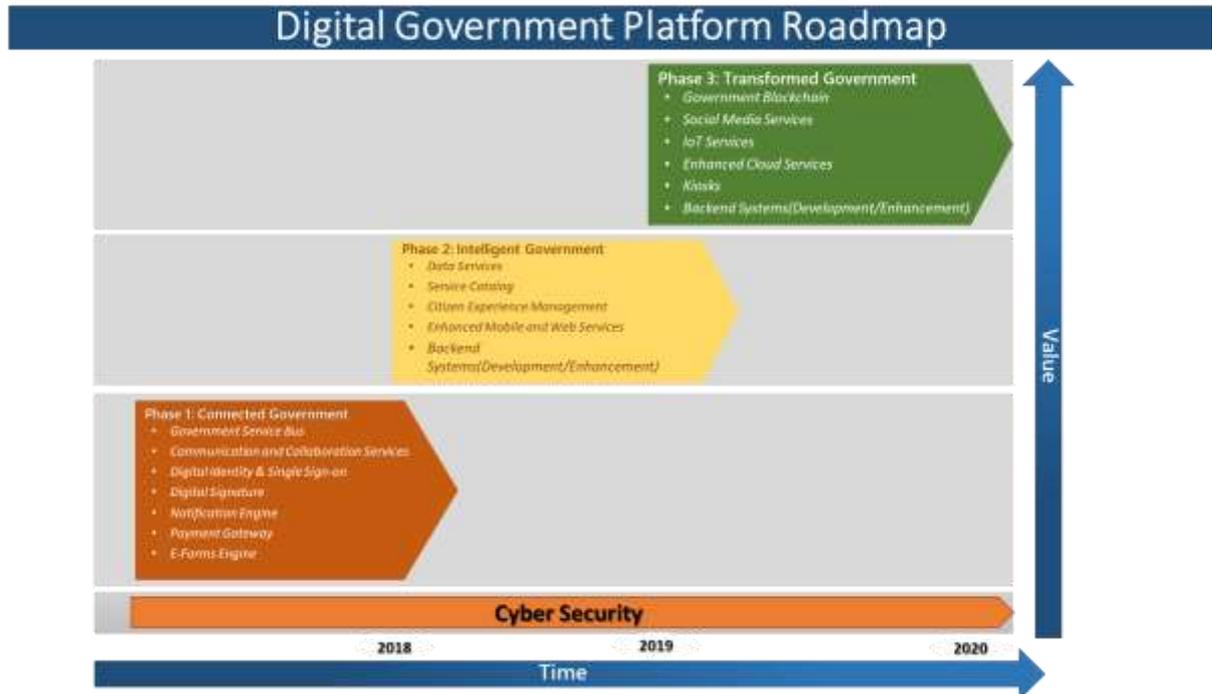


Figure 19 RDGP Roadmap

- **Phase 1 “Connected Government”** focuses on ensuring that connected government services are feasible through ensuring the implementation of a Government Service Bus, Communication and Collaboration, and others.
- **Phase 2 “Intelligence Government”** focuses on data-driven government including big data services, open data, citizen experience management, and others.
- **Phase 3 “Transformed Government”** builds on the previous phases to deliver modern experience based on social media, IoT, as well as provide more robust payment and cloud services.

## 3 Enterprise Architecture Governance

### 3.1 Introduction

The Government of Rwanda under the leadership of RISA has undertaken to develop Enterprise Architecture Practice with the goal of establishing unified IT standards and practices across all public entities. The rationale behind this is the need for seamless and integrated IT solutions across government entities.

It is acknowledged that up until now, despite the close alignment of the services offered by different government entities, the respective IT functional units have applied different standards in developing and deploying solutions.

An assessment conducted in 2013 concluded that there is neither IT governance nor enterprise architecture in place within all public entities and by extension, there is practically no appropriate Enterprise Architecture Governance.

This scenario poses a challenge to the Government of Rwanda as it seeks to integrate IT solutions across all public entities.

In order to address this challenge, RISA has been tasked to drive the implementation of enterprise architecture practices that will ensure the application of unified IT standards across all entities.

To achieve this, there is a need to define an Enterprise Architecture Framework (EAF) as well as the governance model that will drive its implementation.

Rather than applying a leading framework in its entirety, the government of Rwanda has elected to adopt and modify The Open Group Architecture Framework (TOGAF) to suit the specific needs of Rwanda.

Depicted in *Figure 20* below is the modified framework. The detailed description of the framework has been defined in the document titled 'Government of Rwanda Enterprise

Architecture Framework (RGEA)’ which has also outlined the domains that enterprise architecture practice will cover.

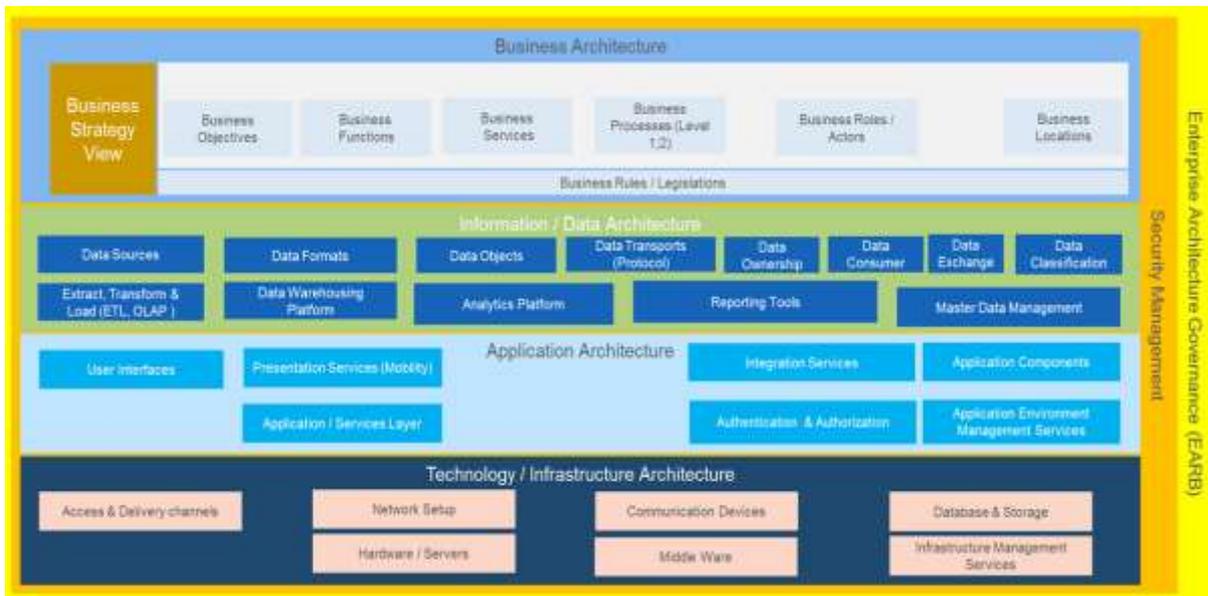


Figure 20: The Rwanda Government-wide Enterprise Architecture Framework

The purpose of this document, therefore, is to outline the governance structures and roles that specific boards and committees will be entrusted with in ensuring adherence to set IT standards and practices.

### 3.2 Background

Management of an IT function is a complex undertaking. This is largely because IT encompasses a number of closely linked sub disciplines which need to be maintained in seamless alignment if the combined service offering is to deliver value to the target audience.

Success of the IT function therefore hinges on a number of inter-related activities which are all coordinated through IT Governance.

Within Government of Rwanda, IT governance should be taken both in the sense of provision of standards and policies for the entire ICT functional unit as well as governance around

Enterprise Architecture practice. This will be referred to as Enterprise Architecture Governance (EAG).

The primary purpose of **Enterprise Architecture Governance** is to ensure that an organization's IT investments are closely aligned to business goals and processes, so that limited IT resources are allocated to areas of highest impact on organizational performance. While the overriding concern of EAG is the effectiveness of the IT investments, the EA program itself needs to be governed as well, since an incorrectly developed EA could adversely impact the IT investment decisions that are based on it. The EAG described in this document has three primary objectives:

- Ensure that the EA program is properly managed and that it produces artifacts and plans that are truly representative of organizational goals and needs.
- Ensure that the IT investment decisions are being continually aligned with the EA Office from the point they are initiated until implemented
- Ensure that the IT decisions are made with consideration for integration goals of government Rwanda

To address these objectives, a well-defined Enterprise Architecture Governance Framework needs to be developed, agreed, communicated and implemented.

The following sections describe the proposed EA Governance Framework for each major component of the EA Program as well as the required governance bodies to ensure the implementation of the defined EAG framework.

### **3.3 EA Governance Implementation**

The purpose of the EAG Framework is to provide policy guidance and advice and assistance in the definition, design and implementation of Enterprise Architecture (EA) discipline and practice throughout organization.

In addition, it serves as the core governance asset providing advocacy for EA integration of business and technology architectures across business units as well external boundaries.

The EAG establishes common terminology definitions and frameworks, including the Enterprise Architecture Framework and Technical Reference Models and Standards; and practical guidance to effectively implement and provide assurance for government of Rwanda technology solutions required to enable business requirements.

The Implementation of any EAG follows a number of steps. Typically, EAG requires formation of a number of governing bodies that share responsibility of overseeing operations of the IT functional unit.

These bodies are systematically arranged along the System Development Lifecycle (SDLC) to not only set and ensure adherence to set standards and principles but also to mitigate the risk of IT delivering a solution that may potentially be misaligned to the business requirements. Furthermore, the governance bodies vet and make recommendations on future IT investment plans.

The rationale behind having multiple governance bodies is to avoid a situation where a single body is entrusted with the responsibility of both making recommendation and approving the same. Best practice requires that there be multiple bodies that will validate each other's decision.

Within the Government of Rwanda, however, it has been noted that the IT functional units are relatively small. In majority of cases, the IT team is composed of less than ten (10) FTEs.

This scenario makes it impossible to create multiple IT governance bodies in such organizations.

It is, however, still imperative that EA governance be instituted in all public entities. It is noted that all public entities have an IT committee whose terms of reference include making decisions for IT investment and operational enhancements.

It is proposed that the terms of reference for such a committee should be extended to include Enterprise Architecture Governance. In this regard, the IT committee should also have the responsibility of ensuring adherence to set standards and application of EA policies.

If, however, this IT Committee is to be the only body responsible for making decision affecting an entity, governance would be a failure in principle for the following reasons:

1. The IT Committee's decisions need to be vetted by another independent body
2. The government of Rwanda's goal of bringing integration between public entities will need to be driven by a common goal across all public entities and therefore needs another body outside each of the entities to validate the decisions that would impact the integration

Since all the entities are organized in Sectors, it is therefore recommended that the IT committees for each entity be aligned to their respective Sectors. At central level, three additional decision making bodies will serve as escalation points for institutions' IT committees and Sector Working Groups. These are:

- RISA EA team.
- GoR Digitization Advisory Committee
- National ICT steering committee.

Described below is the proposed relationship:

1. The IT Committee will be responsible for making IT decisions for respective public entity. These decisions will include future investment plans, system enhancements, solution development etc.
2. Before the decisions are implemented, the IT Sector Working Group should be consulted. This is because the IT Sector Working Group would have a clear view of how each of the entities' architecture fits in with the sector mandate. In order to ensure that there is no disruption to the integration plans, the IT Sector Working Group will be the custodian of the sector architecture models. As such, it would be in a better position to approve decisions that would not compromise the integrations across sector entities.
3. In making its decision, the IT Sector Working Group will liaise with the RISA-EA Team. The RISA-EA Team is responsible for setting architecture standards and policies for all

government entities. As such, it will vet decisions made by IT Sector Working Groups in line with the set standards, policies and architecture goals of the government.

4. All major IT investment plans will be approved by the GoR Digitization Advisory Committee via the RISA-EA Team.
5. All strategic orientations in connection to ICT cross-institutional projects fall under the responsibility of the National ICT steering committee which is composed of GoR's cabinet members.

The roles and compositions of each of the governance groups are depicted below.

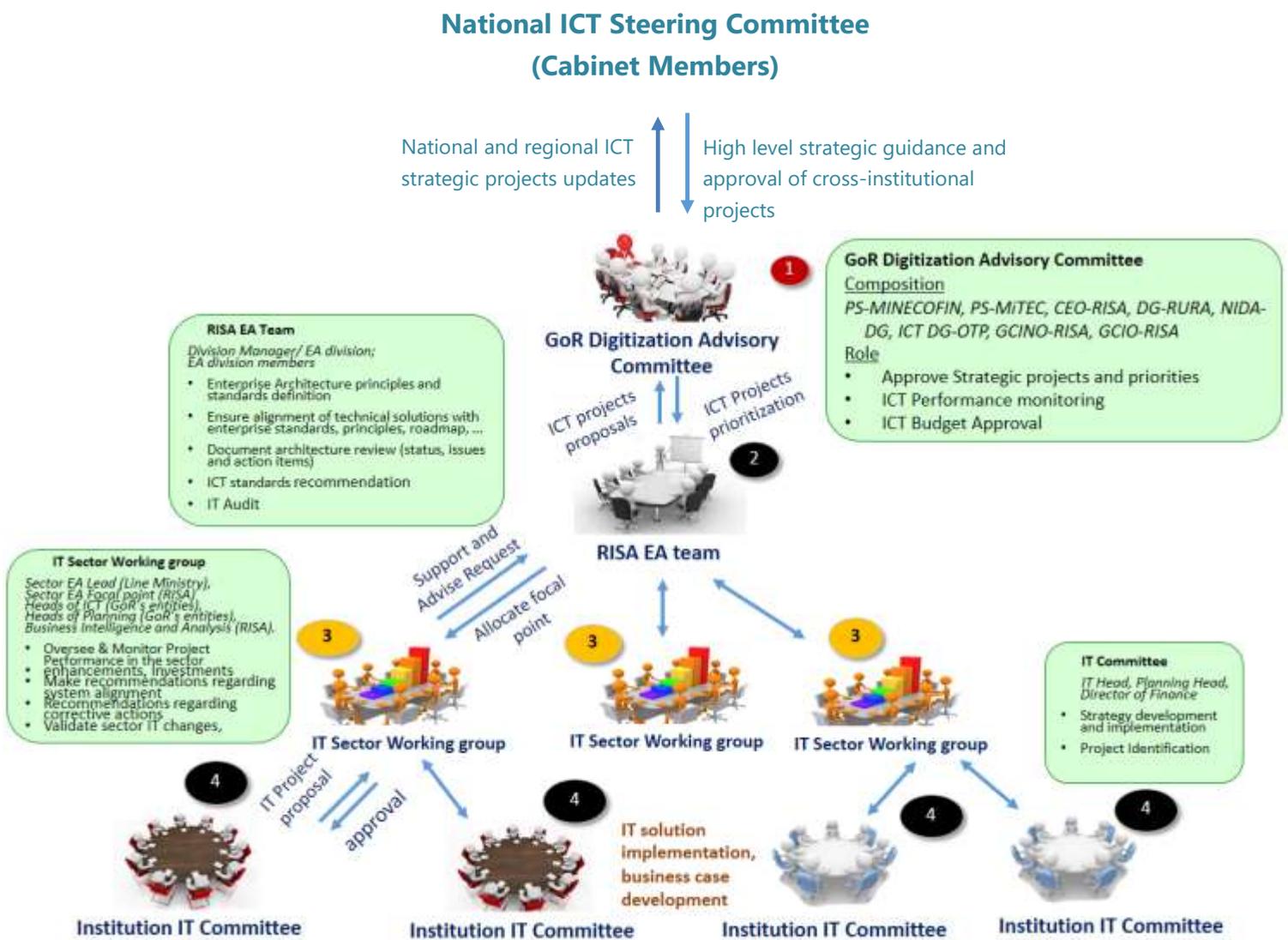


Figure 21: EAG Roles and responsibilities

### 3.3.1 GoR Digitization Advisory Committee

This is the top decision making body within Government of Rwanda regarding IT initiatives. The core of the Advisory Committee’s functional responsibility will rest on National ICT strategic projects approval, prioritization and monitoring in terms of cost and performance. It is therefore important to have the PS / Ministry of Finance as a permanent member of the GoR Digitization Advisory Committee to ensure alignment in terms of ICT projects financing.

The Advisory Committee receives recommendations from the RISA-EA Team on new projects and then advises on prioritization. It also reviews performances of projects as presented by the RISA-EA Team as well as provision of guidance for the Sector IT Working Group.

The ultimate role of the GoR Digitization Advisory Committee is to provide strategic direction to the IT function as well as ensuring that all ICT service delivery initiatives are aligned towards a common vision. In line with that and depending on matters being deliberated, the GoR’s Digitization Advisory committee might invite key ICT players from private sector to take part in the discussions on need basis. This would help capture views of the private sector and strengthen the Public and Private Partnership.

Described below is a summary of the GoR Digitization Advisory Committee roles and responsibilities:

<b>Accountabilities</b>	<ul style="list-style-type: none"> <li>– National ICT master plan approval</li> <li>– Strategic ICT projects approvals and prioritisation</li> <li>– National ICT project performance monitoring.</li> <li>– Guidance on major IT expenditures.</li> <li>– National ICT cost monitoring.</li> </ul>	<b>Suggested Composition</b>	Permanent Secretary / MiTEC (Chair) Permanent Secretary/MINECOFIN CEO-RISA GCINO – RISA GCIO – RISA COO - RDB DG – RURA DG-NIDA DG/ICT – OTP <b>Optional:</b> Key Business Representatives to be invited on need basis.
<b>Responsibilities</b>	<ul style="list-style-type: none"> <li>– Advise on overall IT capital expenditure levels based upon merit of initiatives and overall financial constraints</li> </ul>	<b>Escalation</b>	<b>Escalation point for:</b> <ul style="list-style-type: none"> <li>• RISA EA Team</li> <li>• Sector IT Working Group</li> <li>• IT Committee</li> </ul>

	<ul style="list-style-type: none"> <li>– Review IT performance metrics to track IT performance</li> <li>– Provide input into timing and scope of major IT initiatives.</li> <li>– Prioritisation of major initiatives</li> <li>– Provide approval of major IT initiatives</li> <li>– Review &amp; approve National IT Strategy</li> <li>– Review and advise on expenditures for major initiatives or significant changes from plan</li> <li>– Review status of major initiatives and take action where appropriate</li> <li>– Review significant changes to IT standards, as recommended by the RISA EA team</li> </ul>		<p><b>Escalation to:</b></p> <ul style="list-style-type: none"> <li>• National ICT steering committee</li> </ul>
Frequency	<b>Quarterly (and on need basis)</b>		

Table 1: Roles and Responsibilities for GoR Digitization Advisory Committee

### 3.3.2 RISA EA Team

The RISA-EA Team is the custodian of architecture models and artefact for the entire Government of Rwanda. Its primary role is to set architecture principles and standards for all IT solutions. The EA Team should therefore, always be consulted when change is being considered in an environment. In this regard, when a business requirement is received for either developing, procuring a new solution or enhancements to an existing system, the requirements should be brought before this team for review.

In this role, the RISA-EA team is concerned with mapping the new business requirements to the current architecture landscape and ascertain on the impact that a new change would have across the government IT landscape. The role of the Team therefore transcends beyond setting standards for enterprise architecture. It also includes ensuring that the Government-wide architecture landscape is kept in line with the overall government initiatives. These

initiatives include ensure application of common standards across all entities, maintaining the system alignment and integration among all Government entities, ensuring that investment plans are in line with overall government long term IT goals.

It is the RISA-EA Team that would approve the **'build'** or **'buy'** decisions. This is done after the business and functional requirements have been analyzed against the current IT solutions and investment planning. The assessment is done to ensure that the planned change is in alignment with the business requirement and IT capabilities.

As defined above, the RISA-EA Team should have powers assigned to a board i.e. powers to make decisions. This entails that it may reject or approve requests.

Furthermore, it will also play the role of an innovation board: thus, it should also fulfil an advisory role to IT and business on new innovations. In this regard, its actions should be proactive. Thus, the RISA –EA Team should always strive to bring innovative ways to enable business through provision of advice on trends in the technology field and also possible enhancements to current systems.

To ensure that the RISA-EA Team works well, it should be chaired by the Government Chief Innovation Officer (GCINO) or the Government Chief Information Officer (GCIO). The other members are the Enterprise Architecture Division Manager, the Digitization analyst, Information system security analyst, Business Process Re-Engineering Specialist, Data Architecture Specialist, Infrastructure Architecture Specialist, Systems integration senior engineer, Enterprise & application architecture specialist, Enterprise & application architecture analyst, Business intelligence and analysis specialist.

Summary of the composition and mandate is shown below:

<p><b>Accountabilities</b></p>	<ul style="list-style-type: none"> <li>- Enterprise Architecture direction across infrastructure, applications, processes and tools</li> <li>- Enterprise Architecture roadmaps across technologies</li> <li>- Identification of innovation in IT that can help the business and awareness of new technologies</li> </ul>	<p><b>Suggested Composition</b></p>	<ul style="list-style-type: none"> <li>- Enterprise Architecture Division manager</li> <li>- Digitization analyst</li> <li>- Information system security analyst</li> <li>- Business Process Re-Engineering Specialist</li> <li>- Data Architecture Specialist</li> <li>- Infrastructure Architecture Specialist</li> <li>- Systems integration senior engineer</li> <li>- Enterprise &amp; application architecture specialist</li> <li>- Enterprise &amp; application architecture analyst</li> <li>- Business intelligence and analysis specialist.</li> </ul>
<p><b>Inputs</b></p>	<ul style="list-style-type: none"> <li>- IT Strategy</li> <li>- IT Investment and operating plan(annual)</li> <li>- Project proposals</li> <li>- New technology developments in the marketplace</li> <li>- Learning / experiences / insights from other competitors/ industries/partners</li> </ul>	<p><b>Outputs</b></p>	<ul style="list-style-type: none"> <li>- IT Strategy</li> <li>- IT Policy, Standards</li> <li>- EA framework and Architecture artefacts</li> <li>- IT Investment and operating plan(annual)</li> <li>- Project proposals</li> <li>- New technology developments in the marketplace</li> <li>- Learning / experiences / insights from other competitors/ industries/partners</li> </ul>
<p><b>Responsibilities</b></p>	<ul style="list-style-type: none"> <li>- Review and recommend Enterprise Architecture vision &amp; roadmap, to deliver corporate strategic objectives</li> <li>- Define Enterprise Architecture standards, policies, principles and guidelines</li> <li>- Assess new project proposals for architectural compliance</li> </ul>	<p><b>Escalation</b></p>	<p><b>Escalation point for:</b> IT Sector Working Group IT Committee</p> <p><b>Escalation to:</b> GoR    Digitization    Advisory Committee</p>

	<ul style="list-style-type: none"> <li>- Facilitate collaboration across areas to exploit IT synergies and avoid duplication.</li> <li>- Bring learning / experiences / insights from other clients / industries to IT</li> <li>- Identify potential new business / IT opportunities and recommend new technologies and / or approaches</li> <li>- Work with business management / stakeholders to develop compelling business cases for new technologies</li> </ul>		
<b>Frequency</b>	<b>Quarterly (and on need basis)</b>		

Table 1: Roles and Responsibilities for RISA-EA Team

### 3.3.3 IT Sector Working Group

The IT Sector Working Group will have oversight over all IT initiatives undertaken by public entities that fall within it. This oversight responsibility includes the following:

1. Providing Sector specific IT direction
2. Monitor, advise and enforce IT alignment between different entities within the sector
3. Drive IT and EA initiatives across entities within the sector
4. Approve Business Cases for entities within the sector

**NOTE:**

All major IT projects in respective entities should be approved by the IT Sector Working Group. This will ensure the alignment of IT plans across the sector.

Projects will, however, be run and managed by respective entities.

Each project should also have its own project steering committee with the primary role of ensuring that the project is delivered on time, within budget and as per specifications.

The composition of the project steering committee will be determined by the respective project requirements. Each committee should, at a minimum include a Project Manager, Project Director, representative of the business, lead domain manager e.g. application manager, infrastructure manager etc.

Tabulated below are the responsibilities of the Sector IT Working Group.

<p><b>Accountabilities</b></p>	<ul style="list-style-type: none"> <li>- Alignment of project portfolio to the IT strategy/ business performance</li> <li>- Maintain alignment of IT Investment within the sector</li> </ul>	<p><b>Suggested Composition</b></p>	<ul style="list-style-type: none"> <li>- Sector Enterprise Architecture Lead (Line Ministry),</li> <li>- Sector Enterprise Architecture focal point (RISA),</li> </ul>
--------------------------------	--	-------------------------------------	--

	<ul style="list-style-type: none"> <li>– Approve large IT projects within the sector</li> <li>– Monitor and report on IT governance within the sector</li> <li>– Balance priorities across the Sector at National, Regional and Local levels</li> </ul>		<ul style="list-style-type: none"> <li>– Heads of Planning (GoR’s entities in the sector),</li> <li>– Heads of IT (GoR’s entities in the sector)</li> <li>– Business Intelligence and Analysis Specialist(RISA)</li> </ul>
<b>Inputs</b>	<ul style="list-style-type: none"> <li>– IT Programme Risks, Issues &amp; Benefits</li> <li>– New project proposals and business cases</li> <li>– Forecast of resource supply</li> </ul>	<b>Outputs</b>	<ul style="list-style-type: none"> <li>– Approved proposal for projects / programmes</li> <li>– Prioritised proposals for projects / programmes</li> <li>– Forward Schedule of projects</li> <li>– Performance improvement actions</li> <li>– Resolution of escalated conflicts</li> </ul>
<b>Responsibilities</b>	<ul style="list-style-type: none"> <li>– Review, prioritise &amp; approve IT investment decisions (up to a set value)</li> <li>– Ensure investment decisions align to IT and government-wide strategy</li> <li>– Develop and manage forward schedule of programmes &amp; investments</li> <li>– Facilitate resolution of conflicting priorities amongst functional / geographic areas</li> <li>– Assign accountabilities for programmes</li> <li>– Supervise delivery of the portfolio of programmes and projects</li> </ul>	<b>Escalation</b>	<p><b>Escalation point for:</b></p> <ul style="list-style-type: none"> <li>– IT Committee</li> </ul> <p><b>Escalation to:</b></p> <ul style="list-style-type: none"> <li>– GoR Digitization Advisory Committee</li> <li>– RISA-EA Team</li> </ul>
<b>Frequency</b>	<b>Quarterly (and on need basis)</b>		

Table 2: Roles and Responsibilities for IT Sector Working Group

### 3.3.4 IT Committee

The IT Committee’s primary role is to ensure all IT projects within respective entities are well coordinated and aligned to the overall strategic goals of the entity.

As such, the committee will be entrusted with the responsibility of defining the IT Strategy of the entity, setting up the enterprise architecture practice within the entity, documenting and maintaining the architecture models and artefacts, making IT investment plans and decisions per entity, ensuring effective and efficient IT project executions.

Tabulated is the summary of the role and deliverables of the committee.

Table 3: Roles and Responsibilities for IT Committee

<b>Accountabilities</b>	<ul style="list-style-type: none"> <li>– Define the IT Strategy</li> <li>– Define IT performance matrices</li> <li>– Define composition and terms of reference for project steering committees within the entity</li> <li>– Develop IT budgets</li> <li>– Set up and monitor the operations of the enterprise architecture team within the entity</li> <li>– Maintain architecture models and artefacts</li> <li>– Develop business cases for new projects within the entity</li> <li>– Approve new IT projects</li> </ul>	<b>Suggested Composition</b>	Head of IT (Chair) Planning Head, Director of Finance
<b>Inputs</b>	<ul style="list-style-type: none"> <li>– Project scope and plan</li> <li>– Project status</li> <li>– Project issues, risks, dependencies</li> <li>– Project budget</li> <li>– Resource requirements</li> </ul>	<b>Outputs</b>	<ul style="list-style-type: none"> <li>– Project phase closures (incl. Deliverable sign offs)</li> <li>– Escalated issues and risks (as necessary)</li> <li>– Resource requests</li> <li>– Management reports on status of projects to Portfolio &amp; Programme Governance Committee</li> </ul>
<b>Responsibilities</b>	<ul style="list-style-type: none"> <li>– Ensure that the project proceeds to plan and budget and identify corrective actions where required</li> <li>– Review &amp; approve or escalate project scope changes</li> <li>– Review project quality &amp; progress against business case</li> </ul>	<b>Escalation</b>	<b>Escalation point for:</b> <ul style="list-style-type: none"> <li>• Project Steering Committee</li> </ul> <b>Escalation to:</b> <ul style="list-style-type: none"> <li>• IT Sector Working Group</li> </ul>

	<ul style="list-style-type: none"> <li>– Manage status, cost, phasing of projects (incl. signing off deliverables), stakeholders, issues, risks &amp; dependencies as necessary (resolving where appropriate or escalating to Portfolio &amp; Programme Governance Committee)</li> <li>– Ensure project includes the necessary service elements</li> <li>– Monitor &amp; evaluate performance of suppliers involved in projects</li> </ul>		<ul style="list-style-type: none"> <li>• RISA-EA Team</li> </ul>
Frequency	<b>Quarterly (and on need basis)</b>		

### 3.3.5 Project Steering Committee (per project)

The Project Steering Committee is responsible for on-going project management. It is set specifically for each project. Its prime role is to provide governance and measuring project performance against set goals, budget management.

The composition of the project steering committee will be determined by the size and goals of the project.

Since all projects are approved by the IT Committee, the project steering committee will receive its terms of reference for the IT Committee and will also report to the same.

## 3.4 Enterprise Architecture Documentation

This “Rwanda Digital Government Strategy and Governance” document describes at high level the architecture of the “Digital Government Platform” which seeks to establish a common integration and communication point for all GoR’s IT systems, setting integration and interoperability standards.

The “Rwanda Digital Government Strategy and Governance” proposes also a governance structure which should be implemented in order for GoR’s entities to comply with the standards set for integration with the “Digital Government Platform”.

In addition to the Governance Structure the following complementary documents have been developed to fully guide GoR’s entities in the selection and development of IT systems for ensuring proper alignment with business requirements, proper scoping, and compliance with interoperability standards and integration standards with the “Digital Government Platform”:

The “**Blueprint Development Guidelines for the Government of Rwanda**”: The purpose of these guidelines is to help public entities and GoR’s private partners to have a common understanding of Enterprise Architecture practice and to guide the systematic mapping of the institution’s IT landscape (Blueprint) in clear steps namely: the AS-IS situation, the To-Be situation, the Gap analysis and the Roadmap. The institution’s IT blueprint is a basic requirement for RISA’s approval and MINECOFIN’s funding for IT projects.

The “**Government of Rwanda Enterprise Architecture Framework (RGEA)**”: This document defines the core purpose and complete description of “Enterprise Architecture”. It outlines the boundaries, approach and notation that is used to model the enterprise architecture within Rwandan public entities

The “**The Government of Rwanda Enterprise Architecture Standards**”: It is expected that each Public Entity will document their own enterprise architecture based on the guidance provided in the “Blueprint development guidelines for the Government of Rwanda”. This document provides

standards that should be adhered to while documenting the different “Enterprise Architecture components”.

The “**Rwanda Enterprise Architecture Principles**”: The Enterprise Architecture Principles describe how RISA plans to design and deploy information systems across all government entities. The prime goal of Enterprise Architecture is to define standards through which IT implementation across government institutions become seamlessly aligned. The unified standards across all entities will serve to streamline and reduce the complexity of IT investment decisions.

In this regard, principles are used to:

1. Provide guidelines in solution designing, development, Implementation and support
2. Evaluation of suppliers and service delivery partners
3. Evaluation of products and services
4. Support evidence-based decision making
5. Help define functional requirements