Caribbean Digital Transformation Project

IDA – 6685-DM

Terms of Reference

January 2023

Section VII - Scope of Purchaser’s Requirements

Table of Contents

I. DESCRIPTION OF THE SCOPE OF WORK

Introduction

1. Project Background

The background to this assignment provides necessary context and perspective for the bidders to understand the purpose and importance of this assignment for the Government of Commonwealth of Dominica (GoCD). This is described as under.

Sitting halfway along the Eastern Caribbean archipelago, Dominica is located just a few miles from Martinique to the south and Guadeloupe to the north. Stretching 751 km² (290 square miles), Dominica boasts 148 km (91 miles) of coastal line. Dominica's official name is the 'Commonwealth of Dominica,' which is mostly referenced in official communications and to further distinguish the island from the Dominican Republic, its northerly Caribbean sister. Dominica is the most northerly of the Windward Islands grouping.

The Government of the Commonwealth of Dominica (GoCD), after Hurricane Maria in September 2017, has instituted resilience as a central theme to the country's rebuilding efforts and socioeconomic development plans, with the aim to make Dominica the first climate resilient country in the world. The hurricane resulted in losses and damages of over 200 percent of GDP, with the telecom sector alone suffering over US$40 million in losses and damages. Furthermore, the GoCD lost data and records and suffered losses beyond its infrastructure, highlighting the need to make the government more resilient so that it can better prepare for and respond to incidents and restore operations and services quickly.

The Government recognizes the role digital technologies and solutions can play in strengthening the island and its inhabitants' climate resilience, as well as the importance of integration with the global digital economy to expand markets and drive sustainability of businesses, government, and individuals. In view of this it has formulated the digital strategy viz. "Dynamic Dominica" which gives emphasis to establish an integrated, interoperable and resilient digital infrastructure and service delivery platform for the government, citizens and business to deliver various services.

The GoCD's recovery and resilience building efforts include development of a Government Wide Area Network, and nodal digital infrastructure to lay the foundations for digitization of government. The GoCD has engaged in a partnership with Digicel Dominica Ltd. to connect all government service locations (Government offices, schools, hospitals, and health centers) to high-speed connectivity delivered using fiber optic networks. The network, being developed under the partnership, will provide multiple layers of redundant connectivity—underground and overhead fiber, microwave, and satellite at key locations—in addition to cloud services to host Government data and services. The government connectivity project includes development of a primary data center to host the government cloud and applications, as well as a secondary location to serve as a backup site.

The improved connectivity can be leveraged to develop digital government services and increase the level of digitization of government operations, which is currently lagging. Currently Dominica lacks the enablers of digital government, including an enterprise architecture, interoperability framework, identification, and authentication, but has a recently built limited government payment portal. Uniquely and securely identifying residents through a digital ID is fundamental to enable access to digital services, both public and private, but the current ID ecosystem in Dominica is fragmented and not interconnected. In order to fully utilize and benefit from investments in cross-cutting enablers and specific digital government services, there is also a need for legal and regulatory reforms across key areas of the digital economy. These enabling environment improvements are a key first step towards removing roadblocks to improved adoption of digital services among individuals and businesses, as well as contributing to the development of digital applications and services by emerging entrepreneurs in Dominica.

The Caribbean Digital Transformation Project (CARDTP or the Project) is funded through the World Bank and aims to enhance the use of technology in the public sector as well as the private sector to conduct business transactions, build a robust and resilient IT infrastructure and to develop modern platforms to facilitate and enhance these business transactions. The development objectives are to contribute to increased access to digital connectivity, digital public services and the creation of technology enabled businesses and jobs in Dominica.

National-level activities are financed from an IDA credit to Dominica in the amount of SDR20,500,000 (equivalent to US$28.0 million). The CARDTP comprises four components that address key bottlenecks and harness opportunities to develop the Eastern Caribbean Digital Economy as a driver of growth, job creation and improved service delivery.

The Program is also financed through a regional IDA grant and implemented by a regional Project Implementation Unit (RPIU) housed at the Organisation of Eastern Caribbean States (OECS). RPIU will work with other regional institution stakeholders as relevant depending on the technical area being supported. Regionally implemented activities will focus on strengthening the enabling environment to promote investment, competition, and innovation in telecoms and digital financial services, regional cybersecurity collaboration, and a modernized and harmonized data protection and privacy regime across the region. It will also be complemented by a regional level advanced digital skills program open to high potential digital specialists from Dominica.

It aims to ensure that every individual and business in Dominica is empowered with the access to broadband, digital financial services, and skills needed to actively participate in an increasingly digital marketplace and society. It leverages public sector modernization and digitization to improve service delivery and to drive creation of a digital culture across Dominica.

To support the improved management of digital risks, the project shall bolster cybersecurity policy, capacity, and planning tools in the region. It will facilitate technology adoption to improve productivity of flagship industries and create demand for digitally enabled jobs. It aims to foster regional integration and cooperation to capture the economies of scale and scope required to increase impact and value for money of the project interventions and to create a more competitive, seamless regional digital market to attract investment and provide room for growth of digital firms.

2. Project Components

A brief description of the project components is as follows:

1. Component 1: Digital Enabling Environment

This component shall support the development of a positive enabling environment for Dominica's digital economy that drives competition, investment and innovation while promoting trust and security of online transactions. It will focus on legal, regulatory and institutional reforms consistent with global best practice to support modernization of the telecommunications and digital financial services sectors while mitigating growing risks of a digital economy including cybersecurity and data protection and privacy.

1.1 -Telecommunications: Legal and Regulatory Environment, Institutions and Capacity Support

1.2 - Digital Financial Services: Legal and Regulatory Environment, Institutions, and Capacity

1.3 -Cybersecurity, Data Protection and Privacy: Legal and Regulatory Environment, Institutions and Capacity Support

2. Component 2: Digital Government Infrastructure, Platforms and Services

This component shall support public sector modernization, resilience and delivery of digital public services to individuals and businesses. It will aim to ensure that Dominica has put in place the core infrastructure, platforms, institutions and human capacity needed to efficiently and effectively manage internal government operations, and to build on these core enablers to make public services widely accessible online from anywhere within the country, region or across the globe. It will also prepare Dominica's government for deeper interconnectivity and interoperability of data and information systems across borders to smooth administration of regional trade, immigration and other services. Finally, it will aim to ensure continuity of government operations and services, enable real-time data driven decision making and ability to rapidly target and deliver payments and social services to citizens and businesses in the event of natural or man-made disasters.

2.1 – Development of Cross-Cutting Enablers (or Service Oriented Architectures) of Digital Government Operations and Services

2.2 - Government Productivity Platforms and Citizen-Centric Digital Services

3. Component 3: Digital Skills and Technology Adoption

This component aims to better equip individuals and businesses in Dominica for the jobs and economy of the future and to spur innovation and productivity growth. It aims to create a pool of advanced digital talent to better position Dominica to attract investment by digital firms. It takes a comprehensive supply and demand side approach, supporting greater technology adoption and utilization of digitally enabled business models to drive demand for newly skilled employees and well as making connections with global employment opportunities through online working platforms.

3.1 - Workforce-Ready Digital Skills

3.2 - Technology Adoption

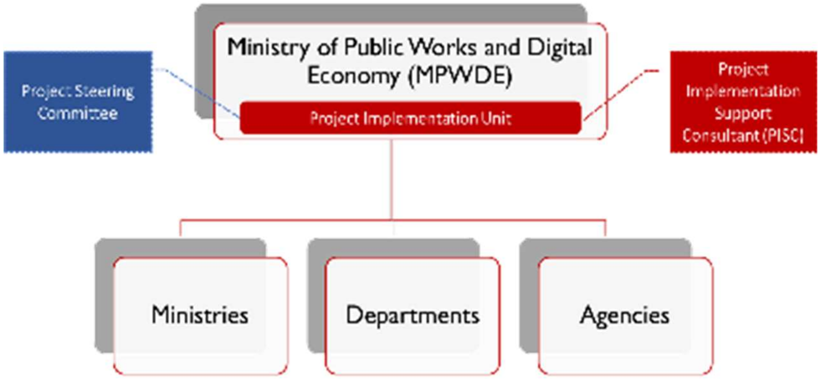
4. Component 4: Project Implementation Support

This component includes support to the Project Implementation Unit (PIU) for the implementation and management of national level project activities, including for staffing of the PIU, capacity building and training initiatives as well as recruitment of a technical advisory and implementation support firm. Key technical functions to be supported can include but will not be limited to project manager, technical specialists, procurement specialists, financial management specialist, environmental and social safeguards specialists, monitoring and evaluation and communications.

II. INSTITUTIONAL ARRANGEMENTS

The Project is being implemented by the Project Implementation Unit (PIU) that is housed in and falls under the Ministry of Public Works and the Digital Economy (MPWDE or the Client) oversight. The PIU is responsible for the overall implementation of the Project with emphasis on reporting and monitoring and evaluation, financial management, contracts management, safeguards oversight, and procurement.

The PIU reports to the Project Steering Committee (PSC) for the lifetime of the Project. PSC is responsible for coordinating and managing all the technical aspects of the Project, facilitating inter-ministerial coordination, and implementing digital initiatives across the various Ministries, Departments and Agencies (MDAs) of the GoCD. The PIU shall support development of key policies and regulations and inter-agency coordination to enable consensus building together with other key agencies like the ICT Unit and the Digital Transformation Unit of the GoCD. Core technical responsibilities include adoption of digital technologies, effective coordination of departmental information system development and implementation. The PSC will


Project Steering Committee
Ministry of Public Works and Digital Economy (MPWDE)
Project Implementation Unit
Project Implementation Support Consultant (PISC)
Ministries
Departments
Agencies

determine if technical committees are required for policy formulation and convene such committees as necessary (i.e., for Cybersecurity, Data Protection and Privacy, Service Delivery, e-Payments, Digital Identity, Interoperability, etc.).

The PIU is also responsible for promoting change management practices, stakeholder engagement and development and delivery of effective programs for digital Government skills enhancement, knowledge exchange and awareness-raising. For the purpose of better coordination and effective and efficient implementation of all Project activities, focal points at MDAs have been established.

Ad-hoc bid evaluation / selection committees are established in consultation with MoPWDE and MDAs and generally consists of 3-5 qualified members each who are normally the Procurement Officer and experts delegated by respective MDAs depending on the required expertise and the procurement scope and complexity.

Under this project, PIU has engaged an Implementation Support Firm as Project Implementation Support Consultant (PISC) largely to address the Component-4 of the project. The PISC supports the PIU in carrying out on-the-ground and remote day-to-day activities to ensure the Project Objectives are achieved in the most efficient, cost-effective and well-coordinated manner. The institutional arrangement is illustrated as above;

The MPWDE has decided to engage a competent and competitive Consultancy Firm ("the Consultant") to support the PIU for conducting a comprehensive system study and perform Business Process Reengineering (BPR) of existing Information Technology (IT) landscape in Dominica for implementing an integrated and interoperable Digital Solution for delivering public as well as other services to the citizens and business at-large.

III. OBJECTIVES

The objectives defined for performing the BPR study for this assignment are described as follows:

Objectives	Description
Objective-1: "As-Is Study"	1.1. To Conduct a comprehensive As-Is study of current IT state including but not limited to; a. Identify the current business/technical roadblocks based on the strategic and business plan and articulate the **problem statements** that the GoCD must overcome to achieve complete digitization b. evaluate the current state of **people, process, technology, resources and security** c. assess the integration/ interfacing between the current/legacy system and new solutions

Objectives	Description
	d. conduct process mapping of the current processes as per the current & future business rules and policies e. Identify the risks, and constraints affecting implementation process
Objective-2: “To-Be Scenario”	1.1 To design the To-Be scenarios and processes based on the As-Is in context to Dominica including but not limited to the provisioning of; a. To-Be processes based on Value Add/Non-Value Add (VA/NVA) analysis. b. Business Process Reengineering (BPR) of the digital service delivery forms based on To-Be. c. Define architecture for including but not limited to; • Interoperable Enterprise Service Bus (ESB) platform Single-Sign-On (SSO) authentication platform using Unique Identifier (UID)/E-Mail/Mobile number with 2-factor/multi/biometric validation. • Artificial Intelligence (AI) engine for intelligent service delivery. • Big data analysis engine to support policy level decision making process. d. Preform Gap Analysis between the As-Is and To-Be State. e. Provide Cost-Benefit analysis of the To-Be solution proposed in terms of Return on Investment (RoI). f. The To-Be should focus on functionality for license free (or perpetual license based) technologies for easy and flexible sustainability. g. The proposed solutions should be aligned to internationally recognized best practices as well as the expected change management, IT infrastructure upgrades, Business processes, Policies and SoP (Standard Operational Procedures) should be determined to facilitate the implementation.
Objective-3: “FRS & SRS identification”	4.1 To perform requirement analysis of the core areas, including but not limited to the: a. Functional and Non-Functional Requirement Specifications (FRS and Non-FRS) of the To-Be scenario. b. Use Cases based on the FRS and Non-FRS. c. Software Requirement Specification (SRS). d. Bill of Material (BoM) based on the Gap Analysis, FRS and Non-FRS and SRS.
Objective-4:	4.1 To develop Enterprise Architecture (EA) for, including but not limited to the:

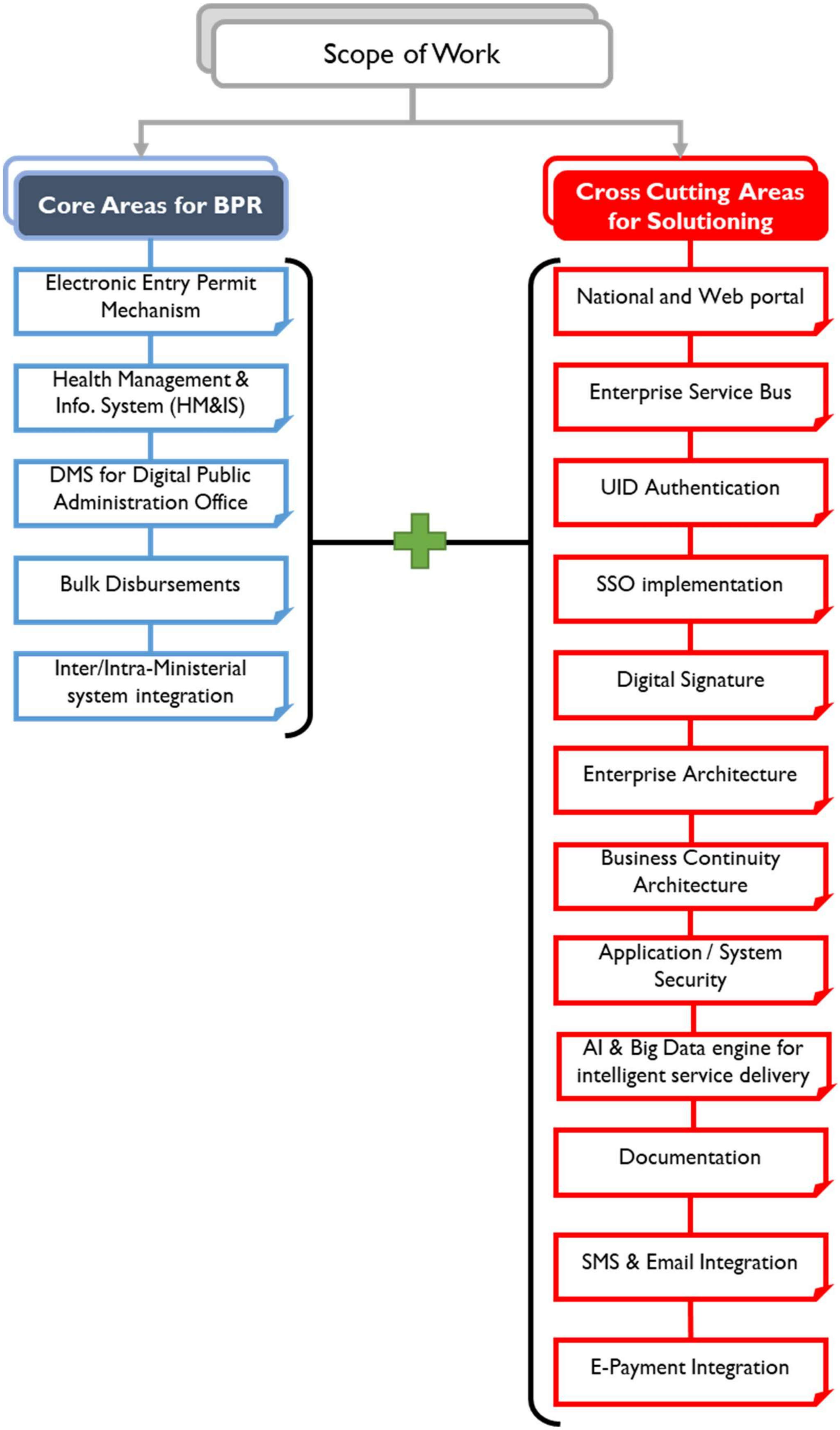
Objectives	Description
"EA Development"	a. Business Architecture. b. Information System (Application & Data) Architecture. c. Technology Architecture. d. Migration Architecture. e. Governance Architecture. f. Enterprise Security Architecture. g. Architecture Change/Requirement Management.
Objective-5: "Development of Guidelines"	5.1 To prepare documents for serving as guidelines for PIU including but not limited to: a. Operation and Maintenance (O&M) guidelines for the To-Be solution. This O&M guideline document shall be used by the PIU and the implementation partner after selection as a minimum standard to be followed during O&M. b. Guidelines for Business Continuity (BC) and Disaster Recovery (DR) . c. Guidelines for Change Management & Capacity Building arising due to the implementation of the new To-Be solution. d. Guidelines for implementation of the initiatives in phased approach along with the costing. e. Terms of Reference (ToR) for RFP for the core areas for the selection of the System Integrator for implementing the solution and performing O&M of the deployed solution. f. Guidelines for application as well as web and mobile portal development.

IV. SCOPE OF WORK

As a part of its digital strategy, the Government of the Commonwealth of Dominica (GoCD) is committed to provide public services online with **interconnectivity** and **interoperability** of data and information systems for smooth **accessibility**. The prime aim of this is to ensure **continuity** for resilient government operations and services, enable real-time data driven decision making, and ability to rapidly target and deliver payments and social services to citizens and businesses in the event of disasters.

In view of the above, this EoI seeks to capture the interest of a Consultant to carry out the comprehensive BPR and design a solution that is interconnected, interoperable, accessible, and available to the government, citizens and the business at large.

The Scope of Work (SoW) for the consultant to achieve the objectives for the Consultant is organized in two categories as shown in the figure below;


Scope of Work
Core Areas for BPR
Electronic Entry Permit Mechanism
Health Management & Info. System (HM&IS)
DMS for Digital Public Administration Office
Bulk Disbursements
Inter/Intra-Ministerial system integration
Cross Cutting Areas for Solutioning
National and Web portal
Enterprise Service Bus
UID Authentication
SSO implementation
Digital Signature
Enterprise Architecture
Business Continuity Architecture
Application / System Security
AI & Big Data engine for intelligent service delivery
Documentation
SMS & Email Integration
E-Payment Integration

4.1. Brief Description of the Core areas for BPR

The Consultant shall perform the comprehensive BPR activities for the following core areas to achieve the objective defined in section-III. The below description is for basic understanding of the scope & expertise that is needed for executing the assignment. The Consultant's detailed study shall include the modules/functionalities, etc. for the envisaged applications in consultations with relevant stakeholders and PIU's signoff. These core areas are:

(a) **Electronic Entry Permit Mechanism (e-Entry)**

The Ministry of National Security and Home Affairs is responsible for performing immigration matters at two (2) airports, six (6) sea-ports including one (1) ferry port, two (2) cargo port, one (1) port with no custom terminal, and one (1) fishing port. Further, the GoCD has plans to have an international airport and additional seaports which shall also be taken into consideration during study.

The Ministry of National Security and Home Affairs desires to automate its airports and sea ports to facilitate the ease of arrival and departure of individuals in Dominica by implementing an e-Entry mechanism and immigration kiosks at all ports of entry. The policies, legislation and regulations related to the implementation of e-Entry is already being reviewed.

It is desired that end-to-end BPR, as per the objectives defined in section-III, of the immigration process shall be carried out to create a single window for all the immigration services along with the interoperability with the legacy/existing systems like Advance Passenger System (APS) for the passengers travelling through vessels, Travel Management Information System (TIMS), Border Control System (BCS) and others for faster movement of cargo and passengers.

(b) Health Management System / Health Management Information System (HMS/HMIS)

The Ministry of Health, Wellness and New Health Investment is the Executing Agency (EA) for the digitization in the health sector. The EA desires to implement fully functional Health Management & Information System (HM&IS) in its Government Hospitals, Health Centers. The HM&IS interface shall also be extended to all private hospitals and private practitioners to access the Electronic Health Records (EHR).

A review and update of legislation and policies relevant to digitization of health information and administration is already in process.

The Pan American Health Organization (PAHO) has taken up an initiative for piloting telemedicine in a government hospital in Dominica. Regarding this, it has conducted a rapid assessment of IT readiness according to which except for few digital infrastructures like internet connectivity etc. other digital aspects like organization, processes, human resource, regulatory matters, etc. are just above the maturity level one (1).

Based on above insights and looking at COVID-19 scenario, implementation of fully functional integrated and interoperable HM&IS is highly desirable. In this regard, the Consultant shall take up the comprehensive BPR study, as per the objectives defined in section-III, to identify HM&IS modules based on the consultations with EA and draw up fully function HM&IS system. The solution shall also align to meet the metrices defined in Project Development Objective (PDO) and Intermediate Results Indicators (Annexures 1 and 2 respectively).

(c) DMS for Digital Public Administration Office (e-Office)

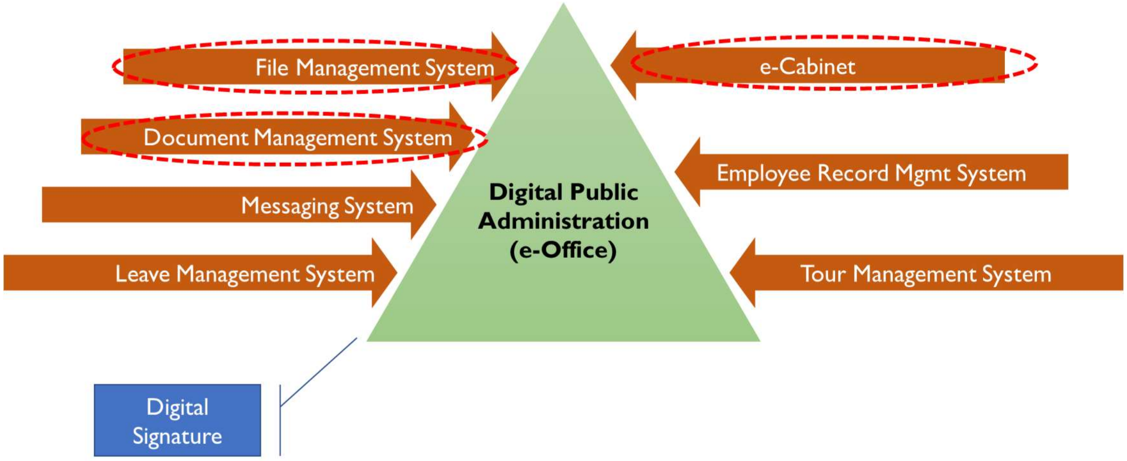
Digital Strategy of Dominica emphasize the digitalization of the public administration from paper based to electronic based system to make the public administration efficient and resilient. In view of this, GoCD is keen to establish electronic workflow-based Document Management System (DMS) to transform Public Administration/Government Office into a digital office (e-Office).

Towards this, GoCD implemented licensed based Document Management and Content Management System from “Questys Solutions”. This application can scan paper documents, import electronic files and email, then Optical Character Recognition (OCR), edit, and store the information in electronic format. The users can create, search and retrieve everything from a desk, from across town, or from the other side of the world. Outputting what is found is easy, too: Just print, fax, email or export information in just a couple of clicks. Currently, due to some licensing matter the application is limited to some basic use only. The Questys Solution was integrated with SMARTSTREAM for provision of the employee Number that is generated from SMARTSTREAM which is a license based financial transaction management solution. Besides this, GoCD implemented a Human Resource Management System that records employee details including hires, transfers, terminations.

These individualistic initiatives did not serve the purpose of a resilient, fully integrated, and automated public administration office. Considering this GoCD is keen to implement full functional e-Office platform with following characteristics;

- Streamline the transmission process of official documents between government organizations.
- Provide an efficient mechanism to track the progress of any transmitted documents or processes that require proper action, or their deadline imposed on task.
- Provide digital repository that can keep all correspondences, paperwork, documents, etc. digitized and archived which can be accessed and used at any time from any organization.
- Support search engine that enables users to look for a particular document as part of document management system.
- Manages leaves, appraisal, tours, employee record, etc.
- Manages Cabinet questions and matters

Following are the priorities encircled in dotted red and brief definitions of the modules for the e-office platform;



i. **e-Cabinet:** This module automates the cabinet affairs like providing all relevant functionalities of cabinet like Pre-Meeting process of circulating volumes of papers, manual, etc. Post-Meeting process, electronic records of agendas and minutes. Helps the Permanent Secretaries and the designated officers only to circulate messages and other confidential information pertaining to Cabinet matters. Following are the highlights of the key e-Cabinet processes including but not limited to;

A. Cabinet Pre and Post Meetings Processes

Pre-Meeting Processes

The pre meeting processes involve the circulation of large volumes of paper to the Ministers with associated manual effort. In addition, the absence of integrated electronic systems results in duplication where data has to be captured electronically on a number of occasions, for example preparing briefings and agendas.

Post Meeting Processes

The current post meeting processes involve the preparation and circulation of volumes of paper associated with decisions, as well as manual compilation of the minutes.

Paper Based

Most of the processes within the Office of the Prime Minister and the Cabinet Secretariat are paper based resulting in large volumes of paper or data circulating in and out of the Office of the Prime Minister. The minutes and agendas are circulated manually for meetings with considerable time and effort involved. The meetings are also paper based with Ministers bringing on average 25 or less sheets of paper to the weekly meetings.

Room for increased efficiencies in the process

The content contained in the agendas forms the basis of many other documents – decisions, briefing notes, and minutes. Because of the absence of integrated systems, the content is rekeyed, or at best, partially cut and re-pasted, to construct the main content of the decisions. The elimination of this duplication of effort would improve process efficiencies.

Search and Retrieval Issues

There are electronic records of agendas and minutes; however, the main filing of all Cabinet documents is paper based. There is a drawback to this in that it can be time consuming for search and retrieval of related documents as well as hindering opportunities for cross referencing of associated documents and cabinet decisions.

Proposed Cabinet Meeting: The Cabinet meeting vision is described as follows:

- Each Minister/Cabinet Member will have his/her own touch screen device from which he or she will be able to access all relevant documentation. There will also be a central monitor displaying the agenda items under discussion at any particular time.
- The agenda and supporting documents will be available on screen for each Minister. Ministers will be able to bring substantially less paper to the meeting or dispense with paper entirely.
- Any agenda items and their supporting documents or extracts a Minister may wish to have in hard copy can also be printed for him or her in the Cabinet environment.
- An integrated e-mail facility will enable Ministers to receive (and reply to) urgent messages while a meeting is in progress.
- Where a sponsoring ministry provides a presentation to support an agenda item, this can be accessed via the minister’s device or on the main screen which follows the progress of the meeting displaying the item currently under consideration.
- Minutes will be automatically constructed and stored electronically. The option to print minutes will continue to be provided for archival and related purposes is always available.

The e-Cabinet shall have features including but not limited to;

- Access meeting materials on any device
- Review meetings and documents securely – both online and offline
- Annotate directly in meetings with both private and shared annotations
- Sign documents securely with eSignature

- Communicate securely with individual ministers or a group with the Conversations feature
- Securely cast your vote through the application for both meetings and resolutions
- Schedule meetings easily with automatic invitations and notifications
- Collate and distribute meeting packs including last-minute updates with a single click
- Automatically generate draft meeting minutes for further customization and finalization
- Track and manage action items
- Export meeting packs as a PDF for distribution and archiving
- Set fine-grained permission controls within the in-house Document Library at a folder, sub-folder and individual document level
- Send notifications to agenda contributors with important details
- Review rooms allow you to work with colleagues to approve documents before they go into the meeting pack

ii. **File Management System (eFile):** This module automates the processing of files and receipts. This includes creation of files (electronic and physical both kind of files), movement of files in the workflow, tracking of files and their management. The Workflow Automation should be built at enterprise level business process management and workflow automation that automatically routes the documents to their destination. The workflow automation should provide the following:

- Rule based processing incoming & outgoing documents and internal memos,
- Configured multi-level approvals
- Automatic creation of records based on documents
- Update records based on documents and
- Documents routing algorithm

iii. **Document Management System (DMS):** This module acts as a centralized repository of various documents such as acts, policies, and guidelines. It enables the functionalities for uploading, indexing, searching, and retrieving digital files for the Government. The indexing functionality must include the following features:

- Indexing of all documents
- Custom automatic document numbering
- Content recognition and indexing
- Indexing meta data

- Support innumerable formats
- Extendable meta data fields

iv. **Dashboard:** In this module should have a simplified and easy to navigate user dashboard which contains;

- Workflow inbox
- Documents inbox
- Alerts and notifications
- Report graphs and charts
- Inbuilt calendar and time.

The other modules that may require integration or inclusion as per the priorities set by GoCD are;

i. **Messaging System:** This enables internal collaboration and messaging. Currently, GoCD uses Microsoft Exchange for internal as well as external messaging.

ii. **Leave Management System (eLeave):** This automates the leave application and approval process. Currently, GoCD manages leaves using its Human Resource Management System (HRMS). The Consultant during its BPR study may determine the feasibility of integrating the existing application or to develop new modules with enhanced functionality.

iii. **Tour Management System (eTour):** This automates employee tour programs. Based on the discussions the Consultant may need to perform BPR as per the objectives defined in section-III

iv. **Employee Record Management System (e-Employee):** This module manages the employee service book, annual appraisals, etc. Some of the functionalities of this module is already build in the HRMS system build by GoCD. The Consultant during its BPR study may determine the feasibility of integrating the existing application or to develop new modules with enhanced functionality.

The DMS shall be implemented across **all the Ministries, Departments, Agencies (MDA) and attached government offices of Dominica**. The Consultant shall conduct detailed BPR study in consultation with EA to identify modules as per the **priorities**. The Consultant shall also identify the integration feasibility of the existing applications as well as Digital Signature as described above. Security is one of the most critical aspects of a document management system. This module should provide a high level of documents encryption and role-based access, as well as;

- User and Role-based access with encryption
- Audit trail,
- Advanced access rights
- Encrypted documents on file system
- Modify ownership and Support SSL

(d) Bulk Disbursements:

GoCD desires to digitize recurring government bulk disbursement streams, including government to citizen, government to business, and vice versa. This activity aims to include technology/distribution choice (cards, wallets, hybrid models) and upgrade financial infrastructure (payment settlement), operational considerations, policy modifications, and monitoring and evaluation to carry out the cash-based social transfers including salaries and other disbursements. It is expected that the consultant shall perform detailed study with the Ministries, Departments and Agencies (MDA) responsible for such cash-based transfers and design the disbursement and management module to perform bulk disbursements.

The Consultant shall also take into consideration cyber incidents, tampering and impersonation in digital communications that can negatively affect organizations, users' privacy and other fundamental rights and should ensure that there is interoperability with Government and external systems. The Consultants should comply with regulations and procedures of international and national authorities regarding the COVID-19 emergency.

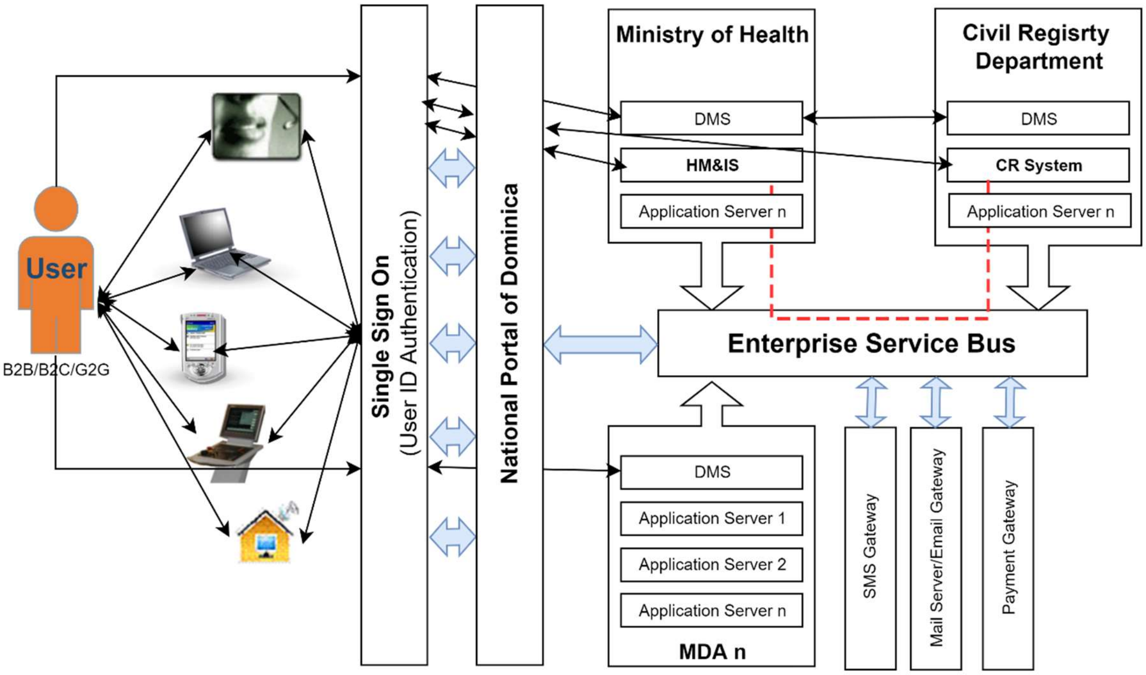
(e) Inter/Intra-Ministerial system integration

Considering the complexity of the assignment and expectation to have an integrated, interoperable and accessible digital solution for delivering above services, it is expected that the Consultant shall carry out the BPR for the MDAs that are directly or indirectly involved in delivering the services. For example, the bulk disbursement under various social schemes may encompass multiple MDAs, in that case it is expected the Consultant may take-up the necessary BPR, as required, in all those MDAs to integrate with the disbursement and management module. The Consultant;

- Must provide system integration service with the various e-service streams within the government sector to ensure that the solution is properly architected end to end to deliver a successful implementation.
- Must ensure the service delivery based on requirement from cross-functional e-service team of various government agencies with development of integrated business processes, implementing project deliverables, with an emphasis on quality, productivity, and consistency.
- Provide technical direction and control of internal and external teams and provide a framework for project planning, communication, reporting and contractual activity.
- Provide required coordination between internal and external agencies for service delivery.

4.2. Brief description of the cross-cutting areas for solutioning

The prime objective of the assignment is to develop a resilient, integrated, interoperable and accessible solution for the government, citizen, and business at large. The high-level architecture as envisaged illustrates interlinking of the cross-cutting areas as described below;



(a) National web and mobile portal

National portal of a Country is the interface to the world and now it is one of the means to showcase the Country's economic and social progression. GoCD is keen to have a national web and mobile portal that meets international standards for its content and dynamism. One of the indicators towards this is UN e-Government Development Index (eGDI) which based on predefined criterions determines the ranking of the Country towards the adoption of e-Government initiatives in the Country. The BPR study must identify the criterions and structure its study in way that the solution designed must fulfill the eGDI criterions.

GoCD has established various portals for information as well as delivery of various services. These portals are largely static with no backend integration. There are efforts especially for the e-payments of few services like COVID test, Work Permit, etc. but this up to the payment and printing of receipt with no backend integration. The e-Payment portal can be accessed using https://epayment.dominica.gov.dm .

Currently, the portal www.dominica.gov.dm serves as the National portal. It provides links to the various Ministries, Department, services and other information. It is expected that this portal may be further developed as National Portal and serve as a single window for accessing the information, services, payments, etc.

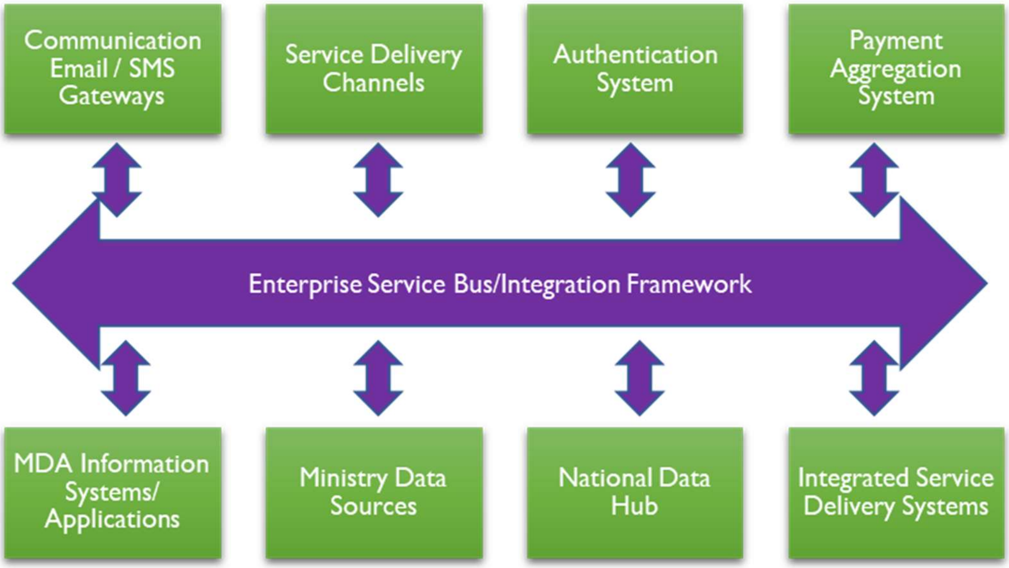
In addition to the web portal, it is also desired to have a mobile portal to add accessibility to government services. Also, the GoCD is expected to have mobile apps for key applications on android as well as iOS platforms.

The BPR for the portal and mobile applications may be carried out to achieve minimum indicative performance standards and response times for each of the following items

Item	**Performance Standard / Response Times**
Screen Navigation: field-to-field	< 5 milliseconds
Screen Navigation: screen-to-screen	< 3 seconds
Screen Refresh	< 2 seconds
Screen list box, combo box	< 2 seconds
Screen grid – 25 rows, 10 columns	< 3 seconds
Report preview – (all reports) – initial page view (if asynchronous)	< 60 seconds in most instances. It is understood that complicated / large volume reports may require a longer period
Simple search – single table, 5 fields, 3 conditions – without screen rendering	< 3 seconds for 100,000 rows
Complex search – multiple joined table (5), 10 fields, 3 conditions – without screen rendering	< 5 seconds for 100,000 rows
Server-side validations / computations	< 2 milliseconds
Client-side validations / computations	< 1 millisecond
Loading pages	< 3 seconds
Saving a record	< 5 seconds
Batch processing per 100 records	< 120 seconds
Login, authentication, and verification	< 5 seconds
Daily backups – maximum duration	4 hours (on-line preferred)
Total Restore – maximum duration	8 hours

(b) Enterprise Service Bus/Integration Framework

Towards its expectation of an integrated, interoperable and accessible digital solution for delivering above services, GoCD intends to implement an Enterprise Service Bus (ESB) & API Gateway/middleware messaging component as a **crucial integration framework required** to connect the services offered by various MDAs to provide a seamless integrated environment to the consumers (citizens and residents). This will also lay the foundation for flexible technology stack needed to support current/future integrations with features such as Service Development, Service registry, Service Orchestration, Service policy enforcement for SLAs and Service Monitoring. High level architecture as envisaged is illustrated below;


Communication Email / SMS Gateways
Service Delivery Channels
Authentication System
Payment Aggregation System
Enterprise Service Bus/Integration Framework
MDA Information Systems/ Applications
Ministry Data Sources
National Data Hub
Integrated Service Delivery Systems

The consultant shall carry out a comprehensive BPR study to draw out Enterprise Integration Architecture and Technical Design Document for implementation of the ESB and API gateway/middleware as information system integration framework exhibiting, at a high level, with the following features:

- Allow for seamless integration of existing technology/application systems and establish technology platform for future enterprise integrations.
- Supporting reliable messaging – Validation, Transformation and Secure delivery of the messages with synchronous/asynchronous invocations.
- Transaction support: Compensation and rollback of committed service requests (transaction support in composite services). Support for rule-based, atomic and process-driven transactions.
- Security of services: Authentication mechanism (LDAP, OpenID, SSO etc.), role-based authorization (OAUTH with JWT token), payload encryption (HSM/Public key).
- The E-Service Bus must support HTTP, HTTPS, Web Socket, POP, IMAP, SMTP and other standard Transport Protocol.
- Must be able to integrate with Payments Gateway, CRM, ERP and any other legacy system as required.
- Must provide message formats and protocol like JSON, XML and SOAP.
- Must have the capabilities to connect with other Enterprise Messaging System, like, MSMQ, Oracle AQ or IBM WebSphere MQ.
- Must be able to connect with any data store like RDBMS, CSV, Excel, ODS, Cassandra, Google Spreadsheets, etc.

- Build services based composite applications and provide support for developing all related service components of Design principles – Service contracts; Loose Coupling; Abstraction; Reusability; Autonomy; Statelessness; Discoverability; Composability o Separation of Concerns of Service Orchestration o Policy Definition, Management and Enforcement.
- High performance, scalability – HA and DR.
- Hybrid Setup (On-Premises and Cloud) with capability to scale out on cloud.
- Supports integration with multiple product connectors like Microsoft Dynamics.
- Supports service level monitoring, auditing for data access and configuration changes, fault detection, root-cause analysis, reporting and historical analysis.
- Must enable various MDAs components to consume functionality implemented in services while being oblivious of the technical details of the components involved. As far as any component is concerned, it is exchanging messages only with the ESB, as if the ESB itself was the provider/consumer of the services.
- The ESB must help to bridge the gaps between the provider and consumer in terms of connectivity and messaging format requirements. The ESB should perform the core functions at the message level to implement service transparency, and thus achieves a service-oriented architecture. The core functions include but not limited to:
    - Providing virtual endpoints
    - Routing requests
    - Transforming messages
    - Translating protocols
    - Orchestrating services
- The ESB or the Integration framework should offers integration, or composite services while using distinct routing, translation, and transformation services to support the disparate GoCD data sources and consumers could violate the loose coupling concept of SOA. That is, one message routed from a provider to a consumer may require a different transformation than another message routed between the provider and consumer, while routing the same message to a different consumer may require different protocol. Instead of creating unique services with specific features to support each instance,
- The ESB or the Integration framework should enable the components to perform a range of small, useful, flexible operations between a consumer and a service provider. Typically, component services implement Enterprise Integration Patterns (EIP) independent of the service descriptions (WSDL and others). Using the EIPs, developers combine business applications (consumers and

service providers) into a composite service. EIP components should include but not limited to:

- Pipe patterns—a single event triggers a sequence of processing steps, each performing a specific function. The EIP component sequences the calls.
- Content based router patterns—the EIP component examines the message content and routes the message onto a different channel, based on data contained in the message.
- Message dispatcher patterns—the EIP component sends the message to a list of service providers (multipoint).
- Scatter gather patterns—the EIP component routes a request message to several service providers, and then aggregates the responses into a single response message.

- The ESB or the Integration framework architecture and components must comply with the following standards:
  - The ESB will serve as the infrastructure to the integration hub.
    - All enterprise services will be exposed through the Integration hub. The ESB provides the infrastructure to the Integration hub and facilitates web services, ETL and MFT (Managed File Transfer) services. Different business and data services across the enterprise will be exposed through the integration hub using the ESB.
    - Direct calls to services exposed through an application server are explicitly discouraged and require enterprise architecture approval with specific reasons why the integration hub and the ESB cannot be used.
  - All enterprise services may expose both a REST and SOAP interface.
    - Proxy services exposed through the ESB may expose both a REST and SOAP interface.
  - The GoCD ITIL framework will govern all enterprise services.
    - All enterprise services exposed outside GoCD via the ESB will managed within the Enterprise Service Catalog and configuration management database and delivered in alignment with ITIL Service Operations processes standards.
  - The service level agreement will dictate the ESB service commitment.
    - Service level agreements will be established for each business and data service according to the design of the service. Information technology (IT) service management tools use these

services level agreements to monitor performance according to the IT Infrastructure Library (ITIL) policies.

- API and Service Management: For system-to-system communication it will be necessary to provide combined easy and managed API access with full API governance and analysis:
  - System should have the ability to publish APIs/Services to a selected set of gateways in a multi-gateway environment
  - System should support enforcement of government and system policies for actions like
  - API/Service subscriptions, application creation, etc., via customizable workflows
  - Manage API/Service visibility and restrict access to specific agencies or systems
  - Manage API/Service lifecycle
  - Ensure API/Service security by restricting API access tokens to domain/IPs, validating APIs payload contents against a schema, applying security policies to APIs authentication and authorization and provide threat protection, bot detection and token- fraud detection
  - System should generate JSON web tokens for consumption by back-end servers
  - System should provide developer portal to search APIs by provider, to provision the API keys, subscribe API, notification for new version of subscribed APIs and view of the API consumer analytics.
  - System should have proper capabilities to manage and scale API traffic and enforces rate limiting and dynamic throttling based on usage quotas and bandwidth quotas.
  - System should be horizontally scalable with easy deployment into cluster using proven routing infrastructure
  - System should have high performance pass-through message routing with minimal latency
  - System should provide a pluggable analytics framework for API usage, like, requests, responses, faults, throttling, subscriptions etc.
  - System should track consumer analytics per API, per API version, per tiers and per consumers
  - System should have configuration payment schemes to monetize API usage

  - ▪ System should monitor SLA compliance for the API
  - ▪ System should have the capability to do the required integration with SSO System

- The following are critical aspects should be considered during the study for the successful implementation of the ESB or the Integration framework in the GoCD:

  - Authentication and authorization
  - High availability and load balancing
  - Process logging and error logging
  - Exception handling
  - Monitoring and tracking

(c) Unique Digital Identifier and Authentication Platform

GoCD intends to develop an identification and authentication platform unique digital identifier that builds on previous efforts around the development of a regionally-standardized identifier – the Unique ID (UID) number. This platform will be used across GoCD for authentication and delivery of digital public services. It is envisioned that this UID system will be available to all the residents of Dominica for a greater unique identification across all of society.

The use of UID number will enable the backend integration of various identification registries in the country (and possibly the rest of the OECS), and when combined with an authentication layer and payment platform to facilitate digital public service delivery while maintaining privacy of individuals' data.

The Ministry of National Security and Home Affairs is responsible for the UID System and the authentication platform that will include the following specific tasks:

(i) legal and regulatory review and assessment and recommendations on necessary reforms to implement an integrated ID system and authentication platform. This task is part of this assignment;
(ii) assignment of the MPID numbering system based UIN to individuals on a foundational ID registry (civil registry, as currently agreed);
(iii) development of a digital authentication layer to access digital government services and linked with currently accepted forms of ID; and
(iv) design and rollout of a new physical ID card (national ID).

The consultant shall carryout the comprehensive BPR to draw out the linkage between services and UID as well as authentication of the user for the delivery of the services.

(d) Single Sign-On (SSO)

GoCD towards the increased user adoption of e-Services desires to implement a Single Sign-On (SSO) platform that allows users to access all e-Services without having to log in separately for each service which mean it will allow the same username and password to be used across many generic modules and Apps. The SSO shall be a single, trusted, secure, scalable and multi factor user authentication for all the e-Services offered by the Government and Businesses through multiple channels.

Understanding this, the following key business requirements are envisaged;

- User Registration: To provide one time registration for all categories of Users i.e., Citizens/Residents, Business entities, Government entities and Visitors
- Authentication Mechanisms: To provide multiple authentication mechanisms i.e., Username/password, Smart Cards, Biometric, Digital Certificates.
- Login Anomalies: To track user activities and detect suspicious logins in real time and to support API driven mechanism to detect anomalies where details are provided through SSO
- Assurance levels: To define assurance level required to provide information /service to the user
- Integration: To integrate with services delivered using multiple channels such as National / Ministry Portal, Mobile Portal, Kiosks and National Call Center (NCC)
- Security protocols: To comply with the internationally recognized security protocols such as: SAML2.0 (**S**ecurity **A**ssertion **M**arkup **L**anguage), OAuth2.0 (**O**pen **Auth**orization) and OpenID Connect 2.0
- Must provide white label login and registration process
- Must provide Rule-based authorization support for SSO
- Must support for multi-option/multi-step authentication
    - X.509 Authentication
    - 2-factor authentication (2-FA)
    - Time-based one-time password (TOTP) based authentication
- Must provide Users and Group Management
- Must provide flexible profile management for users supporting multiple profiles per user and have the ability to link multiple user accounts to a single user
- Must support heterogeneous user stores, e.g., ApacheDS or any RDBMS
- System should support configurable password policies
- Should have account locking for invalid failed login attempts
- Should have account recovery with email and secret questions
- Should have password history validation
- Should have password pattern configuration
- Should have account locking in single and multi-tenant environments

- Should have account suspension reminders and locking of idle accounts
- should provide multi-option/multi-step approval template-based workflows for user and role management operations
- should manage role-based access control
- Should have user friendly policy administration point
- Should have easy to integrate option with Service Bus
- Should support for SAML2 bearer grant type, JWT assertion grant type and NTLM- IWA grant type
- Should have OAuth2 token revocation support
- Should have OAuth token introspection
- Should have proper monitoring, reporting and auditing support by providing login events and session monitoring, user session termination, forced password reset and real- time security alerting for suspicious login activities and abnormal sessions based on rules
- System should provide flexible deployment mechanism by supporting clustering for high availability deployment and centralized configuration management across different development environment.

Other requirements: To support high availability, security, auditing, scalability and open standards

The consultant shall conduct BPR to determine the business requirements

- Identify the services to be provided online
- Assess the risk associated with each online service
- Define the sensitivity level for each online service
- Identify the appropriate authentication mechanism

(e) **Digital Signature**

GoCD in its electronic communication/transactions desires to include the provision of Digital Signatures for irrefutable authenticity to stand legal scrutiny and to ensure reliability and trust worthiness.

It's highly recommended that the digital signature relay on the AES (Advanced Electronic signature) certificate type. These certificates are available to users and organizations that wish to transact and communicate with clear legal status. A high level of independent identity authentication is provided through the collection of personal identity information, including fingerprints, and the verification of the information provided by the GoCD. Advanced Electronic Signatures are strongly recommended for strong authentication, signing, and encryption of electronic communications, transactions, and processes

The consultant shall carry out the BPR study to make the provisions for integrating Digital Signatures with the relevant government systems, including those developed under the assignment.

(f) Enterprise Architecture

The **United Nations e-Government Survey 2016** has emphasized three aspects - an Integrated Government approach, Integrated Policy and use of Data Analytics - as the important means of achieving the Sustainable Development Goals (SDGs). The purpose of adopting the Integrated Government Approach is to provide integrated and joined up service delivery that cut across not only the economic, social and environmental dimensions, but also various sectors, sub-sectors and activities. Policy integration entails recognition of the inter-linkages between different areas of policy and adopting a holistic approach. Data Analytics is a tool for gaining deep insights into a range of complex issues and using the same for policy formulation and decision support. All these three globally significant trends make it imperative that the government adopts a strategy of having uniform, integrated and accessible architecture to give a feel of ONE GOVERNMENT despite its inevitable diversities.

This calls for the need of designing and adopting an Enterprise Architecture Framework for Dominica that helps in breaking the sectoral (individual ministerial) barriers and silos and re-architecting the Government as a single enterprise.

Enterprise Architecture recommends a federated architecture, whereby the participant entities design their own solutions adhering to the principles and standards laid down by the Enterprise Architecture, so as to make them interoperable with all other entities within and outside the enterprise. Enterprise Architecture does not amount to a monolithic architecture. It is technology-agnostic and therefore, enables heterogeneous technologies to coexist and interoperate. It facilitates an autonomous evolution of multiple solutions in different domains of the enterprise, all conforming to a set of principles and standards. The centralization, if at all, is confined to the EA Principles and Standards, but does not extend to the technologies, solutions and implementations.

In view of the above, the Consultant shall develop a Dominica Enterprise Architecture Framework (DEAF) based on the universally accepted frameworks such as, TOGAF, ZACHMAN, including but not limited to following frameworks;

- Business Architecture
- Information System (Application & Data) Architecture
- Technology Architecture
- Migration Architecture
- Governance Architecture
- Enterprise Security Architecture
- Architecture Change/Requirement Management

(g) Business Continuity (BC) and Disaster Recovery (DR) Architecture

Business Continuity (BC) and Disaster Recovery (DR) is one of the key considerations that GoCD envisages for a resilient government operations and services in the event of any disruption/crisis/catastrophe. Following are the broad expectations of the business architecture;

- To put in place, in advance, measures to minimise the occurrence of disruptions as well as to mitigate the impact of such events, if they do occur
- Human resource management during a disaster/crisis
- Assure the continuity of IT services based on service level agreements
- Restoration of critical applications and core business processes and functions
- Maintaining a high level of confidence that the business continuity arrangements are effective through regular testing of BCP arrangements
- Ensure that BCM arrangements are ongoing and subject to regular reviews, audits and exercises

The consultant shall carry out BPR to implement a Business Continuity Architecture to meet the above expectations in reference to the international standards such as ISO 27031, or the NIST SP 800-34

(h) Application and System Security:

For a healthy and resilient operations and services, it is necessary to implement the security at application and resource level to deal with various cyber vulnerabilities. The IT Security includes collection of policies, security concepts, security safeguards, guidelines, risk management approaches, tools, training, best practices, assurances and technologies that can be used to protect the cyber environment, organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

GoCD towards this, desires to establish a Cyber-Security Operation Centre (CSOC) to monitor, assess and defend information systems in order to protect confidentiality, integrity and availability of the services. The CSOC shall be equipped with tools such as Security Information and Event Management Tool (SIEM), Incident Management tool, Anti-APT, PIM, etc., and Security Intelligence services for better security monitoring and response capabilities.

The BPR study should capture following the broad expectations for the application and system security requirements & objectives;

- Complying with the Internationally recognised standards or best practices refers to the "ISO/IEC 27000-series," published jointly by the International Organisation for Standardisation (ISO) and the International Electro-technical Commission (IEC), which provides best practices on information security management, risks, and controls within the context of an overall ISM system. A relevant organisation should be able to demonstrate that it has an information security framework that is consistent with the ISO 27000-series (or with another equivalent standard), or that it has an equivalent framework.
- Provide architecture for an appropriate overall Information Security Management system including but not limited to:

    - Displaying a clear understanding of the lifecycle of exchanged information within the organisation, and be committed to safeguard its confidentiality and appropriate use
    - Managing information security through the medium of a written information security policy that is part of an overarching security framework that clearly defines security roles and responsibilities owned by senior management and is kept up to date
    - Addressing information security, including technology, through appropriate operational arrangements and as well as an integrated part of the management of relevant business processes
    - managing r information security risks, taking into account the threats, vulnerabilities, and impacts; and
    - Having appropriate arrangements to manage and maintain business continuity.

- Provide appropriate human resources controls including but not limited to:
    - Ensure that security roles and responsibilities of potential systems users are defined, documented, and clearly communicated in terms of engagement, and regularly reviewed in accordance with the information security policy (this should include confidentiality and nondisclosure agreements)
    - Ensure that all potential system users receive regular and up to date security training and awareness, with special focus in sensitive roles receiving additional guidance relevant to the handling of more sensitive material
    - Provide appropriate access controls, including physical and logical access which include developing, maintaining and implementing policies, processes and procedures, owned by senior management and not solely the organisation's IT function, that govern logical access, and effective processes for the provisioning and auditing of logical access and for the identification and authentication of users
- Provide appropriate IT System Security which should make security an integral part of providing technology services, have a security plan for applications, and harmonise their systems with security
- Provide an appropriate operations management framework, including incident management, change management, monitoring as per the following guidelines:
    - Be aware of the controls that protect exchanged information and have appropriate plans in place to manage them
    - Have appropriate monitoring and logging arrangements in place, including to detect unauthorised access, use or disclosure of information
    - Analyse and act upon security risks such as: Cyber attacks.

- Have processes and procedures for the identification and management of known vulnerabilities
- Have a change management process, with security integrated into it
- Have an incident management system that covers all types of security incidents; and
- Have internal audit and external audit functions

The consultant shall conduct the BPR to design the CSOC as an intrinsic component of the IT management.

(i) AI and Big data analytics engine for intelligent service delivery

GoCD, towards making its service delivery system efficient, inclusive and responsive, is keen to implement an Artificial Intelligence (AI) and Big Data analytics engine that interacts with various systems to fetch data, identifies eligible beneficiaries/cases based on business rules, authenticates the genuinity and subsequently deliver services or social benefits, etc.

The AI engine should also be able to provide analytics, fraud detection and management complaint management for a seamless service delivery from online application to disbursement. It shall also be extended to design/recommend the policy formulation and business cases for various government initiatives based on a mature Decision Support System (DSS) which incorporate Big Data Analytics and AI. The Consultant may focus on including but not limited to;

- Core Application Function for data input/collection/storage/core application process integration ->;

- Input to a data lake/ ETL or ELT process/input to a data warehouse (or subset data mart) common to all contributing agencies (e.g., every MDA contributes to the data warehouse/marts);

- Data is which can be available to BI/AI/BD Analytics programs, plus access to static or reference data sources, and real-time or streaming data sources as needed for input to DSS and integration with other MDA or external stakeholder systems. This is of course dependent on having a formal data classification policy or standard, and decisions made on exposing non-sensitive or protected data as open data. The Consultant may draft guidelines based on need-to-know, authentication, authorization, and data owner permission.

The Consultant shall perform BPR to incorporate AI, analytics and emerging technologies to automate the service delivery and policy formulation based on business algorithm and intelligence.

(j) Documentation

The Consultant shall prepare documents for including but not limited to;

- Operation and Maintenance (O&M) guideline for the To-Be solution after deployment and Go-Live
- Business Continuity (BC) and Disaster Recovery (DR) Plan
- Change Management & Capacity Building Plan arising due to the implementation of the new To-Be solution
- Terms of Reference (ToR) for RFP for the selection of the System Integrator for implementing the solution and performing O&M of the deployed solution
- Standards, Guidelines for application as well as web and mobile portal development

(k) SMS and e-Mail Integration

An SMS and e-mail gateway allows a computer (also known as a Server) to send or receive text messages in the form of SMS transmissions and e-mails between local and/or international telecommunications networks. In most cases, SMS are eventually routed to a mobile phone through a wireless carrier. SMS gateways are commonly used as a method for person-to-person to device-to-person (also known as application-to-person) communications.

Similarly, the e-mail gateway allows a computer (also known as a Server) to send or receive messages through mail.

The consultant shall preform the BPR for the integration of SMS and e-mail gateway to facilitate the transmission of messages, OTPs, etc over mobile and portable devices. It is expected that the Consultant shall develop FRS/SRS as a guideline for GOCD for integration of SMS and e-mail gateway to facilitate the transmission of messages.

(l) e-Payment Integration

GoCD has implemented an e-Payment system for facilitating the online payments for availing various government (G2C) services. Currently, the payment can be done using credit cards only. It is expected that the Consultant should perform the comprehensive BPR have provision to accept payments using the modes described below including but limited to.

- **Internet banking** – In this case, the payment is done by digitally transferring the funds over the internet from one bank account to another. Some popular modes of net banking are, NEFT, RTGS, IMPS.
- **Card payments** – Card payments are done via cards e.g., credit cards, debit cards, smart cards, stored valued cards, etc. In this mode, an electronic payment accepting device initiates the online payment transfer via card
- Credit/ Debit card – An e payment method where the card is required for making payments through an electronic device.
- **Smart card** – Also known as a chip card, a smart card, a card with a microprocessor chip is needed to transfer payments.
- **Stored value card** – These types of cards have some amount of money stored beforehand and are needed to make funds transfer. These are prepaid cards

like gift cards, etc.

- **Direct debit** – Direct debit transfers funds from a customer's account with the help of a third party
- **E-cash** – It is a form where the money is stored in the customer's device which is used for making transfers.
- **E-check** – This is a digital version of a paper check used to transfer funds within accounts.
- **Alternate payment methods** – As technology is evolving, e-payment methods kept evolving with it (are still evolving.) These innovative alternate e-payment methods became widely popular very quickly thanks to their convenience.
- **E-wallet** – Very popular among customers, an E-wallet is a form of prepaid account, where customer's account information like credit/ debit card information is stored allowing quick, seamless, and smooth flow of the transaction.
- **Mobile wallet** – An evolved form of e-wallet, mobile wallet is extensively used by lots of customers. It is a virtual wallet, in the form of an app that sits on a mobile device. Mobile wallet stores card information on a mobile device. The user-friendly nature of mobile wallets makes them easier to use. It offers a seamless payment experience making customers less dependent on cash.
- **QR payments** – QR code-enabled payments have become immensely popular. QR code stands for 'Quick Response' code, a code that contains a pixel pattern of barcodes or squares arranged in a square grid. Each part of the code contains information. This information can be merchant's details, transaction details, etc. To make payments, one has to scan the QR code with a mobile device.
- **Contactless payments** – Contactless payments are becoming popular for quite some time. These payments are done using RFID and NFC technology. The customer needs to tap or hover the payment device or a card near the payment terminal, earning it a name, 'tap and go'.
- **UPI payments** – Unified Payment Interface (UPI) is an instant real-time payment system to facilitate interbank transactions. Payments via UPI can be made via an app on a mobile device.
- **Biometric payments** – Biometric payments are done via using/scanning fingerprint scanning, eye scanning, facial recognition, etc. These payments are replacing the need to enter the PIN for making transactions making these payments more accessible and easier to use.
- **Payments are done via Wearable devices** – Wearable devices are rapidly becoming popular among customers. These devices are connected to the customer's bank account and are used to make online payments. An example of a wearable used for making an online payment is a smartwatch.
- Provision for generating successful transaction slip

- Provision for generating failed transaction slip

V. IMPLEMENTATION PERIOD

The time input of key experts is estimated at 264 person-days*. The assignment is expected to start in April 2023 and to be completed within three (3) months.

VI. TEAM COMPOSITION AND QUALIFICATION REQUIREMENTS

A. Qualification Requirements for the Consultant as a Firm

The Consultant as a firm must have the following experience:

1. Minimum 5 years of Experience in the areas of Business Process Re-Engineering (As-Is, Gap Analysis and To-Be), Enterprise Architecture in the digital transformation in the role of prime contractor, JV member, subcontractor, or management contractor;
2. Similar demonstrative experience in the core areas for BPR and cross-cutting areas for solutioning as mentioned in the ToR;
3. Demonstrative experience of at least Five (5) years in similar areas of working with the World Bank or other Multi-lateral Development agencies;
4. Experience in working with digital transformation programs in small-island countries is desirable.

B. Team Composition

The Consultant will provide a dedicated Team Leader who will be responsible for the contract management and co-ordination.

The Team will comprise of the following key experts as mentioned in the table below.

The following are the indicative details of the key experts which **will not be evaluated at EoI stage.** The consultant may provide the indicative list of experts below to showcase strength and expertise available.

#	Key Experts	Experience Level	Person-Days
KE-1	Team Leader & BPR Specialist	• Should be a Postgraduate in Business Administration, Public Administration, Computer Science/IT or relevant areas with 10 years’ experience in project	66

#	Key Experts	Experience Level	Person-Days
		management and leading BPR project of this nature. • PMP or Prince-2 certification would be an advantage • Should have experience in handling AI/emerging technologies/Analytics based solutions • Experience in working in small island countries or similar countries would be beneficial	
KE-2	Enterprise Architect (EA)	• Should be a Postgraduate in Business Administration, Public Administration, Computer Science/IT or relevant areas with 8 years' experience in business analysis and working as EA in the project of similar nature. • Should be TOGAF / Zachman certified	66
KE-3	BPR Specialist-e-Entry Mechanism	• Should be a Graduate in Business Administration, Public Administration, Computer Science/IT or relevant areas with 8 years' experience in business analysis of the public/government sector projects. • Should have carried out BPR of at least three (3) projects in e-Entry/ Customs/Immigration	22
KE-4	BPR Specialist-e-Office/DMS	• Should be a Graduate in Business Administration, Public Administration, Computer Science/IT or relevant areas with 8 years' experience in business analysis of the public/government sector projects. • Should have carried out BPR of at least three (3) projects in e-Office/DMS/ Workflow Management or similar areas for public/government sector projects.	22

#	Key Experts	Experience Level	Person-Days
KE-5	BPR Specialist-Health	• Should be a Graduate in Business Administration, Public Administration, Computer Science/IT or relevant areas with 8 years’ experience in business analysis of the public/government sector projects. • Should have carried out BPR of at least three (3) projects in Health systems	44
KE-6	Interoperability/Cloud Architect	• Should be a Graduate in Business Administration, Public Administration, Computer Science/IT or relevant areas with 8 years’ experience in working in public/government sector projects. • Should have carried out BPR for developing FRS/SRS/Use cases for Interoperable/Cloud Architecture • Should have experience in designing cloud architecture	22
KE-7	IT Security & Business Continuity/Disaster recovery Architect	• Should be a Graduate in Business Administration, Public Administration, Computer Science/IT or relevant areas with 8 years’ experience in IT Security & Business Continuity/Disaster Recovery Architect • Should be CISA/CISM	22
	Total Person-days		**264**

Note:

*1 Person-month = 22 person days

*1 Person-day = 8hours

VII. DELIVERABLES

List of Deliverables and Milestones

The Consultant is required to prepare:

#	Deliverables	Indicative Timeline (T) in person-days
1	Signing of Contract	**T_0**
2	Inception Report, including an updated preliminary workplan based on the schedules and priorities of the Project activities	**$T_1 = T_0 + 5$**
3	Comprehensive As-Is Report towards achieving the objective-1 for each Core Areas for BPR and Cross Cutting Area for Solutioning, except for Enterprise Architecture (EA)	**$T_2 = T_1 + 17$**
4	To-Be Report towards achieving the objective-2 by identifying various scenarios and processes for each Core Areas for BPR and Cross Cutting Area for Solutioning, except for EA	**$T_3 = T_1 + 22$**
5	Requirement Analysis report towards achieving objective- 3 for each Core Areas for BPR and Cross Cutting Area for Solutioning, except for EA	**$T_4 = T_1 + 22$**
6	Enterprise Architecture report in line with the objective-4	**$T_5 = T_4 + 17$**
7	Operation and Maintenance (O&M) guideline for the To-Be solution after deployment and Go-Live	**$T_6 = T_5 + 5$**
8	Guidelines for Business Continuity (BC) and Disaster Recovery (DR)	**$T_7 = T_5 + 5$**
9	Guidelines for Change Management & Capacity Building	**$T_8 = T_5 + 5$**
10	Guidelines for Implementation and estimates of cost for the Core Areas for BPR and the Cross Cutting Areas for Solutioning, except for EA	**$T_9 = T_5 + 5$**
11	Terms of Reference for selection of the System Integrator for implementing the solution and performing O&M of the deployed solution for the core areas	**$T_{10} = T_1 + 45$**

#	Deliverables	Indicative Timeline (T) in person-days
12	Guidelines for application as well as web and mobile portal development.	**$T_{11} = T_5 + 5$**
13	Draft Final Report of the engagement	**$T_{12} = T_{10} + 11$**
14	Final Report of the engagement	**$T_{13} = T_{12} + 5$**

Submission and Approval of Deliverables

The Consultant will report to the Project Manager, PIU who will be responsible for approval process of the deliverables and invoices.

All reports and deliverables should be in English.

All draft and final reports should be submitted electronically in the format(s) agreed by the parties.

Within twenty-one (21) calendar days from the date of the reports and deliverables receipt, the PIU shall review in consultation with relevant MDAs, and:

(a) approve the reports and deliverables; or

(b) notify the Consultant of any respects in which the PIU considers that the reports and deliverables do not comply with the contract provisions. The reports and deliverables shall be revised and submitted to the Client by the Consultant within two (2) weeks following the receipt of Client's comments unless otherwise agreed by the parties.

VIII. CLIENT'S CONTRIBUTION

The PIU will provide the Consultant with the following documents and data:

(a) National Digital Transformation Strategy "Dynamic Dominica"

(b) Financing Agreement (IDA-6685-DM) - http://documents1.worldbank.org/curated/en/780941597092384320/pdf/Official-Documents-Financing-Agreement-for-Credit-No-6685-DM.pdf;

(c) Project Appraisal Document (PAD3724) - http://documents1.worldbank.org/curated/en/848701593136915061/pdf/Dominica-Grenada-St-Lucia-St-Vincent-and-the-Grenadines-and-the-Organization-of-Eastern-Caribbean-States-Caribbean-Digital-Transformation-Project-Digital-Caribbean.pdf

(d) the Procurement Plan – https://projects.worldbank.org/en/projects-operations/project-procurement/p171528

(e) the Project Operations Manual

(f) the Environmental and Social Commitment Plan (ESCP) - http://documents1.worldbank.org/curated/en/206801599068520268/pdf/Environmental-and-Social-Commitment-Plan-ESCP-Caribbean-Digital-Transformation-Project-P171528.pdf

(g) Stakeholder Engagement Plan

(h) E-waste Management Plan

Besides above, the links for the necessary documents is placed at Annexure-3. The Authorized Representative of PIU will facilitate the Consultant and make available Project-related reports and data relevant to successful completion of the contract, and will act as liaison between the Consultant, the World Bank, the MDAs, the PSC and other Project stakeholders.

Office accommodation, including access to the Internet, and conference and meeting facilities in Dominica for experts working on the Contract will be provided by the Client.

Additionally, the MDAs will provide suitably qualified and experienced staff for each area with which the contract is concerned to work with the Consultant's team.

ANNEXURE 1. PROJECT DEVELOPMENT OBJECTIVE INDICATORS

Indicator Name	Baseline	End Target
Increase access to digital services & technologies by governments, businesses & individuals		
Dominica: Internet penetration (Percentage)	69.60	90.00
Dominica: Adults with access to an e-money account (Percentage)	0.00	15.00
Of which percentatage women (Percentage)	0.00	50.00
Dominica: Percentage of users of digital public services reporting satisfaction with the efficiency of the transaction (Percentage)	0.00	65.00
Increase access to digital technologies and skills by businesses and individuals		
Aggregate number of individuals utilizing digital skills to improve workplace productivety or secure new employment opportunitites (Number)	0.00	2.050.00
Of which percentatage women (Percentage)	0.00	40.00
Regional: Number of individuals uilizing advanced digital skills to improve workplace productivity or secure new employment opportunitties (Number)	0.00	250.00
Of which percentatage women (Percentage)	0.00	40.00
Dominica: Number of individuals utilizing digital skills to improve workplace productivity or secure new employment opportunitties (Number)	0.00	480.00
Of which percentatage women (Percentage)	0.00	40.00
Aggregate: Number of fimrs adopting digital technologies and platforms for business purposes (Number)	0.00	400.00
Of which percentatage women (Percentage)	0.00	30.00
Dominica: Number of fimrs adopting digital technologies and platforms for business purposes (Number)	0.00	100.00
Of which percentatage women (Percentage)	0.00	30.00

ANNEXURE 2. INTERMEDIATE RESULTS INDICATORS BY COMPONENTS

Indicator Name	Baseline	End Target
Component 1: Digital Enabling Environment		
Eastern Caribbean electronic Communications Bill adopted at national level (Number)	0.00	4.00
Dominica: Effective retail price per GB for least costly 30-day prepaid mobile package (amount(USD))	9.25	7.40
Comprehensive Payment systems Law adopted at regional level (Yes/No)	No	Yes
Updated/harmonized licensing and oversight framework for digital finncial services adopted at national level (Number)	0.00	4.00
Computer Emergency Response Team (CERTs) or cyber agencies are established and operational with staff and procedures in place and incident monitoring reporting being carried out in project countries (Number)	0.00	4.00
Component 2: Digital Government Infrastructure, Platforms, and Services		
Government enterpriser architecture adopted	0.00	2.00
Action Plans to strengthen busness continuity, resilience and post-disaster recovery of critical digital infrastucture, operations, and services adopted at national level (Number)	0.00	3.00
Dominica: Number of digital government functions and services using shared services platform (Number)	0.00	12.00
Component 3: Digital Skills and Technology Adoption		
Aggregate: Number of individuals trained in digital skills programs (Number)	0.00	2,700.00
Of which pertenctage women (Percentage)	0.00	40.00
Regional: Number of individuals trained in digital skills program (Number)	0.00	300.00
Of which pertenctage women (Percentage)	0.00	40.00
Dominica: Number of individuals trained in digital skills program (Number)	0.00	800.00
Of which pertenctage women (Percentage)	0.00	40.00
Regional: Number of individuals acquiring internationally or regionally recognized professional certification (Number)	0.00	300.00
Of which pertenctage women (Percentage)	0.00	40.00
Aggregate: Number of firms completing technology adoption programs	0.00	400.00

Indicator Name	Baseline	End Target
(Number)		
Of which pertenctage women (Percentage)	0.00	30.00
Dominica: Number of firms completing technology adoption programs (Number)	0.00	100.00
Of which pertenctage women (Percentage)	0.00	30.00

ANNEXURE-3. PRELIMINARY LIST OF LEGISLATION, POLICIES AND REGULATIONS FOR THE SELECTED AREAS

A. Cross-cutting Acts and Bills that are relevant to Digital Identifier, Authentication Platform and Digital Signature

N	Document Description	Link
1.	Electronic Filing Act No 20 of 2013	http://www.dominica.gov.dm/laws/2013/Electronic Filing, 2013 ACT 20 of 2013.pdf
2.	Electronic Evidence Act No 13 of 2010	http://www.dominica.gov.dm/laws/2010/Electronic Evidence no. 13.pdf
3.	Electronic Funds Transfer Act No 17 of 2013	http://www.dominica.gov.dm/laws/2013/Electronic Funds Transfer Act, 2013 ACT 17 of 2013.pdf
4.	Electronic Transactions Act No 19 of 2013	http://www.dominica.gov.dm/laws/2013/Electronic Transactions Act, 2013 Act 19 of 2013.pdf
5.	Electronic Crimes Bill Fourth Draft 6 October 2011	PDF Computer and Computer Related C
6.	Data Protection Bill Fourth Draft 6 October 2011	PDF Data Protection Bill 2013.pdf

B. Immigration and Passport

N	Document Description	Link
1.	Immigration and Passport Act Chapter 18:01 Act 5 of 1941	http://www.dominica.gov.dm/laws/chapters/chap18-01.pdf
2.	Immigration and Passport Regulations Statutory Rules and Orders No 21 of 1996	http://www.dominica.gov.dm/laws/1996/sro21-1996.pdf
3.	Immigration and Passport (Amendment) Act No 3 of 2000	http://www.dominica.gov.dm/laws/2000/act3-2000.pdf
4.	Immigration and Passport Regulations Statutory Rules and Orders No 36 of 2001	http://www.dominica.gov.dm/laws/2001/sro36-2001.pdf
5.	Immigration and Passport (Amendment) Regulations	http://www.dominica.gov.dm/laws/2002/sro2-2002.pdf

N	Document Description	Link
	Statutory Rules and Orders No 2 of 2002	
6.	Immigration and Passport (Amendment) Act No. 3 of 2002	http://www.dominica.gov.dm/laws/2002/act3-2002.pdf
7.	Immigration and Passport Regulations Statutory Rules and Orders No 51 of 2002	http://www.dominica.gov.dm/laws/2002/sro51-2002.pdf
8.	Immigration and Passport (Amendment) Act No. 19 of 2003	http://www.dominica.gov.dm/laws/2003/act19-2003.pdf
9.	Immigration and Passport Regulations Statutory Rules and Orders No 22 of 2003	http://www.dominica.gov.dm/laws/2003/sro22-2003.pdf
10.	Immigration and Passport (Amendment) Regulations Statutory Rules and Orders No 25 2003	http://www.dominica.gov.dm/laws/2003/sro25-2003.pdf
11.	Immigration and Passport (Amendment) Act No. 4 of 2007	http://www.dominica.gov.dm/laws/2007/act4-2007.pdf
12.	Immigration and Passport (Amendment) Act No. 11 of 2007	http://www.dominica.gov.dm/laws/2007/act11-2007.pdf
13.	Immigration and Passport (Amendment) Act No. 24 of 2013	http://www.dominica.gov.dm/laws/2013/Immigration and Passport (Amendment) Act, 2013, Act 24 of 2013.pdf
14.	Immigration and Passport Amendment Statutory Rules and Orders No 10 of 2016	http://www.dominica.gov.dm/laws/2016/Immigration and Passport (Amendment) Regulations, 2016.pdf
15.	Immigration and Passport (Amendment) Statutory Rules and Orders No 42 of 2016	http://www.dominica.gov.dm/laws/2016/Immigration and Passport (Amendment) (No. 2) Regulations 2016.pdf

C. Health Information and Administration

N	Document Description	Link
1.	Bills of Health Act Chapter 49:03 Act of 3 of 1907 amended by 7 of 1925	http://www.dominica.gov.dm/laws/chapters/chap49-03.pdf
2.	Hospital and Health Care Facilities Act No 21 of 2002	http://www.dominica.gov.dm/laws/2002/act21-2002.pdf
3.	Hospital and Health Care Facilities Statutory Rules and Orders No 8 of 2004	http://www.dominica.gov.dm/laws/2004/sro8-2004.pdf