**SAINT VINCENT AND THE GRENADINES**

**CARIBBEAN DIGITAL TRANSFORMATION PROJECT**

**TERMS OF REFERENCE**

**FOR**

Services for Business Continuity, EA Standards, and Interoperability Framework

# INTRODUCTION

## CARDTP Project Background

St. Vincent and the Grenadines is considered a Small Island Developing State (SIDS) and comprises the mainland of St. Vincent and 32 islands and cays, which comprise the Grenadines, of which the largest seven are inhabited. These are Bequia, Canouan, Mayreau, Mustique, Prune (Palm) Island, Petit Saint Vincent and Union Island. The total country area is 150 square miles (389 square kilometres).

The Government of St. Vincent and the Grenadines (GoSVG) has received financing from the World Bank Group to implement the Caribbean Digital Transformation Project (CARDTP or the Project). 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 CARDTP's development objective is "to increase access to digital services, technologies, and skills by governments, businesses, and individuals in the participating Eastern Caribbean countries. It leverages public sector modernisation and digitisation to improve service delivery and drive a digital culture across the region." As such, the CARDTP will finance the cross-cutting enablers of digital government, digitise specific priority services, fill existing infrastructure gaps, and contribute to the expansion of the benefits of public sector modernisation to citizens and businesses. It also aims to foster regional integration and cooperation to capture the economies of scale and scope required to increase the impact and value for money of the project interventions and create a more competitive, seamless regional digital market to attract investment and provide room for the growth of digital firms.

The CARDTP includes activities to be implemented at the regional and national levels.

National-level activities will be financed through an IDA credit to Saint Vincent and the Grenadines in the amount of US$30 million.

The Project 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 modernised and harmonised 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 Saint Vincent and the Grenadines.

## Background information on the TOR

This section provides information about other related ongoing initiatives.

Priority initiatives under the SVG CARDTP project include the transformation and digitisation of critical business processes such as Customs, Tax, Civil Registration, and Land Management, the implementation of digital identification and authentication, and the digitisation of citizen-facing services. These projects will have an overarching positive impact on Government Ministries, Departments and Agencies, as well as citizens and the general public. For a resilient digital government, enablers such as enterprise architecture, business continuity protocols, data centre and disaster recovery technologies, cyber security, data protection and privacy, and digital skills and capacity building are crucial.

This project focuses on cross-cutting resiliency measures required to sustain the digital transformation. The following table provides the overall context by illustrating the planned projects. The scope of work involves implementing a Business Continuity Management System (BCMS) in accordance with ISO 22301, as outlined in the following sections.

| Project | Scope | Relevance to the current TOR |
|---|---|---|
| Digital government standards, business continuity and protocols (DGSSP) (***This project)*** | Services covering risk assessment, Disaster Recovery and Business continuity planning, data gathering for Data Centre Consolidation and digitization opportunities for of public services. Tasks include (i) architecture, risk and opportunity assessment (ii) design of governance mechanisms and operating procedures (iii) training and roll out of procedures | To be started under this TOR. Related projects – Data Centre upgrade and procurement of IT HW in tranches. The recommendations from this project will be fed into other projects |
| Cyber Security Management Implementation | Deployment of comprehensive cyber security program at National and Government levels<br>(i) National-level risk assessment, CERT framework deployment, and training<br>(ii) Risk assessments, information security management system | |

| | | |
|---|---|---|
| | upgrade, CERT deployment and training for Govt Data Centres<br>(iii) Security operations support services | |
| Technology Architecture Upgrade and Data Centre Implementation (TAUDC) | - Phased IT Hardware procurement (Goods).<br>- establish/reinforce/consolidate a data centre to host government data and services. | A modular prefab data centre container is under procurement. This along with the existing data centre will be the main hosting facilities to handle both real time and DR loads. A certification and support from ISF for the deployments. |

Figure 1: The Path to Resilient Digital Government

## OBJECTIVES OF THE SERVICES

**Scope and Applicability**
The Digital Government Standards, Business Continuity and Protocols (DGSSP) project aims to deploy robust business resiliency protocols.

The goal of the project is to improve the resiliency of government Departments and provide uninterrupted services in times of natural disasters as well as during cyber incidents.

**Objectives of BCMS**

- Improve the continuity of critical government services during disruptions.
- Improve resilience and recovery capabilities.
- Standardise business continuity management across all government departments
- Reduce operational, financial, and reputational impacts.

# SCOPE OF WORK

## DESCRIPTION OF THE ASSIGNMENT

### Project Requirements

**Scope of the project**:

- Development, deployment, and training of a Business Continuity Management System (BCMS) based on international standards such as ISO 22301 for the prioritised departments.
- Design of IT Disaster recovery (DR) plans, policies, and architectures for ITSD for (i) the transition period for the next 2 years and (ii) long term. The transition period includes the time period when the current DC is upgraded with new hardware in the interim for launching the digital transformation applications, and a new modular container DC will be implemented in 2026. These two DCs are expected to be back up for each other. The BCP should also cover recovery operations for cyber resiliency. However, the planning of CERT is not included in the scope.
- Deliver a government-wide business country strategy and policy templates for those Departments not part of BCMS studies and assessments

The developed BCMS will be the Government's standard for Resiliency. The reviews and impact assessments shall be carried out with the following Departments under the digital transformation project.

- Internal Revenue Department (IRD)
- Customs & Excise Department
- Treasury Department
- Land Registry
- Civil Registry
- ITSD

A central coordinating agency is expected to oversee BCMS deployment and oversight. Initially, the Project Implementation Unit (PIU) will be undertaking the responsibility until the BCMS framework and governance models have been worked out.

**The Consultant is required to refer to the National Emergency Telecom Plan approved in 2024 to align the BC and DR activities with this plan.**

The project output shall be:

- The GoSVG Government-wide BCP strategy and standard for all Government departments to follow as a government mandate.
- Robust Disaster Recovery (DR) Architecture, options, and final designs for procurements.

- Complete BCMS implementation for all MOF departments, with at least one drill completed for at least one department (likely to be IRD).

## Implementation Timelines and Deliverables

### Component 1 – Inception

**Output**

- Vision, Charter, and BC Framework for GoSVG.
- Project and Change Management Plans
- Gap Analysis and BCMS implementation roadmap.

**Activities:**

**Part 1:**

1. Conduct the project kick-off meetings with all the project stakeholders together.
2. Carry out a knowledge-sharing workshop on the criticality of the need for a formal BC and DR policy and operating procedures.
3. Carry out discovery sessions with the stakeholder departments (individually and collectively).
4. Outline the relationships between all internal and external groups involved in the project.
5. Confirm project objectives and outcomes.
6. Agree on the project approach and key project milestones.
7. Propose and agree on standards and approaches for scheduling and conducting interviews, Business Impact Analysis (BIA) / Risk Analysis (RA)
8. Conduct initial stakeholder analysis and engagement.
9. Prepare change management (training and awareness, and communication activities of the process changes.

**Part 2:** In parallel with Part 1:

1. Assess the Business Continuity Management (BCM) and Disaster Recovery Management (DRM) current state assessment against the ISO 22301:2019 requirements with the key stakeholders from every department/function in scope and the IT infrastructure in charge.
2. Schedule meetings with the department/facility point of contacts from the departments and facilities in scope. Tools, methods and schedules of stakeholder engagement and assessment must be provided as detailed in sections below.
3. Evaluate the current business continuity management practices and documentation for each department and facility (against the broad requirements of ISO 22301)
4. Document the findings from the assessment as a current state assessment report.
5. Develop a plan for updating existing BCM Framework (if available) documents, including BCM Policy, Business Impact Analysis Procedure, Risk Assessment Procedure, and other BCM Framework documents.
6. Develop a roadmap/plan to implement BCMS.

7. Develop outlines of governance structure that include coordinating organisation structure, communication structure, project risk, issue management, problem management, and project management approach.
8. Identify roles and responsibilities within the BCMS project governance structure.
9. Review existing BCM processes in the Departments, establish a target framework and propose a governance structure. Develop a formal BC project charter for SVG, which is to be reviewed and approved by SVG.

## Component 2 – Business Impact and Risk Analysis

### Business Impact Analysis

1. Customise the approach for conducting Business Impact Analysis, in coordination with the key project stakeholders.
2. Validate with Stakeholders the Business Impact Analysis toolkit for conducting BIA.
3. Identify the processes for which BIA is required (prioritisation).
4. Conduct the BIA for the processes in scope to identify associated recovery time and recovery point objectives (RTO and RPO, respectively) and the Maximum Tolerable Period of Disruption (MTPD).
5. Identify the process dependencies and the minimum operating requirements for the identified critical business processes in terms of people, site, and technology. Document the BIA report.
6. Validate the BIA results with the stakeholders.
7. Conduct a workshop for BCM Coordinators on BCM and BIA as part of the Train-the-trainer initiative.

### Technical Infrastructure Analysis

1. Analyse current infrastructure, application architecture, and end-user access methodologies.
2. Identify and analyse specific vulnerabilities[1] against business impact for infrastructure, application architecture, and end-user access.
3. Perform single-point failure analysis for critical business processes considering reference to redundancies and backups.
4. Analyse the current application deployment process, integration, and dependencies and map vulnerabilities with applicable threats in the Application deployment process.
5. Analyse current support and operational processes, integration and dependencies, and identify and analyse specific vulnerabilities, and map vulnerabilities with applicable threats in the operational processes.

[1] Here vulnerabilities not dot imply security vulnerabilities but rather it should be read as critical points of failure in the BIA

6. Develop the risk treatment guidelines considering various risk treatment options such as accept, avoid, mitigate, and transfer. Development of a risk treatment plan and implementation roadmap.

**Threat Risk Assessment**

1. Develop the Risk Assessment approach and Risk Assessment templates in coordination with the project stakeholders.
2. Assess the Threat Risk Landscape. Understand the risks from vendors, customers, and interested parties. The Supplier, in consultation with business stakeholders, shall identify business continuity threats and risks. However, the following indicative threats and risks are provided below
    a. Business disruptions due to natural calamities such as volcanic eruptions and high-intensity hurricanes, impacting both people's ability to work, as well as disruptions in telecommunication rendering remote work difficult.
    b. IT systems and network rendered unavailable due to potential cyber-attacks. While a separate Computer Emergency Response Team (CERT) is being formed to manage cyber risks, the recovery process of IT systems subjected to cyber-attacks will be part of the Business Continuity project.
3. Identify and analyse the organisation-specific vulnerabilities. Perform single-point failure analysis for critical enablers, map vulnerabilities with applicable threats, and identify the risks associated with the identified vulnerabilities.
4. Validate the risk assessment results with the project stakeholders.
5. Develop the risk treatment guidelines considering various risk treatments. Update the risk treatment plan and implementation roadmap.

**Tools and Methods**

1. The consultant is required to detail the tools and methods to be used for BIA and is required to submit sample templates to be included.
2. Methods such as questionnaires, workshops, and interviews must be specified and linked with the project plan, and resource requirements from SVG. An indicative schedule of data collection must be provided as part of Response Set 2, as indicated in Table 2: Technical Responses Required
3. Supplier is encouraged to consider a remote (desk review) data collection process for cost-effectiveness.

## Component 3 – Business Continuity Strategy Development

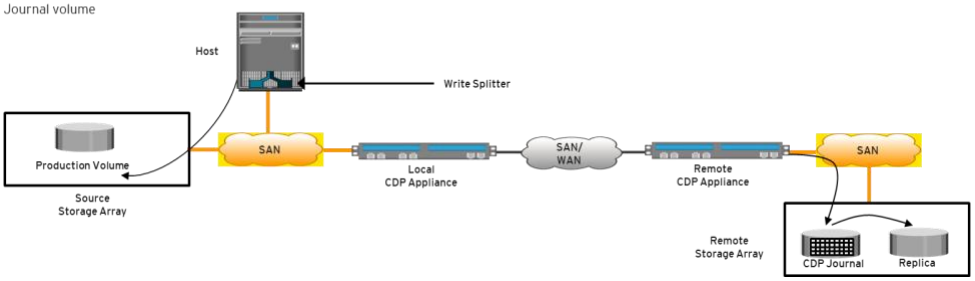
1. Document IT asset inventory (applications and infrastructure) and the current level of digitization of business process.

2. Review existing DR Strategies against practical recovery capability.
3. Identify Response, Continuity, and Recovery Options as appropriate to critical activities.
4. Work with the stakeholders to evaluate the impact of the recovery strategies on the business and technology.
5. Analyse the response and recovery options, selection of strategies, obtaining approval, and documenting the analysis and selection process as appropriate.
6. Design BCM strategy options for people, sites, technology and vendors on the basis of the output of BIA and risk assessment exercise (samples provided below).
7. Determine technology architecture options for replication:

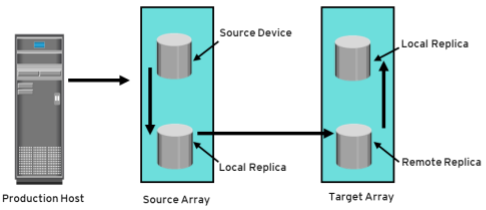
CURRENT STRATEGY

| | Buy-and-Build | Cold Site | Warm Site | Hot Site | Hot-Mirrored Site |
|---|---|---|---|---|---|
| Recovery Strategy | Identify an alternate site, buy or lease equipment, re-build servers | Designate a fully operational data center as alternate site in advance of disaster. Recovery similar to Buy-and-Build at designated site | Establish alternate site with stand-by hardware and operating systems. Load applications and restore data from tape after a disaster | Establish alternate site with stand-by hardware, operating system, and applications. Load data on a daily basis from tape | Operate two remote data centers both for production processing. Traffic is dynamically routed between sites |
| Recovery Time | 5 days or more | More than two days, exact time depends upon hardware availability | 24 to 36 hours | 3 to 12 hours | Instantaneous |
| Technical Architecture | None | Data center with environmental controls and telecommunications | Load applications and restore data from tape during a disaster | Restore data from tape on a daily basis before a disaster | Mirroring<br>Load Balancing |
| Key Benefits | Inexpensive | Accommodates web-based systems<br>Inexpensive | Can use as alternate site for development and lab<br>Good compromise between recovery time and cost | Reliable recovery method<br>Rapid recovery of critical applications | Instantaneous recovery<br>Risk of data loss limited to last few uncommitted transactions<br>Operational efficiencies |
| Key Weaknesses | Potentially unreliable<br>Can not accommodate web-based systems<br>May take up to a week to recover | Potentially unreliable<br>May take up to a week to recover<br>Loss of data since most recent back-up | If servers are used for development recovery may be hindered by configuration changes<br>Loss of data since most recent back-up | Can't use alternate site for test or lab purposes<br>Expensive<br>Loss of data since most recent back-up | Expensive<br>Potentially complex to operate |

Provides any-point-in-time recovery capability during its normal operation
Components of CDP include:
- CDP appliance: CDP appliances are present at both source and remote sites
- Write splitter
- Journal volume




- Replication is performed by array-operating environment. Three replication methods: synchronous, asynchronous, and disk buffered
  - Synchronous: Writes are committed to both source and replica before it is acknowledged to host
  - Asynchronous: Writes are committed to source and immediately acknowledged to host. Data is buffered at source and transmitted to remote site later
  - Disk Buffered




| | |
|---|---|
| 1 | Production host writes data to source device. |
| 2 | A consistent PIT local replica of the source device is created |
| 3 | Data from local replica is transmitted to the remote replica at target. |
| 4 | Optionally a PIT local replica of the remote replica on the target is created. |

8. Perform a cost-benefit analysis for all the designed strategies and prepare a business case for the most relevant.
9. Validate the BCM strategies with the concerned departments / operational units per process in scope.
10. Obtain approvals and sign-off on the BCM strategies workbook.

While redundancies can be built using technologies, it is crucial that cost-effective and yet workable business continuity strategies be proposed for finalisation by GoSVG.

## Component 4 - BCP Plan Development

Develop an organisation structure (standard), and roles and responsibilities for managing BCP for each business stakeholder department appropriate for a SIDS based on international best practices, consisting of but not limited to (**note: the following are indicative and the Consultant must propose and review with GoSVG the required processes and teams**):

- Site emergency response team
- IT Disaster Management Team
- Crisis Management Team
    1. Damage Assessment Team
    2. Communication Team
    3. Transition Team
    4. IT Recovery Team
    5. Functional Recovery Team

Establish BC and DR test plans, test requirements, and templates, test assessment framework

1. Test guidelines
2. Test reporting format
3. Test checklist

**Prepare and plan for BCP Exercises**

1. Review past business disruptions and/or incidents that impacted essential services.
2. Review existing BCPs for essential services.
3. Develop BCP processes and assets such as process documentations, templates, guidelines, training materials, etc.
4. Assess past and current BC exercise/testing plans.
5. Prepare an exercise/testing schedule together with defined roles and responsibilities of each party during the test
6. Identify the type of exercise/testing to be conducted, validate exercise/testing scope options, and finalise the scope with stakeholders
7. Identify exercise/test participants and communicate test requirements, expectations, and dates to participants.
8. Document test scenarios.
9. Develop the remote work guide to enable employees to work from home during the crisis.
10. Conduct Crisis Management, BCM & DR Training Sessions
    a. Develop Training Materials
    b. Define the target audience and plan the training sessions per site in scope.
    c. Deliver classroom training to all the identified BCM roles using the train-the-trainer approach.
    d. Deliver role-specific training to identified members.

11. Conduct a disaster simulation exercise/testing per group based on the existing Business continuity plan of the teams.
12. Design the exercise survey.
13. Identify, communicate, and prepare participants for the exercises

**Conduct Pilot Exercises**

a. Facilitate the following BCM exercises:
    i. Notification tree exercise
    ii. Desktop Walkthrough exercise
    iii. Crisis Simulation Exercise
    iv. Testing of recovery operations at least for one department
b. Facilitate distribution of the Post Exercise Survey (online surveys – like Survey Monkey)
c. Collate the survey observations
d. Prepare a post-exercise report, with lessons learned and an improvement strategy.

- After-Action Report – overall summary, lessons learned, timelines, etc.
- Gaps and issues identified, e.g. missing documents, unclear roles, etc.
- Updates to BCP documents to reflect lessons learned RTO/RPO Validation
- Compliance evidence vs ISO or NIST standards
- Recommendations for follow-up

## Component 5- Change Management and BCM Rollout

Change management and training is a critical component. Comprehensive change management and training deliverables must be produced.

In continuation of Component 4, prepare a change management plan for the identified stakeholders involved in the BCP activities. The Change Management Plan must include an operational manual for triggering BC activities, a process for cascading of activities within the roles and responsibilities identified in the BCP, monitoring of RTOs and formal completion of the BCP. The developed BCMS

1. Customise training content and evaluation of training effectiveness (digital).
2. Training content (digital) will include all business continuity policies followed by Client A, along with good BCM practices.
3. Content must be designed for reuse by GoSVG for future cohorts.
4. Awareness sessions for all BCM Coordinators to enable the train-the-trainer model.
5. Develop a BCM training program and train all stakeholders in each department within the scope of the project

## PERIOD OF PERFORMANCE

Table 1: Key Activities

| Component | Key Activities (Summary) | Indicative Timelines for completion (T=0 at project start). Vendor may propose shortened time |
|---|---|---|
| Inception, and Gap Analysis | - Establishment of Vision and Charter for the BC implementation for SVG.<br>- Development of Project and Change management plans<br>- Awareness creation<br>- Assess the level of BCM and DRM<br>- Evaluate the current business continuity management practices and documentation for each department. | Initial discoveries: T+6 weeks<br>Vision, Charter and Governance: T+10 weeks |
| Business Impact Analysis and Risk Analysis | - Review business process criticality with stakeholders<br>- Review Impact to the business process and establish/review RPO/RTO<br>- | T+ 12 weeks |
| Business Continuity Strategy development | - IT DR requirements definition | T+16 weeks |
| Design BCMS Roadmap and establishment of Govt-wide BCMS | - Staged implementation of BCMS in phase<br>- Governance roles and responsibilities TOR | T+ 18 weeks |
| IT DR Design | - Technology design keeping in consideration RPO/RTO | T+16 weeks |
| BCP Plan implementation | - Development of policies and procedures<br>- Set up of governance | T+ 24 weeks |
| BCM Roll out | - Training including mock BC Drills | T+30 weeks |

## QUALIFICATIONS OF CONSULTANT FIRM

1. Potential Supplier for this assignment shall be experienced in carrying out business continuity and IT Disaster recovery services, taking ISO 22301 as a reference (ISO certification is not planned in the near future)
2. The company should be present on the market for at minimum 10 years and during this time should have practical experience in the areas indicated above in the country of origin and internationally.
3. At minimum 5 years of experience in the implementation of international projects of similar scope and magnitude in developing countries, including in projects in the areas of assessment, establishment, computation, and BCP and IT DR.
4. The company shall be financially sound and able to organise and implement the project according to the requirements.
5. The company shall be able to provide a team of high-level consultants, as the key experts for this assignment, according to the qualification requirements listed below.
6. The evaluation of the Supplier will take into consideration the qualifications of the key experts as well as the company profile.

The Firm shall provide qualified consultants, including the Project Manager and Technical Experts, necessary to complete the project tasks on time and professional level.

***Project Manager/Team Leader***

The Project Manager/Team Leader's minimal qualification requirements are as follows:

1. The Team Leader should be certified in ISO 22301 business continuity domains. Additional certifications in Governance, Risk, and Compliance (GRC) domains will also be necessary.
2. Minimum of 15 years of work and practical experience in Business Continuity Management and IT Disaster recovery programs.
3. At minimum 5 years of experience in international projects on establishing BCMS, including business continuity drills.
4. Proven experience in conducting risk assessments, BIAs, and DR plans.
5. Practical experience in leading teams. A project management certification will be preferred.
6. Good reporting, presentation skills, and communication skills working in multicultural environments.

***Key Technical experts***

The Key Technical Experts' minimal qualification requirements are as follows:

1. The key expert shall have a minimum of 10 years in IT infrastructure and DR architecture designs.
2. Certification in one or more of ITIL, Cyber Security Resiliency, and Business Continuity Management will be necessary.
3. A minimum of 3 years of experience in carrying out complex BCP and DR designs.

4. Experience in detailed assessment of the business processes, risks, and mitigation
5. Ability to design BCP DR processes.
6. Excellent communication skills. Shall be able to train the users and carry out change management.

The Firm may also provide resumes of other non-key specialists involved in the project, but they will not be used for evaluation.

## TECHNICAL RESPONSE REQUIRED

The Firm must provide responses indicating the following:

1. Company background and ability to execute the project
2. Technical approach and indicative timelines for carrying out the BCMS based on the requirements provided above. The approach must indicate the framework, methodology, tools, templates, etc to be used in the project. The response must demonstrate the supplier's depth of understanding of the scope of work
3. Sample case studies and similar project experience.
4. Information about the company's resource pool is available to execute the project.