GOVERNMENT OF
SAINT CHRISTOPHER AND NEVIS

Request For Proposals

DIGITAL TRANSFORMATION MANAGEMENT UNIT

Creation of the Government of Saint Christopher and Nevis
DATA AND INFORMATION MANAGEMENT FRAMEWORK

26th May, 2025

Government of Saint Christopher and Nevis

Request for Proposal (RFP)

Project Name:	**Consultancy for the Development of a Data and Information Management Framework**
Issued by:	**Digital Transformation Management Unit**

1. INTRODUCTION

The Government of Saint Christopher (St. Kitts) and Nevis (GoSKN), through its Digital Transformation Management Unit, Ministry of Information and Communication Technology, and Posts, invites qualified consulting firms or individual consultants to submit proposals for the development of a comprehensive Data and Information Management (DIM) Framework. This initiative is a key deliverable under the Whole-of-Government Digital Transformation Strategy aimed at enhancing data security, interoperability, operational efficiency, and improved service delivery across government agencies.

The proposed framework is intended to provide comprehensive guidance for managing information across its lifecycle, encompassing information planning and governance to ensure strategic alignment and oversight. It should address critical aspects such as information access, privacy, and security, alongside robust data management practices that include master data, metadata, and data quality assurance. Knowledge management and the reuse of digital assets must be promoted to support organisational learning and operational efficiency. Additionally, the framework must define clear policies for records retention and compliance, integrating cybersecurity controls, data classification protocols, and audit requirements to safeguard against risks, and support accountability. Adherence to relevant legislative and regulatory obligations is essential, and the framework must also incorporate considerations for cloud data management, ensuring secure, compliant, and scalable use of cloud-based services.

2. BACKGROUND

GoSKN has embarked on a whole of government digital transformation programme. One of the critical challenges is the limited ability to share data and information among departments and with other stakeholders seamlessly and securely. This situation is a limiting factor in achieving interoperability and high levels of operational efficiency. The proposed DIM Framework will guide the strategic planning, access, governance, security, lifecycle management, and use of data and information assets across the entire public sector.

The basic principles governing data and information management to which GoSKN has subscribed include the following. Data and Information should be:

1. Aligned with business needs and user outcomes.
2. Secure, and managed as valuable assets.
3. Trustworthy so that they can be used and reused with confidence.
4. Of high quality and spatially enabled.
5. Managed across their full lifecycle.
6. Reasonably available to departments, agencies, entities and individuals to whom it should be lawfully accessible.

3. EXPECTED BENEFITS AND OBJECTIVES

EXPECTED BENEFITS OF THE CONSULTANCY

By developing and implementing the DIM Framework, GoSKN intends to achieve the following:

- Drive data and information coordination, consistency and maturity across the government.
- Highlight data and information management for strong governance, business outcomes and improved services in a digital environment.
- Enable strategic planning and manage data and information assets for transformation and quality service delivery for citizens.
- Consolidate and share knowledge while coordinating the management of all its data and information.
- Foster public confidence in government data and information management due to effective information management.
- Build and promote data and information maturity and capacity across agencies.
- Drive information access and sharing across government.

OBJECTIVES OF THE CONSULTANCY

The core objective of this consultancy is to develop a DIM Framework that:

- Establishes common standards and principles for managing data and information as strategic assets.

- Enables secure, appropriate, and effective sharing and use of data and information across government agencies.

- Enhances data quality, privacy, accessibility, and governance.
- Aligns with national priorities, international best practices, and legislative requirements.

- Is accompanied by an implementation plan.

4. SCOPE OF WORK

The objective of this assignment is to create a strategy document which outlines how data and information is collected, organized, secured, analyzed, and effectively utilized, then archived or disposed. The following major items, at a minimum, must be considered. Additional items or considerations may be added at the discretion of the vendor. Additional consideration will be given to proposals which meet or exceed ISO15489-1:2016 and ISO/IEC 27001:2022 and other international best practice standards.

Broadly speaking, the consultant will be required to execute the following tasks:

- Conduct an information needs and risk assessment across GoSKN ministries and agencies.
- Develop a high-level information architecture and data model.
- Define policies and processes for data lifecycle management, access, privacy, classification, retention, and security.
- Establish mechanisms for data sharing, open data, and public access.
- Propose governance structures, roles and responsibilities, and performance metrics.
- Address areas such as metadata management, content management, data sovereignty, cyber risk, and compliance with international standards.
- Support capacity-building activities and stakeholder consultations.
- Create an implementation plan for the DIM Framework.

DETAILED SCOPE OF WORK

The consultant will be required to carry out activities encompassing

1. Information Planning and Design,
2. Information Access, Security, Privacy and Risk Management,
3. Data Management and
4. Knowledge Management.

These activities are specified below.

4.1 Information Planning and Design

4.1.1 Information Needs Assessment

4.1.1.1 Assess the data/information that GoSKN needs to design, create and keep.

4.1.1.2 Identify where information requirements need to be built into process, system, service or contract design.

4.1.2 Information Risk Assessment

4.1.2.1 Identify where risks to information exist in processes, capabilities or services.

4.1.2.2 Identify policy and compliance risks.

4.1.2.3 Create a plan to mitigate identified risks.

4.1.3 Information Architecture

4.1.3.1 Assess the organizational architecture needed to support information creation, use, governance and management.

4.1.3.2 Align the information management needs to enterprise architecture and future conceptual architecture planning.

4.1.4 Data Modeling and Design

4.1.4.1 Create a model for the assessment, design and development of the data required to support business operations.

4.1.5 Information Life-Cycle Planning

4.1.5.1 Identify the requirements and processes needed to support the use and management of information as an asset throughout its lifecycle.

4.1.5.2 Design a framework to align systems, services, processes, and requirements to support information creation, management, use and deletion/disposal.

4.1.6 Information Asset Registration

4.1.6.1 Identify and document core data/information assets and systems.

4.1.7 Accountability Management

4.1.7.1 Assess the need for evidence and accountability for the access and use of data and information.

4.1.7.2 Develop a framework for ensuring that information required to support evidence and accountability needs is appropriate, fit for purpose, and kept for as long as required.

4.1.8 Information System and Service Management

4.1.8.1 Develop a framework for planning and assurance activities to ensure systems and service offerings remain appropriate to business needs.

4.1.8.2 Create a framework to manage the transition of information out of existing systems and services and into new business appropriate environments.

4.2 Information Access, Security, Privacy and Risk Management

4.2.1 Cyber Risk

4.2.1.1 Identify high value information systems and assets, and create a framework for risk assessment and management of these and similar assets.

4.2.1.2 Develop a governance framework to support strong asset management and cyber-security.

4.2.1.3 Define the controls needed to protect high value information assets.

4.2.1.4 Develop and recommend relevant security by design approaches.

4.2.2 Information Access

4.2.2.1 Create a framework for public information access requirements, including proactive and managed public release of information.

4.2.2.2 Propose arrangements that ensure that access to information is controlled, monitored and appropriate to risk and business requirements.

4.2.2.3 Design processes to maintain currency and appropriateness of access and restriction arrangements, including during staff onboarding, off-boarding or movement through the organization.

4.2.2.4 Develop monitoring processes for information access arrangements.

4.2.3 Privacy Management

4.2.3.1 Develop privacy by design approaches that support compliant and effective information design, use and management.

4.2.3.2 Develop a framework of processes and practices to support the protection, control and management of personal information.

4.2.3.3 Define a process for conducting Privacy Impact Assessments (PIAs) and Threat Risk Assessments (TRAs).

4.2.4 Data Opening and Public Release

4.2.4.1 Recommend mechanisms to ensure data is made available for public use and reuse.

4.2.4.2 Develop governance and control procedures to ensure that personal and sensitive information is protected in open data arrangements.

4.2.5 Data Sharing

4.2.5.1 Propose a model for sharing data within government to drive service improvement and outcome delivery, including governance and monitoring for data sharing.

4.2.5.2 Recommend tools, processes, frameworks and arrangements to facilitate data sharing

4.2.5.3 Propose data integration and interoperability approaches.

4.2.6 Information Classification

4.2.6.1 Develop a system for the identification, organization and classification of information and information systems to enable their appropriate use and protection.

4.2.7 Legislative Compliance

4.2.7.1 Determine the laws (specific legal provisions) that should be put in place to regulate vendors, IT systems, and data and information sharing (e.g. laws compliant with GDPR, PIPEDA, FIPPA, etc).

4.2.7.2 Include provisions that give an appropriate entity within the government to perform a security audit of any data/information system.

4.2.8 Data Encryption

4.2.8.1 Propose requirements and standards for data encryption and encryption keys management, including whether in transit or at rest.

4.2.8.2 Identify other information security related policies that may be required -credential mapping, device profiling, tokenization, data loss prevention (DLP), logging, alerting, malware detection/prevention, etc.

4.2.9 Records Retention and Disposition Schedules

4.2.9.1 Recommend and design records retention policies and disposition schedules including for cloud data and vendor services. Retention policies should take account of data storage costs.

4.2.10 Security and Audit Certifications

4.2.10.1 Recommend security and audit industry certifications and standards that GoSKN should require that external service providers to comply with. For example:

- Information Security – ISO 27001
- Attestation – SSAE 16 Type II

- Audit – CICA 9110
- Other – COBIT, COSO, ISO/IEC, PCI/DSS, NIST

4.2.11 Security Breaches

4.2.11.1 Design requirements for notification of security and privacy breaches.

4.3 Data Management

4.3.1 Master Data Management

4.3.1.1 Define the critical data assets used across GoSKN.

4.3.2 Metadata Management

4.3.2.1 Define policies, rules and practices to ensure metadata definition, access, integration, linking, sharing, maintenance and analysis.

4.3.3 Data Quality

4.3.3.1 Define a framework to assess and improve the quality of data.

4.3.4 Content Management

4.3.4.1 Create a framework for tracking and managing information content to enable its appropriate definition, management, use and reuse.

4.3.5 Data Storage

4.3.5.1 Develop a framework for the planning, management and coordination of data storage environments.

4.3.6 Data Residency/Sovereignty

4.3.6.1 Recommend requirements and policies for data residency (in state or out of state)

4.3.7 Data Ownership.

4.3.7.1 Propose guidelines for data ownership including what constitutes "agency-owned" data / intellectual property and vendor-owned data /intellectual property, and how long vendors (including Cloud platforms) can retain GOSKN data post contract.

4.3.8 Data Segregation

4.3.8.1 Propose requirements for physical and logical segregation of GoSKN data including defining what systems interconnections are permissible and the use of Firewall blocking, and VLAN isolation.

4.4 Knowledge Management

4.4.1 Digital asset management

4.4.1.1 Propose a model for the organization and management of digital information to enable its controlled and managed reuse.

4.4.2 Government-wide search and Collaboration

4.4.2.1 Propose a model for making content from multiple environments available for coordinated searching and access, and for building and sourcing knowledge from interagency and cross-government collaborations, and collaboration with the community, research and industry.

5. DELIVERABLES

The expected outputs of this assignment are as follows:

5.1 **An inception report**: A report outlining the approach, methodology, and general work plan and stakeholder engagement plan, clearly indicating how synergies among the various requirements will be exploited to efficiently execute the consultancy.

5.2 **Needs Assessment and Gap Analysis:** A detailed survey of infrastructure, systems, persons and skills and any other factor which may have to be considered.

5.3 **An Inception meeting:** to inform stakeholders and others of what the engagement is about, their participation and give major highlights and activities.

5.4 **Collaboration Model**: for Cross-Government and Multi-Stakeholder Engagement.

5.5 **Interim Reports**: with findings from assessments and initial framework design.

5.6 **A whole of GoSKN Data and Information Management Strategy.** This strategy should address all the objectives, listed in this document and include at a minimum ISO15489-1:2016 and ISO/IEC 27001:2022 standard considerations.

Draft DIM Framework and Implementation Plan including the following specific deliverables:

5.6.1 Information Planning and Design

7.6.1.1 Information Needs Assessment

5.6.1.1.1 Report on GOSKN's information and data creation, usage, and retention requirements

5.6.1.1.2 Framework for GOSKN's information and data creation, usage, and retention requirements

5.6.1.1.3 Process/System Design Guidelines for embedding information requirements

5.6.1.2 Information Risk Assessment

5.6.1.2.1 Information Risk Register (including process, capability, and service-level risks)

5.6.1.2.2 Policy and Compliance Risk Identification Framework with Risk Mitigation and Treatment Plan

5.6.1.3 Information Architecture

5.6.1.3.1 Current-State Information Architecture Assessment

5.6.1.3.2 Future-State Information Architecture Framework

5.6.1.3.3 Alignment Report with Enterprise and Conceptual Architectures

5.6.1.4 Data Modeling and Design

5.6.1.4.1 Data Modeling Guidelines and Reference Architecture

5.6.1.4.2 Conceptual and Logical Data Models to support business operations

5.6.1.5 Information Life-Cycle Planning

5.6.1.5.1 Information Life-Cycle Requirements Matrix

5.6.1.5.2 Lifecycle Framework aligning systems, services, and processes

5.6.1.6 Information Asset Registration

5.6.1.6.1 Core Data and Information Asset Register

5.6.1.7 Accountability Management

5.6.1.7.1 Evidence and Accountability Needs Assessment Framework

5.6.1.7.2 Accountability Framework for information use, access, and retention

5.6.1.8 Information System and Service Management

5.6.1.8.1 System/Service Planning and Assurance Framework
Information Transition Management Framework

5.6.2 Information Access, Security, Privacy and Risk Management

5.6.2.1 Cyber Risk

5.6.2.1.1 High Value Asset (HVA) Register and Risk Management Plan

5.6.2.1.2 Cyber-security Governance Framework

5.6.2.1.3 Control Requirements for HVA Protection

5.6.2.1.4 Security-by-Design Guidelines

5.6.2.2 Information Access

5.6.2.2.1 Public Information Access Framework

5.6.2.2.2 Controlled Access Governance Model

5.6.2.2.3 Access Restriction and Update Management Procedures

5.6.2.2.4 Access Monitoring and Audit Process

5.6.2.3 Privacy Management

5.6.2.3.1 Privacy-by-Design Implementation Guidelines

5.6.2.3.2 Personal Information Management Framework

5.6.2.3.3 PIA and TRA Process Framework

5.6.2.4 Data Opening and Public Release

5.6.2.4.1 Open Data Release Policy and Procedures

5.6.2.4.2 Personal/Sensitive Data Protection Controls for Open Data

5.6.2.5 Data Sharing

5.6.2.5.1 Intra-Government Data Sharing Model

5.6.2.5.2 Data Sharing Tools, Processes, and Governance Framework

5.6.2.5.3 Interoperability and Data Integration Strategy

5.6.2.6 Information Classification

5.6.2.6.1 Information and Systems Classification Scheme

5.6.2.7 Legislative Compliance

5.6.2.7.1 Legal Gap Analysis and Recommendations Report including draft Legislative Provisions for IT/Data Governance and Audit Authority

5.6.2.8 Data Encryption

5.6.2.8.1 Encryption Standards and Key Management Requirements

5.6.2.8.2 Comprehensive Information Security Policy Pack (DLP, Tokenization, Logging, etc.)

5.6.2.9 Records Retention and Disposition Schedules

5.6.2.9.1 Records Retention Policy and Cloud/Vendor Disposition Schedules

5.6.2.10 Security and Audit Certifications

5.6.2.10.1 Security & Audit Compliance Requirements for Vendors

5.6.2.10.2 Recommended Certifications List (ISO 27001, SSAE 16 Type II, etc.)

5.6.2.11 Security Breaches

5.6.2.11.1 Security/Privacy Breach Notification Requirements and Protocol

5.6.3 Data Management

5.6.3.1 Master Data Management

5.6.3.1.1 Critical Data Asset Inventory and Definitions

5.6.3.2 Metadata Management

5.6.3.2.1 Metadata Policy and Management Framework

5.6.3.3 Data Quality

5.6.3.3.1 Data Quality Assessment Framework

5.6.3.3.2 Data Quality Improvement Plan

5.6.3.4 Content Management

5.6.3.4.1 Content Management Framework for Information Reuse

5.6.3.5 Data Storage

5.6.3.5.1 Data Storage Architecture and Management Plan

5.6.3.6 Data Residency/Sovereignty

5.6.3.6.1 Data Residency Policy (Local vs. Foreign Hosting)

5.6.3.7 Data Ownership

5.6.3.7.1.1 Data Ownership and Intellectual Property Guidelines (Government Agency vs. Vendor)

5.6.3.8 Data Segregation

5.6.3.8.1 Physical and Logical Data Segregation Policy

5.6.3.8.2 Network Security and Isolation Requirements

5.6.4 Knowledge Management

5.6.4.1 Digital Asset Management

5.6.4.1.1 Digital Asset Reuse and Management Model

5.6.4.2 Government-wide Search and Collaboration

5.6.4.2.1 Integrated Search and Discovery Framework

5.7 **Final DIM Framework: incorporating feedback from stakeholders**.

5.8 **Implementation sequence:** Recommended department implementation sequence plan, based on survey's conducted, feasibility, asset importance, resource availability, and any other relevant factor.

5.9 **Executive Summary and PowerPoint** presentation for senior leadership.

5.10 **Wrap-Up Workshop 1**: to inform stakeholders and others of what the engagement has found, the survey, and give major highlights and activities completed and to go through the draft strategic plan in detail.

5.11 **A Wrap-Up Workshop 2**: to allow stakeholders and others, one week after the Workshop 1, to ask questions about the draft strategic plan.

5.12 **GoSKN Data and Information Management Strategy:** Three weeks after the Wrap-Up Workshop the submission of the final draft of the GoSKN Data and Information Management Strategy will be due.

5.13 **Post Delivery Consultation:** The vendor will have to reserve fifty (50) hours of consultation after delivery of the strategy for GoSKN to ask questions on the strategy. This 50 hours must be used within the proceeding twenty-four (24) months after the delivery date of the plan.

5.14 **Training workshop:** Four (4) workshops on Data and information management.

6. DURATION

The assignment is expected to be completed within approximately six (6) months from contract commencement to the provision of the Data and Information Management Strategy, excluding the 7.1.3 **Post Delivery Consultation** and **7.1.4 Training workshop**. Alternative timelines and activities may be recommended.

7. REQUIRED QUALIFICATIONS

7.1 Proven experience in developing data and information management frameworks for governments or large public sector institutions.

7.2 Demonstrated knowledge of data governance, security, privacy regulations (e.g., GDPR), and enterprise information architecture.

7.3 Strong understanding of cloud computing, digital identity, cyber-security, and government digital transformation strategies.

7.4 Experience in stakeholder engagement and capacity building.

7.5 Excellent communication, training, research and documentation skills.

8. SUBMISSION OF PROPOSAL

Vendors are invited to submit proposals for the Data and Information Management Strategic Plan. All proposals submitted in response to this Request for Proposal (RFP) must adhere strictly to the guidelines set forth herein. All proposals must be submitted electronically in PDF format. Proposals must be in English, comprehensive, well-structured, and fully compliant with all stipulated requirements.

Any submission failing to meet these requirements may be deemed non-responsive and, consequently, disqualified from consideration.
Interested parties should submit:

8.1 Submission

8.1.1 **Cover Letter** – Signed by an authorized representative of the bidding entity.

8.1.2 **Executive Summary** – A concise overview of the proposal.

8.1.3 **Technical Approach** – Detailing approach, methodology, and work plan.

8.1.4 **Development methodology** and project management approach. Training and support services, timeline for delivery of services with key milestones.

8.1.5 **Company Qualifications and Experience** – A demonstration of relevant expertise, organizational structure, and key personnel including CVs.

8.1.6 **References** – Contact details for previous clients or partners.

8.1.7 **Personnel and Communication -** project management team, including roles, responsibilities, and experience. Also includes project governance, risk management, and communication plans.

8.1.8 **Appendices** (if applicable) – Any supporting documentation or additional materials.

8.2 Submission Deadline and contact

8.2.1 Proposals must be received no later than **30th June, 2025 4pm AST**.

8.2.2 All inquiries and correspondence related to this RFP shall be directed to the designated contact person with the subject line "**Confidential Proposal Submission – Development of a Data and Information Management Framework for the Government of St Christopher and Nevis**”

Addressed to:

Eric Haynes
Programme Manager
Digital Transformation Management Unit

Ministry of ICT and Post

Government of St Christopher and Nevis

eric.haynes@gov.kn **copy** dtmu.technology@gov.kn
PH: 1 (869) 467-1389

8.3 Clarifications and Questions

8.3.1 Bidders may seek clarification regarding this RFP by submitting written inquiries to eric.haynes@gov.kn no later than **22nd June, 2025.**

9. EVALUATION

9.1 **Technical Merit:** Assessment of the proposed solution's technical soundness, functionality, performance, and compliance with requirements.

9.2 **Management Capability:** Evaluation of the proposer's project management experience, team qualifications, and proposed approach.

9.3 **Cost:** Assessment of the reasonableness and competitiveness of the proposed costs.

9.4 **Past Performance, experience and qualifications:** Evaluation of the proposer's track record on similar projects.

9.5 **Other Factors:** Other criteria may include innovation, security, accessibility, and compliance with specific government regulations or policies, implementation and surpassing of international best standards.