

## SUMMARY

# ICT Assessment (February 2020)



ADOBE STOCK

## Overview

This assessment provides a comprehensive diagnostic of the Government of Sint Maarten’s (SXM) information and communication technology (ICT) landscape as of early 2020. It is part of the Bank-Executed Trust Fund work underpinning the Sint Maarten Digital Government Transformation Project (DGTP), with a focus on “Pillar 2: Digital Platforms.” The document inventories and evaluates existing systems, platforms, infrastructure, governance arrangements, and institutional capacities across the government, and connects these findings to service delivery outcomes that affect citizens and businesses.

The scope spans the principal ministries—Ministry of General Affairs (MGA), Ministry of Finance, Ministry of Health, Social Development and Labor (VSA), Ministry of Education, Culture, Youth and Sport, Ministry of Public Housing, Environment, Spatial Development and Infrastructure (VROMI), and the Ministry of Tourism, Economic Affairs, Transport & Telecommunication (TEATT). The Ministry of Justice is noted as an exception: it operates its ICT stack largely independently and was not fully covered at the time of reporting.

The context is an economy and public sector seeking to modernize and improve resilience, competitiveness, and service quality. Sint Maarten faces legacy ICT, institutional fragmentation, and capacity constraints. These challenges are compounded by the island’s exposure to climate and disaster risks and rising cyber threats. A successful digital government transformation requires both foundational ICT building blocks and institutional reforms that enable coherent, secure, and user-centered services. This assessment serves as the baseline for identifying the gaps and prioritizing investments under the DGTP.

## Objectives and Audiences

The primary purpose is to establish a clear, evidence-based foundation for Sint Maarten’s digital transformation agenda by:

- Cataloging and characterizing existing ICT systems, infrastructure, and capabilities across ministries.
- Diagnosing weaknesses in core registries and line-of-business systems, including their interoperability, data quality, and technology lifecycle status.
- Identifying cross-cutting constraints in governance, institutional capacity, cybersecurity, business continuity, and connectivity.
- Assessing how legacy systems, manual processes, and siloed operations hinder efficiency, transparency, and service delivery.
- Translating diagnostic findings into priorities for DGTP investments (e.g., digital identity, electronic payments, interoperability platform, cybersecurity, network upgrades, and cloud-first approaches).

The objective is to ensure DGTP interventions are targeted, sequenced, and proportionate to the core barriers, thereby creating an enabling environment for modern, integrated, and citizen-centric digital services.

The target audiences include Government of Sint Maarten leadership and technical officials—ministers, permanent secretaries, department heads (particularly ICT and Public Service Centers), and ministry IT/business owners responsible for implementing digital reforms. The World Bank project team, comprising Task Team Leaders and specialists, supports design, appraisal, and supervision of the DGTP. The Project Implementation Unit (PIU) and management firm, as delivery partners, lead day-to-day execution and will use this assessment to prioritize investments, sequence activities, and monitor transformation progress.

## Methodology

The analysis draws on multiple data sources, including a systematic ICT inventory conducted across ministries that documents system lists, technical specifications, commissioning dates, interfaces, and vendor details. Additional inputs include internal strategy materials, such as integration visualizations, as well as operational reports, including audits of business license processing times and summaries from forums like a Tax Summit. Using these inputs, a diagnostic assessment synthesizes inventory findings to identify cross-cutting issues, such as legacy systems, lack of standardization, manual interfaces, and data quality challenges. The analysis benchmarks selected aspects against international norms—for example, data center tier classifications and service delivery timeliness—and maps identified problems to DGTP solution pillars. Where quantitative data were unavailable, qualitative or anecdotal observations were recorded to flag key risks and gaps.

## Key Findings

The assessment paints a consistent picture: a fragmented, aging, and under-resourced ICT landscape that constrains service delivery and poses resilience and security risks. The findings are grouped thematically.

### A. Institutional and governance gaps

- **Weak central ICT function:** The government’s central ICT Department, housed in the Ministry of General Affairs, is severely understaffed and not positioned as a strategic enterprise leader. At the time of the assessment, it had only four staff positions (with two vacancies) to serve roughly 1,200 public employees, leaving minimal bandwidth for policy, standards, or architecture work.

- Siloed operations: Ministries operate independently, and the Ministry of Justice maintains its own separate systems and processes. This undermines the development of a coherent whole-of-government ICT architecture and complicates enterprise planning and resource pooling.
- Reactive posture: Limited resources push the ICT Department into a reactive, firefighting mode. Strategic activities—governance, standards, roadmaps, enterprise architecture, and portfolio management—are underdeveloped, which perpetuates fragmented decision-making and technology choices across entities.

## **B. Aging and fragmented systems**

- Legacy platforms past end-of-life: Critical systems date to the 1990s and early 2000s. The Civil Registry runs on a 23-year-old solution atop an aging Oracle database. The government’s financial management system (“Decade,” commissioned in 1997) reflects obsolete architectures and limited vendor support.
- Non-standardized solutions: Ministries use different tools for similar functions (e.g., accounting on QuickBooks, Excel, and other ad hoc solutions). This creates heterogeneous data models and complicates consolidated reporting and transparency.
- Manual interfaces and data duplication: Data sharing is often manual or dependent on brittle extract-transform-load (ETL) routines. Synchronization lags and inconsistency are common—for instance, addresses across registries fall out of sync. An online student loan portal does not interface with Civil or Tax registries, forcing manual verification and undermining efficiency and integrity.

## **C. Foundational infrastructure deficiencies**

- Data center and business continuity: The main data center is described as Tier II but lacks basic physical security (no cameras) and has minimal UPS coverage (2–4 hours). While adequate for small loads, it is not robust for enterprise continuity in the face of power outages or disasters. Business continuity planning is not systematic, exposing services to significant downtime risks.
- Cybersecurity posture: The government lacks comprehensive ICT security policies and has limited operational capacity to monitor and respond to threats. Although some technical controls (firewalls, antivirus) are present, staffing and processes are insufficient to handle cyber incidents—an acute concern given recent ransomware episodes. A specific vulnerability is the Unique Identification Number (UIN): it is insecure, easily discoverable, and reused across credentials (National ID and Driver’s License), increasing identity theft risks.
- Connectivity and network architecture: Government connectivity relies on consumer-grade internet at the main building and a microwave-based wireless network across roughly 23 buildings. While reportedly stable, the architecture is suboptimal for enterprise performance, real-time data exchange, and scalable security. It also limits the adoption of centralized services and cloud architectures.

## **D. Inefficient service delivery and user experience**

- Limited service accessibility: Public Service Centers (PSCs) operate with restricted hours, reportedly open only about 15% of the year, and most services require in-person visits. This constrains access and increases transaction costs for users.

- Long processing times: Analog processes and manual verifications drive delays. About 68% of business licenses take 84–126 days, and 16% exceed 168 days, far above global good practice—undercutting the island’s competitiveness and ease of doing business.
- No end-to-end digital payments: Citizens must pay in person at the Receiver’s Office (with limited hours) and then return with proof of payment, adding friction and opportunities for error. There is no legal and technical framework enabling end-to-end electronic payments.
- Fragmented digital identity: Each system implements its own basic credentials and access controls. Without a unified, secure digital identity and authentication framework, “single sign-on” or one-stop, end-to-end digital services remain out of reach.

## Lessons Learned

- **Adopt a cloud-first strategy for resilience and scalability**

Given staffing and budget constraints, disaster exposure, and the need for elastic capacity, on-premise expansion is not cost-effective or sufficiently resilient. A cloud-first or cloud-native strategy enables more reliable hosting, backup, and recovery options; elastic scaling aligned with demand; lower upfront capital expenditure and improved lifecycle management; and faster deployment of modern platforms and security services. In parallel, mirroring critical registries to the cloud can strengthen business continuity and data preservation.

- **Make interoperability the organizing principle**

The core barrier to efficiency and transparency is fragmented data locked in siloed systems. A government-wide interoperability layer—based on service-oriented architecture, standardized APIs, and secure data exchange protocols—should be a keystone investment. This platform would enable authoritative “single source of truth” registries; reduce manual data reconciliation and errors; allow business process reengineering across agencies; and accelerate rollout of end-to-end digital services (e.g., licensing, benefits).

- **Build foundational building blocks first**

Transformation depends on a few non-negotiable enablers:

- Secure digital identity: Replace insecure identifiers and establish a robust digital ID for authentication, authorization, and signatures. This unlocks cross-agency transactions and trust in online services.
- Electronic payments: Introduce legal/technical frameworks for digital payments (cards, mobile, online banking) integrated with service workflows. This reduces in-person queues and enables truly end-to-end services.
- Cybersecurity framework and capacity: Develop whole-of-government security policies, incident response, monitoring, and training. Invest in security tooling and operational capacity commensurate with risk.
- Enterprise network upgrade: Migrate to a fiber-based backbone with enterprise-grade connectivity, segmentation, and quality-of-service controls to support secure, high-bandwidth, real-time operations.

- **Elevate the ICT function and reform governance**

Technology cannot substitute for institutional reforms. The ICT Department requires a clear mandate, resourcing, and authority to set architecture standards, oversee portfolio management, and drive enterprise solutions. Options include (i) establishing a central Digital Transformation Office or strengthening the ICT Department to act as an enterprise architect and service broker; (ii) defining governance processes for project intake, standards compliance, and investment prioritization; and (iii) creating capacity for policy development, vendor management, and contract oversight to avoid fragmentation and vendor lock-in.

- **Prioritize data quality and registry consolidation**

Authoritative registries (e.g., civil, business, property) must be cleansed, deduplicated, and standardized. Without data quality remediation, interoperability will propagate inconsistencies rather than solve them. Actions include (i) data profiling and cleanup campaigns with clear ownership and stewardship roles; (ii) uniform data models and validation rules; and (iii) master data management practices to maintain integrity over time.

- **Reengineer services around users**

Process redesign should accompany platform investments. The evidence of long waits and multiple in-person steps suggests the need to streamline application, verification, and payment steps; digitize forms and documents with e-signatures; provide status tracking and proactive notifications; and extend service hours via online channels and call centers, not just physical PSCs.

- **Strengthen continuity and risk management**

A systematic business continuity and disaster recovery posture is essential. Priorities include tier-appropriate hosting with redundant power, connectivity, and backups; tested recovery plans for critical systems; and clear continuity roles, escalation paths, and communication protocols.

## Identified Constraints

- *Incomplete coverage of the Ministry of Justice:* This is a significant gap, given the ministry's independent ICT environment. Bringing Justice into the enterprise architecture process is essential for a whole-of-government approach.
- *Some reliance on anecdotal performance observations:* For example, the microwave network's stability is noted anecdotally. A subsequent phase should validate performance using quantitative network monitoring and service-level metrics.
- *Emphasis on technical diagnostics:* Although the report links ICT shortcomings to service outcomes, it does not deep dive into political economy, legal/regulatory reforms, or change management. These factors are critical to successful implementation and may be covered in other DGTP components.

## Conclusion

The assessment underscores that Sint Maarten's digital transformation hinges on addressing foundational ICT deficits and institutional fragmentation. Priorities include a secure digital identity, interoperable data exchange, modern payment capabilities, improved cybersecurity, resilient hosting (cloud-first), and enterprise-grade connectivity. These enablers must be paired with governance reforms, data quality efforts, and service reengineering to deliver tangible improvements in citizen and business services. While the

baseline reveals substantial challenges—aging systems, manual processes, and limited capacity—the path forward is clear and actionable through the DGTP’s targeted investments and change program.

This summary was produced with the assistance of an AI language model based on the original report. The full report is available at [sintmaartenrecovery.org/analytical-studies](https://sintmaartenrecovery.org/analytical-studies)