

SUMMARY

Enterprise Architecture Inputs (November 2020)



Overview

The Enterprise Architecture (EA) Inputs document is a strategic blueprint for building a modern, resilient, and citizen-centric digital government in Sint Maarten. It responds to a pressing need revealed by recent crises—Hurricanes Irma and Maria in 2017 and the COVID19 pandemic—which exposed deep vulnerabilities across the public administration's ICT landscape: fragmented systems, data silos, paper-based or manual processes, weak interoperability, and limited disaster recovery and cybersecurity capabilities. These weaknesses undermine service delivery, reduce efficiency, and put continuity of government at risk.

The document's scope is whole of government. It sets a vision for a unified operating model where data and digital services flow securely and seamlessly across ministries and agencies. It defines the principles, governance, and architectural building blocks the government should adopt to move from ad-hoc ICT decisions toward a disciplined, standards-driven, and interoperable ecosystem.

The EA vision has five defining characteristics:

- **Centralized interoperability:** A government data exchange layer becomes the canonical way systems share information, reducing one-off integrations and enforcing common controls.
- **Shared foundational services:** Cross-cutting capabilities—digital identity/single sign-on, e-signature, e-payments, notifications—are built once and reused everywhere.
- **Cloud-first resilience:** A gradual but purposeful shift toward cloud-native and cloud-hosted solutions to strengthen business continuity and disaster recovery.
- **Citizen-centric access:** A single, user-friendly portal that aggregates services from multiple ministries into joined up, “once only” journeys for people and businesses.

- Data driven government: A common data model, authoritative “single sources of truth” (SSoT), and analytics that improve decisions, transparency, and service quality.

Methodologically, the document anchors to TOGAF (with emphasis on the Architecture Development Method) and uses the US Federal ACMM for maturity assessment—giving Sint Maarten an accepted frame to measure progress and iterate responsibly.

Objectives and Audiences

- Establish an actionable enterprise architecture vision and guiding principles for Sint Maarten’s digital transformation.
- Diagnose current state gaps in governance, capacity, infrastructure, security, and interoperability.
- Recommend a target operating model, roles, and decision rights to manage ICT coherently across government.
- Identify near-term priorities and a pragmatic roadmap (people, process, technology) to accelerate impact.
- Align investments and procurement to a coherent architecture, reducing duplication, risk, and lock-in.

The note targets a tiered audience: **primary** senior decision-makers, including the Council of Ministers, Prime Minister’s Office, Secretaries General, ministry CIOs, and central ICT and security leadership; **secondary** supporting bodies like the National Recovery Program Bureau, World Bank task teams, implementation partners, and oversight authorities; and **tertiary** ministry business owners, data stewards, and operational teams managing service delivery and system integration.

Key Findings

Current Maturity and Gaps

Using the ACMM, Sint Maarten’s enterprise architecture capability is assessed around Level 0 (No EA) with pockets of Level 1 (Initial). Key gaps include:

- Governance: No unified enterprise-wide process to guide investments, enforce standards, or align with business strategy. Decision-making is skewed by funding availability and agency-specific needs.
- Interoperability: No mandated standards or integration layer; ministries rely on bespoke, point-to-point links and ETL workarounds, creating data quality problems and fragility.
- Capacity: A small central ICT team supports a large and diverse environment (thousands of users across seven ministries), with shortages in architecture, security, and operations skills.
- Infrastructure and continuity: Aging on-prem assets, inconsistent network bandwidth to government buildings and the data center, and limited DR/BCP capabilities.
- Security posture: Practices are ad-hoc; there is rising awareness after cyber incidents, but no formal, enforced baseline or enterprise roles for risk management and incident response.

Proposed Governance and Operating Model

The document recommends a two-stage institutional pathway:

- Stage 1: Establish a Special Projects Unit (SPU) via national decree, reporting to a cross-government Steering Committee. The SPU coordinates architecture, standards, security baselines, portfolio oversight, and change management across the transformation program.
- Stage 2: Transition the SPU into a permanent Digital Transformation Agency (DTA) with the mandate, authority, and skills to govern the EA, set standards, run shared platforms (e.g., identity, exchange,

portal), and steward continuous improvement. A RACI-based role model clarifies accountability across ministries, the CIO/ICT function, NRPB/World Bank partners, vendors, and the management firm.

Guiding Principles

The document codifies design and policy principles to anchor all ICT work.

- Business: Digital by default; inclusive access; user-centered design; outcomes over outputs.
- Data: Once-only collection; data minimization; SSoT for authoritative registries; openness/transparency where appropriate; privacy and protection by design.
- Applications/Technology: Security by design; interoperable by default; government data exchange as the standard path; open standards and modularity to limit lock-in; reuse of shared services and components.

Architecture Building Blocks and Layers

- Business layer: End-to-end service journeys prioritized by citizen/business needs (e.g., permits, registrations, benefits). Emphasis on simplification, elimination of redundant steps, and digital channels.
- Data layer: A common data model (CDM) to harmonize semantics; formal designation of SSoTs (e.g., civil registry, address, business registry). Data governance roles (owners, stewards, custodians) and quality rules.
- Integration layer: A centralized Interoperability Exchange Point (IEP) for all cross-entity data flows, providing secure ingress/egress, routing, policy enforcement, auditing, and monitoring. Carefully governed direct links may be permitted only when aligned to standards and explicitly approved.
- Application layer: Shared capabilities (digital ID/SSO, e-sign, payments, notifications) plus line-of-business systems across ministries. Preference for configurable platforms and APIs over bespoke builds.
- Technology layer: Network modernization (fiber/routed redundancy to ministries and the data center), cloud-first infrastructure for resilience, endpoint management, and modern security tooling.
- Security layer (crosscutting): Defense-in-depth controls; identity and access management; key management; encryption at rest/in transit; continuous monitoring; incident response; independent audits.

Immediate Priorities and “Quick Wins”

To demonstrate early value while establishing foundations, six fast-tracked services are prioritized:

1. Certificate of Good Conduct
2. Change of Address
3. Registration of a Death, Divorce, or Marriage
4. Building Permit Application
5. Economic Licenses
6. Request for Vaccination Record

Strategic ICT plans underway or recommended:

- *Public Financial Management modernization*: Replace legacy systems (e.g., Decade/GEFIS) with a modern, integrated platform for transparency and fiscal control.
- *Microsoft Dynamics CRM expansion*: Leverage existing investments for case/workflow management across more ministries, with an eye toward future cloud migration (Dynamics 365).

- *Cloud adoption for resilience*: Prioritized migration of suitable systems to cloud for DR/BCP and scalability; careful cost planning to ensure sustainability post-project.
- *Cybersecurity uplift*: Progressive roll-out of baseline controls (patching, EDR, vulnerability management), sandboxing, privileged access management, backups, and user awareness training.
- *Network modernization*: Build a resilient, highband-width government network connecting ministries and the data center to support cloud backhauls and reliable service delivery.

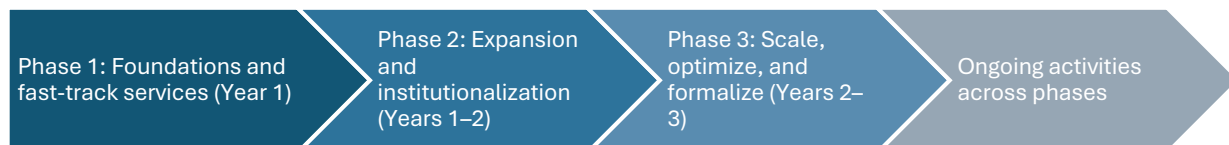
Risks and Mitigations

Key risks include high-severity institutional capacity gaps, fragmentation across ministries, ICT talent scarcity, cloud and connectivity costs, and potential shifts in political priorities. Mitigation strategies emphasize early engagement with management and specialist partners, embedding knowledge transfer, and developing local talent pipelines. Governance agreements and shared platform incentives address fragmentation. Targeted hiring, scholarships, and blended delivery tackle skills shortages. Financial pressures are managed through multi-year TCO planning and optimized architectures, while cabinet-approved policies, transparent metrics, and early wins support political continuity and legitimacy.

Lessons Learned

Effective implementation and interoperability depend on governance, shared platforms, and disciplined change management. Strong decision rights, standards, and enforcement—anchored by a mature SPU or DTA—prevent fragmented investments. Early deployment of central exchanges, digital ID/SSO, and common notification/payment rails generates compounding benefits, while “once-only” data collection requires SSoT designation, controlled access, and legal reinforcement. Coexistence with legacy systems, cloud-first architecture, security-by-design, standards-based procurement, people-focused change initiatives, and meaningful metrics collectively enable sustainable, interoperable, and high-performing digital government.

Implementation Roadmap



Phase 1: Foundations and fast-track services (Year 1)

- Legal/policy anchoring of EA principles and shared-platform mandates.
- Establish SPU and Steering Committee; approve reference architectures, data governance, and security baselines.
- Stand up the Interoperability Exchange Point (MVP) and digital ID/SSO; pilot e-signature and notifications.
- Network uplift for priority sites; basic SOC/monitoring; endpoint hardening.
- Launch the six fast-track services to exercise the shared stack and demonstrate value.

Phase 2: Expansion and institutionalization (Years 1–2)

- Broaden onboarding of ministries and systems to the exchange; designate SSoTs and data stewards.
- Extend the common data model with sector accelerators; publish API standards and developer playbooks.
- Migrate appropriate workloads to cloud; modernize PFM; extend CRM-based workflows.
- Run annual independent security audits; refine incident response; scale capacity building.
- Codify SPU processes; begin transition planning toward a DTA with a formal mandate.

Phase 3: Scale, optimize, and formalize (Years 2–3)

- Formalize the DTA; evolve portfolio governance; embed EA gates in procurement and project approvals.
- Expand shared capabilities (payments, consent management, case orchestration, document exchange).
- Implement comprehensive data governance (catalogs, quality monitoring, role-based access).
- Optimize costs (FinOps), performance SLAs, and resilience (regular DR exercises).
- Extend the portal to more joined-up services; launch analytics/insights for performance and policy.

Ongoing activities across phases

- Communications and change management; training and communities of practice.
- Continuous improvement loops from audits, metrics, and user feedback.
- Vendor/partner management with knowledge transfer milestones and exit ramps to limit lock-in.

Operating Model, Roles, and Accountability

- Council of Ministers: Endorses policy/standards; arbitrate exceptions; sustains political ownership.
- Steering Committee: Cross-ministry oversight; prioritization; risk/issue escalation; benefit tracking.
- SPU → DTA: Owns architecture, standards, shared platforms, developer enablement, onboarding, and compliance monitoring; runs the exchange, identity, and portal.
- Ministry CIOs/IT leads: Implement standards locally; manage line-of-business systems; coordinate data stewardship; ensure onboarding and security alignment.
- Data owners/stewards: Maintain SSoT quality; manage access rules; enforce data lifecycle and quality controls.
- Security function (CISO/SOC): Define baselines; monitor and respond to threats; drive security by design; report independently on risk posture.
- Vendors/partners: Deliver to standards and reference architectures; provide knowledge transfer; meet security and interoperability acceptance criteria.

Methodology

The approach follows TOGAF principles, emphasizing the Architecture Development Method across vision, principles, target state, governance, and iterative delivery. Capability maturity is assessed using the US Federal ACMM to diagnose current state and guide development. RACI matrices and stakeholder mapping clarify roles across ministries, SPU/DTA, oversight bodies, and delivery partners. Framing the transition from fragmented, ad hoc integrations to standardized shared platforms and end-to-end digital journeys, the implementation focuses on foundational building blocks, prioritized services, and a phased roadmap to manage risk and deliver early, demonstrable results.

Conclusion

This document positions digital government as a sovereign capability encompassing law, policy, operating model, and engineering, rather than a set of discrete projects. Its cornerstone is a managed, standards-based interoperability layer, anchored by a common data model. Early investment in shared platforms and select high-impact services generates momentum, demonstrates value, and mitigates risk. Sustainable success requires institutionalization through the DTA, continuous capacity building, rigorous security, and disciplined procurement aligned with open standards and reusable components.

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