

OPERATIONAL SOVEREIGNTY for Canadian Organizations

Capstone Research Brief

From digital-sovereignty principles to evidence-backed decisions about critical digital services

The question this research asks

When an organization depends on cloud, SaaS, identity, AI, networks or other technology providers, which consequential actions must remain possible on its own terms, and what evidence proves that capability?

Gopi Haran M

MBA, Technology Innovation & Entrepreneurship
International Business University, Toronto
Industry Capstone Sponsor: Creative Emergy Inc.
External brief prepared August 2026

Purpose: A concise, shareable summary of the capstone research. This brief is not a certification, legal opinion, accredited assurance method, or substitute for CAN/DGSI 100-8 conformity assessment.

01 Executive overview

The project began as a Canadian sovereign-cloud / sovereign-compute market-entry study and evolved into a narrower organizational decision method: determine how much operational sovereignty a critical digital service requires, establish what the available evidence actually demonstrates, identify the dependency that caps the service, and recommend proportionate action.

Working definition

Organizational digital sovereignty is the degree to which a legally constituted organization retains lawful, accountable and revocable decision authority over a defined critical digital service and can exercise that authority within accepted limits despite external providers, jurisdictions and dependencies.

What I built

Component	Purpose
Five-position Sovereignty Ladder	Sets a proportionate target and reports the highest operationally demonstrated service position.
Four business outcomes	Explains why the target matters: continuity; protection; accountability and assurance; strategic choice and exit.
Six capability families	Tests what the organization must be able to decide, control, verify, recover, replace and adapt.
Ten cross-cutting control domains	Shows where a capability can be enabled or defeated across technology, operations, legal and commercial dependencies.
Capability Test Matrix (CTM)	Normalizes each test around actor, action, object, condition, acceptance limit, dependency and required evidence.
Evidence and critical-gate logic	Separates claims from tested proof and prevents strong averages from hiding one decisive dependency.
Readiness Assessment workflow	Turns the framework into a vendor-neutral advisory process: discover, set target, test, conclude, prioritize and reassess.

Four findings that changed the project

- Sovereignty is not data residency. Domestic location can help, but location alone does not establish decision authority, continuity, reversibility or provider exit.
- Sovereignty is not complete self-sufficiency. The practical objective is governed interdependence: understand dependencies, accept some deliberately, and make critical ones non-decisive or reversible.
- Sovereignty is not a single enterprise score. The correct unit is a bounded critical service because different services can justify different target levels.
- Evidence matters as much as design. A policy, contract or provider claim is weaker than an exercised recovery, revocation, migration or substitution test.

02 How the Canadian standard fits

CAN/DGSI 100-8:2026 became a critical external benchmark during the capstone. Its publication validated much of the project direction, but it also required a correction to the originality claim. Canada now has a formal organizational digital-sovereignty baseline. OSAF is therefore positioned as a complementary operationalization and advisory method, not as a competing Canadian standard.

CAN/DGSI 100-8 baseline	OSAF V1 complementary contribution
Organizational digital-sovereignty framework	A bounded critical-service assessment with target and achieved ladder positions

CAN/DGSI 100-8 baseline	OSAF V1 complementary contribution
Organizational objectives and desired degree	Five cumulative service positions from External Dependence to Operational Sovereignty
Data, operational and technology indicators	Four outcomes, six capabilities and ten detailed cross-cutting diagnostic domains
Evidence-based assessment	Canonical action tests plus evidence-strength and confidence treatment
Portability, exit and transition expectations	Move-and-Replace tests constrained by time, cost, functionality, loss and required provider cooperation
Governance and accountability	Explicit decision-authority, revocability, observability and assurance tests
Degree / readiness result	One service-level conclusion with critical-gate rationale and drill-down diagnostics
Conformity-assessment potential	A pre-assurance readiness and improvement workflow; no certification claim

Positioning in one sentence

CAN/DGSI 100-8:2026 provides the Canadian normative baseline. OSAF asks how to apply that baseline to one critical service, test whether required actions are actually exercisable, grade the evidence, expose decisive dependencies and convert the gap into a management roadmap.

Research base

The capstone used a structured mix of academic literature, Canadian law and government material, standards, regulatory resilience guidance, institutional research, vendor documentation and selected practitioner commentary. Source authority was matched to claim strength rather than treating all references equally.

- Conceptual lineage: political sovereignty, organizational legal agency, digital sovereignty, technological sovereignty and governed interdependence.
- Canadian baseline: CAN/DGSI 100-8:2026 and Government of Canada digital-sovereignty guidance.
- Operational prior art: OSFI B-10 and E-21, DORA, NIST risk and supply-chain frameworks.
- Structural ladder precedent: European Commission Cloud Sovereignty Framework (SEAL-0 to SEAL-4), adapted transparently rather than copied semantically.

03 The Sovereignty Ladder

The Ladder represents the service's posture on a spectrum. The target is the level the business requires; the achieved level is the highest cumulative level whose critical gates are demonstrated with sufficient evidence. The highest level is not automatically the goal.

OS-0 External Dependence	OS-1 Formal Protection	OS-2 Business Continuity	OS-3 Operational Autonomy	OS-4 Operational Sovereignty
--------------------------------	------------------------------	--------------------------------	---------------------------------	------------------------------------

Level	Executive meaning	What must be demonstrated
OS-0	External Dependence	Boundary, authority or evidence is unknown, or an external actor can block the required action without an effective remedy.
OS-1	Formal Protection	Law, governance, contracts, responsibilities, protection and accountability are established, but continuity under disruption is not yet demonstrated.
OS-2	Business Continuity	The complete service can continue or recover within approved tolerances for defined disruptions; strategic exit may still be provider-dependent.
OS-3	Operational Autonomy	The organization can decide, revoke, administer, verify, recover, move and replace within accepted limits without case-by-case permission from the actor being tested.

Level	Executive meaning	What must be demonstrated
OS-4	Operational Sovereignty	Independent or reversible paths are tested and independently assured; no single unaccepted external actor or jurisdiction can defeat a critical action within scope.

Critical-gate rule

No averaging away a decisive dependency

If one indispensable condition fails, the achieved level is capped below that gate. Strong results in other domains remain useful diagnostics, but they cannot compensate for an inaccessible emergency identity, unusable recovery key, incomplete export, untested recovery path or other dependency that defeats the required service action.

04 From business outcome to evidence

OSAF uses a deliberate drill-down. The executive sees one target and one achieved level; the layers below explain why.

Framework layer	Question answered	Output
Sovereignty Ladder	How sovereign must the service be, and how sovereign is it?	Target and achieved OS level
Business outcomes	Why does that level matter?	Required business result and acceptance condition
Capabilities	What must the organization be able to do?	Six capability requirements and diagnostics
Control domains	Where can the capability be enabled or defeated?	Dependency map and domain coverage
Canonical tests + evidence	What proves or disproves the claim?	CTM result, evidence strength and confidence

Four business outcomes

Outcome	Plain-language purpose
Critical Service Continuity	Keep or restore the complete service within approved disruption tolerances.
Data, Rights and Knowledge Protection	Protect data, privacy rights, intellectual property, keys, models, source and records, while keeping relevant rights exercisable.
Accountability and Assurance	Know who did what, prove controls operated, meet obligations and challenge or defend consequential decisions.
Strategic Choice and Exit	Change, exit, substitute or reverse delegated authority within accepted limits.

Six capability families

Decide and Govern

Set requirements, assign authority, approve/deny, revoke, invoke rights and accept residual dependency.

Observe and Verify

Inspect activity, monitor dependencies, reconstruct decisions and prove what happened.

Move and Replace

Export, migrate, switch or substitute data, applications,

Administer and Control

Configure, operate, issue/revoke access, use keys and stop or reverse actions.

Continue and Recover

Maintain or restore the complete service within RTO/RPO, safety and degraded-mode limits.

Maintain and Adapt

Patch, rebuild, modify and evolve the service as technology,

platforms, models or suppliers.

obligations and suppliers change.

05 Ten cross-cutting control domains

The domains are not a technology stack and they are not separate scores. They identify where a required capability may be enabled or defeated. A single capability, such as recovery, can depend simultaneously on identity, keys, applications, networks, contracts and provider operations.

Domain	What it examines
1. Infrastructure and hosting	Facilities, power, hardware, storage, virtualization and capacity
2. Cloud platform and control plane	Tenant administration, orchestration, provider operations, support and region controls
3. Data and cryptographic control	Access, flow, retention, deletion, export, backup, encryption, keys and secrets
4. Identity and privileged access	Identity issuance, federation, privilege, emergency access and revocation
5. Applications and middleware	Code, runtime, configuration, interfaces, databases, integrations and licences
6. AI models, compute and deployment	Models, APIs, data, evaluation, compute, guardrails and deployment
7. Security, monitoring and incident response	Logs, detection, investigation, response, forensics and assurance
8. DevOps and digital supply chain	Source, repositories, pipelines, artifacts, dependencies, provenance and updates
9. Network and connectivity	Telecom, routing, DNS, certificates, registries, peering and alternate paths
10. Governance, legal, compliance and commercial	Decision rights, policies, contracts, audit, law, procurement, exit and accountability

How a test is written

Canonical test grammar

The organization can [perform a defined action] over [an asset or dependency], under [a named threat, disruption or material change], within [an accepted limit], without [unacceptable reliance on the actor or environment being tested], supported by [required evidence].

Evidence strength is separate from sovereignty level

Evidence strength	Meaning
Claimed	A person or provider states that the control or capability exists.
Documented	Policies, contracts, designs or procedures describe it.
Implemented	The control is observable in the operating environment.
Monitored	Operation, exceptions and failures are tracked.
Tested	The required action has been demonstrated under a relevant condition.
Independently Assured	A sufficiently separate party assesses the control and supporting evidence within scope.

06 How the Readiness Assessment works

The client-facing workflow is intentionally simpler than the full research model. It converts sovereignty from an abstract concern into a governed decision about one service.

1	DISCOVER	Define service boundary, actors, jurisdictions, dependencies and business impact.
2	SET TARGET	Approve one proportional ladder level, scenario set, acceptance limits and risk authority.
3	TEST	Run CTM interviews, inspect evidence and perform feasible walkthroughs or exercises.
4	CONCLUDE	Apply cumulative gates, assign achieved level and confidence, identify blocking dependencies.
5	PRIORITIZE	Recommend actions based on target gap, business impact, feasibility, cost and trade-offs.
6	REASSESS	Verify remediation, retest critical gates and respond to material change.

Minimum client outputs

- Executive scope and decision statement; service boundary, actor, jurisdiction and dependency map.
- Approved target Sovereignty Ladder level and level-specific acceptance criteria.
- Capability Test Matrix and evidence register; achieved level with High/Moderate/Low confidence.
- Business-outcome, capability and control-domain diagnostic; critical-gate and residual-dependency register.
- Prioritized recommendations with owner, required proof and trade-offs; board-ready briefing and reassessment plan.

What differentiates the method

Choice	Why it matters
Standards-aligned, not standards-replacing	Keeps CAN/DGSI 100-8 as the baseline and makes the OSAF additions traceable.
Critical-service scope	Avoids one enterprise-wide score that hides different dependencies across services.
Authority and revocability	Separates retained decision rights from provider-delegated administration.
Evidence and exercised capability	Treats a test as stronger than self-attestation or marketing language.
Buyer-side neutrality	Supports recommendations across suppliers rather than steering toward one platform.

07 What is adapted, and what is author-developed

The capstone deliberately declares its source lineage. The objective is not to re-label existing frameworks as original work; it is to integrate them transparently into a coherent service-level decision method.

Construct	Source basis	Status in this project
Organizational digital-sovereignty definition	Political/rights lineage; Canadian corporate law; digital-sovereignty literature; Government of Canada; CAN/DGSI	Author synthesis
Five-position architecture	European Commission SEAL-o to SEAL-4; Canadian spectrum corroboration	Structurally adapted

Construct	Source basis	Status in this project
OS-0 to OS-4 labels and criteria	SEAL structure; CAN/DGSI; OSFI; literature; sponsor feedback	Author-developed organizational adaptation
Four business outcomes	Structured source-cluster review	Author synthesis
Six capability families	Recurring actions in standards, regulation and literature	Author synthesis
Ten control domains	Cloud, identity, data, AI, resilience, supply-chain and legal prior art	Author-developed diagnostic structure
Canonical-test grammar / CTM	NIST assessment methods; resilience and third-party testing practice	Author-developed assessment schema
Evidence-strength ladder	NIST assessment; OSFI/DORA testing; assurance practice	Author-developed evidence scale
Critical-gate rule	EC minimum-level logic plus critical-operation/dependency prior art	Author-developed roll-up rule

Current status and limitations

OSAF V1 should be treated as an initial literature- and standards-grounded synthesis, not a proven assessment standard. The capstone includes an illustrative fictional service walkthrough, but no live client pilot or external expert validation was completed within the academic project.

- The ladder, outcomes, capability families, control domains, CTM and gate rule require pilot calibration and inter-assessor testing.
- Legal and jurisdictional analysis is general and cannot replace fact-specific legal advice.
- Market evidence supports relevance and concentration concerns, but does not establish addressable market, willingness to pay or revenue.
- New 2026 standards and policy sources may be interpreted, supplemented or revised over time.
- The proposed next step is a controlled pilot with design partners before any certification, software product or scaled commercial claim.

Proposed next step

Finalize and map OSAF V1 clause-by-clause to CAN/DGSI 100-8:2026, then pilot it on bounded critical services with independent reviewers to test construct clarity, evidence feasibility, inter-assessor consistency and decision usefulness.

08 Selected references

The full academic report contains the complete reference list. The sources below are the most useful external anchors for understanding the project's lineage and positioning.

Digital Governance Council. (2026). CAN/DGSI 100-8:2026 Data Governance – Part 8: Framework for Digital Sovereignty (2nd ed.). [Link](#)

European Commission. (2025). Cloud Sovereignty Framework (Version 1.2.1). [Link](#)

Treasury Board of Canada Secretariat. (2025). Digital sovereignty: A framework to improve digital readiness of the Government of Canada. [Link](#)

Office of the Superintendent of Financial Institutions. (2024). Third-party risk management guideline (B-10). [Link](#)

Office of the Superintendent of Financial Institutions. (2024). Operational risk management and resilience guideline (E-21). [Link](#)

Couture, S., & Toupin, S. (2019). What does the notion of “sovereignty” mean when referring to the digital? *New Media & Society*, 21(10), 2305–2322. [Link](#)

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4). [Link](#)

Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy. *Research Policy*, 52(6). [Link](#)

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, 8(1). [Link](#)

Canadian Shield Institute. (2026). Foundations of Digital Sovereignty. [Link](#)

About this brief

This document is an external summary of an MBA capstone research project developed with Creative Emergy Inc. It is intended for professional discussion and feedback. OSAF V1 remains a research and pilot-stage method and should not be represented as an approved Digital Governance Council methodology, a National Standard of Canada, or an accredited conformity-assessment scheme.