Linux Association of Canada

A PRACTICAL GUIDE TO DIGITAL SOVEREIGNTY

FOR CANADIAN ORGANIZATIONS

Understanding Data, Technology, Control and Digital Resilience

PROTECT YOUR DATA | MAINTAIN CONTROL | REDUCE DEPENDENCIES | BUILD RESILIENCE | STRENGTHEN CANADA

Contents

Part One — Foundations of Digital Sovereignty

About This Guide....4

What Is Digital Sovereignty?....6

The Five Elements of Digital Sovereignty....7

Digital Sovereignty, Data Sovereignty, and Data Residency....9

Why Digital Sovereignty Matters....11

Complete Independence Is Not the Goal....13

Part Two — Assessing Your Dependencies

Know What You Depend On....16

Classify Your Information....18

Understand Where Your Data Goes....20

Canadian Hosting Is Not the Same as Canadian Control....22

Privacy and Cross-Border Processing....24

Part Three — Technical Foundations

Vendor Lock-In....27

Open Standards and Interoperability....30

How Open Source Supports Digital Sovereignty....32

Cloud, On-Premises, or Hybrid?....34

Encryption and Control of Keys....36

Part Four — Governance and Administrative Control

Identity and Administrative Control....40

Part Five — Assessing and Prioritizing Risk

A Digital Sovereignty Risk Assessment....43

Practical Steps for Small Organizations....46

Part Six — Tools for Ongoing Practice

Digital Sovereignty Checklist....21

Myth vs. Reality....52

Creating a Digital Sovereignty Policy....54

Part Seven — Resources and Closing Thoughts

Where to Learn More....58

Final Thoughts....60

About the Linux Association of Canada....62

Note: The provided script for “Identity and Administrative Control” cuts off mid-list, then resumes at “A Digital Sovereignty Risk Assessment.” Topics that may fall in between (domain names, backups, exit planning, supply chain awareness, operational resilience, procurement questions) were not included in the material provided. Send them along and they can be inserted in sequence.

PART ONE

Foundations of Digital Sovereignty

About this guide, core concepts, and why they matter

About This Guide

Canadian organizations depend on digital technology for virtually every aspect of their operations. Email, document management, financial systems, websites, databases, cloud storage, video conferencing, and communication platforms have become essential infrastructure—not optional conveniences.

Many of these services are provided by companies operating across multiple countries and legal jurisdictions. This creates a complex web of dependencies that most organizations have not systematically examined.

Consider these questions:

- Where is your organization's data actually stored? Is it in Canada, the United States, Europe, or distributed across multiple jurisdictions?
- Which country's laws may apply to your information? Data stored in Canada may still be subject to foreign legal authority if the provider operates under another nation's jurisdiction.
- Who truly controls the systems your organization depends on? Can you administer them independently, or are you entirely reliant on a single vendor?
- Can your information be exported or migrated to another provider? Are your files in open, portable formats, or locked into proprietary systems?
- What happens if a supplier changes its prices, policies, or terms of service? Do you have credible alternatives, or are you locked in?
- Could your organization continue operating during an outage, cyberattack, or geopolitical disruption? Are your continuity plans tested and realistic?

These questions are at the heart of digital sovereignty—an organization's ability to make meaningful and independent decisions about its digital systems, information, and operations.

This guide is designed for small businesses, non-profits, schools, municipalities, community organizations, and public institutions across Canada. It provides a practical framework for understanding digital sovereignty and taking concrete steps toward greater control, resilience, and independence.

Digital sovereignty does not mean rejecting international technology or disconnecting from the global digital economy. It means understanding your dependencies, managing your risks, and preserving your ability to make informed choices about the technologies that run your organization.


OUR DIGITAL INFRASTRUCTURE
SECURE • RELIABLE • UNDER OUR CONTROL
Linux Association of Canada
STRONGER COMMUNITIES. SECURE SYSTEMS. BETTER CANADA.
CLOUD SERVICES
Email
Collaboration
Document Storage
Backup
USERS & DEVICES
Desktop
Laptop
Mobile
Printers
OUR NETWORK
WEBSITES & PUBLIC SERVICES
• Municipal Website
• School Website
• Non-Profit Site
• Business Site
EMAIL SYSTEM
Municipal Email
School Email
Group Email
FILE STORAGE
Shared Files
Departments
Projects
APPLICATIONS
Finance
HR / Payroll
Permits / Records
Donations / CRM
OUR PRINCIPLES
WE OWN OUR DATA
WE PROTECT OUR COMMUNITY
WE CHOOSE OPEN STANDARDS
WE PLAN FOR RESILIENCE
KEY CONTROL POINTS
ACCESS CONTROL
Who can access what and why
DATA OWNERSHIP
We own our data
ENCRYPTION
Data protected in transit and at rest
BACKUPS
Regular, tested and independent
MONITORING
We detect and respond quickly
VENDOR MANAGEMENT
We choose wisely and review regularly
SECURE RELIABLE RESILIENT
PUBLIC SERVICE MATTERS
PROTECT OUR DATA PROTECT OUR COMMUNITY
COMMUNITY IMPACT
ACTION ITEMS
MFA
BACKUPS
UPDATES
TRAINING
REVIEW ACCESS
INCIDENT PLAN
SMART CHOICES. STRONGER FUTURE.
DIGITAL SOVEREIGNTY STARTS WITH INFORMED CHOICES.
OPEN SOURCE STRONG CANADA

What Is Digital Sovereignty?

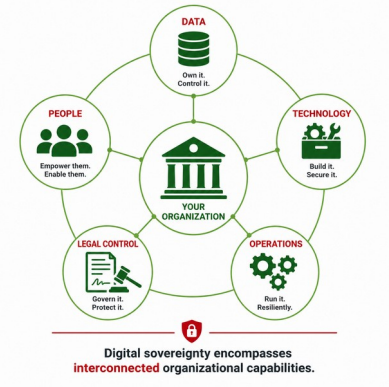
Digital sovereignty is an organization's ability to make meaningful and independent decisions about its digital systems, information, and operations.

The Government of Canada defines digital sovereignty as the ability to exercise autonomy over digital infrastructure, data, and intellectual property, regardless of where technologies are developed, hosted, or supported. This definition extends beyond the physical location of data to include operational resilience, system integrity, legal authority, and institutional control.

For smaller organizations—businesses, non-profits, schools, municipalities, and community groups—digital sovereignty means being able to answer fundamental questions about your technology environment:

- Do we know where our information is stored? Can we identify the physical and legal jurisdictions involved?
- Can we access and export our data? Is our information available in formats we can use elsewhere?
- Are we overly dependent on a single supplier? Would losing access to one platform cripple our operations?
- Can we continue operating if a critical service becomes unavailable? Do we have tested backup and continuity plans?
- Do we control our domain names, administrator accounts, and encryption keys? Or are these held by individuals or third parties?
- Can we migrate to another platform without losing essential information? Have we tested our export and portability options?
- Do we understand the legal and privacy implications of our technology choices? Are we compliant with Canadian privacy law when using foreign providers?

Digital sovereignty is not a single product, certification, or purchasing decision. It is an ongoing approach to governance, technology selection, and risk management. It requires organizations to think strategically about the technologies they adopt, the dependencies they create, and the control they retain.



The Five Elements of Digital Sovereignty

Digital sovereignty rests on five interconnected elements. Organizations that understand and address each element are better positioned to maintain control, manage risk, and preserve operational independence.

1. Data Control

Knowing what information your organization holds, where it is located, who can access it, and how it can be retrieved.

Data control begins with visibility. Organizations must maintain inventories of their information assets, classify data by sensitivity, understand where information is stored and processed, and ensure they can export or migrate data when necessary. Data control also means understanding who—employees, contractors, service providers, or foreign governments—may have access to organizational information.

2. Technological Choice

Maintaining the ability to select, replace, modify, or integrate technologies without unreasonable restrictions.

Technological choice means avoiding vendor lock-in. Organizations should prefer open standards, interoperable systems, and technologies that allow migration to alternative providers. This does not require avoiding commercial software—it means ensuring that technology decisions preserve future flexibility rather than creating permanent dependencies.

3. Operational Resilience

Ensuring that essential services can continue during outages, supplier changes, cyber incidents, or geopolitical disruptions.

Operational resilience requires backup systems, documented procedures, alternative suppliers, and tested continuity plans. Resilient organizations can recover from ransomware attacks, survive cloud service outages, and continue operating when a critical vendor fails or changes terms. Resilience is not optional—it is a core requirement for organizational sustainability.

4. Legal and Jurisdictional Awareness

Understanding which laws, contracts, and foreign jurisdictions may apply to organizational data and services.

Legal awareness means understanding that data stored in Canada may still be subject to foreign legal authority if the service provider operates under another country's jurisdiction. Organizations must evaluate privacy obligations, contractual terms, government access risks, and compliance requirements. Legal awareness also means seeking appropriate legal counsel when handling sensitive, regulated, or confidential information.

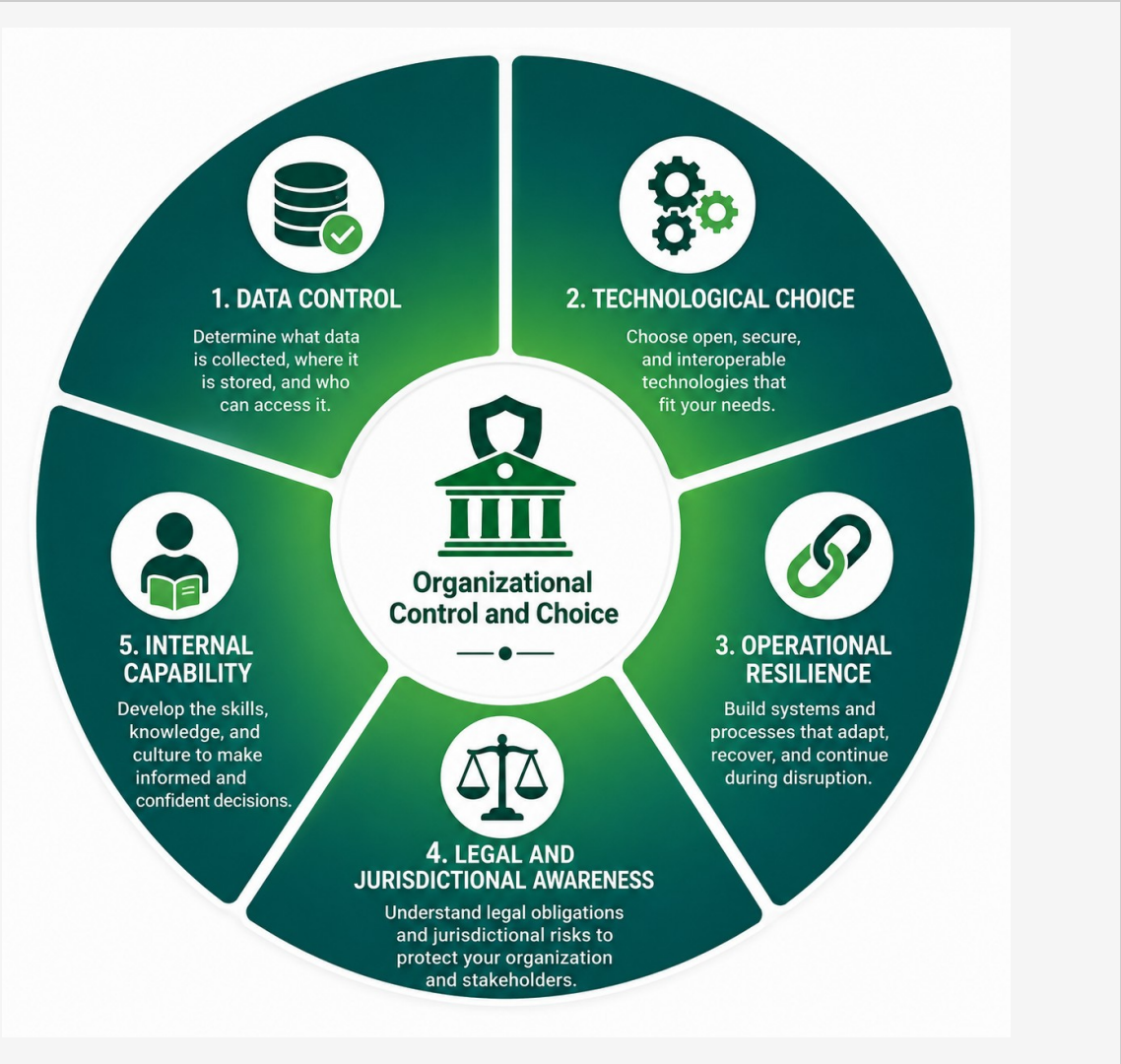
5. Internal Capability

Maintaining sufficient knowledge, documentation, and technical skill to make informed decisions rather than depending entirely on outside suppliers.

Internal capability does not require organizations to employ large IT departments. It means ensuring that someone within the organization understands critical systems, maintains documentation, can evaluate vendor claims, and can make informed technology decisions. Organizations that lack internal capability are vulnerable to vendor manipulation, poor purchasing decisions, and inability to respond effectively during crises.

These five elements are interconnected. An organization may store its data in Canada (data control) but still have limited sovereignty if it cannot export that data (technological choice), lacks backup systems (operational resilience), is subject to foreign legal authority (jurisdictional awareness), or has no one who understands the system (internal capability).

Effective digital sovereignty requires attention to all five elements, not just one or two.



Digital Sovereignty, Data Sovereignty, and Data Residency

These three terms are related but distinct. Understanding the differences is essential for making informed technology decisions.

Data Residency

Data residency refers to the physical or geographic location where information is stored.

A file stored on a server in a Toronto data center has Canadian data residency. A database hosted in a Montreal facility has Canadian data residency. Data residency is about physical location—where the hardware and storage media are located.

Example: An organization contracts with a cloud provider that operates data centers in Canada. The organization selects the Toronto region for storage. The data has Canadian residency.

Data Sovereignty

Data sovereignty concerns the laws and legal authorities that may apply to information.

Data sovereignty recognizes that the physical location of data does not always determine which laws govern it. Data stored in Canada may still be managed by a company that is incorporated in the United States, operates under U.S. legal jurisdiction, and may be subject to U.S. government access requests under laws such as the CLOUD Act.

Example: The same organization stores data in Toronto, but the cloud provider is a U.S.-based company. While the data has Canadian residency, it may still be subject to U.S. legal authority because the provider operates under U.S. jurisdiction.

Digital Sovereignty

Digital sovereignty is the broadest concept. It includes:

- Data – location, access, and control
- Infrastructure – servers, networks, and hosting
- Software – applications, platforms, and code
- Intellectual property – ownership and licensing
- Legal control – jurisdiction, contracts, and compliance
- Supplier dependencies – vendor relationships and lock-in risks
- Technical capability – internal knowledge and skills
- Operational continuity – resilience and recovery

Digital sovereignty encompasses data residency and data sovereignty, but it also addresses technology choice, operational resilience, administrative control, and organizational capability.

The Government of Canada similarly distinguishes these concepts. Its guidance defines data residency as the physical location of data, data sovereignty as the legal right to control access to and disclosure of digital information, and digital sovereignty as the broader ability to exercise autonomy over digital infrastructure, data, and intellectual property.

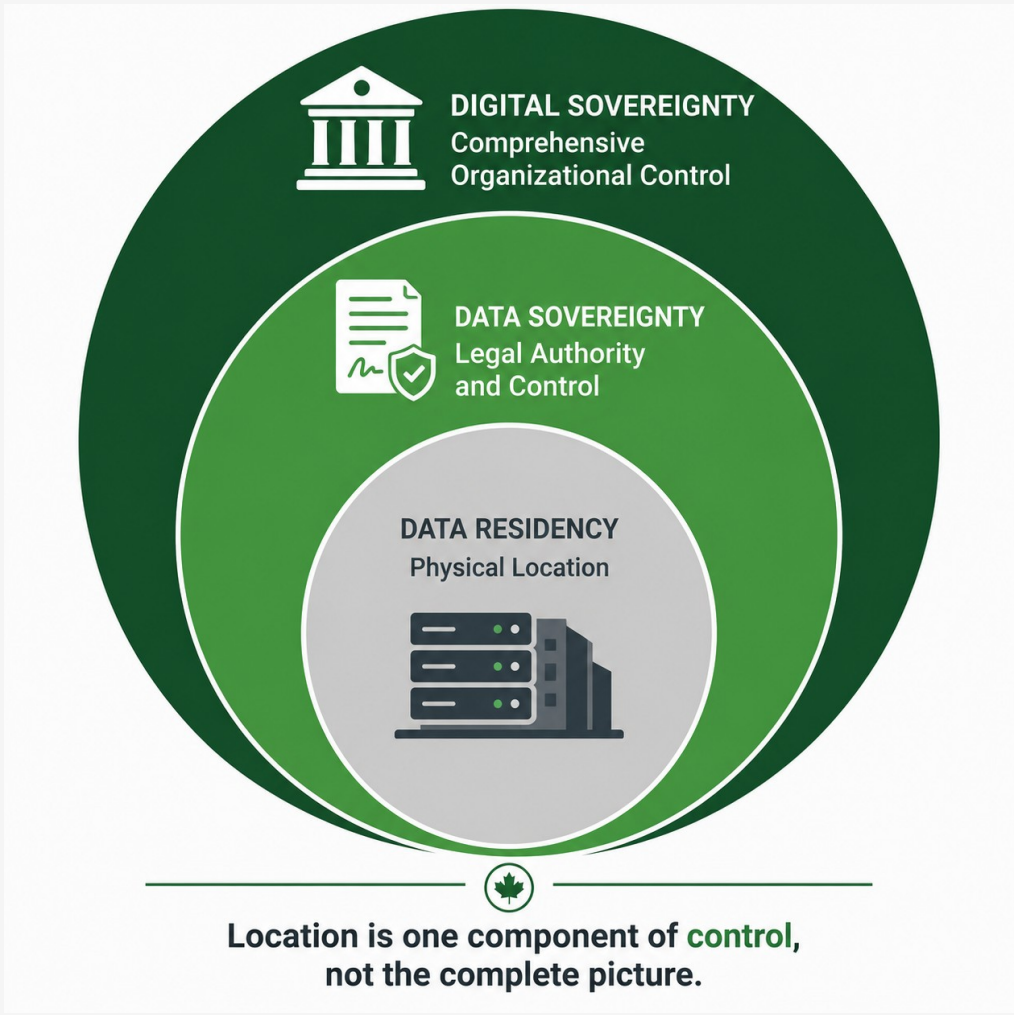
Key Point

Keeping data in Canada can reduce certain risks, but location alone does not guarantee complete control.

An organization that stores data in Canada but uses proprietary software, lacks export capabilities, depends entirely on one vendor, and has no internal technical capability has limited digital sovereignty—even though it has Canadian data residency.

Conversely, an organization that uses open-source software, maintains independent backups, controls its encryption keys, and has documented migration plans may have strong digital sovereignty—even if it uses some international services.

Digital sovereignty is about control, choice, and resilience—not just location.



Why Digital Sovereignty Matters

Digital services are often treated as simple utilities—like electricity or water. However, each digital service creates long-term operational, legal, and financial dependencies that can significantly affect an organization's ability to function independently.

A lack of digital sovereignty can lead to serious consequences:

Loss of Access to Organizational Information

If a vendor terminates service, experiences a business failure, or suspends an account, organizations without proper backups and export capabilities may lose access to years of critical information—emails, documents, financial records, customer data, and institutional knowledge.

Unexpected Price Increases

Organizations locked into proprietary platforms have limited negotiating power. Vendors can increase prices significantly, knowing that migration is difficult or impossible. Small organizations and non-profits are particularly vulnerable to pricing changes that strain limited budgets.

Difficult or Expensive Migrations

Vendor lock-in can make it prohibitively expensive to change providers. Migration costs may include data extraction fees, format conversion, system reconfiguration, staff retraining, and operational disruption. Some organizations remain with unsuitable vendors simply because leaving is too costly.

Exposure to Foreign Legal Demands

Data stored or processed by companies subject to foreign jurisdiction may be accessible to foreign governments through legal mechanisms such as national security letters, court orders, or extraterritorial legislation. Organizations handling sensitive information—health records, legal files, confidential business information—may face privacy and compliance risks.

Service Interruptions

Dependence on a single provider creates a single point of failure. Cloud outages, cyberattacks, network disruptions, or geopolitical events can render essential services unavailable. Organizations without backup systems or alternative providers may be unable to operate during extended outages.

Reduced Privacy and Confidentiality

Some service providers collect extensive metadata, analyze user behavior, or share information with third parties. Organizations may inadvertently expose confidential information through analytics, advertising networks, or data-sharing agreements embedded in terms of service.

Restricted Access to Source Code or System Configurations

Proprietary systems often prevent organizations from understanding how their technology works, customizing functionality, or fixing problems independently. This creates dependence on

vendor support and limits an organization's ability to adapt systems to specific needs.

Inability to Recover Data After Supplier Failure

When vendors go out of business, are acquired, or discontinue products, organizations may lose access to their data entirely. Without independent backups and documented export procedures, information may become permanently inaccessible.

Dependence on Proprietary File Formats

Proprietary formats can make information unusable outside a specific application. Organizations may find that years of documents, databases, or records cannot be opened, migrated, or preserved without continued access to legacy software.

Difficulty Meeting Contractual or Regulatory Obligations

Organizations subject to privacy laws, records retention requirements, or contractual obligations may struggle to comply when they lack control over their data, cannot produce required reports, or cannot demonstrate where information is stored and who has access.

Digital sovereignty helps organizations protect more than data. It protects their ability to operate, serve members, deliver programs, and make independent decisions.

Organizations that understand their dependencies, maintain control over critical systems, and build resilience are better positioned to navigate technological change, economic pressure, and operational disruption.

Complete Independence Is Not the Goal

No modern organization can operate in complete technological isolation.

Computers, processors, network equipment, cloud infrastructure, and software are produced through global supply chains. Even locally hosted systems depend on international standards, open-source projects, hardware manufacturers, and technical expertise developed collaboratively across borders.

Complete digital independence is neither achievable nor desirable.

The global digital economy enables innovation, reduces costs, provides access to specialized expertise, and allows organizations to benefit from technologies they could never develop independently. Canadian organizations participate in and benefit from this interconnected ecosystem.

The Goal Is Not Isolation—It Is Informed Dependency Management

Digital sovereignty is about understanding and managing dependencies, not eliminating them.

The goal is to:

- Understand important dependencies – Know which systems, vendors, and technologies your organization relies on
- Avoid unnecessary lock-in – Choose technologies that preserve future flexibility and choice
- Maintain credible alternatives – Ensure that you can change providers if necessary
- Protect sensitive information – Apply stronger controls to confidential and regulated data
- Retain access to organizational data – Ensure you can export, migrate, and preserve your information
- Build recovery and migration options – Maintain backups, documentation, and tested continuity plans
- Make risk-based technology decisions – Evaluate vendors, contracts, and technologies based on your organization's specific needs and risk tolerance

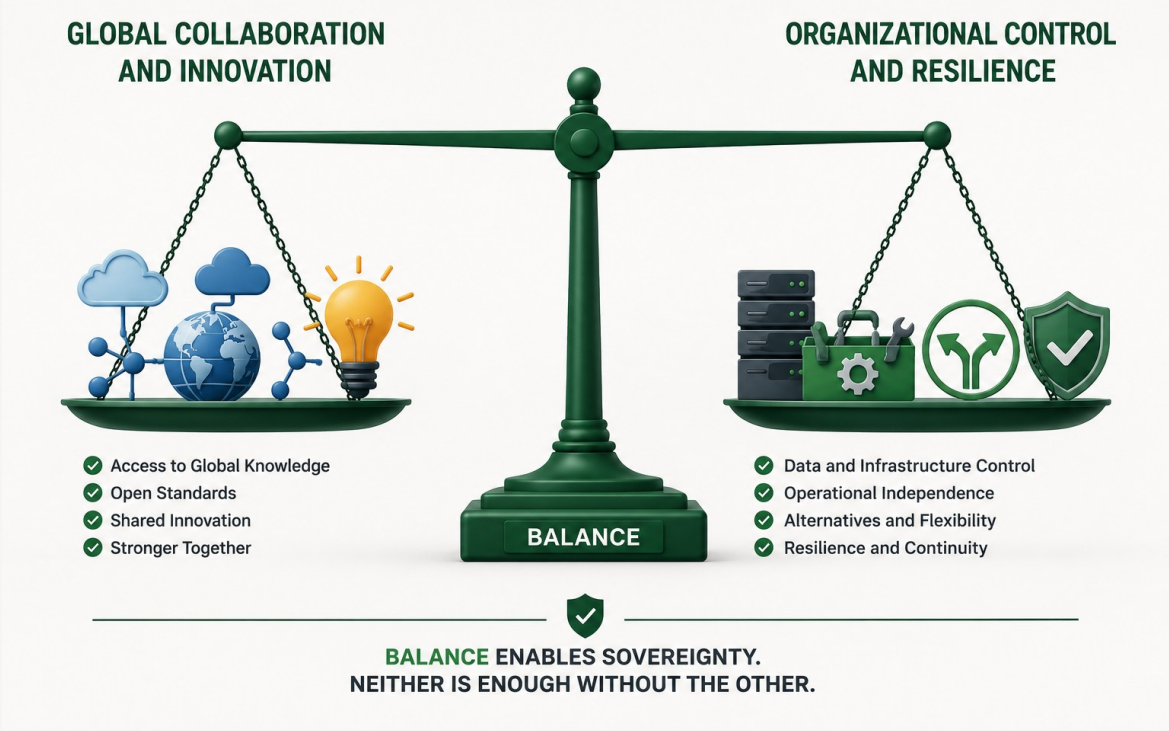
The Government of Canada similarly recognizes that complete digital autonomy is not realistically achievable in an interconnected world. Its approach focuses on managing legal, supply-chain, technical, and operational risks proportionately—applying stronger controls where risks are higher and accepting reasonable dependencies where risks are manageable.

Digital Sovereignty Is About Balance

Organizations must balance:

- Global collaboration with organizational control
- Innovation and capability with resilience and independence
- Cost and convenience with risk and long-term sustainability
- Vendor expertise with internal capability
- Standardization with flexibility

The strongest approach is not to reject international technology, but to use it strategically—understanding what you depend on, maintaining alternatives, and preserving your ability to make independent decisions when circumstances change.



PART TWO

Assessing Your Dependencies

Inventory, classification, data flows and hosting risk

Know What You Depend On

An organization cannot control risks it has not identified.

The foundation of digital sovereignty is visibility—understanding what systems you use, who provides them, where your data is stored, and what would happen if a critical service became unavailable.

Create a Digital Inventory

Begin by creating a comprehensive inventory of your organization's digital systems and services.

Record the systems used for:

- Email and communication
- File storage and document management
- Websites and web hosting
- Accounting and financial management
- Payroll and human resources
- Customer, client, or member records
- Online meetings and video conferencing
- Project management and collaboration
- Fundraising and donor management
- Marketing and communications
- Databases and information systems
- Backups and disaster recovery
- Cybersecurity and threat protection
- Identity and account management

For Each System, Record:

- Service provider – Who provides the service?
- Country of ownership – Where is the company incorporated?
- Hosting location – Where is data physically stored?
- Type of information stored – What data does the system contain?
- Primary administrator – Who manages the system?
- Contract renewal date – When does the agreement expire?
- Export options – Can data be exported? In what format?
- Backup arrangements – Are independent backups maintained?
- Alternative providers – What other options exist?
- Importance to operations – How critical is this system?

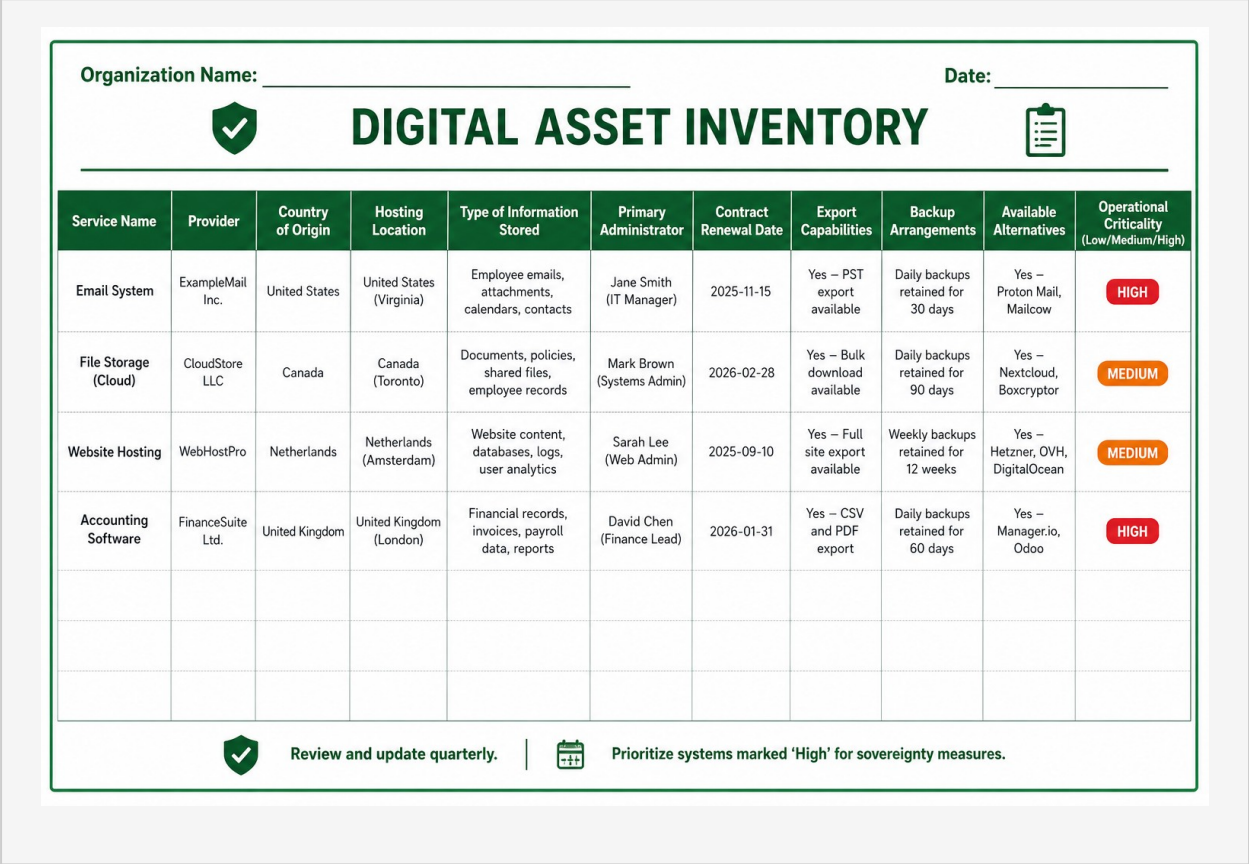
Practical Question

What would happen tomorrow if this service suddenly became unavailable?

For each system in your inventory, ask:

- Could we continue operating?
- How long could we function without it?
- Do we have a backup or alternative?
- Can we access our data independently?
- Who would we contact for support?
- What is our recovery plan?

Systems that would cause immediate operational failure if unavailable are your highest-priority dependencies. These systems require the strongest sovereignty measures—independent backups, documented procedures, tested alternatives, and clear administrative control.



Organization Name: _____ Date: _____

DIGITAL ASSET INVENTORY

Service Name	Provider	Country of Origin	Hosting Location	Type of Information Stored	Primary Administrator	Contract Renewal Date	Export Capabilities	Backup Arrangements	Available Alternatives	Operational Criticality (Low/Medium/High)
Email System	ExampleMail Inc.	United States	United States (Virginia)	Employee emails, attachments, calendars, contacts	Jane Smith (IT Manager)	2025-11-15	Yes – PST export available	Daily backups retained for 30 days	Yes – Proton Mail, Mailcow	HIGH
File Storage (Cloud)	CloudStore LLC	Canada	Canada (Toronto)	Documents, policies, shared files, employee records	Mark Brown (Systems Admin)	2026-02-28	Yes – Bulk download available	Daily backups retained for 90 days	Yes – Nextcloud, Boxcryptor	MEDIUM
Website Hosting	WebHostPro	Netherlands	Netherlands (Amsterdam)	Website content, databases, logs, user analytics	Sarah Lee (Web Admin)	2025-09-10	Yes – Full site export available	Weekly backups retained for 12 weeks	Yes – Hetzner, OVH, DigitalOcean	MEDIUM
Accounting Software	FinanceSuite Ltd.	United Kingdom	United Kingdom (London)	Financial records, invoices, payroll data, reports	David Chen (Finance Lead)	2026-01-31	Yes – CSV and PDF export	Daily backups retained for 60 days	Yes – Manager.io, Odoo	HIGH

Review and update quarterly. | Prioritize systems marked 'High' for sovereignty measures.

Classify Your Information

Not every piece of information requires the same level of protection.

A public event poster does not carry the same risk as employee records, health information, or financial data. Applying uniform controls to all information is inefficient and impractical.

A simple classification model helps organizations apply appropriate protections based on the sensitivity and importance of information.

A Four-Tier Classification Model

Public

Information intended for public distribution.

Public information can be freely shared without risk to individuals or the organization. Loss, disclosure, or unauthorized access creates minimal or no harm.

Examples: Website content, public newsletters and announcements, event information and promotional materials, published reports and documents, social media posts, press releases.

Technology considerations: Public information can be stored on any platform, including international cloud services, content delivery networks, and third-party hosting. Sovereignty concerns are minimal, though organizations should still maintain backups and control over accounts.

Internal

Routine organizational information not intended for public distribution.

Internal information supports day-to-day operations but does not contain sensitive personal information or confidential business details. Unauthorized disclosure would be inconvenient but would not cause significant harm.

Examples: Meeting notes and agendas, internal procedures and policies, project plans and schedules, non-confidential correspondence, general operational documents.

Technology considerations: Internal information can generally be stored on commercial platforms, but organizations should understand where data is located, ensure it can be exported, and maintain reasonable access controls.

Confidential

Information that could harm individuals or the organization if disclosed.

Confidential information requires stronger protections. Unauthorized access, disclosure, or loss could result in privacy violations, financial harm, reputational damage, or legal liability.

Examples: Donor and member records, employee files and personnel information, membership databases, contracts and agreements, financial records and banking information, business plans and strategic documents, client or customer information.

Technology considerations: Confidential information should be stored with stronger controls: encryption, access restrictions, Canadian hosting where practical, independent backups, and

careful vendor evaluation. Organizations should understand jurisdictional risks and ensure compliance with privacy laws.

Highly Sensitive

Information requiring the strongest controls.

Highly sensitive information, if disclosed, could cause severe harm to individuals, violate legal obligations, or create significant organizational liability. This information requires the highest level of protection.

Examples: Health information and medical records, legal files and privileged communications, credentials, passwords, and encryption keys, protected government information, information subject to solicitor-client privilege, personal information of vulnerable individuals.

Technology considerations: Highly sensitive information should be stored with maximum controls: strong encryption with organization-controlled keys, Canadian hosting, restricted access, comprehensive audit logging, independent backups, and careful legal review. Organizations handling highly sensitive information should seek legal and technical advice to ensure compliance with applicable laws and regulations.

Technology Decisions Should Reflect Information Sensitivity

- Public information → Minimal sovereignty requirements
- Internal information → Moderate sovereignty requirements
- Confidential information → Strong sovereignty requirements
- Highly sensitive information → Maximum sovereignty requirements

Organizations that apply the same controls to all information waste resources. Organizations that fail to protect sensitive information appropriately create unacceptable risks. Classification enables proportionate, risk-based decision-making.

Understand Where Your Data Goes

Information may travel through more locations and systems than organizations expect.

A document uploaded to a cloud platform may be stored, copied, processed, analyzed, and synchronized across multiple countries, data centers, and third-party services—often without the organization's explicit knowledge.

Data Flow Example

Consider a seemingly simple action: uploading a document to a cloud storage service. The document may be:

- Uploaded from a staff computer – The file leaves the organization's direct control
- Transmitted across the internet – Data passes through multiple network providers
- Stored in a primary data center – The file is written to storage in one geographic location
- Copied to a backup location – A redundant copy is created, possibly in a different country
- Processed by analytics services – Metadata is extracted and analyzed
- Accessed by technical support teams – Provider personnel may have administrative access
- Synchronized to mobile devices – Copies are created on smartphones and tablets
- Retained after account closure – Data may remain on provider systems even after deletion

Each step in this process may involve different legal jurisdictions, subcontractors, and access controls.

Questions to Ask Service Providers

Storage and Location

- Where is the primary data stored? (Country and region)
- Where are backups stored?
- Can we select a specific geographic region?
- Is data ever transferred to other locations?

Processing and Access

- Is data processed in countries other than where it is stored?
- Can subcontractors or third-party services access our data?
- Where are support personnel located?
- Who has administrative access to our information?

Retention and Deletion

- How long is deleted information retained?
- Is data permanently deleted upon request?
- Are backups and archives also deleted?
- Can we verify deletion?

Metadata and Analytics

- What metadata is collected?
- Is our data used for analytics, training, or product improvement?
- Can metadata collection be disabled?

Notification and Control

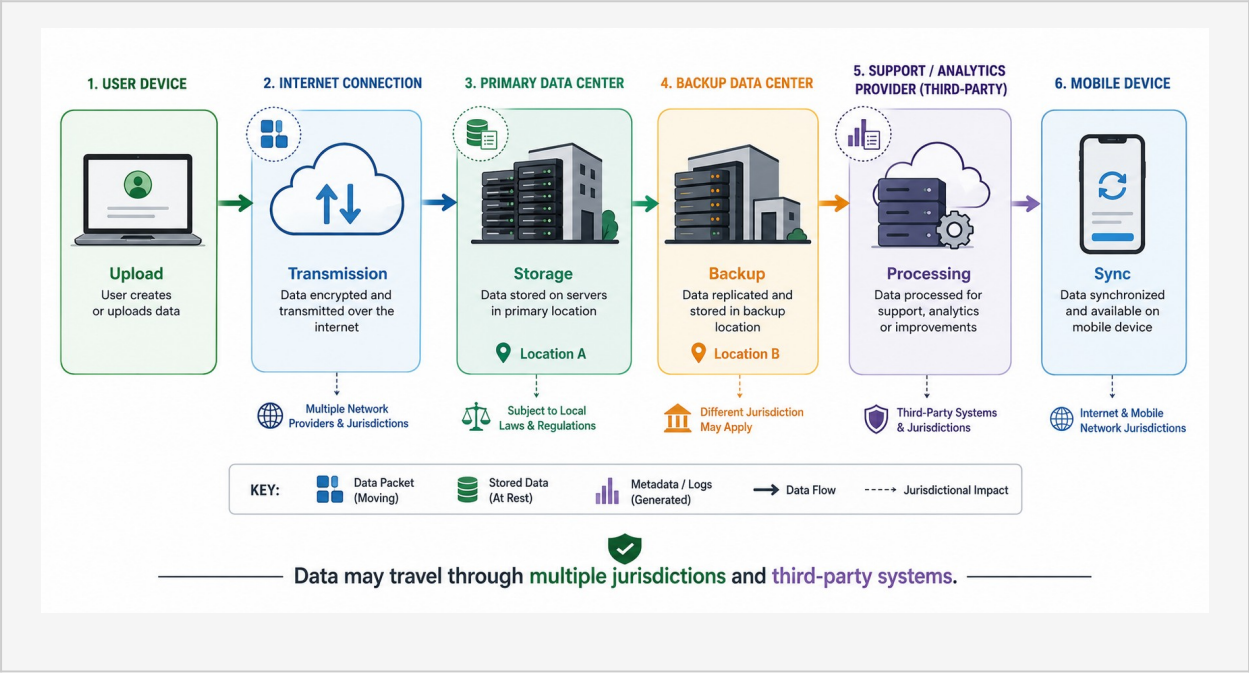
- Will we be notified before data is moved to a new location?
- Can we restrict data transfers?
- Do we have visibility into where our data is at any given time?

Organizations Remain Responsible

Even when data is entrusted to a service provider, the organization remains responsible for compliance with privacy laws, contractual obligations, and duty of care to individuals whose information is held.

“We didn't know where the data was stored” is not a defense against privacy violations or regulatory penalties.

Organizations must understand their data flows, evaluate provider practices, and ensure that contractual agreements include appropriate safeguards.



Canadian Hosting Is Not the Same as Canadian Control

Selecting a Canadian data center is an important step in a digital sovereignty strategy—but it is not sufficient on its own.

Data stored in Canada may still be subject to foreign legal authority, vendor control, and operational dependencies that limit an organization's sovereignty.

Location Is Only One Factor

Corporate Ownership and Jurisdiction

- Where is the provider incorporated?
- Which countries does it operate in?
- What laws may apply to the company?
- Is the company subject to foreign government access requests?

Administrative Access and Control

- Who controls administrator access to the systems?
- Where are support personnel located?
- Can provider employees access organizational data?
- Are access logs available for review?

Encryption and Key Management

- Where are encryption keys held?
- Does the organization control its own keys?
- Can the provider decrypt data?

Subcontractors and Third Parties

- Are subcontractors involved in service delivery?
- Where are subcontractors located?
- What access do they have to data?

Data Transfers and Mobility

- Can data be transferred to other locations without notice?
- Does the organization have control over data location?
- What happens if the provider is acquired by a foreign company?

Government of Canada Guidance

The Government of Canada notes that information stored in Canada may still be affected by foreign law when a service provider is subject to another country's jurisdiction.

For example, a U.S.-based company operating a data center in Canada may still be subject to U.S. legal process and court orders, national security letters and government access requests, the U.S. CLOUD Act (which allows U.S. law enforcement to compel disclosure of data stored anywhere in

the world), and corporate policies and terms of service governed by U.S. law.

The Government of Canada recommends evaluating legal exposure alongside technical, contractual, and security controls. Location is important, but it is not the only consideration.

This Does Not Make International Providers Unsuitable

Understanding jurisdictional risk does not mean organizations must avoid all international providers. Many international providers offer advanced security capabilities, robust infrastructure, competitive pricing, specialized features, and strong contractual protections.

The key is to make informed decisions based on:

- The sensitivity of the information
- The organization's risk tolerance
- Available alternatives
- Contractual safeguards
- Technical controls (such as encryption with customer-managed keys)
- Legal advice where appropriate

Canadian hosting is valuable—but it should be part of a broader sovereignty strategy, not the only consideration.

Privacy and Cross-Border Processing

Canadian organizations remain responsible for personal information entrusted to service providers—even when that information is processed or stored outside Canada.

When personal information is transferred to third parties, including cloud providers, organizations must understand the risks, evaluate providers carefully, and implement appropriate safeguards.

Legal Obligations Under Canadian Privacy Law

The Personal Information Protection and Electronic Documents Act (PIPEDA) applies to private-sector organizations across Canada (with some provincial variations). PIPEDA requires organizations to:

- Obtain meaningful consent for collection, use, and disclosure of personal information
- Limit collection to what is necessary
- Protect personal information with appropriate safeguards
- Be transparent about privacy practices
- Remain accountable for information in the custody of third parties

When personal information is processed outside Canada, it may be subject to the laws of another country—including government access, surveillance, and disclosure requirements that differ from Canadian law. Organizations must understand these risks and communicate them appropriately.

Guidance from the Office of the Privacy Commissioner of Canada

The Office of the Privacy Commissioner of Canada (OPC) provides guidance on cross-border processing of personal information. Key principles include:

1. Understand Which Privacy Laws Apply

Organizations must determine whether PIPEDA, provincial privacy laws (such as Alberta's PIPA or British Columbia's PIPA), or public-sector privacy laws apply to their operations.

2. Limit Collection to Necessary Information

Collect only the personal information required for identified purposes. Avoid collecting unnecessary information that increases risk.

3. Use Written Service Agreements

Contracts with service providers should include a clear description of permitted uses, prohibition on unauthorized disclosure, security and safeguard requirements, breach notification obligations, audit and compliance rights, and data retention and deletion terms.

4. Require Appropriate Safeguards

Service providers must implement security measures appropriate to the sensitivity of the information. Organizations should evaluate provider security practices and require evidence of compliance.

5. Understand Breach Notification Responsibilities

Under PIPEDA's breach notification requirements, organizations must report breaches of security safeguards involving personal information that pose a real risk of significant harm. Organizations remain responsible even when breaches occur at third-party providers.

6. Document Cross-Border Processing

Organizations should document what personal information is transferred, where it is processed and stored, which service providers are involved, what safeguards are in place, and what risks have been identified and mitigated.

7. Explain Practices in Privacy Notices

Privacy policies should inform individuals when their personal information may be processed outside Canada, which countries may be involved, and the purposes for such processing.

8. Seek Legal Advice for Sensitive or Regulated Information

Organizations handling health information, financial records, legal files, or other regulated information should seek legal advice to ensure compliance with applicable laws.

Provincial and Public-Sector Requirements

Provincial privacy laws and public-sector legislation may impose additional obligations. Some provincial laws require consent for cross-border transfers, public-sector organizations may face restrictions on storing data outside Canada, health information is subject to specific provincial legislation, and educational institutions may be governed by sector-specific privacy laws.

Organizations should consult applicable privacy commissioners and legal counsel to understand their specific obligations.

PART THREE

Technical Foundations

Lock-in, open standards, open source, hosting and encryption

Vendor Lock-In

Vendor lock-in occurs when changing service providers becomes unusually difficult, expensive, or disruptive—often to the point where organizations feel they have no realistic alternative.

Lock-in is one of the most significant threats to digital sovereignty. It limits choice, reduces negotiating power, and can trap organizations in relationships that no longer serve their interests.

How Vendor Lock-In Occurs

Proprietary File Formats

Files saved in formats that can only be opened by one application create dependence on that application. If the vendor discontinues the product, increases prices, or changes terms, organizations may be unable to access their own information.

Unavailable or Incomplete Export Tools

Some platforms make it difficult or impossible to export data in usable formats. Export tools may be missing, incomplete, or produce files that cannot be imported into other systems.

High Data Transfer Charges

Vendors may charge significant fees to export large volumes of data, making migration prohibitively expensive.

Custom Integrations and Dependencies

Systems that are deeply integrated with other vendor products create complex dependencies. Changing one system may require changing multiple systems simultaneously.

Long-Term Contracts with Penalties

Contracts with multi-year commitments and early termination penalties can lock organizations into unsuitable arrangements.

Limited or Undocumented APIs

Application Programming Interfaces (APIs) that are proprietary, undocumented, or restricted prevent organizations from integrating with other systems or building migration tools.

Exclusive Identity Systems

Platforms that use proprietary identity and authentication systems make it difficult to move users to alternative platforms without recreating accounts and access controls.

Undocumented Configurations

Systems that do not provide access to configuration details, system settings, or customization code prevent organizations from replicating functionality elsewhere.

Staff Familiarity and Training

Organizations may remain with a platform simply because staff are trained on it and changing would require retraining—even when better alternatives exist.

Questions to Ask Before Adopting a Platform

Export and Portability

- Can we export all our information?
- Is the export complete and usable, or are some data types excluded?
- Are open, standard file formats available?
- Can another system import the exported data?

Migration Costs and Complexity

- What will migration cost in terms of time, money, and disruption?
- How long would a transition take?
- Will we retain access to our data after cancellation?
- Are there data transfer fees?

Alternatives and Competition

- What other providers offer similar functionality?
- Are there open-source alternatives?
- Can we host the software ourselves if necessary?

Contract Terms

- What is the contract length?
- Are there early termination penalties?
- Can we cancel with reasonable notice?

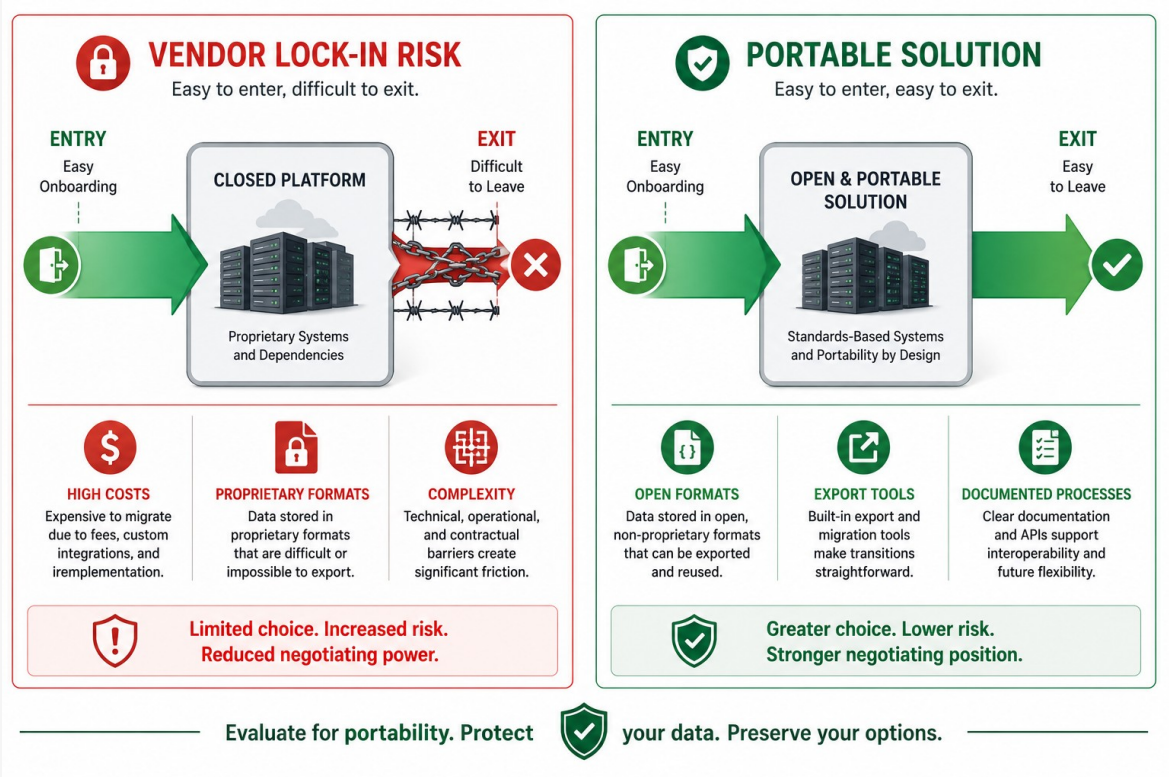
Technical Flexibility

- Does the platform use open standards?
- Are APIs documented and accessible?
- Can we integrate with other systems?
- Can we customize functionality?

The Cost of Lock-In

- Reduced negotiating power – Vendors can increase prices or change terms with little consequence
- Inability to adopt better technologies – Organizations cannot take advantage of innovation elsewhere
- Operational risk – Dependence on a single vendor creates a single point of failure
- Strategic limitations – Technology choices constrain organizational strategy rather than enabling it

A service may be convenient today but difficult to leave later. Evaluate exit options before entry.


VENDOR LOCK-IN RISK
Easy to enter, difficult to exit.
ENTRY
Easy Onboarding
CLOSED PLATFORM
EXIT
Difficult to Leave
Proprietary Systems and Dependencies
HIGH COSTS
Expensive to migrate due to fees, custom integrations, and iremplementation.
PROPRIETARY FORMATS
Data stored in proprietary formats that are difficult or impossible to export.
COMPLEXITY
Technical, operational, and contractual barriers create significant friction.
Limited choice. Increased risk.
Reduced negotiating power.
PORTABLE SOLUTION
Easy to enter, easy to exit.
ENTRY
Easy Onboarding
OPEN & PORTABLE SOLUTION
EXIT
Easy to Leave
Standards-Based Systems and Portability by Design
OPEN FORMATS
Data stored in open, non-proprietary formats that can be exported and reused.
EXPORT TOOLS
Built-in export and migration tools make transitions straightforward.
DOCUMENTED PROCESSES
Clear documentation and APIs support interoperability and future flexibility.
Greater choice. Lower risk.
Stronger negotiating position.
Evaluate for portability. Protect your data. Preserve your options.

Open Standards and Interoperability

Open standards are publicly documented technical specifications that allow different systems to communicate, exchange information, and work together.

Using open standards improves digital sovereignty by reducing vendor lock-in, preserving long-term access to information, and enabling organizations to integrate systems from multiple providers.

What Are Open Standards?

Open standards are technical specifications that are:

- Publicly available – Anyone can access the specification
- Vendor-neutral – Not controlled by a single company
- Implementable by anyone – Multiple vendors can create compatible products
- Stable and maintained – Specifications are updated through transparent processes

Open standards enable interoperability—the ability of different systems to work together and exchange information.

Examples of Open Standards

Document Formats

- PDF and PDF/A – Portable Document Format for documents and archival
- OpenDocument Format (ODF) – Open standard for office documents
- HTML and CSS – Web page structure and styling
- Markdown – Lightweight text formatting

Data Exchange

- CSV (Comma-Separated Values) – Simple tabular data
- JSON and XML – Structured data exchange
- SQL – Database query language

Communication and Collaboration

- SMTP, IMAP, POP3 – Email protocols
- CalDAV and CardDAV – Calendar and contact synchronization
- XMPP – Instant messaging
- WebRTC – Real-time communication

Identity and Authentication

- OAuth and OpenID Connect – Authentication and authorization
- SAML – Single sign-on
- LDAP – Directory services

Web and Internet

- HTTP/HTTPS – Web communication

- DNS – Domain name resolution
- TLS/SSL – Encrypted connections

Benefits of Open Standards

Reduced Vendor Lock-In

Files saved in open formats can be opened by multiple applications. Organizations are not dependent on a single vendor to access their information.

Long-Term Preservation

Open standards are more likely to remain accessible over time. Proprietary formats may become obsolete when vendors discontinue products.

Integration and Interoperability

Systems that use open standards can communicate with each other, enabling organizations to build integrated technology environments from multiple providers.

Competition and Choice

Open standards enable competition. Multiple vendors can offer compatible products, giving organizations more choices and better pricing.

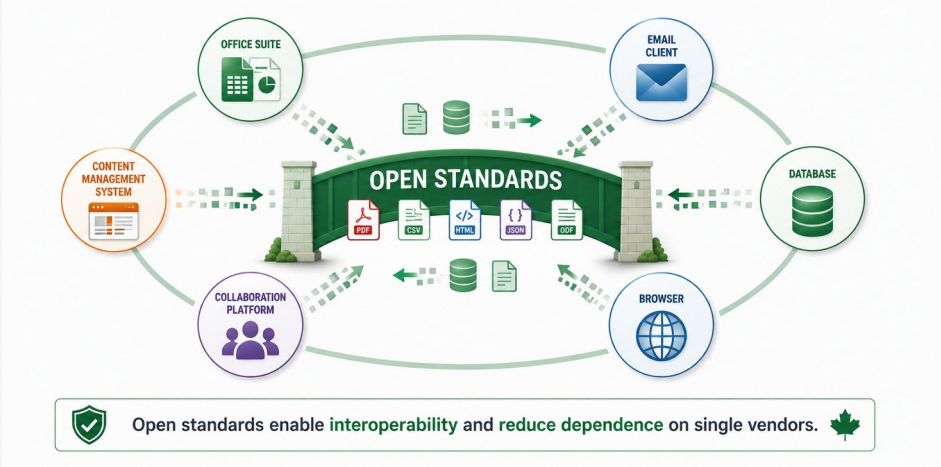
Transparency and Security

Open standards can be reviewed by security researchers and the broader technical community, leading to more robust and trustworthy implementations.

Open Standards Do Not Require Avoiding Commercial Software

Using open standards does not mean organizations must avoid commercial software or proprietary platforms. Many commercial products support open standards alongside proprietary features. Organizations can use commercial software while saving files in open formats, export data in standard formats for backup and portability, integrate commercial systems using open APIs and protocols, and maintain flexibility while benefiting from vendor innovation.

The goal is to preserve choice and portability, not to reject commercial technology.



How Open Source Supports Digital Sovereignty

Open source software can significantly strengthen digital sovereignty because its source code is publicly available, can be inspected by anyone, and can be modified and operated by multiple providers.

Unlike proprietary software, where only the vendor controls the code, open source software distributes control across a broader community—reducing dependence on any single organization.

What Is Open Source Software?

Open source software is software whose source code is publicly available (anyone can view it), modifiable (users can change and customize it), redistributable (modified versions can be shared), and community-developed (often maintained by collaborative communities). Open source software is licensed under terms that grant users significant freedoms, such as the GNU General Public License (GPL), MIT License, Apache License, or similar open source licenses.

How Open Source Strengthens Digital Sovereignty

Reduced Vendor Lock-In

Open source software can be supported by multiple providers. If one vendor becomes unsuitable, organizations can switch to another provider or support the software internally.

Transparent Technology

Source code can be inspected for security vulnerabilities, privacy issues, or unwanted functionality. Organizations are not dependent on vendor claims—they can verify how the software works.

Local Hosting Options

Many open source applications can be hosted on-premises or with Canadian providers, giving organizations direct control over infrastructure.

Open Standards

Open source projects typically use and support open standards, improving interoperability and data portability.

Long-Term Access

Open source software cannot be discontinued in the same way proprietary software can. Even if the original developers stop maintaining a project, others can continue development.

Customization and Flexibility

Organizations can modify open source software to meet specific needs, integrate with other systems, or add functionality.

Community Review and Collaboration

Open source projects benefit from review by global communities of developers, security

researchers, and users, often resulting in more robust and secure software.

Opportunities to Build Internal Expertise

Working with open source software can help organizations develop internal technical capability and reduce dependence on external consultants.

Open Source Does Not Automatically Create Sovereignty

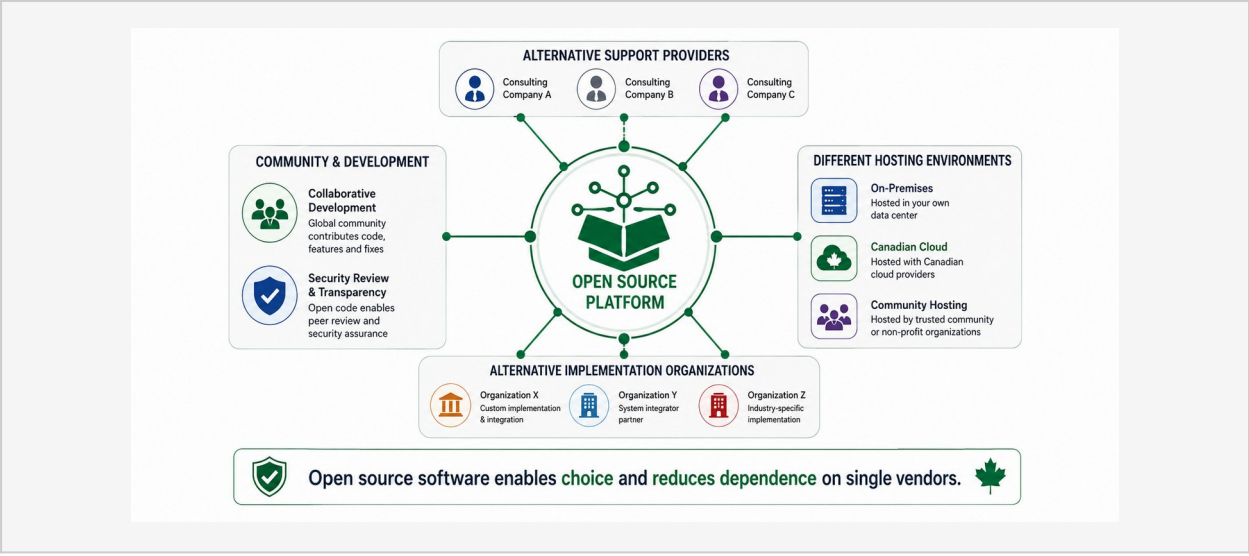
Open source software is a tool—it must be used well to provide sovereignty benefits. An organization can still deploy open source software poorly, depend entirely on one consultant or vendor, fail to maintain backups and documentation, neglect security updates, or lack internal expertise to manage the system.

The strongest approach combines open source software with:

- Proper governance – Clear policies and accountability
- Skilled administrators – Internal or contracted expertise
- Security updates – Regular patching and maintenance
- Reliable support – Access to knowledgeable assistance
- Open data formats – Ensuring information remains portable
- Documented procedures – Clear instructions for common tasks
- Tested recovery plans – Verified backup and restoration processes

Examples of Open Source Software

Operating Systems: Linux distributions (Ubuntu, Debian, Fedora, Rocky Linux). Office Productivity: LibreOffice, OnlyOffice. Web Servers: Apache, Nginx. Databases: PostgreSQL, MySQL, MariaDB. Content Management: WordPress, Drupal, Joomla. Email: Postfix, Dovecot, Roundcube. Collaboration: Nextcloud, Rocket.Chat, Mattermost. Security: ClamAV, Snort, OpenVPN. Virtualization: KVM, Proxmox.



Cloud, On-Premises, or Hybrid?

Organizations must decide where to host their digital systems: in public cloud environments, on their own premises, or in a hybrid model combining both approaches.

Each model offers distinct advantages and considerations. There is no universal answer—the right choice depends on information sensitivity, organizational capability, budget, operational needs, and risk tolerance.

Public Cloud

Public cloud services are hosted and managed by third-party providers such as Amazon Web Services, Microsoft Azure, Google Cloud, or Canadian providers like OVHcloud.

Advantages: Rapid deployment without purchasing hardware; scalability based on demand; professional infrastructure and security; reduced hardware responsibilities; access to advanced features; geographic redundancy.

Considerations: Provider dependence; recurring subscription costs that can increase over time; jurisdictional exposure depending on provider ownership; limited infrastructure control; possible export or migration challenges; a shared responsibility model dividing security and compliance duties between provider and customer.

On-Premises

On-premises hosting means operating servers, storage, and infrastructure within the organization's own facilities or in a colocation data center under the organization's direct control.

Advantages: Direct physical control; customized configuration; local data storage; reduced dependence on external connectivity; predictable capital costs; no third-party administrative access.

Considerations: Significant hardware costs; maintenance responsibilities; staffing requirements; local disaster risks (fire, flood, theft); full cybersecurity responsibility; scalability challenges; power and cooling requirements.

Hybrid

A hybrid model combines on-premises systems with selected cloud services, allowing organizations to keep sensitive or essential services under closer control while using cloud platforms where they provide clear benefits.

Advantages: Flexibility to choose the best environment for each workload; risk distribution; sensitive data kept on-premises; cloud used for scalability, collaboration, or specialized services; gradual transition path.

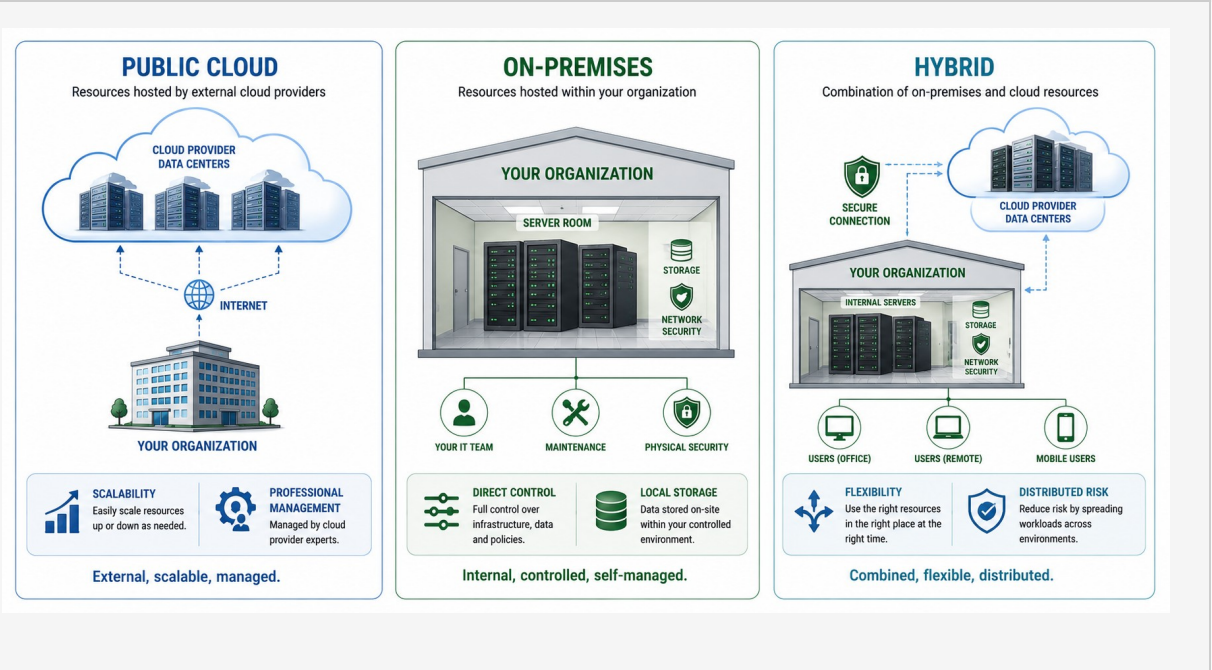
Considerations: Added complexity of managing both environments; integration challenges; increased management overhead; potential cost inefficiencies in either model.

Making the Decision

- Information sensitivity – Highly sensitive data may warrant on-premises control

- Organizational capability – Does the organization have technical staff to manage infrastructure?
- Budget and cost structure – Capital investment vs. operational expenses
- Operational needs – Scalability, geographic distribution, collaboration requirements
- Risk tolerance – Comfort with third-party dependencies and jurisdictional exposure
- Regulatory requirements – Some sectors face specific hosting or data residency requirements

Many organizations benefit from a hybrid approach—keeping essential systems and sensitive data on-premises while using cloud services for collaboration, public-facing websites, or specialized applications.



Encryption and Control of Keys

Encryption protects information by making it unreadable without the correct decryption key. It is one of the most important technical controls for protecting data confidentiality and supporting digital sovereignty.

However, encryption provides the greatest sovereignty benefit when the organization understands and controls who holds the encryption keys.

Where Encryption Should Be Used

Data in Transit

Information traveling across networks—including the internet, email, file transfers, and web traffic—should be encrypted to prevent interception.

Data at Rest

Information stored on servers, databases, laptops, mobile devices, and backup media should be encrypted to protect against unauthorized access if devices are lost, stolen, or improperly disposed of.

Backups

Backup files should be encrypted to protect organizational information if backup media is lost or accessed by unauthorized parties.

Sensitive Communications

Email, messaging, and file sharing involving confidential or sensitive information should use end-to-end encryption where practical.

Portable Devices

Laptops, smartphones, tablets, and USB drives should use full-disk or device encryption to protect information if devices are lost or stolen.

Who Controls the Encryption Keys?

Encryption is only as strong as the control over the keys used to decrypt information. There are two primary models:

Provider-Controlled Encryption Keys

In this model, the service provider manages all encryption keys. The provider encrypts data, stores the keys, and can decrypt information when needed—including for technical support, legal requests, or government access demands.

Advantages: Simpler to implement with no key management burden on the organization; provider handles key backup and recovery; reduced risk of losing access due to lost keys.

Considerations: Provider personnel can decrypt organizational data; keys may be accessible to foreign governments through legal process; the organization has limited control over who can access information; encryption protects against external threats but not provider access.

Organization-Controlled Encryption Keys (Customer-Managed Keys)

In this model, the organization generates, manages, and controls its own encryption keys. The service provider cannot decrypt data without the organization's keys.

Advantages: The organization retains exclusive control over who can decrypt information; the provider cannot access data even if compelled by legal process; stronger protection for highly sensitive information; reduced jurisdictional risk, since encrypted data is less useful to foreign authorities.

Considerations: The organization is responsible for key management, including secure storage, backup, and recovery; losing keys means losing access to data permanently; more complex to implement and maintain; may limit some provider features that require access to unencrypted data (such as search or analytics).

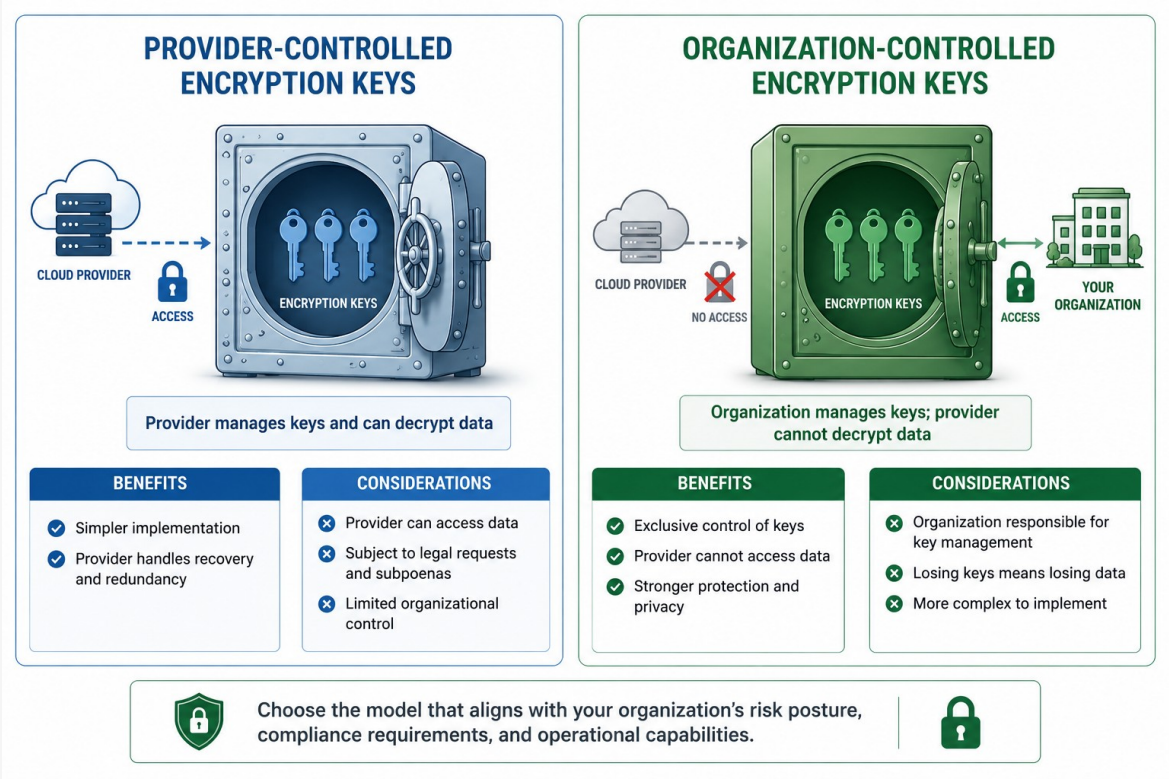
Questions to Ask About Encryption

- Does the provider encrypt data at rest and in transit?
- Who manages the encryption keys—the provider or the customer?
- Can provider personnel decrypt organizational information?
- Where are encryption keys stored?
- Can the organization manage its own keys?
- What happens if encryption keys are lost?
- Are keys stored separately from the encrypted data?
- Is there a documented key recovery process?
- Can the organization verify that encryption is properly implemented?

Government of Canada Guidance

The Government of Canada identifies encryption as an important technical control for reducing exposure in cloud environments. Its guidance notes that customer-managed encryption (where the organization controls keys) provides stronger protection against unauthorized access—but also creates responsibilities for key management, backup, and recovery.

Organizations handling highly sensitive information should consider customer-managed encryption as part of a comprehensive sovereignty strategy.


PROVIDER-CONTROLLED ENCRYPTION KEYS
CLOUD PROVIDER
ACCESS
ENCRYPTION KEYS
Provider manages keys and can decrypt data
BENEFITS
Simpler implementation
Provider handles recovery and redundancy
CONSIDERATIONS
Provider can access data
Subject to legal requests and subpoenas
Limited organizational control
ORGANIZATION-CONTROLLED ENCRYPTION KEYS
CLOUD PROVIDER
NO ACCESS
ENCRYPTION KEYS
ACCESS
YOUR ORGANIZATION
Organization manages keys; provider cannot decrypt data
BENEFITS
Exclusive control of keys
Provider cannot access data
Stronger protection and privacy
CONSIDERATIONS
Organization responsible for key management
Losing keys means losing data
More complex to implement
Choose the model that aligns with your organization's risk posture, compliance requirements, and operational capabilities.

PART FOUR

Governance and Administrative Control

Identity, accounts and organizational ownership

Identity and Administrative Control

Control over digital systems begins with control over accounts, credentials, and administrative access.

An organization does not truly control a service if only one person can access it, if accounts are tied to personal email addresses, or if administrative credentials are not properly managed.

Essential Identity and Access Controls

Every important platform and system should have:

Designated Organizational Owner

Critical accounts—domain registrations, cloud platforms, email systems, financial services—should be registered in the organization's name, not an individual's personal name.

Multiple Authorized Administrators

More than one trusted person should have administrative access to essential systems. Single points of failure create unacceptable risk.

Multi-Factor Authentication (MFA)

All administrative accounts and systems containing sensitive information should require multi-factor authentication—combining something you know (password) with something you have (authentication app, hardware token, or SMS code).

Role-Based Access

Users should have access appropriate to their role. Not everyone needs administrative privileges. Limit access to sensitive systems and information based on job function.

Documented Recovery Procedures

Organizations should document how to recover access if an administrator leaves, loses credentials, or becomes unavailable. Recovery procedures should be tested and kept secure.

Prompt Removal of Former Users

When employees, volunteers, or contractors leave the organization, their access should be removed immediately. Delayed deprovisioning creates security and control risks.

Secure Password Management

Organizations should use password managers to generate, store, and share credentials securely. Passwords should be strong, unique, and never reused across systems.

Regular Account Reviews

Periodically review who has access to what. Remove unnecessary accounts, adjust permissions, and verify that access remains appropriate.

Avoid Personal Email Addresses for Organizational Accounts

Critical systems should never be tied to an individual's personal email address.

Problems with personal email addresses:

- Individual may leave the organization
- Personal email may be compromised or abandoned
- Organization loses control when the individual is unavailable
- Recovery processes may be impossible
- Ownership disputes can arise

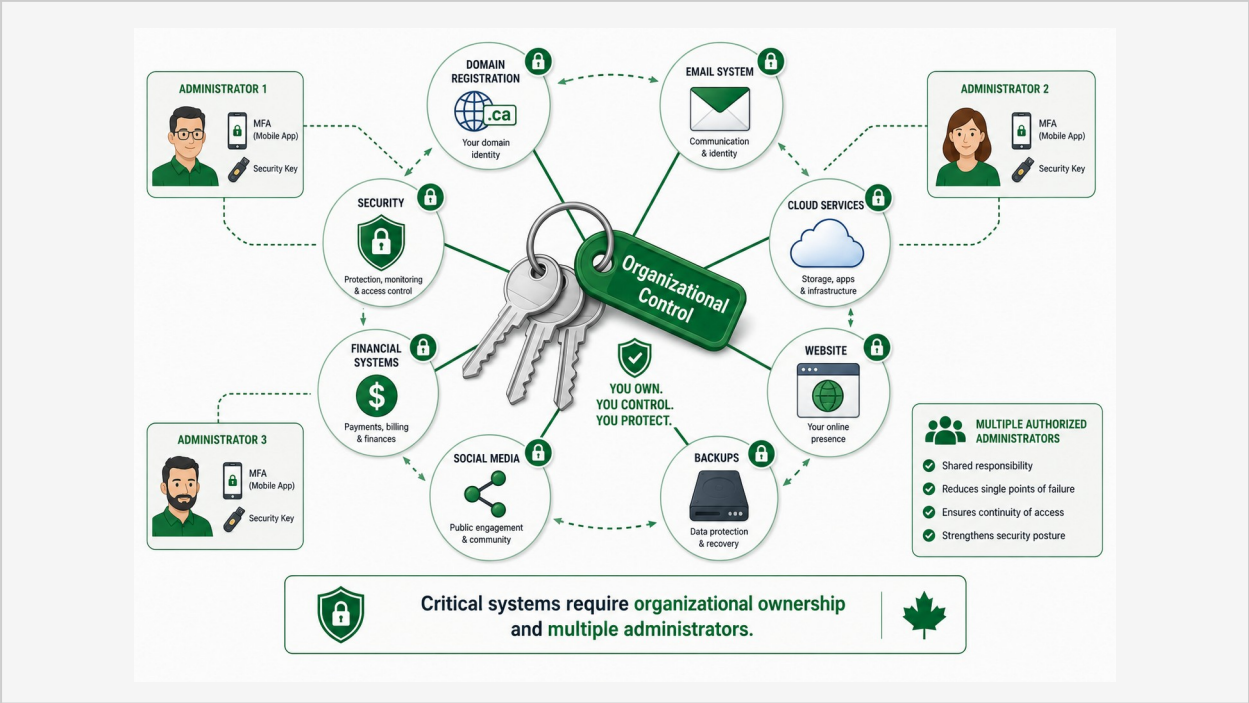
Use organizational email addresses (e.g., admin@organization.ca, it@organization.ca) for:

- Domain registrations
- Cloud administrator accounts
- Website hosting
- Financial and payment systems
- Software licenses
- Social media accounts
- Backup and recovery systems

Organizational Control Over Critical Assets

The organization should directly control:

- Domain registrations – The organization's domain name and DNS settings
- Website hosting – Access to web servers and content management systems
- Cloud administrator accounts – Primary accounts for cloud platforms
- Social media accounts



PART FIVE

Assessing and Prioritizing Risk

A risk matrix and a practical roadmap for small organizations

A Digital Sovereignty Risk Assessment

Not all digital services present the same level of sovereignty risk.

Organizations should prioritize attention and resources based on both the importance of a service and the level of supplier dependence it creates.

A Two-Axis Risk Matrix

Assess each important digital service using two dimensions.

Vertical Axis: Operational Importance — how critical is this service to organizational operations?

- High Importance – Service is essential; an outage would stop critical operations
- Medium Importance – Service is important; an outage would cause significant disruption
- Low Importance – Service is convenient; an outage would cause minor inconvenience

Horizontal Axis: Supplier Dependence — how dependent is the organization on this specific supplier?

- High Dependence – No practical alternatives; migration would be extremely difficult or costly
- Medium Dependence – Limited alternatives; migration would be challenging but possible
- Low Dependence – Multiple alternatives available; migration would be straightforward

Assessment Criteria

Operational Importance

- Would an outage stop essential operations?
- How many people depend on this service?
- What is the maximum acceptable downtime?
- Could the organization function without this service?
- What would be the financial impact of an outage?
- Would an outage affect the organization's ability to serve its mission?

Supplier Dependence

- How difficult would it be to migrate to another provider?
- Are practical alternatives available?
- Can data be easily exported and imported elsewhere?
- How much would migration cost (time, money, expertise)?
- Are there contractual barriers to leaving?
- Does the service use proprietary formats or protocols?
- How much organizational knowledge is tied to this specific platform?
- Would migration require significant retraining?

Data Sensitivity

- Does the system contain confidential or regulated information?
- What would be the impact of a data breach?
- Are privacy laws applicable to this data?
- Would unauthorized access cause harm?

Jurisdictional Risk

- Which laws and countries may apply to this service?
- Is data stored or processed outside Canada?
- Is the provider subject to foreign government access requests?
- Are subcontractors in other jurisdictions involved?

Administrative Control

- Does the organization control accounts and credentials?
- Can the organization manage its own encryption keys?
- Are there multiple authorized administrators?
- Are recovery procedures documented and tested?

Resilience and Backup

- Are independent backups in place?
- Have backups been tested?
- Are continuity arrangements documented?
- Could the organization recover from a supplier failure?

Internal Capability

- Does anyone in the organization understand how the system works?
- Is the system documented?
- Does the organization have the expertise to manage alternatives?
- Is knowledge concentrated in one person?

Prioritization Matrix

High Importance + High Dependence — Priority: Immediate Action Required

These services present the greatest sovereignty risk. They are critical to operations and difficult to replace. Actions: develop detailed exit plans, implement independent backups, identify and test alternatives, negotiate better contract terms, build internal expertise, consider migration to lower-risk alternatives.

High Importance + Low Dependence — Priority: Maintain Flexibility

These services are critical but alternatives are available. Actions: maintain awareness of alternatives, keep exit plans current, ensure backups are tested, monitor for changes in dependence.

Low Importance + High Dependence — Priority: Reduce Dependence

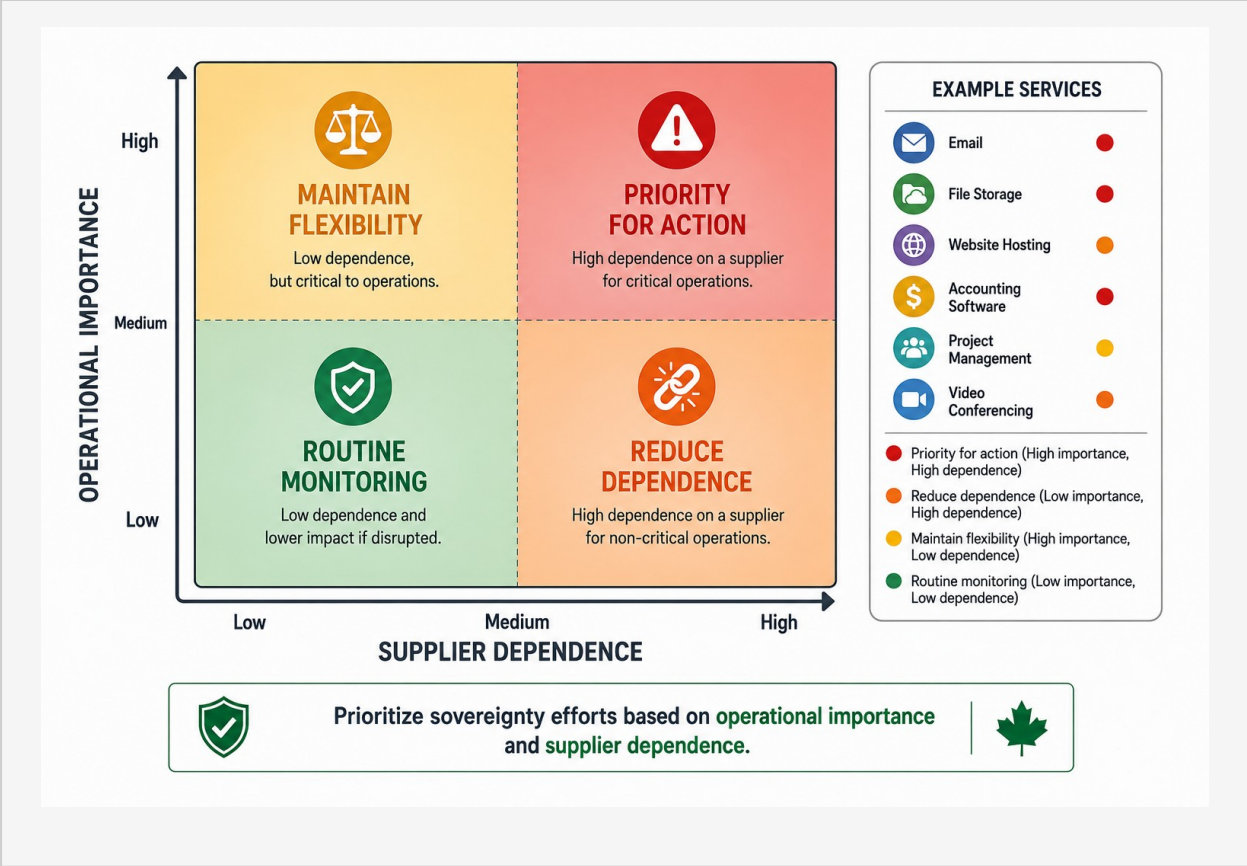
These services are not critical but are difficult to leave. Actions: consider whether the service is necessary, evaluate simpler alternatives, reduce reliance on the service, plan eventual migration.

Low Importance + Low Dependence — Priority: Routine Monitoring

These services present minimal sovereignty risk. Actions: apply standard governance practices, monitor for changes in importance or dependence, maintain basic documentation.

Regular Reassessment

Digital sovereignty risk is not static. Reassess services annually as part of regular technology planning, when contracts come up for renewal, after significant organizational changes, when providers change ownership, policies, or pricing, after security incidents or service disruptions, and when new alternatives become available.



Practical Steps for Small Organizations

Digital sovereignty does not require a large technology department or significant budget. Small organizations can make meaningful progress through manageable, incremental improvements.

First 30 Days: Establish Visibility

Week 1-2: Identify Critical Digital Services

- List all digital services the organization uses
- Identify which services are essential to operations
- Note which services contain sensitive information
- Document who uses each service and for what purpose

Week 2-3: Confirm Ownership and Access

- Verify that domains are registered in the organization's name
- Confirm that administrator accounts use organizational email addresses
- Identify who has administrative access to each critical system
- Ensure at least two people can access each critical account

Week 3-4: Enable Multi-Factor Authentication

- Enable MFA on all critical accounts
- Prioritize email, cloud storage, financial systems, and domain registrars
- Document MFA recovery procedures
- Store backup codes securely

Week 4: Document Data Locations and Verify Backups

- Record where important data is stored (which services, which countries)
- Identify which services process data outside Canada and which are subject to foreign jurisdiction
- Create a simple inventory spreadsheet
- Confirm that backups are being created for critical data and note where they are stored
- Schedule a backup test for the 90-day milestone

Within 90 Days: Build Capability

Month 2: Test Data Exports and Review Contracts

- Export data from critical services and verify that exported files open correctly and are complete
- Document the export process for future reference
- Collect contracts for all major digital services and note renewal dates and cancellation terms
- Identify services with upcoming renewals and review pricing and service level agreements

Month 2-3: Classify Sensitive Information

- Categorize information as Public, Internal, Confidential, or Highly Sensitive
- Identify which services store confidential or highly sensitive information
- Assess whether current controls are appropriate for information sensitivity
- Document classification decisions

Month 3: Address Single Points of Failure and Recovery

- List services where only one person has access or knowledge
- Identify critical systems without backup administrators
- Document how to recover access to critical accounts and test recovery for at least one system
- Create a basic supplier inventory noting country of incorporation, hosting location, and contract terms

Within One Year: Strengthen Sovereignty

Quarter 2: Exit Plans and Open Formats

- Create written exit plans for the 3-5 most critical services
- Identify alternative providers, migration procedures, and estimated costs
- Review exit plans with organizational leadership
- Begin saving documents in open formats (PDF, OpenDocument, CSV) and train staff accordingly

Quarter 3: Test Restoration and Evaluate Alternatives

- Conduct a full restoration test of at least one critical system and measure restoration time
- Identify and address gaps in backup procedures
- Research Canadian providers and open source alternatives for critical services
- Compare costs, features, and sovereignty implications; consider pilots or trials

Quarter 4: Policy and Procurement

- Draft a simple organizational policy on digital sovereignty and adopt it formally
- Add digital sovereignty questions to procurement processes
- Create a standard questionnaire for new service providers and train relevant staff

Year-End: Review and Plan

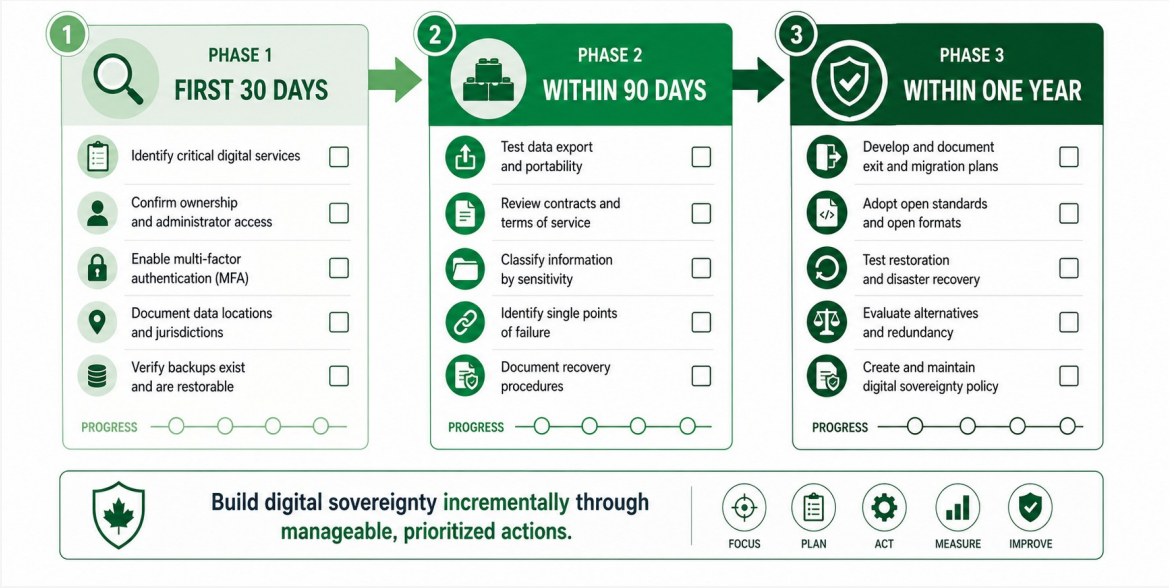
Review progress over the past year, identify remaining gaps and priorities, plan next year's initiatives, and celebrate improvements to build momentum.

Building Momentum

- Start with high-priority, low-effort actions – Quick wins build confidence and momentum
- Focus on one or two initiatives at a time – Avoid overwhelming limited resources
- Document as you go – Simple documentation prevents knowledge loss
- Involve multiple people – Distribute knowledge and responsibility
- Celebrate progress – Recognize improvements, even small ones

- Be patient and persistent – Digital sovereignty is built incrementally over time

Digital sovereignty is a journey, not a destination. Every step forward increases organizational resilience and independence.



PART SIX

Tools for Ongoing Practice

A checklist, common myths, and a sample policy

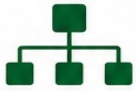
DIGITAL SOVEREIGNTY CHECKLIST

A Practical Self-Assessment for Stronger Digital Independence

Organization Name: _____ Reviewer: _____

Date: _____ Next Review Date: _____

1. GOVERNANCE



Strong governance ensures accountability, ownership and informed decisions.

- ☐ 1.1 Roles and responsibilities for digital assets are clearly defined.
- ☐ 1.2 Key decisions consider digital sovereignty and long-term independence.
- ☐ 1.3 Critical digital assets are inventoried and documented.
- ☐ 1.4 Third-party relationships are reviewed and documented regularly.
- ☐ 1.5 Policies and procedures address digital sovereignty principles.

2. DATA

You can't protect what you don't know.

- ☐ 2.1 We know where our data is stored and who processes it.
- ☐ 2.2 Data classification is in place based on sensitivity and importance.
- ☐ 2.3 We understand the legal jurisdictions that apply to our data.
- ☐ 2.4 Data is backed up regularly and stored securely.
- ☐ 2.5 We can export our data in open, standard formats.

3. TECHNOLOGY

Choose technology that supports choice, portability and control.

- ☐ 3.1 We prefer solutions that use open standards and open formats.
- ☐ 3.2 We can migrate or export our data without excessive barriers.
- ☐ 3.3 We have alternatives identified for critical technology services.
- ☐ 3.4 Proprietary lock-in risks are understood and documented.
- ☐ 3.5 Our technology stack is reviewed for sovereignty considerations.

4. ACCESS

Control access to protect your organization and your data.

- ☐ 4.1 We own and control critical accounts and domain names.
- ☐ 4.2 Multi-factor authentication (MFA) is enabled for all critical accounts.
- ☐ 4.3 Access privileges follow the principle of least privilege.
- ☐ 4.4 Administrator access is limited and regularly reviewed.
- ☐ 4.5 Access can be maintained even if key individuals are unavailable.

5. RESILIENCE

Resilience ensures continuity even when disruptions occur.

- ☐ 5.1 We have documented backup and recovery procedures.
- ☐ 5.2 Backups are tested regularly for restoration.
- ☐ 5.3 We have plans for service disruption or provider failure.
- ☐ 5.4 Critical services have alternatives or redundancy in place.
- ☐ 5.5 We test our resilience plans at least annually.

OVERALL ASSESSMENT

Based on this assessment, our organization's digital sovereignty posture is:

- ☐ Strong
- ☐ Moderate
- ☐ Weak

PRIORITY ACTIONS

Top 3 actions we will focus on:

1. _____
2. _____
3. _____

NOTES

_____

_____

_____

_____

_____

_____

Review this checklist annually or when significant technology changes occur.

Myth vs. Reality

Digital sovereignty is sometimes misunderstood. Here are common misconceptions and evidence-based responses.

Myth 1: “Data stored in Canada is automatically under complete Canadian control.”

Reality: Location is important, but it is not the only factor affecting control.

Data stored in a Canadian data center may still be managed by a company subject to foreign laws, accessible to provider personnel in other countries, subject to foreign government access requests, governed by contracts under foreign jurisdiction, or processed and backed up in other countries. Complete control requires considering provider incorporation, applicable laws, administrative access, encryption key location, and contractual terms. Canadian data residency is valuable, but it should be combined with other sovereignty measures.

Myth 2: “Digital sovereignty means avoiding all foreign technology.”

Reality: Digital sovereignty means understanding dependencies and preserving meaningful control and choice.

Complete technological independence is neither possible nor desirable in an interconnected world. Even locally hosted systems depend on international hardware supply chains, global software ecosystems, international standards, and cross-border expertise. The goal is to understand important dependencies, avoid unnecessary lock-in, maintain credible alternatives, protect sensitive information, and retain the ability to make informed choices. Many international providers offer excellent services that can be used responsibly within a sovereignty framework.

Myth 3: “Moving everything on-premises solves sovereignty concerns.”

Reality: On-premises hosting creates its own staffing, security, backup, and resilience responsibilities.

Organizations that move to on-premises infrastructure must purchase and maintain hardware, hire or contract skilled technical staff, implement robust cybersecurity measures, maintain reliable backups, ensure physical security, provide redundant power and cooling, plan for hardware failures and disasters, and keep systems updated and patched. On-premises hosting can strengthen sovereignty when the organization has appropriate expertise and resources—but without them, it can actually increase risk.

Myth 4: “Open source automatically guarantees independence.”

Reality: Open source improves choice and transparency, but organizations still require skills, maintenance, documentation, and governance.

Open source software provides transparent code, freedom from single-vendor control, and support from multiple providers. However, organizations must still maintain technical expertise, keep systems patched, document configurations, implement proper backups, and govern the technology responsibly. Open source is a powerful tool for digital sovereignty, but it is not a substitute for organizational capability and governance.

Myth 5: “Small organizations do not need an exit plan.”

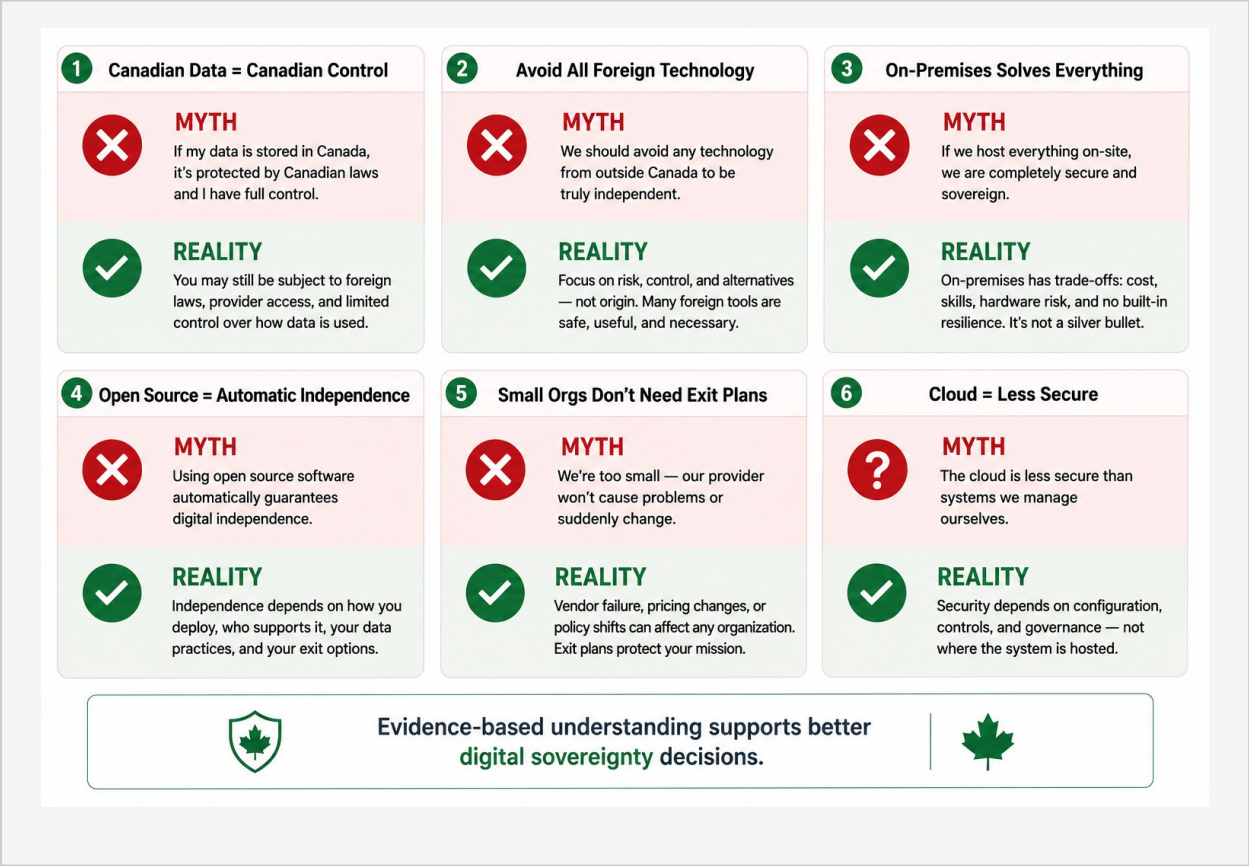
Reality: Smaller organizations may be especially vulnerable when a critical supplier changes or fails.

Small organizations often have limited resources to respond to sudden changes, depend heavily on specific services, lack redundant systems, have less negotiating power with vendors, and face greater disruption from service interruptions. Exit planning is not pessimism—it is responsible stewardship of organizational resources.

Myth 6: “Cloud services are always less secure than on-premises systems.”

Reality: Security depends on configuration, governance, data sensitivity, and the controls provided by both customer and supplier.

Major cloud providers often offer professional security teams, advanced threat detection, regular audits, and compliance certifications. But cloud security also depends on how the customer configures the service, who has access, and whether encryption and credentials are properly managed. On-premises systems can be highly secure when properly implemented, or vulnerable when expertise and resources are lacking. Neither model is inherently more secure—security is determined by implementation, governance, and context.



Creating a Digital Sovereignty Policy

A formal organizational policy establishes expectations, guides decision-making, and demonstrates governance commitment. A digital sovereignty policy does not need to be lengthy or complex—it should be clear, practical, and actionable.

Sample Policy Statement

[Organization Name] Digital Sovereignty Policy

Purpose: This policy establishes principles and practices for selecting and operating digital services in a manner that protects organizational information, preserves operational resilience, and maintains reasonable control over our technology choices.

Policy Statement: [Organization Name] will select and operate digital services in a manner that protects the confidentiality, integrity, and availability of organizational information; preserves the organization's ability to make independent technology decisions; maintains operational resilience during disruptions; complies with applicable privacy and data protection laws; and supports the organization's mission and values.

Scope: This policy applies to all digital services that store, process, or transmit organizational information, including cloud services and software-as-a-service platforms, email and communication systems, file storage and collaboration tools, websites and online services, databases and information systems, and financial and administrative systems.

Elements a Policy Should Address

1. Information Ownership

The organization owns all information created, collected, or managed in the course of organizational activities. Service providers are processors, not owners, of organizational information. Contracts must clearly establish organizational ownership.

2. Privacy and Legal Compliance

All digital services must comply with applicable privacy laws (PIPEDA, provincial privacy legislation). Cross-border data transfers must be assessed for privacy and legal risks. Privacy impact assessments are required for services handling sensitive personal information.

3. Data Location and Jurisdiction

The organization will consider data location and jurisdictional risks in technology decisions. Canadian hosting is preferred for sensitive or confidential information. Data location requirements will be specified in contracts where appropriate.

4. Open Standards and Interoperability

Open standards and file formats are preferred where practical. Proprietary formats that create vendor lock-in should be avoided when alternatives exist. Services should support data export in open, usable formats.

5. Software and Supplier Evaluation

Technology procurement will include assessment of sovereignty implications. Suppliers will be evaluated for data practices, jurisdictional risks, and exit options. Open source alternatives will be

considered alongside proprietary options.

6. Account Ownership and Access Control

Critical accounts must be registered in the organization's name using organizational email addresses. Multi-factor authentication is required for all critical systems. At least two authorized personnel must have access to each critical account.

7. Backup and Recovery

Independent backups are required for all critical information and must be tested at least annually. At least one backup must be independent of the primary service provider. Recovery procedures must be documented and accessible.

8. Portability and Exit Planning

Exit plans are required for critical services. Data export capabilities must be verified before adopting new services. Contracts must include clear terms for data export and service termination.

9. Operational Resilience

Essential services must have documented continuity plans. Alternative methods for critical functions must be identified. Single points of failure are avoided where possible.

10. Documentation and Review

Digital services are inventoried and documented. This policy is reviewed annually and updated as needed. Responsibility for policy implementation is clearly assigned.

Integrating With Existing Policies

Digital sovereignty should be integrated into existing organizational policies rather than treated as an isolated issue: reference sovereignty principles in privacy impact assessments and privacy notices; include sovereignty considerations in cybersecurity frameworks and encryption key management; add sovereignty questions to procurement and vendor selection; address data retention and deletion in records management; and integrate sovereignty into business continuity planning and exercises.

Policy Implementation

- Assign responsibility – designate a person or role, ensure leadership support, provide resources for compliance
- Communicate the policy – share with relevant personnel, provide training, make it easily accessible
- Monitor compliance – review technology decisions for alignment, conduct periodic audits, address non-compliance promptly
- Review and update – review annually, update based on lessons learned and changing circumstances


Privacy & Compliance
Business Continuity
Technology Procurement
DIGITAL SOVEREIGNTY POLICY
Access & Training
Cybersecurity
Records & Data
Integrate digital sovereignty into existing organizational policies and practices.

PART SEVEN

Resources and Closing Thoughts

Where to learn more, final reflections, and about the LAC

Where to Learn More

Organizations should consult trusted and authoritative resources when developing digital sovereignty practices. The following Canadian and international sources provide reliable guidance.

Government of Canada Resources

Digital Sovereignty and Cloud Guidance

- Digital Sovereignty Framework – Government of Canada's approach to digital sovereignty
- Data sovereignty and public cloud – guidance on data sovereignty considerations for cloud services
- Guideline on Service and Digital – direction on digital service delivery
- Cloud security guidance – security considerations for cloud adoption
- Direction on Enabling Access to Web Services – guidance on web service accessibility and standards

Website: canada.ca/en/government/system/digital-government

Canadian Centre for Cyber Security

- ITSG-33: IT Security Risk Management – comprehensive security guidance
- Cloud security guidance – baseline security controls for cloud
- Cryptographic algorithms guidance – encryption and key management
- Patch management guidance – security update practices
- Cyber threat bulletins – current threat information

Website: cyber.gc.ca

Privacy Guidance

Office of the Privacy Commissioner of Canada (priv.gc.ca)

- PIPEDA guidance – Personal Information Protection and Electronic Documents Act interpretation
- Cross-border data flows – guidance on transferring personal information outside Canada
- Cloud computing guidance – privacy considerations for cloud services
- Breach notification guidance and privacy impact assessment guidance

Provincial and Territorial Privacy Commissioners

Organizations should also consult their applicable provincial or territorial privacy commissioner: British Columbia (oipc.bc.ca), Alberta (oipc.ab.ca), Saskatchewan (oipc.sk.ca), Manitoba (ombudsman.mb.ca), Ontario (ipc.on.ca), Quebec (cai.gouv.qc.ca), and the access and privacy offices of New Brunswick, Nova Scotia, Prince Edward Island, and Newfoundland and Labrador. Provincial privacy laws may impose requirements beyond federal PIPEDA, particularly for public-sector organizations.

Open Source and Standards Organizations

Linux and Open Source Resources

- Linux Foundation – global open source collaboration and education (linuxfoundation.org)
- Linux distribution documentation – official documentation for Ubuntu, Debian, Fedora, Rocky Linux, and others
- Open Source Initiative – open source licensing and standards (opensource.org)
- Free Software Foundation – software freedom advocacy and resources (fsf.org)
- Apache Software Foundation – open source software projects and community (apache.org)

Standards Organizations

Internet Engineering Task Force (ietf.org), World Wide Web Consortium (w3.org), International Organization for Standardization (iso.org), OASIS Open (oasis-open.org).

Linux Association of Canada

The Linux Association of Canada provides resources specifically for Canadian organizations: digital sovereignty guidance, open source software directories, community support and connection to Canadian Linux user groups, educational materials (workshops, webinars, training), hardware refurbishment programs, and school and community outreach.

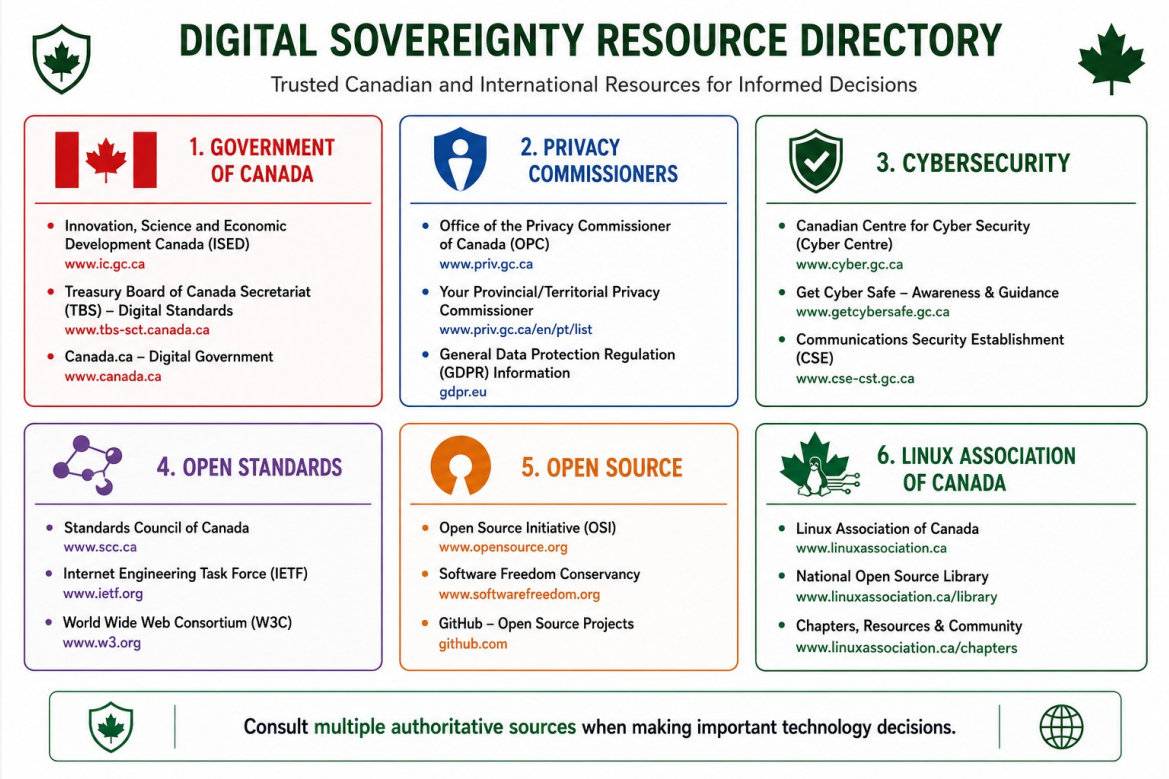
Website: linuxassociation.ca • Email: info@linuxassociation.ca • Phone: (639) 477-0111

Community and Professional Resources

Canadian Internet Registration Authority (cira.ca), provincial technology associations, and local Linux user groups provide community support. Organizations should also consult legal counsel for contract review and jurisdictional questions, information security professionals for cybersecurity assessment, technology consultants for migration support, and privacy professionals for impact assessments and compliance programs.

Staying Current

Digital sovereignty is an evolving field. Organizations should subscribe to relevant government bulletins, monitor privacy commissioner guidance, follow cybersecurity advisories, participate in professional communities, review contracts and services regularly, and reassess risks periodically. Digital sovereignty requires ongoing attention, not one-time implementation.


DIGITAL SOVEREIGNTY RESOURCE DIRECTORY
Trusted Canadian and International Resources for Informed Decisions
1. GOVERNMENT OF CANADA
Innovation, Science and Economic Development Canada (ISED)
www.ic.gc.ca
Treasury Board of Canada Secretariat (TBS) – Digital Standards
www.tbs-sct.canada.ca
Canada.ca – Digital Government
www.canada.ca
2. PRIVACY COMMISSIONERS
Office of the Privacy Commissioner of Canada (OPC)
www.priv.gc.ca
Your Provincial/Territorial Privacy Commissioner
www.priv.gc.ca/en/pt/list
General Data Protection Regulation (GDPR) Information
gdpr.eu
3. CYBERSECURITY
Canadian Centre for Cyber Security (Cyber Centre)
www.cyber.gc.ca
Get Cyber Safe – Awareness & Guidance
www.getcybersafe.gc.ca
Communications Security Establishment (CSE)
www.cse-cst.gc.ca
4. OPEN STANDARDS
Standards Council of Canada
www.scc.ca
Internet Engineering Task Force (IETF)
www.ietf.org
World Wide Web Consortium (W3C)
www.w3.org
5. OPEN SOURCE
Open Source Initiative (OSI)
www.opensource.org
Software Freedom Conservancy
www.softwarefreedom.org
GitHub – Open Source Projects
github.com
6. LINUX ASSOCIATION OF CANADA
Linux Association of Canada
www.linuxassociation.ca
National Open Source Library
www.linuxassociation.ca/library
Chapters, Resources & Community
www.linuxassociation.ca/chapters
Consult multiple authoritative sources when making important technology decisions.

Final Thoughts

Digital sovereignty is ultimately about preserving organizational choice, control, and resilience in an interconnected digital world.

It does not require organizations to reject international technology, operate in isolation, or achieve complete technological independence. These goals are neither realistic nor desirable in a globally connected economy.

Digital sovereignty requires organizations to understand:

- What they depend on – which systems, suppliers, and services are essential to operations
- Who controls their systems – where administrative authority, encryption keys, and access rights reside
- Where their information travels – which jurisdictions, subcontractors, and legal frameworks may apply
- Which laws may govern their data – how corporate ownership and service location affect legal exposure
- Whether they can change direction – how difficult and expensive it would be to migrate to alternatives
- How they will continue during disruption – what happens when suppliers fail, prices increase, or services become unavailable

Sovereignty Is Built Through Informed Decisions

Organizations that maintain clear inventories, independent backups, open data formats, secure administrative control, and realistic exit plans are better prepared for technological change, economic pressure, legal evolution, operational disruption, and strategic opportunity.

Digital sovereignty is not achieved through a single purchase, migration, or policy. It is built through ongoing governance, responsible stewardship, and long-term planning.

The Path Forward

- Start with visibility – understand what you have, where it is, and who controls it before making changes
- Prioritize based on risk – focus first on systems that are both critical to operations and difficult to replace
- Build incrementally – small, consistent improvements are more sustainable than ambitious transformations that stall
- Document as you go – knowledge that exists only in one person's mind is a vulnerability, not an asset
- Test your assumptions – verify that backups restore, exports work, and continuity plans function before you need them urgently
- Integrate with existing governance – digital sovereignty should strengthen existing privacy, security, procurement, and continuity practices
- Seek trusted guidance – consult authoritative resources, professional advisors, and peer

organizations

- Review and adapt regularly – technology, threats, and organizational needs evolve, and sovereignty practices must evolve with them

A Call to Responsible Digital Stewardship

Canadian organizations—whether small businesses, non-profits, schools, municipalities, healthcare providers, or community groups—are stewards of important information and essential services.

Digital sovereignty is about fulfilling that stewardship responsibility with awareness of dependencies and risks, intention in technology selection and governance, capability to understand, control, and recover systems, resilience to continue serving stakeholders during adversity, and independence to make choices that serve organizational missions.

The organizations that thrive in an uncertain digital future will be those that understand their dependencies, preserve their options, and maintain the capability to adapt.

Digital sovereignty is not a destination. It is a continuous practice of informed, responsible, and resilient technology governance.

About the Linux Association of Canada

The Linux Association of Canada is a national non-profit organization dedicated to advancing Linux, open source software, digital sovereignty, and technology education across Canada.

We believe that Canadians—individuals, organizations, and communities—should have the knowledge, skills, and choices needed to participate confidently, securely, and independently in the digital world.

Our Mission

We work to ensure that Canadian organizations of all sizes can understand their digital dependencies and make informed technology decisions, access open source alternatives to proprietary and foreign-controlled platforms, build technical capability within their teams and communities, preserve digital sovereignty while participating in the global digital economy, and adopt sustainable technology practices that serve long-term organizational interests.

Our Work

Digital Sovereignty Education

Public education materials and guides, workshops and webinars, digital sovereignty assessments and planning support, policy development guidance, and procurement frameworks and evaluation tools.

Open Source Advocacy and Resources

Curated directories of open source alternatives, software evaluation and comparison resources, migration guides and case studies, technical documentation, and connection to open source communities and support providers.

Community Building and Support

Support for local Linux user groups across Canada, community forums and knowledge-sharing, mentorship and peer learning, collaboration with educational institutions, and partnerships with technology and civil society organizations.

School and Youth Outreach

Educational programs for K-12 and post-secondary institutions, student technology clubs and competitions, teacher training and curriculum resources, scholarship and recognition programs, and career pathway development in open source technology.

Hardware Refurbishment and Sustainability

Computer refurbishment programs using Linux, e-waste reduction initiatives, technology donation and redistribution, support for community technology access, and advocacy for right-to-repair and device longevity.

Research and Policy Engagement

Research on digital sovereignty and technology governance, submissions to government consultations, collaboration with policymakers and regulators, public interest advocacy, and evidence-based policy recommendations.

Why Digital Sovereignty Matters to Us

Digital sovereignty is not about rejecting global technology or retreating into isolation. It is about ensuring that Canadian organizations can make informed choices, maintain control over their information and operations, preserve alternatives when suppliers or policies change, build resilience against disruption, and serve their missions without unnecessary dependence on external parties.

Open source software and open standards are powerful tools for digital sovereignty because they reduce vendor lock-in, enable transparency through inspectable code, support local hosting and control, foster competitive markets, and preserve long-term access to information and systems.

Who We Serve

Small and medium businesses, non-profit organizations, schools and educational institutions, municipalities and local governments, healthcare and social service providers, libraries and community organizations, Indigenous communities exercising digital self-determination, and individual Canadians learning about Linux, open source, and digital rights.

Join Us

Digital sovereignty is strengthened through community, collaboration, and shared knowledge. Learn by exploring our resources and guides, connect by joining or starting a local Linux user group, contribute your knowledge and expertise, advocate for policies that strengthen Canadian digital sovereignty, adopt Linux and open source software in your organization, and support us through membership or donations.

Together, we can build a more secure, independent, and resilient digital future for all Canadians.

Contact Us

Website: linuxassociation.ca • Email: info@linuxassociation.ca • Phone: (639) 477-0111

Take Control of Your Digital Future

Where is our data? Who controls our systems? Can we recover, migrate, and continue operating?

This guide provides practical answers and actionable steps for Canadian organizations seeking greater control, resilience, and independence in their digital operations.

Linux Association of Canada

Advancing Linux, open source software, and digital sovereignty across Canada.

linuxassociation.ca • info@linuxassociation.ca • (639) 477-0111

Open Source. Strong Communities. A Resilient Canada.