



Red Hat

LEVEL 101 - INTRODUCTION TO DIGITAL SOVEREIGNTY

Executive Enablement Guide

Understanding Digital Sovereignty: Concepts, Risks, and Business Value

Version 1.1 - 7th March 2026

Enablement Guide Levels

This is the **101 - Introduction** guide for executives and newcomers. Other levels available:

- 101 - Introduction to Digital Sovereignty** - Executive overview (1-2 hours) [You are here]
- 201 - Domain Overview & Assessment** ([facilitator-guide-201.php](#)) - Full assessment (2-4 hours)
- 301 - Deep Dive Implementation** - Coming soon

Session Overview

Learning Objectives

By the end of this session, participants will be able to:

Understand what Digital Sovereignty means and why it matters to modern organizations

Recognize the key business risks and regulatory drivers

Identify the seven domains of Digital Sovereignty at a high level

Articulate the business value and competitive advantages of Digital Sovereignty

Understand next steps for assessing and improving their organization's maturity

Recommended Agenda

Introduction & Context (10 minutes) - Set the stage, explain why now

What is Digital Sovereignty? (15 minutes) - Core concepts and definitions

Business Drivers & Risks (15 minutes) - Why it matters to your organization

The Seven Domains (25 minutes) - High-level overview of each domain

Real-World Examples (10 minutes) - Success stories and cautionary tales

Next Steps & Q&A (15 minutes) - Path forward and discussion

What is Digital Sovereignty?

The Simple Definition

Executive Summary

Digital Sovereignty is the ability of an organization to maintain control over its digital assets, operations, and decision-making without undue dependence on external vendors or foreign jurisdictions.

It's about **strategic autonomy** in the digital age.

Key Concepts to Communicate

Control Over Data - Where your data lives, who can access it, and under what legal jurisdiction

Vendor Independence - Ability to switch providers without business disruption or prohibitive cost

Regulatory Compliance - Meeting increasingly strict data protection and sovereignty requirements

Operational Resilience - Ability to operate independently of single vendors or geographic regions

Strategic Freedom - Making technology decisions aligned with business goals, not vendor roadmaps

Discussion Point

Ask the group: "Can you think of a time when vendor lock-in or regulatory requirements created challenges for your organization?"

This helps make the concept concrete and relevant to their experience.

Business Drivers & Risks

Why Digital Sovereignty Matters Now

1. Regulatory Landscape

Governments worldwide are enacting strict data sovereignty laws:

GDPR (EU) - €20M fines or 4% of global revenue for violations

NIS2 Directive (EU) - Critical infrastructure cybersecurity requirements

DORA (EU Financial) - Digital operational resilience requirements

Cloud Act (US) - Gives US government access to data held by US companies globally

Data Localization Laws - Growing number of countries requiring data to stay within borders

Real Cost Example

In 2020, the EU-US Privacy Shield was invalidated, leaving 5,300+ US companies unable to legally transfer European customer data. Companies had to scramble to implement new data transfer mechanisms, costing millions in legal fees, infrastructure changes, and potential fines.

2. Geopolitical Risks

Foreign Government Access - Risk of foreign intelligence agencies accessing your data

Economic Sanctions - Sudden service disruptions due to international conflicts

Supply Chain Vulnerabilities - Dependence on single-region vendors or components

3. Business Continuity Risks

Vendor Lock-in - Inability to change providers leads to escalating costs

Service Dependencies - Single point of failure if critical vendor has outages

Pricing Power - Vendors raise prices knowing migration is difficult/impossible

Technology Obsolescence - Locked into vendor's technology evolution path

4. Competitive Advantages

Business Value

Customer Trust - Demonstrable data protection and privacy controls

Market Access - Meet regional requirements to operate in regulated markets

Negotiating Power - Ability to switch vendors gives leverage in contract negotiations

Innovation Speed - Not constrained by single vendor's roadmap

Risk Mitigation - Reduced exposure to geopolitical and regulatory changes

The Seven Domains of Digital Sovereignty

Digital Sovereignty is measured across seven interconnected domains. For this executive overview, focus on the **business value and risks** of each domain, not technical details:

1. Data Sovereignty

What it means: Control over where your data is stored, processed, and who can access it under what legal jurisdiction.

Business risk if lacking: Foreign government access to sensitive data, GDPR/regulatory fines, customer trust erosion.

2. Technical Sovereignty

What it means: Freedom from vendor lock-in through open standards, APIs, and data portability.

Business risk if lacking: Trapped with single vendor, escalating costs, inability to innovate independently.

3. Operational Sovereignty

What it means: Ability to operate systems and services independently without relying on single vendors or

4. Assurance Sovereignty

What it means: Independent verification and auditing of security controls, not just trusting vendor

regions.

Business risk if lacking: Business continuity threats, service outages beyond your control, operational blind spots.

claims.

Business risk if lacking: Hidden vulnerabilities, compliance gaps, inability to prove security to regulators or customers.

5. Open Source Sovereignty

What it means: Leveraging transparent, community-driven software you can inspect, modify, and control.

Business risk if lacking: Proprietary software "black boxes," forced upgrades, hidden security vulnerabilities.

6. Executive Oversight

What it means: Leadership actively manages sovereignty risks and makes informed strategic decisions.

Business risk if lacking: Sovereignty risks not understood at board level, reactive rather than strategic approach.

7. Managed Services

What it means: When outsourcing, maintaining contractual controls and exit rights to protect sovereignty.

Business risk if lacking: Losing control to service providers, difficult/impossible to change providers, hidden dependencies.

Facilitation Tip

For each domain, ask: "**Which of these domains do you think represents the biggest risk or opportunity for your organization?**"

This engages participants and helps them connect the concepts to their business context.

Real-World Examples

Success Stories

European Central Bank (ECB)

Challenge: ECB needed to modernize IT infrastructure while maintaining strict data sovereignty and operational independence.

Solution: Adopted hybrid cloud built on open-source technologies (Red Hat OpenShift) with data kept within EU jurisdiction and no single vendor dependency.

Outcome: Full regulatory compliance, operational flexibility, and ability to innovate without vendor constraints.

Major Healthcare Provider

Challenge: Patient data sovereignty requirements, HIPAA compliance, and vendor lock-in preventing innovation.

Solution: Migrated from proprietary cloud to sovereign cloud infrastructure with bring-your-own-key (BYOK) encryption and regional data storage.

Outcome: Met all regulatory requirements, reduced vendor dependency, 40% cost reduction over 3 years.

National Australia Bank

Challenge: One of Australia's largest banks needed to modernize legacy infrastructure while meeting strict financial regulatory requirements and maintaining operational control.

Solution: Deployed Red Hat OpenShift Container Platform to create a modern, open hybrid cloud foundation with full operational sovereignty and no vendor lock-in.

Outcome: Accelerated application delivery from months to weeks, maintained full control over critical financial systems, and achieved regulatory compliance across all domains. Reduced infrastructure costs by 30%.

Deutsche Börse Group

Challenge: Europe's largest stock exchange operator required sovereign infrastructure to handle mission-critical trading systems while meeting strict EU regulatory requirements.

Solution: Built private cloud infrastructure using Red Hat OpenStack and OpenShift, keeping all data within EU jurisdiction with full operational independence.

Outcome: Achieved 99.99% uptime for trading systems, complete data sovereignty compliance, and ability to rapidly innovate without external dependencies. Processes over €8 trillion in annual trading volume with full control.

Telefónica

Challenge: One of the world's largest telecommunications providers needed to modernize infrastructure for 5G while maintaining sovereignty over critical network infrastructure and customer data.

Solution: Deployed Red Hat OpenShift to build cloud-native 5G core network with open standards, avoiding vendor lock-in and maintaining full operational control.

Outcome: Successfully deployed sovereign 5G infrastructure across Europe and Latin America, reduced vendor dependency, and accelerated service deployment by 60%. Full control over network operations and customer data.

UK Ministry of Defence

Challenge: Required sovereign cloud infrastructure for defense applications with absolute data sovereignty, no foreign dependencies, and complete operational control.

Solution: Built secure private cloud using Red Hat Enterprise Linux and OpenShift, with all infrastructure UK-based and managed internally with open-source transparency.

Outcome: Achieved complete digital sovereignty for defense operations, full security audit capability, and ability to rapidly deploy mission-critical applications without external vendor dependencies. Zero foreign government access risk.

Lufthansa Group

Challenge: Europe's largest airline group needed to modernize IT operations while maintaining sovereignty over passenger data and operational systems across multiple jurisdictions.

Solution: Implemented Red Hat Ansible Automation Platform and OpenShift to create standardized, portable infrastructure with data kept in appropriate jurisdictions and no single cloud provider lock-in.

Outcome: Reduced automation time by 90%, maintained full GDPR compliance with data sovereignty, and achieved operational flexibility to move workloads between cloud providers as needed. Saved €10+ million in infrastructure costs.

Cautionary Tales

Privacy Shield Invalidation (2020)

What happened: EU court invalidated EU-US Privacy Shield, leaving 5,300+ companies unable to legally transfer European customer data to US.

Impact: Companies faced millions in legal fees, emergency infrastructure changes, potential GDPR fines up to 4% of global revenue.

Lesson: Relying on single jurisdiction for data storage creates regulatory risk. Geographic data sovereignty essential.

Major Vendor Service Outage

What happened: Global cloud provider had 7-hour outage affecting thousands of businesses.

Impact: Companies with no operational sovereignty couldn't access critical systems, losing millions in revenue.

Lesson: Operational sovereignty (multi-cloud, hybrid strategies) provides resilience against single-vendor failures.

Measuring Digital Sovereignty Maturity

Organizations progress through five maturity levels as they strengthen their Digital Sovereignty posture:

Level 1	Initial - Ad-hoc, reactive approach. High vendor dependency and sovereignty risks.
Level 2	Managed - Basic awareness and controls in place. Beginning to address risks.
Level 3	Defined - Documented processes and standards. Consistent approach across organization.
Level 4	Quantitatively Managed - Metrics-driven, measured controls. Data-based decision making.
Level 5	Optimizing - Continuous improvement culture. Strategic sovereignty leadership.

Assessment Recommendation

After this introduction, organizations typically benefit from a **Full Maturity Assessment** to understand their current state and prioritize improvements.

The assessment evaluates all seven domains and provides:

- Current maturity level for each domain
- Specific gaps and risks
- Prioritized roadmap for improvement
- Business case and ROI analysis

Next Steps & Path Forward

Immediate Actions

Executive Alignment - Ensure leadership understands sovereignty risks and opportunities

Current State Assessment - Conduct full maturity assessment across seven domains

Risk Prioritization - Identify highest-risk areas based on your industry and regulatory requirements

Roadmap Development - Create phased improvement plan with quick wins and strategic initiatives

Assessment Options

Quick Assessment

15-minute online self-assessment provides initial maturity baseline. Good starting point for understanding current state.

Full Assessment

2-4 hour facilitated workshop with deep-dive into all seven domains. Provides detailed roadmap and recommendations.

[Start Quick Assessment → \(ds-readiness/index.php\)](#)

[View 201 Guide → \(facilitator-guide-201.php\)](#)

Additional Resources

[Workshop Templates & Materials \(templates/index.html\)](#) - Email templates, agendas, executive summaries

[Facilitator Guide 201 \(facilitator-guide-201.php\)](#) - For conducting full maturity assessments

Red Hat Consulting - Expert guidance on Digital Sovereignty implementation

Common Questions & Answers

Q: Doesn't Digital Sovereignty mean we can't use cloud services?

A: No! Digital Sovereignty is about *control and choice*, not avoiding cloud. You can absolutely use cloud services while maintaining sovereignty through:

Sovereign cloud providers (EU-based with EU-only data storage)

Hybrid cloud architectures (sensitive data on-premises, other workloads in cloud)

Multi-cloud strategies (avoiding single-vendor lock-in)

Bring-your-own-key encryption (you control the keys, not the cloud provider)

Q: Isn't Digital Sovereignty just a European concern?

A: While EU regulations like GDPR and NIS2 have driven awareness, Digital Sovereignty matters globally:

US organizations face foreign government access risks (e.g., Chinese intelligence laws)

Financial institutions worldwide need operational resilience (DORA-like requirements)

Healthcare providers everywhere must protect patient data sovereignty

Critical infrastructure requires resilience regardless of location

Vendor lock-in costs affect all organizations equally

Q: How much does improving Digital Sovereignty cost?

A: The investment varies based on current state and goals, but key points:

Cost avoidance: Preventing regulatory fines (GDPR fines average €2.5M) and vendor lock-in price increases

Quick wins: Many improvements (contractual controls, data classification) require minimal investment

Strategic investments: Migration to sovereign cloud or open-source platforms pays back through flexibility and reduced licensing costs

ROI timeframe: Most organizations see positive ROI within 18-24 months

Q: We're already ISO 27001 certified. Isn't that enough?

A: ISO 27001 is excellent for information security, but Digital Sovereignty addresses different concerns:

Jurisdictional control: ISO doesn't address foreign government access or data localization

Vendor independence: ISO doesn't measure lock-in or portability

Operational sovereignty: ISO doesn't require multi-vendor resilience

Complementary frameworks: Digital Sovereignty builds on ISO 27001, addressing modern geopolitical and vendor risks

© 2026 Red Hat, Inc. | Viewfinder - Digital Sovereignty Assessment Platform