Digital Sovereignty
Protect your Minimum Viable Operations

Maintain resilience, autonomy, and access to best-in-class technology

Capgemini

Control, where it counts

In a world being reshaped by geopolitical volatility, with nations seeking ways to exert influence and control, many organizations face increased risk exposure through an overdependence on foreign technology provider. With increased risk, there's growing pressure in the boardroom to reclaim sovereignty over the digital value chain to bolster operational resilience and reclaim strategic autonomy.

But there's no single solution; digital sovereignty looks different for every organization. Leaders must make strategic decisions about choosing and managing dependencies to strike the right balance between risk and reward. Assessing and strengthening digital sovereignty requires a structured, pragmatic, and risk-driven approach and a strategic mindset to ensure sovereignty doesn't come with unacceptable costs or disruption.

At its heart, a digital sovereignty strategy should ensure the organization can sustain its Minimum Viable Operations (MVO) the smallest set of digital services that must remain operational and governed in the event of disruption. And during less volatile periods, sovereignty should allow organizations to preserve the freedom to choose, adapt, and innovate.

In this executive guide, you'll discover:

- Why digital sovereignty must be a critical strategic priority
- Key considerations for creating an effective digital sovereignty strategy
- A strategic approach to assessing sovereignty risk and planning mitigation actions

Why is digital sovereignty necessary?

As digitalization accelerates, organizations have become increasingly dependent on a small number of global technology providers for critical services. This concentration can limit strategic autonomy and expose organizations to external control, jurisdictional risk, and geopolitical disruption.

What is digital sovereignty?

We define digital sovereignty as an organization's ability to maintain operational resilience and strategic autonomy while minimizing external interference across the digital value chain.

Alongside these developments, cybersecurity threats have increased, with critical national infrastructure and organizational networks becoming prime targets for criminal and state-affiliated attackers. And while data security regulations tighten in response, the sophistication and operational impact of cyber attacks continue to grow.

The consequences of inaction

These forces combine to create vulnerabilities that could prevent organizations from maintaining their MVO. This makes the need for the control and autonomy of digital sovereignty more urgent than ever. Without a defensible sovereignty posture, organizations increase their exposure to:

- Value chain disruption from unanticipated dependencies that make the organization vulnerable to geopolitical events.
- Vendor lock-in that impedes independent decision-making and weakens resilience.
- Loss of intellectual property and sensitive data due to insufficient control or jurisdictional exposure.
- Legal and financial penalties for non-compliance with local and regional regulations.
- Damage to customer trust through a lack of transparency and control.

In response to these potentially existential threats, leaders need to determine how to deliver the right balance between cost, security, and speed-to-value. They're asking new questions about the level of digital sovereignty they require, including:

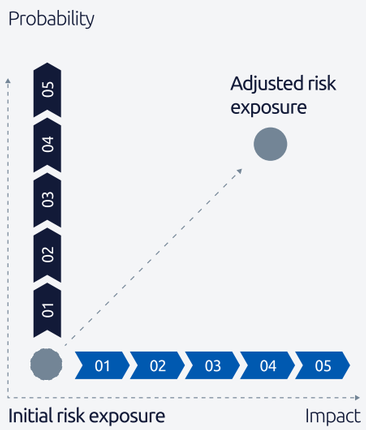
- What risks and dependencies could impact our operational resilience?
- How can we ensure we have strategic autonomy and freedom of choice?
- How can we strengthen our sovereignty without sacrificing speed-to-value?

Is the current level of investment sufficient to maintain exposure risk at an acceptable level?

Probability drivers

- **01.** Geopolitical fragmentation
- **02.** Provider consolidation
- **03.** Regulatory shifts
- **04.** Technology innovation
- **05.** Cyberthreats

Risk transition



Impact drivers

- **01.** Digitalization adoption
- **02.** Business criticality
- **03.** Reputational damage
- **04.** System dependencies
- **05.** Financial exposure

Establishing the right digital sovereignty posture

Digital sovereignty isn't about having complete independence; very few organizations actually require total sovereignty, and it would be extremely hard to achieve in practice. Sovereignty means being able to make independent strategic decisions about the organization's digital domain without incurring prohibitive costs or disruption.

✓ Digital sovereignty is...

A board-level concern.

It is about managing operational risk and maintaining strategic autonomy across the business.

A risk management framework.

It helps organizations make strategic decisions based on their risk exposure and appetite.

Freedom of choice.

It enables organizations to make informed decisions about where dependencies are acceptable and where they are not.

An innovation protector.

It creates the trust, resilience, and control needed to accelerate AI, data, and digital initiatives.

A spectrum of approaches.

Organizations can adopt different sovereignty postures depending on their needs, priorities, and risk profile.

An evolving discipline.

It requires continual adaptation of people, processes, technology, and governance as circumstances change.

✕ Digital sovereignty is not...

Just an IT project.

It's not simply about selecting technology vendors or infrastructure platforms.

An ideology.

It is not a political or geopolitical position in itself.

Isolation.

It does not mean eliminating every dependency or building everything in-house.

An innovation blocker.

It should not slow transformation or delay time-to-value.

A single answer.

There is no universal template or one-size-fits-all model.

A one-off project.

It's not something that can be implemented once and then left unchanged.

Sovereignty across the key dimensions of the digital value chain

To achieve an appropriate level of digital sovereignty and protect their MVO, organizations must consider eight risk dimensions.

- Cybersecurity
- AI
- Software
- Hardware
- Cloud
- Energy
- Data
- Connectivity

It's also important to remember that these dimensions shouldn't be treated as separate workstreams; they all have an impact on each other. For example, having a sovereign cloud will provide limited resilience if network connectivity routes through infrastructure are subject to extraterritorial legislation or executive orders.

Cybersecurity

Can you prevent, detect, respond, and recover independently of foreign actors?

If infrastructure components originate from jurisdictions with conflicting security standards, it can create network vulnerabilities and compliance risk. There's also the potential for critical updates or patches to be delayed or withheld due to geopolitical tensions.

Cyber sovereignty means having the ability to prevent, detect, contain, respond to, and recover from incidents without being dependent on foreign threat intelligence, security providers, or security software vendors.

AI

Who controls the models, training data, and inference you depend on?

AI is becoming the primary driver of digital sovereignty. Without control over models, data, and inference, organizations risk losing control over their IP, decision-making, and competitive advantage.

AI sovereignty concerns who builds and controls the models, whose data trains them, and where and how inference runs. Organizations need access to models they can audit, fine-tune, and govern without overdependence on vendors.

Software

Do you have portability, auditability, and freedom from vendor lock-in?

Software supply chains often rely on third-party, open-source, and foreign components that may contain hidden vulnerabilities or malicious code. Organizations are also exposed to compliance risk if upstream suppliers fail to meet required data sovereignty or security standards.

And while open source may seem like an ideal sovereignty solution, it's not enough to have the source code. Organizations also need the internal capability to maintain and evolve software without becoming dependent on external communities.

Hardware

Is your compute and semiconductor supply chain resilient?

With numerous components sourced from multiple jurisdictions, hardware devices can leave organizations exposed to geopolitical disruptions such as export bans, security vulnerabilities from compromised parts, and compliance gaps if suppliers don't adhere to the correct standards.

Chip dependency is the most obvious source of hardware risk. It's also the hardest to immediately resolve, so the focus should be on supply chain diversity to increase resilience.

Cloud

Who controls the infrastructure running your workloads?

In a market dominated by major SaaS providers and cloud platforms, organizations are at risk of overdependency and lock-in. They may also be subject to extraterritorial legal frameworks that allow foreign authorities to request access to data regardless of where it's stored, even if it's on overseas servers. [ii]

However, as hyperscalers provide many critical digital services, organizations must establish an acceptable balance between risk and reward when making cloud infrastructure decisions.

Energy

Is your digital infrastructure's energy supply resilient and controlled?

When organizations are dependent on specific energy sources for digital operations, they can experience operational resilience challenges during periods of geopolitical turbulence or supply volatility.

Specifically for AI-intensive organizations, energy is now a strategic asset, making it even more critical to have a resilient yet environmentally sustainable power supply that isn't dependent on a single energy source or grid operator.

Data

Who can access your data or compel disclosure?

Poor visibility and control over data increases the risk of IP loss and regulatory non-compliance, especially when the location of data is difficult to pinpoint in complex hybrid environments.

Having data sovereignty means being able to decide who can access, process, share, or compel disclosure of data, under which legal jurisdiction, and on what terms.

Connectivity

Is your network infrastructure under domestic legal and operational control?

When organizations rely on global networks, they can become susceptible to foreign influence and experience service disruptions during geopolitical crises.

The sovereignty posture in this dimension will depend on the degree to which the network infrastructure must be under domestic control, without exposure to foreign surveillance or sabotage.

Gartner predicts that, by 2030, over 75% of enterprises outside the US will have a digital sovereignty strategy.

Sovereignty cannot be standardized

The right path depends on your risk profile, regulatory environment, business ambitions, and operating model. By taking a holistic and structured approach, you can reduce the complexity of accurately assessing your sovereignty posture and risk exposure, enabling you to make informed decisions about appropriate mitigation actions. To build a pragmatic and effective strategy for protecting your MVO, you should assess digital sovereignty from four perspectives:

01

Data and AI

- Identify where your data is stored and processed, and ensure appropriate safeguards are in place during the data lifecycle and for cross-border data transfers.
- Ask yourself how dependent your organization is on thirdparty data – and whether you can guarantee its continuous availability
- Understand where AI models and training data originate from, and assess their relevance for the local language, values, and culture.
- Assess your compliance with relevant security, privacy, and sector-specific standards and regulations.
- Determine whether you can you trust the organizations that manage your data.

02

Technology

- Assess whether your systems offer portability, interoperability, reversibility, and adherence to open standards.
- Evaluate how dependent your hardware and software supply chains are on foreign suppliers.
- Decide if you can trust the end-to-end supply chain that’s needed to deliver your digital services.
- Gauge whether your cloud-native approach is aligned with your sovereignty ambition.

03

Operations

- Determine whether your digital services and platforms operated by entities subject to regional and local laws.
- Assess your providers' standards for staff nationality, location, and security clearance.
- Identify where your physical servers and management infrastructure located.
  Establish how reliant your infrastructure operations are on foreign energy sources.
- Identify who has access to the technology that delivers your services.
- Appraise your ability to ensure business continuity in day-to-day operations and maintain the resilience to adapt to future disruptions.

04

Legal and jurisdiction

- Understand whether all your operations and data fall under the laws of an appropriate jurisdiction and are immune to foreign influence or control.
- Assess whether your providers can operate across multiple jurisdictions in a compliant manner.
- Identify any sector-specific sovereignty requirements for your organization.
- Determine whether you have legal control over your digital services.
- Pinpoint critical services that could be subject to foreign interference.

It's also essential that your digital sovereignty strategy – and any partner that helps you design and execute it – considers these critical success factors:

Define sovereignty postures that work in the real world.

Sovereignty should have clear operational accountability, continuous enforcement, and be crisis-ready by design.

Deliver industrialized sovereignty at speed.

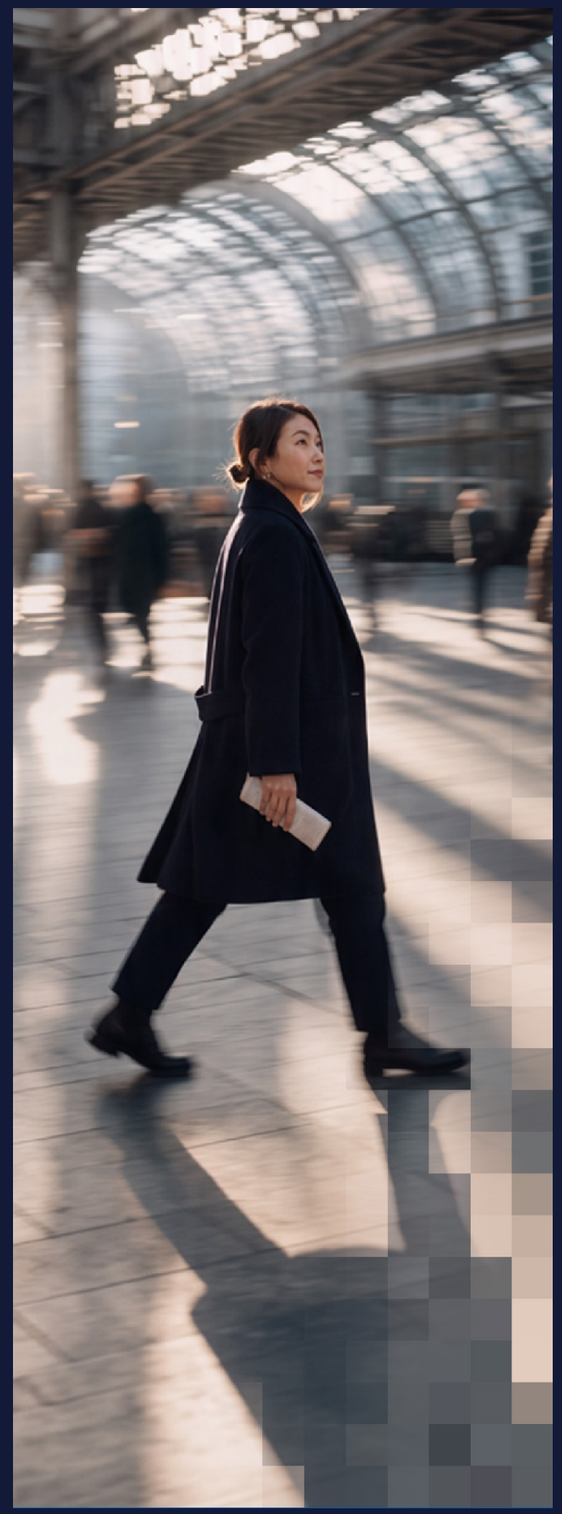
Design repeatable foundations and codified sovereignty to accelerate delivery and realize consistent outcomes across markets.

Create sovereign AI that can run the business.

Build sovereign, production-grade platforms to deliver trusted AI, governed and operated based on real risk.

Make sovereignty a strategic business decision.

Use digital sovereignty assessments to base decisions on risk and make balanced, deliberate trade-offs.



Planning your next steps with Capgemini

At Capgemini, we combine global scale with local sovereignty expertise to help organizations understand their digital sovereignty risk exposure and plan corrective actions in line with their strategic goals.

Our Digital Sovereignty Assessment offers a structured, strategic way to evaluate your risk and plot a path to the right sovereignty posture for your organization.

1 week

Start the assesment and delivery questionnaire

Collect and analyze information

Collect and analyze sovereignty - related documents, validate the scope to be assessed (3 critical applications) and share the questionnaire.

1-2 week

Discover the digital sovereignty context

Host qualitative workshops

Conduct quantitative workshops with key stakeholders to review & deep dive on client position.

Assess digital sovereignty

Score the sovereignty level per pillar (sovereign compass) and at organization level (sovereignty continuum).

1 week

Analyze digital sovereignty risks

Identify risk scenarios

Based on the ratings, collected information, identify key risk scenarios and define the sovereignty risk profile of the organization.

1 week

Report results and arbitrate on risk mitigation scenarios

Define risk mitigation scenarios

Identify key risk mitigation scenarios and associate remediation actions.

Analyze high-level impact

Analyze high-level impact on IT, TOM and budget, share recommendations and prepare arbitration with board of directors.

With Capgemini, your digital sovereignty strategy benefits from:

01 **A unique builder–integrator–orchestrator model,** combining strategy, platform engineering, and sovereign operations to ensure sovereignty isn't just designed, but enforced and sustained.

02 **A vendor-plural ecosystem approach,** orchestrating hyperscalers alongside European and national sovereign cloud providers to power innovation while controlling risk.

03 **End-to-end sovereignty across the full digital value chain,** industrialized through repeatable platforms and delivery models.

04 **Proven sovereign platforms and assets,** sovereign AI capabilities, and in-region delivery centers – turning strategy into compliant, scalable operations.

05 **AI-ready sovereign foundations,** enabling organizations to retain control over models, data, and inference to unlock secure, scalable AI adoption.

06 **European-native scale with regulatory alignment,** combining local delivery, sovereign operations, and deep relationships with European institutions to ensure legal defensibility.

Mitigate the risk to your MVO

Disruption is certain, but its impact can be hard to predict. So, every organization has a duty – to customers, employees, and regulators – to maintain its MVO during volatile conditions. But without the right levels of digital sovereignty, organizations can't guarantee they'll fulfill that duty.

Managing this risk requires a carefully considered strategy to ensure your organization sustains a digital sovereignty posture that's viable, defensible, and scalable. By taking an informed, strategic approach to digital sovereignty, you can strengthen your operational resilience. But beyond that, sovereignty gives you the strategic autonomy to make the right digital choices for your organization. And it allows you to build a launchpad that accelerates time-to-value for future innovation.

It's time to identify your sovereignty risk exposure and establish a defensible posture before regulatory, geopolitical, or AI-driven disruption forces you into reactive action.

Start protecting your MVO today. **Get in touch with our experts** to assess your sovereignty risk exposure and identify your next steps.

Authors

Nicolas Gaudilliere
Chief Technology Officer,
Capgemini Invent, France
nicolas.gaudilliere@capgemini.com

James Dunn
Director of Global Cloud and Sovereign Strategy, Cloud Infrastructure Services
james.dunn@capgemini.com

Stefan Zosel
VP Cloud, Lead Global Public Sector / Sovereign Cloud
stefan.zosel@capgemini.com

Rob Kernahan
Vice President,
Northern & Central Europe
robert.kernahan@capgemini.com

About Capgemini

Capgemini is the business transformation partner for enterprises in the age of AI. We help organizations imagine and build an intelligent, sustainable future, combining AI, technology and human ingenuity to transform how they operate, innovate and grow. With unique end-to-end capabilities spanning strategy, technology, engineering and intelligent operations, we bring together deep industry expertise and market-leading capabilities in AI, cloud and data to turn ambition into measurable business outcomes at scale. Supported by a robust ecosystem of partners and nearly 60 years of expertise, Capgemini is a responsible and diverse global organization of over 410,000 team members in more than 50 countries. The Group reported 2025 revenues of €22.5 billion.

Make it real | www.capgemini.com.

[i] U.S. Congress, H.R. 4943—CLOUD Act, 115th Congress (2017–2018), Congress.gov, introduced February 6, 2018, accessed July 8, 2026, https://www.congress.gov/bill/115th-congress/house-bill/4943

[ii] Gartner, Gartner Survey Reveals Geopolitics Will Drive 61% of CIOs and IT Leaders in Western Europe to Increase Reliance on Local Cloud Providers, Gartner.com, 12 November, 2025, accessed July 8, 2026, https://www.gartner.com/en/newsroom/press-releases/2025-11-12-gartner-survey-reveals-geopolitics-will-drive-61-percent-of-cios-and-information-technology-leaders-in-western-europe-to-increase-reliance-on-local-cloud-providers

Make it real .