Sovereignty is not optional anymore

Turning Digital Sovereignty into a strategic lever for trust, resilience, and competitive advantage

ATOS GROUP Accelerating intelligence

Managing critical dependencies: A board imperative, now!

C-Suite brief

Digital Sovereignty has moved to the top of executive agendas. Geopolitical fragmentation, expanding regulation, extraterritorial access laws, and concentration of critical digital capabilities among a small number of global providers are reshaping the technology risk landscape. AI adoption is accelerating this shift. Data sensitivity, automated decision making, and dependency on complex digital supply chains are increasing operational and strategic exposure.

Organizations therefore need to maintain control over critical data, systems, and digital operations while continuing to scale innovation globally. Cybersecurity is central to this objective as the enforcement layer of digital sovereignty. Sovereign intent becomes real only when control is implemented, monitored, and proven in operations across identities, privileges and encryption.

☑ **The following do's and don'ts set clear stakes in the ground for organizations looking to turn Digital Sovereignty from a stated ambition into something they can design, operate and prove.**

Do's

- ✓ **Do** start with business criticality
- ✓ **Do** engineer sovereignty workload by workload
- ✓ **Do** treat cybersecurity as the enforcement layer
- ✓ **Do** secure identities, privileges, keys and operating paths
- ✓ **Do** govern sovereignty across the full stack
- ✓ **Do** build a horizontal control plane across environments
- ✓ **Do** make trade-offs explicit
- ✓ **Do** preserve freedom of choice through open standards and portability
- ✓ **Do** extend sovereignty guardrails to AI agents
- ✓ **Do** run sovereignty as Managed Sovereignty, proven continuously in operations

Don'ts

- ✗ **Don't** apply the same sovereignty level everywhere
- ✗ **Don't** reduce it to a cloud, provider or certification level
- ✗ **Don't** confuse paper compliance with actual control
- ✗ **Don't** assume data residency alone solves the problem
- ✗ **Don't** optimize one layer and ignore the rest
- ✗ **Don't** let each platform become its own sovereignty island
- ✗ **Don't** pretend maximum control comes with zero cost, zero friction or zero time-to-market impact
- ✗ **Don't** hardwire irreversible lock-in
- ✗ **Don't** let autonomous systems act across workflows without policy, logging, escalation and kill-switch authority
- ✗ **Don't** declare victory at contract signature, certification day or migration cut-over

Atos definition of Digital Sovereignty

Digital Sovereignty is the ability of an organization to **retain control, authority, and accountability over its data, infrastructure, applications, and digital operations,** continuously managing its critical dependencies, exposure, and disruption risks from external jurisdictions, vendors, or technologies.

Context

Digital Sovereignty has been a recurring topic for years, rising and falling on executive agendas depending on political cycles, regulatory initiatives, or major incidents. In periods of relative stability, it was often treated as a policy concern, a compliance topic, or a niche requirement limited to public sector, defense or highly regulated industries.

This has changed. Digital Sovereignty has now become a critical priority. Geopolitical fragmentation, accelerating regulation, extraterritorial regulations, and the concentration of critical digital capabilities among a small number of global providers (where rising licensing and platform costs amplify dependency and expose customers to escalating, hard-to-reverse financial commitments) have materially altered the risk landscape. At the same time, the rapid adoption of AI is increasing data sensitivity, automation of decisions, and dependency on complex digital supply chains raising the operational, financial, and strategic consequences of loss of control.

Digital Sovereignty must also be seen through the lens of resilience. As recent outages, cyber incidents, and attacks on critical infrastructure have shown, excessive dependency concentration can rapidly turn into operational disruption.

Together, these forces have turned Sovereignty from a contextual consideration into a structural concern for enterprises and institutions alike. The pace and priority vary by geography and sector, but the direction is consistent: organizations are progressively strengthening their Sovereignty posture in response to evolving risk assessments.

An overwhelming share of CxOs are now embedding a Sovereignty approach across their IT stack.

IDC estimates that

84%[1]

of companies using cloud technologies are either currently using or planning to use sovereign cloud solutions, and Gartner estimates that more than

50%

of companies will have set up sovereign digital strategies by 2029, versus 10% today[2].

Digital Sovereignty is therefore emerging as a core strategic capability for organizations to manage critical digital dependencies, preserve architectural optionality, and retain control over data, technology, and operations.

Atos Group speaks to this topic as a long-standing operator of mission-critical, regulated, and sovereign digital environments. For decades, we have designed, built, and run systems where control and resilience are mandatory. This experience gives us a practical, operational perspective on Sovereignty with strong convictions and unique perspectives.

Sources: [1] IDC, 2025, How Sovereign Cloud is impacting organizations in Europe [2] Gartner, 2025, Top trends shaping the future of cloud

1. Business-critical and no longer optional

Our conviction is that **Digital Sovereignty is now firmly on your 2026 agenda.** It will be driven by diverse triggers: geopolitical context, regulatory evolution, post-crisis risk mitigation, vendor concentration, and increasingly, as a strategic lever supporting your growth and differentiation.

You are facing multiple Sovereignty pressures at once. You must ensure business continuity under stress, protect sensitive data and intellectual property, comply with tightening regulatory requirements, and manage stakeholder perception and reputational risks in an environment where digital integrity is under scrutiny.

Yet Sovereignty is not only about constraints and risk containment. **It is also a strategic opportunity.** Properly engineered, it creates trust, reinforces brand credibility, and becomes a differentiator in competitive markets. Customers and partners increasingly expect companies to demonstrate control over their data, systems, and dependencies. In public tenders, Digital Sovereignty is already a decisive criterion, with a growing trend toward measurable frameworks and auditable commitments. And Stakeholders will increasingly expect Sovereignty to be **evidenced through concrete indicators such as reduced concentration risk, faster response to regulatory change, stronger control effectiveness, and improved resilience across critical workloads.**

Digital Sovereignty also enables sustainable, long-term digital transformation. By preserving freedom of choice, limiting irreversible dependencies, and protecting intellectual property, you regain the freedom of innovating, disrupting and transforming with confidence.

For all these reasons, **Digital Sovereignty is not optional.** You cannot treat it as an afterthought or delegate it down the organization. It must sit at the core of any company's digital strategy, as a strategic driver of resilience, differentiation, and growth. It must be an enterprise-wide priority, with graduated level of control at data and workload levels.

2. No easy answers, and definitely not binary

The first challenge of Digital Sovereignty is defining it. For some, Sovereignty means data residency. For others, it means national cloud providers, legal immunity, operational autonomy, or cyber resilience. Boards speak in terms of risk and accountability. Technical teams translate this into architecture choices. Legal teams focus on jurisdiction. Security teams focus on access and control. Procurement hears vendor labels and certifications.

Jurisdictional and legal immunity will remain uncertain until tested in court. Court outcomes are slow, country-specific, and rarely provide operational protection when pressure rises. Therefore, they cannot be relied upon as a primary line of defense.

What leadership teams can actively control today are concrete levers embedded in their digital environments: data, technology, and operations. As a result, executive teams need to answer three simple but critical questions:

Where are my data and models hosted and computed, how are they encrypted?

This is the most visible dimension of Sovereignty, as it reflects jurisdictional exposure. But location is only part of the answer. Effective control depends on enforceable security mechanisms, in particular sovereign encryption schemes where cryptographic keys remain under your ownership and control, managed through sovereign and external cryptographic solutions reinforced by confidential computing.

Who can access, operate, and ultimately control my systems and my data?

This has two dimensions. First, providers must prove how access is restricted within their own operating model, including privileged roles and cross-border exposure. Second, customers must retain enforceable control at the layers they own (data layer in SaaS, application and configuration layer in PaaS). Sovereignty depends on the ability to explicitly grant and revoke access across identities, privileges, and operational paths, with controls that are technically enforced and continuously auditable.

How resilient and robust are my technology and my operations in case of disruption, dependency, or escalation?

Resilience, continuity of service and preservation of the minimal viable company or organization are as strategically important as where data is processed, stored, and secured. This includes the ability to preserve autonomy of choice over time: credible alternatives to critical dependencies, limited stickiness to any single provider or platform, and architectural options (typically supported by open standards and open-source components) that allow systems to continue operating (even in degraded mode), migrate, or be reconfigured when conditions change (or when a kill switch is activated).

Answering these questions requires enterprises to step back and review the full mosaic of technologies and digital enablers that underpin their ability to operate safely. The strategic importance of workloads varies significantly across the enterprise, and not all parts of the IT stack contribute equally to Sovereignty risk. Blanket approaches and averages are misleading; Sovereignty requires deliberate and differentiated methods. This assessment must extend beyond the technology layers themselves. Sovereignty is equally determined by operating models, delivery models such as SaaS, supplier and software supply chains, governance mechanisms, and the enforceability of legal controls across jurisdictions.

While the core questions of Sovereignty are often reduced to a choice of cloud or infrastructure provider, that is a misconception. In reality, addressing them is complex and multi-dimensional. Organizations must take Sovereignty de-risking decisions at a highly granular level, applying differentiated levels of protection and control depending on criticality and risk trade-offs.

In practice, Sovereignty is enforced through a dense set of technical and operational control points that sit deep in the stack and at its seams. These include data access isolation, encryption and key ownership, identity and privilege management, logging and auditability, regionalized backup and recovery, controlled software supply chains, operational access constraints, and resilience mechanisms against dependency or disruption. None of these controls is sufficient in isolation. Sovereignty emerges from how they are combined, governed, and operated consistently over time. This demands a set of key design principles that ensure consistency across all layers of the sovereignty posture, so that controls reinforce each other rather than operate as disconnected safeguards. These principles must be applied across all dimensions:

Across the full IT stack

Sovereignty must be assessed and engineered from foundational layers (networks, cloud and infrastructure, platforms, cyber-security) to business-facing capabilities (applications, end-user devices, AI and analytics), each layer introducing distinct exposure points, control levers and dependency risks

By business workload and use cases

Not all workloads carry the same level of sensitivity or strategic importance; core, mission-critical or highly sensitive workloads in your given industry may justify higher level of Sovereignty controls. You therefore need to understand and assess your risks and business priorities, and orchestrate the right guardrails for the specific workloads

By geography and jurisdiction

Sovereignty requirements vary significantly by country and region, driven by local and industry regulations, legal frameworks, geopolitical exposure and enforcement practices. Architecture, operating model and partner choices must be adapted accordingly, reflecting local specificities rather than assuming global uniformity

This complexity is compounded by an unavoidable reality: Sovereignty comes with a price. Enhanced Sovereignty controls often come with higher costs, restricted access to innovation, and time-to-market trade-offs. These trade-offs must be made explicit, intentional, and workload specific. Like cybersecurity, Sovereignty is fundamentally a risk appetite decision. There is no universal right answer: the appropriate level of control depends on what an organization is willing to accept in terms of exposure, dependency, and potential disruption, weighed against cost, speed, and access to innovation. This makes the framing of the decision as important as the decision itself. Without a structured, fact-based approach, Sovereignty choices risk being driven by perception or politics rather than by measurable risk and business priority. Effective Digital Sovereignty is not about maximizing control everywhere, but about finding the right balance between all the Sovereignty controls considered and associated tradeoffs.

In practice, Sovereignty ambitions are shaped across four core objectives: autonomy, resilience, control, and security. Within the constraints of a Sovereignty budget, organizations must balance investments across these dimensions, which requires close alignment between business and IT to identify critical workloads, assess dependencies, and agree on the appropriate Sovereignty level and associated funding.

However, they should not become blockers. For one, the cost of non-Sovereignty can be far steeper. But more importantly, Sovereignty does not automatically mean higher cost. Through deliberate architectural choices, use of open standards, open-source components, modular designs, and diversified ecosystems, organizations can strengthen control while preserving innovation and economic efficiency. Agentic capabilities further shift this equation: by automating enforcement, monitoring, and remediation across sovereign environments, they reduce the operational cost of maintaining higher levels of control, turning what would traditionally be a cost and innovation trade-off into a scalable operating model.

The Sovereignty question deepens as delivery shifts toward automation and agentic execution. When AI can initiate workflows and act across systems, Sovereignty guardrails must extend to the agents themselves – covering identity, privileges, policy enforcement, logging, escalation paths, and kill-switch authority including controls on the underlying models.

At the same time, a Sovereignty-driven IT transformation creates the opportunity to implement agentic-first workflows across infrastructure, cybersecurity, and operations: embedding automated controls, continuous policy enforcement, and AI-supervised remediation directly into the stack. This will allow organizations to enhance sovereign control while improving efficiency and cost discipline.

3. Convictions forged in our operational experience

For decades, Atos Group, with Eviden as a Sovereignty insurance factor, has been a trusted partner at the forefront of digital systems, delivering solutions to the most complex, high-stakes problems across the world's most demanding enterprise environment. These include brownfield and mainframe-adjacent realities, heavily regulated sectors, mission-critical operations, sovereign infrastructures, all under constant cyber scrutiny. This includes environments held to military-grade standards, where reliability, security, resilience, trust and traceability are non-negotiable. Systems are designed to operate under failure, under attack, in degraded modes, and under extreme operational constraints. Software must work, fail safely, preserve command and control, and stand up to continuous audit and regulatory oversight.

Built on the trust of our clients, this experience has given us a deep understanding of how complex, real-world digital environments truly operate. They are not clean-sheet architecture, but deeply nuanced systems shaped by real world constraints. They are layered, interconnected, and shaped by years of technology, regulatory, and operational decisions. Each layer of the stack introduces its own parameters, dependencies, and constraints. This complexity creates risk, exposure, and blind spots. Control can be lost in data flows, in operational access, in inherited dependencies, or in the seams between systems, vendors, and teams. The more critical the environment, the more these weak points matter.

Atos Group's core mission is to operate this complexity and these dependencies with trust. Our role is to orchestrate end-to-end environments, anticipate and manage risk before it materializes, and bring transparency to systems that must remain controllable, auditable, and resilient over time. We design, run, and govern sovereign digital environments consistently across the IT stack, including extending into AI models, finetuned LLMs and agentic business delivery platforms that carry the fundamental business critical knowledge and trade secrets of the organizations. For us, Digital Sovereignty is a core design principle, engineered into architectures, operating models, and technology and provider choices from day one, then proven continuously in operations.

In practice, this requires a unified control and orchestration plane to link Sovereignty objectives to enforceable policies across assets, data, workloads, and security domains, ensuring that governance rules are monitored and implemented consistently across environments. Without this layer, multi-stack architectures risk fragmenting into isolated islands of control, where the weakest component ultimately determines the effective level of Sovereignty.

This heritage underpins a set of clear convictions.

First, Sovereignty is not absolute or monolithic. It does not mean autarky or building a disconnected doomsday vault. While it is often framed as a binary choice, Atos Group views Sovereignty as a continuum, with various levers of controls that can be activated based on the level of Sovereignty required by customers. For example, on Cloud, Atos Group proposes a framework with Sovereignty archetypes, ranging from Native to Controlled, Trusted and Disconnected – each with specific controls to suit the specific needs and requirements of customers' workloads. Actual Sovereignty therefore results from a combination of choices across data, technology, operations, and legal exposure.

Second, labels and certifications are not Sovereignty guarantees. Certifications and regulatory labels are valuable signals, particularly early in decision-making and when working against a formal compliance goal. However, they do not create Sovereignty by themselves. Real Sovereignty is determined by architecture choices, including through open standards and open-source components, operating model, governance, and the effectiveness of control points in day-to-day operation, enabling transparency and reduced dependency.

Third, organizations are only as sovereign as their weakest link. Data localization and cloud choices are necessary, but insufficient. Sovereignty must be holistic, covering the full IT stack and the full lifecycle with cybersecurity as a foundational layer and with a homogeneous set of measures consistent with the required level of Sovereignty.

Finally, Sovereignty is never achieved once and for all. It must be continuously tested, monitored, and adapted. This requires strong governance, ongoing oversight, and the ability to respond to change, whether driven by regulation, technology evolution, or geopolitical events

In short, we believe that Digital Sovereignty means actively managing dependencies through transparency, control and freedom of choice.

Atos Group’s bet:

Making Digital Sovereignty business as usual for customers

For CxOs and their teams, Atos Group turns Sovereignty into an operating capability built on transparency, freedom of choice, and control. We make dependencies visible, enforce controls consistently, and keep options viable over time. This is how Sovereignty becomes manageable at scale instead of becoming a permanent source of ambiguity and friction.

Atos Group acts as an advisor and orchestrator, managing the complexity of clients’ sovereign requirements securely, efficiently, and transparently through an end-to-end approach. This starts with a deep understanding of clients’ business context, and IT and operational realities, and the critical questions they face. Atos Group helps organizations identify their vulnerabilities, clarify their Sovereignty needs, and determine which workloads require which level of sovereign controls. We structure concrete options and transformation scenarios: defining what can remain as is, what must be reinforced, and what should evolve over time. Clients are presented with informed architectural choices, phased migration paths, and trade-offs made explicit. Strong governance frameworks are then put in place to steer and sustain Digital Sovereignty over time.

From there, Atos Group, with its Atos, Atos Amplify and Eviden teams, designs, builds, and deploys the right sovereign architectures, leveraging a strong ecosystem of certified partners across multiple geographies. Sovereignty is embedded not only in cloud and infrastructure choices, but across applications, data, AI, cybersecurity, and operations, supported by clear sovereign governance and management frameworks.

Atos Group then operates and evolves these environments over time, ensuring that data, technology frameworks, and operational models remain aligned with the required level of Sovereignty, with a clear view of legal exposure and risk. When Sovereignty issues arise, Atos Group steps in to help clients recover quickly and reinforce safeguards to reduce future exposure.

Case in point | Sovereign Agentic AI

Sovereign Agentic AI will not succeed as thin wrappers around models. Sovereignty issues in agentic are actual, concrete failure modes that organizations encounter when moving from experimentation to live operations. Atos Group's Sovereign Agentic AI offerings are designed to address these challenges directly, through architecture, operating discipline, and enforceable controls.

Identity, access, control, and human oversight

Agents operate under explicit non-shared identities with tightly defined permissions. Access to tools and systems is governed through zero trust principles, enforced centrally, with just in time access, where appropriate, and the ability to revoke access in real time. Privilege escalation paths are controlled and auditable, ensuring agents cannot silently expand their authority as autonomy increases and that high impact actions can be constrained to the right identities and approval paths. Agent goals, intent, and boundaries are explicitly defined and continuously monitored, with mandatory human oversight for goal changes and confidence-based escalation to prevent a silent drift away from the original business intent.

Data quality and sovereignty by design

Agents operate on curated, governed, and trusted data sets with clear ownership and lifecycle management. Data readiness, provenance, sovereignty constraints, and privacy requirements are assessed upfront and enforced continuously, ensuring autonomy does not amplify inconsistent, stale, or untrusted information.

Orchestration and architecture at scale

Atos Group provides a dedicated orchestration layer and reference architectures including secure zero trust multi context protocol (MCP) servers to manage coordination between agents, systems, and humans. State awareness, handoffs, escalation logic, and recovery mechanisms are engineered explicitly, including deterministic rollback paths, kill-switch authority, and controlled restart of agents and workflows, avoiding brittle point-to-point integrations and enabling predictable behavior at scale.

Security propagation across workflows with secure Agentic supply chain

Atos Group designs Agentic workflows as distributed systems, with explicit orchestration, state management, and failure handling. Security controls such as prompt-injection defenses, input validation, memory isolation, and tool-use constraints, are applied at workflow level and not at model level. This is across the full chain of inputs, retrieval, memory, coordination, and tool execution. Architectural mechanisms are in place to isolate failures and prevent vulnerabilities from propagating across agents and systems. This includes securing the Agentic supply chain itself: third-party agents, partner components, model dependencies, and external tools are vetted, versioned, and governed as production dependencies, with continuous integrity checks to prevent compromised components from entering live workflows.

Traceability, auditability, accountability, and response readiness

Every agent action is observable and traceable. Decisions, tool invocations, data access, and outcomes are logged in a way that supports operational analysis, regulatory reporting, and security investigation. This traceability underpins response readiness, enabling rapid investigation, controlled rollback, and decisive intervention when anomalies, policy breaches, or failures are detected.

Cost discipline and value-linked scaling

AgentOps and FinOps are implemented from day one, tying agent run-cost to business KPIs like cycle time, cost-to-serve, throughput, quality, and tracking correlation as autonomy expands. Real-time monitoring and controls are in place before scale, enabling teams to allocate budgets and throttle or stop spend at the right level (feature, workflow, project, program, business unit). Reusable, governed agents are curated and shared through a controlled library, promoting reuse over duplication and preventing agent sprawl while accelerating time to value. This allows teams to manage token usage, tool calls, retries, and execution loops while preserving freedom of choice and limiting lock-in.

Intellectual property protection through sovereign model and delivery choices

As AI becomes embedded in core operations, proprietary knowledge, processes, and training data flow through models and orchestration layers that may sit outside your control. Atos Group addresses this through deliberate model selection, including private, open-weight, or purpose-built models from trusted partners, combined with deployment architectures (private cloud, hybrid, air-gapped) and specific sovereignty guardrails that keep proprietary data and model outputs within controlled boundaries. Confidential computing provides an additional safeguard, ensuring data remains encrypted even during processing. The goal is to ensure that your competitive differentiation is never exposed to a third party's training pipeline or subject to another jurisdiction's access claims.

Atos Group does not approach Sovereignty as a linear journey toward a single end state, but as a set of progressive choices aligned with business priorities. In practice, most organizations start with a limited scope: a subset of critical workloads, specific data domains, or high-exposure dependencies. This creates an initial, pragmatic level of Sovereignty that enables transformation to begin, while keeping risk and costs under control. Recognizing that every organization has a different Sovereignty profile, Atos Group embeds sovereign design principles across its entire portfolio. This enables tailored transformation and operational services, workload by workload, across the full stack. From advisory and sovereign cloud frameworks to cybersecurity solutions (including Eviden-owned sovereign products) and sovereign AI capabilities for regulated environments, we preserve freedom of choice and avoid irreversible lock-in. Sovereignty becomes an enabler of innovation. Beyond designing and operating sovereign architectures, Atos Group builds sovereign capability within our clients' organizations. We work alongside business, IT, security, and risk teams to develop the internal expertise, decision frameworks, and operational reflexes required to manage Sovereignty autonomously over time.

Going forward:

Digital Sovereignty will remain a defining topic for boards and executive teams in the years ahead. We will continue to deepen and structure this conversation in the coming months, sharing new offers, industry-specific applications, partnerships, and geo specific initiatives. Digital Sovereignty is and will continue to be a strategic commitment for Atos Group.

Let's talk!

We want to know what Digital Sovereignty means for you—and what to do next.

Wherever you are on the journey, we'd love to compare notes and help you:

- **Assess** what Digital Sovereignty means for your organization—and benchmark your current posture across data, workloads, and dependencies—so you can **focus first on the risks that matter most.**
- **Define** a sovereignty strategy and pragmatic roadmap aligned to your business priorities, risk appetite, and regional requirements.
- **Act** on concrete steps to strengthen control, resilience, and transparency across your digital stack—so you can continuously shape and improve your Digital Sovereignty posture.

Connect with us at **digitalsovereignty@atos.net**

About Atos Group

Atos Group is a global leader in digital transformation with c. 59,000 employees and annual revenue of c. € 7.2 billion, operating in 61 countries under two brands — Atos for services and Eviden for products and systems. European number one in cybersecurity and cloud, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos Group is the brand under which Atos SE (Societas Europaea) operates. Atos SE is listed on Euronext Paris.

The purpose of Aos Group is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Atos is a registered trademark of Atos SE. © 2026 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.