

Cloud sovereignty is not enough

**Why financial services must combine sovereignty
and operational autonomy**

by David Mullins and Josema Cavanillas



AtoS

Financial services is entering a new era of cloud and AI

Cloud and AI have fundamentally transformed financial services. They have accelerated digital transformation, enabled new customer experiences and unlocked capabilities that would have been difficult to imagine only a few years ago. For most institutions, the question is no longer whether to adopt these technologies; it is how to use them to remain competitive in an increasingly digital and intelligent economy.

Yet as organizations deepen their reliance on hyperscale cloud platforms and AI ecosystems, a new strategic challenge is emerging:

How do you continue to benefit from innovation without progressively surrendering operational authority over the services that define your business?

For many institutions, the answer has been digital sovereignty. If data is protected, infrastructure is secure, and regulatory obligations are met, then the organization has retained control. It is an understandable assumption, and one that has shaped much of the industry's response to cloud adoption over the past decade.

However, the environment is changing.

Today, an institution can own its data, govern its infrastructure and satisfy regulatory requirements, yet still become increasingly dependent on external technology platforms to execute critical business services. Capabilities like identity management, orchestration, resilience mechanisms and AI execution are progressively becoming deeply embedded within cloud ecosystems rather than remaining under institution-controlled governance.

As a result, the question facing financial services is evolving.

It's no longer simply: How do we secure our technology?

Increasingly, it's: How do we retain operational authority over our business while continuing to benefit from cloud and AI innovation?

This distinction may seem subtle, but it fundamentally changes how institutions should think about the next generation of operating models.



Why operational autonomy matters now

Several powerful forces are converging to make operational autonomy a strategic issue for business and technology leaders.

The regulatory environment has fundamentally changed.

The Digital Operational Resilience Act (DORA), now fully applicable across the European Union, places unprecedented emphasis on operational resilience, ICT third-party risk management, continuity planning and the ability to demonstrate control over critical services. The discussion has moved beyond cybersecurity towards ensuring that regulated services continue to operate under disruption and that institutions understand, manage and can respond to technology dependencies.

This shift reflects a broader industry trend. According to [the GARP Operational Resilience & 2025 Risk Outlook](#), operational resilience is becoming an enterprise imperative for financial institutions: **78% of financial risk professionals say their firms have improved their ability to respond to operational disruptions over the past three years**, underscoring that resilience is no longer viewed simply as an IT concern but as a core business and governance responsibility.

Cloud adoption has matured.

Most major financial services organizations have already embraced hybrid and multi-cloud strategies and increasingly rely on hyperscale providers to deliver resilience, scalability and access to advanced AI capabilities. These investments have delivered significant business value, but they have also created deeper operational dependencies that extend well beyond infrastructure.

Cloud has become the industry's default operating model. [Flexera's 2024 State of the Cloud Report](#) found that **89% of organizations have adopted a multi-cloud strategy**, while **73% operate hybrid cloud environments**. As financial institutions become more dependent on cloud ecosystems, maintaining visibility, governance and operational control across those environments becomes increasingly important.

AI is redefining how work is performed.

AI is no longer confined to isolated use cases or productivity tools. It is increasingly becoming embedded within customer journeys, operational workflows, decision support and core business processes. As AI moves closer to the execution of regulated services, questions of governance, accountability and operational control become significantly more important.

In fact, the pace of AI adoption has accelerated dramatically. [McKinsey's 2025 State of AI](#) research found that **78% of respondents said their organizations use AI in at least one business function**, demonstrating that AI has become an operational capability rather than an experimental technology. As AI becomes more deeply embedded in business-critical processes, institutions must ensure that operational authority, oversight and accountability remain firmly under their control.

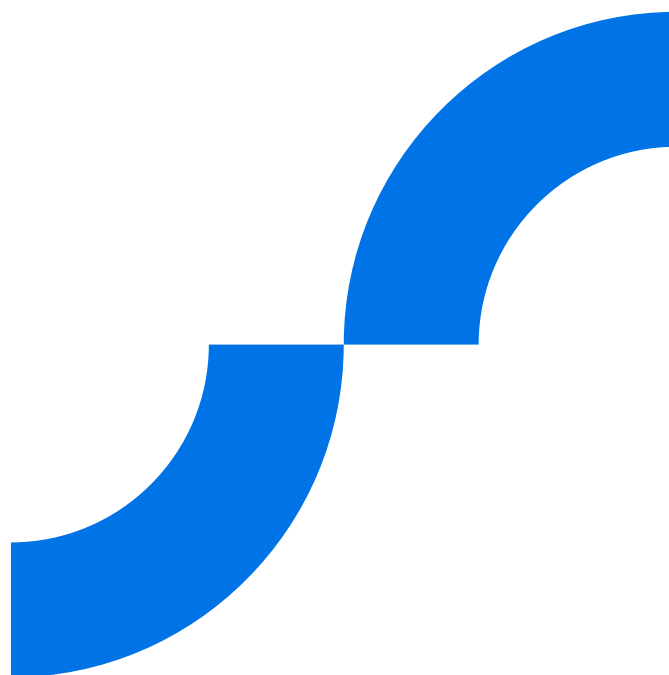
Geopolitical developments and broader European policy initiatives

Technology dependency is no longer viewed simply as a sourcing or procurement issue. Increasingly, it's being treated as a matter of strategic resilience.

Discussions surrounding European technology sovereignty, operational resilience and the proposed Cloud and AI Development Act (CADA) reflect a growing recognition that critical sectors, including financial services, must balance continued access to global technology ecosystems with greater strategic optionality and operational control.

These developments should not be interpreted as a move away from hyperscale cloud providers. On the contrary, hyperscalers will continue to play a central role in delivering innovation, scale and AI capability.

The challenge is different. It's determining how institutions can continue to benefit from those capabilities while ensuring that operational authority remains with the institution rather than progressively migrating into provider-managed ecosystems.



The emerging challenge: Why today's cloud models create tomorrow's strategic risk

Most cloud architectures were designed to optimize scalability, resilience and innovation. They were not designed to maximize operational independence.

As organizations adopt more cloud-native services, operational capabilities such as identity management, orchestration, monitoring, encryption services, resilience mechanisms and increasingly AI execution become tightly integrated with provider platforms. Even with multi-cloud strategies, operational continuity can still depend upon governance models, control planes and services owned and operated by individual providers.

This introduces a subtle but increasingly significant form of dependency. The issue is no longer simply where workloads are hosted. Nor is it simply a question of vendor lock-in. Increasingly, institutions must consider whether they retain sufficient authority over

the execution of regulated services should technology, regulatory or geopolitical conditions change.

At the same time, there is no realistic alternative to the innovation offered by today's hyperscale ecosystems. European cloud and AI initiatives continue to develop rapidly, but few organizations can realistically replace existing investments without compromising agility, innovation or economic viability.

This creates a genuine strategic paradox. Financial services institutions must continue leveraging hyperscale cloud and AI to remain competitive, while simultaneously reducing dependency risk, strengthening resilience and preserving the flexibility to evolve as technologies, regulations and geopolitical conditions continue to change.

The challenge, therefore, is not choosing between innovation and control. It is establishing an operating model capable of delivering both.



The sovereignty-autonomy paradox

Digital sovereignty and operational autonomy are often used interchangeably, but they address fundamentally different challenges. Understanding the distinction is critical because it changes how financial services institutions should think about the next phase of cloud and AI transformation.

Digital sovereignty is concerned with **control over technology assets**. It focuses on where data resides, how infrastructure is governed, how identities are managed and how regulatory requirements are met. Sovereignty helps organizations demonstrate control, resilience and trust.

Operational autonomy addresses a different question.

It is concerned with **control over business execution**. It reflects an institution's ability to determine how regulated business services operate, adapt and evolve regardless of the underlying technology platform.

While sovereignty establishes the foundation for control, operational autonomy determines whether that control can be maintained as technology, regulation and geopolitical conditions change.

This distinction becomes increasingly important as organizations adopt more cloud-native services and AI-enabled capabilities. An institution may retain

ownership of its data, satisfy regulatory requirements and maintain secure infrastructure, while simultaneously becoming dependent upon provider-controlled identity services, orchestration engines, resilience mechanisms or AI execution environments. In these circumstances, the institution retains technical control, but may have less influence over how business services are ultimately executed.

The challenge therefore is not to choose between sovereignty and autonomy.

Financial services institutions need both.

Sovereignty provides the governance, resilience and regulatory confidence necessary to operate in highly regulated markets. Operational autonomy provides the flexibility to innovate, adapt and execute business services independently of any single technology ecosystem. The opportunity lies in combining these complementary capabilities within a single operating model that preserves both innovation and institutional authority.

The three dimensions of operational autonomy

Operational autonomy is often associated with resilience, but it represents a broader organizational capability.

Resilience focuses on recovering from disruption. Operational autonomy focuses on ensuring that the institution retains the authority to determine how critical services are executed before, during and after that disruption occurs. It is therefore a strategic capability rather than simply an architectural characteristic. It can be understood through three complementary dimensions.

1) Execution autonomy

Execution autonomy ensures that institutions retain authority over regulated business processes rather than allowing those processes to become defined by the capabilities of an underlying technology platform. For example, a bank may use cloud-based AI services to support fraud detection or credit assessment, but the institution should remain responsible for determining how decisions are made, what policies apply and when human intervention is required. Business workflows, policy enforcement, AI decision points and operational governance remain institution-defined, rather than platform-defined.

As AI becomes increasingly integrated into operational processes, execution autonomy becomes increasingly important. It ensures that intelligent automation operates within institution-defined policies, risk tolerances and regulatory boundaries. The goal is not to limit innovation. It's to ensure innovation is enabled without compromising operational control.

2) Decision autonomy

Technology strategies are no longer static. New AI platforms emerge, cloud services evolve, regulations change and sovereign technology initiatives continue to mature. Decision autonomy ensures that these developments remain strategic business choices rather than architectural constraints imposed by previous implementation decisions. Institutions with strong decision autonomy can evaluate new providers, adopt emerging technologies or incorporate sovereign cloud capabilities without fundamentally redesigning their operating model. This flexibility reduces structural dependency and preserves strategic optionality, allowing technology decisions to remain aligned with business priorities rather than platform limitations.

3) Continuity autonomy

Continuity autonomy extends beyond traditional business continuity planning. It reflects an institution's ability to continue delivering regulated services even when provider capabilities, regulatory expectations or geopolitical conditions change.

Increasingly, regulators expect organizations not only to recover from disruption but also to demonstrate that they understand and can manage dependencies on critical third parties. Continuity autonomy helps meet this expectation by ensuring that operational authority remains with the institution, enabling it to adapt services, policies and execution models without becoming constrained by a single technology ecosystem.

Taken together, these three dimensions transform operational autonomy from a technical aspiration into a strategic business capability. They enable institutions to continue benefiting from cloud and AI innovation while maintaining the flexibility, resilience and authority expected by regulators, customers and shareholders.

A different operating model

Resolving the sovereignty–autonomy paradox does not require financial services institutions to replace hyperscale cloud providers, nor does it require them to abandon the innovation and scale they provide. The challenge is not the infrastructure itself; it is where operational authority resides.

A different operating model is therefore required—one that separates operational authority from infrastructure consumption. Rather than allowing governance, identity, execution policies, resilience mechanisms and AI orchestration to remain embedded within individual cloud platforms, these capabilities can be externalized into an institution-controlled operating layer that sits between business services and the underlying infrastructure.

This approach fundamentally changes the relationship between the institution and its technology providers. Business services continue to benefit from hyperscale cloud, advanced AI capabilities and cloud-native innovation, but the institution retains authority over how regulated services are executed, governed and evolved. Infrastructure becomes an interchangeable resource, while the operating model remains as defined by the organization.

This is not an argument against hyperscale cloud. It is an argument for ensuring that innovation and operational authority evolve together.

From business architecture to technical architecture

The transition from sovereignty to operational autonomy requires more than a conceptual framework. It requires a technical architecture capable of translating governance principles into operational capability.

At the business level, the objective is straightforward: enable financial services institutions to benefit from cloud and AI while maintaining regulatory confidence, operational resilience and strategic flexibility. Achieving this objective requires an operating model in which sovereignty and autonomy complement rather than constrain one another.

The technical architecture realizes this through a series of interconnected layers, each addressing a distinct aspect of operational authority. [Figure 1 illustrates this progression.](#)

The convergence of sovereignty and operational autonomy: a governed operating model for financial services

Sovereignty and Autonomy Paradox

A practical operating model for balancing innovation, control and resilience

The emerging solution is not to replace hyperscalers, but to regain **operational control** through an **institution-controlled sovereign layer**.

- Critical controls remain institution-owned and policy enforced
- Regulated services operate within an auditable, resilient runtime
- AI execution, governance and security remain under institutional oversight
- Innovation is retained while dependency risk is progressively reduced

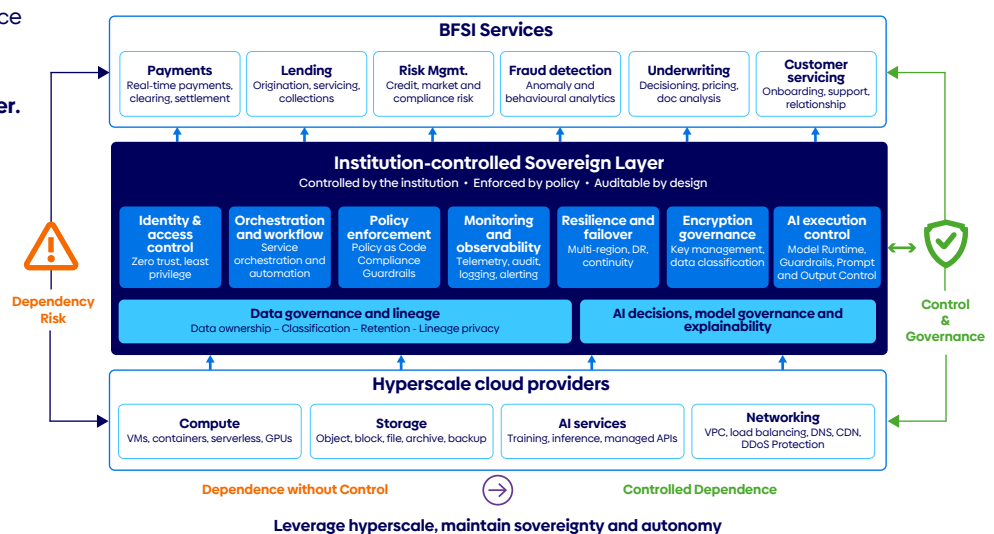


Figure 1. The business architecture defines the capabilities required to balance sovereignty and autonomy. The technical architecture demonstrates how those capabilities can be realized through an institution-controlled operating model spanning governance, execution, observability and infrastructure.

A technical blueprint: Enabling governed autonomy

At the highest level sit the regulated business capabilities of the institution, including payments, lending, underwriting, claims, fraud management, customer servicing and risk operations. These are the services that regulators, customers and shareholders ultimately depend upon and whose continuity must be preserved irrespective of changes in technology or operating conditions.

Beneath these services sits the **institution-controlled sovereign layer**, which provides the operational boundary between business execution and infrastructure. This layer externalizes identity, governance, security, resilience and execution policies so that they remain under institutional control.

Supporting this layer is a **governance and policy framework** that embeds institutional rules directly into operational execution. Policy-as-code, identity services, encryption governance and operational controls ensure that AI, applications and business processes execute consistently within institution-defined risk, compliance and regulatory boundaries. Governance therefore becomes an active part of execution rather than a retrospective audit activity.

Operational autonomy is delivered through an **intelligent execution layer**, where workflow orchestration, automation and AI-enabled capabilities support the execution of regulated business services.

The objective is not unrestricted autonomy, but **governed autonomy**—the ability to automate increasingly complex activities while ensuring that execution remains transparent, explainable and aligned with institutional policies. AI becomes an enabler of operational excellence rather than a source of uncontrolled decision-making.

An equally important component is the **observability and assurance layer**. As AI assumes greater operational responsibility, institutions must be able to understand how decisions are reached, how workflows execute and how operational outcomes are produced. Comprehensive monitoring, tracing, evaluation, auditability and explainability provide the transparency required by regulators while enabling organizations to maintain confidence in increasingly autonomous operations.

Human judgement remains an integral part of this operating model. Approval processes, exception handling and higher-risk decisions continue to require appropriate human oversight. Operational autonomy therefore complements human expertise rather than replacing it, ensuring that institutions retain accountability for decisions affecting customers, markets and regulatory compliance.

The underlying infrastructure continues to be provided through hyperscale cloud platforms and associated AI ecosystems. These platforms remain the engines of innovation, scalability and advanced digital capability. The difference is that they no longer define how regulated business services execute. Operational authority remains with the institution, allowing technology choices to evolve without fundamentally altering the operating model.



Looking ahead: The next phase of digital transformation

The conversation around cloud sovereignty is entering a new phase. For much of the past decade, the emphasis has been on protecting data, strengthening cybersecurity and achieving regulatory compliance. Those priorities remain essential, but they no longer fully address the challenges created by increasingly intelligent and interconnected technology ecosystems.

The next phase of digital transformation will be characterized not simply by greater adoption of cloud and AI, but by the ability of institutions to determine how these technologies are integrated into critical business services.

The financial services organizations that establish this capability will be better positioned to adopt emerging AI innovations, incorporate evolving sovereign cloud initiatives and respond confidently to changes in regulation, market conditions and geopolitics. Most importantly, they will preserve the freedom to determine how their business operates rather than allowing those decisions to become progressively embedded within external technology ecosystems.

Cloud and AI are redefining financial services, creating unprecedented opportunities for innovation, efficiency and customer value. At the same time, they are reshaping the relationship between institutions and

the technology platforms upon which they increasingly depend.

The discussion therefore needs to move beyond cloud adoption alone. The strategic challenge is no longer simply one of infrastructure, security or compliance. It is about ensuring that institutions retain operational authority as technology, regulation and geopolitical conditions continue to evolve.

Digital sovereignty provides the governance, resilience and trust required to operate in highly regulated markets. Operational autonomy provides the capability to execute, adapt and innovate without becoming constrained by any single technology ecosystem. Neither is sufficient in isolation. Together, they form the foundation of a new operating model that enables institutions to benefit from cloud and AI while preserving the authority to govern their own business.

For financial services institutions, the question is no longer whether cloud and AI will shape the future of the industry—they already are. The question is whether the institution will continue to determine how that future is executed.



About the authors



David Mullins

Head of Financial Services & Insurance Portfolio

David Mullins is Global Head of the Financial Services & Insurance Portfolio at Atos, where he develops industry-led propositions that connect digital, AI, cloud and cybersecurity capabilities to business outcomes across banking and insurance. He has held senior practitioner and consulting roles spanning financial services, technology and large-scale transformation, including leadership positions in banking strategy, architecture and operations. His work focuses on applying emerging technologies within regulated environments, with particular emphasis on AI-enabled operating models, cloud sovereignty, resilience and domain-led transformation.

E-mail: david.2.mullins@atos.ai

LinkedIn: <https://www.linkedin.com/in/david-mullins-32562521/>



Josema Cavanillas

Product Manager - Sovereign Cloud & Infrastructure - Global CMI

Josema Cavanillas has spent many years working on projects that address significant shockwaves in infrastructure technologies, such as the emergence and growth of the public cloud and its integration into business processes, the trend back to the private cloud, the search for hybrid computing and data storage solutions, and, more recently, the seemingly enduring trend of sovereign cloud. He has helped Atos evolve into a master of these technologies, applying Artificial Intelligence wherever it provides clear added value. Josema helps to ensure that the value Atos brings to the market lies in its extraordinary knowledge, experience, and ability to advise clients on their growth options and to anticipate and resolve problems before they escalate.

E-mail: jose-maria.cavanillas@atos.ai

LinkedIn: <https://www.linkedin.com/in/josemacavanillas/>

About Atos

[Atos](#) is the Atos Group brand dedicated to AI-powered, secure, end-to-end digital services. Atos designs, develops, and operates critical digital environments that drive performance, resilience and sovereignty, helping public and private organizations worldwide retain control over their data and infrastructures, while meeting regulatory requirements.

With more than 52,000 employees serving over 4,500 clients across 54 countries, Atos helps modernize core IT systems, accelerate cloud and data transformation, strengthen cybersecurity, and deliver secure digital workplace environments to support its clients, its employees and society. Atos also provides consulting and advisory services through its Atos Amplify brand.

A trusted partner in operating complex and mission-critical environments, Atos supports organizations across highly regulated and sovereign contexts.

[Find out more about us](#)
atos.ai

Let's start a discussion together



About Atos Group

[Atos Group](#) is a global leader in digital transformation with c. 54,000 employees and annual revenue of c. €7.2 billion, operating in 54 countries under two brands - Atos for services and Eviden for products and systems. European number one in cybersecurity and a leader in 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 listed on Euronext Paris.

Atos Group is a registered trademark. Confidential information owned by Atos Group, 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 Group.