



Balancing control, resilience and innovation:

Digital sovereignty for EU
and UK financial institutions ■

Abstract

Digital sovereignty has emerged as a strategic concern for financial institutions as cloud adoption, AI-driven transformation, geopolitical fragmentation, and increasing third-party dependency reshape the operating environment. While often framed as a technology issue, sovereignty is fundamentally a business challenge centered on maintaining trusted operations, protecting critical data and services, and retaining sufficient control over key digital dependencies.

This paper argues that sovereignty extends beyond traditional concerns such as data residency and compliance. It is increasingly about an institution's ability to exercise decision authority, demonstrate control, and maintain resilience across complex ecosystems of cloud providers, technology platforms, outsourcing arrangements, and ecosystem partners. For financial institutions, the consequences of losing control can extend beyond regulatory non-compliance to include customer harm, operational disruption, erosion of trust, and reduced strategic freedom.

The paper identifies three forces that challenge sovereignty in practice: the speed of change, the complexity of modern technology estates, and growing interdependence on external providers and ecosystems. It introduces practical scenarios to help organizations understand where control is most exposed and how sovereignty risks materialize across different operating models.

Rather than advocating a single sovereign cloud architecture, the paper proposes a risk-based approach built around explicit sovereignty postures and control decisions. It introduces sovereignty control profiles, governance principles, and a five-step leadership framework to help organizations determine where control is essential, where dependency creates value, and how innovation can be accelerated without creating unacceptable risk.

The central conclusion is that sovereignty is not about pursuing self-sufficiency or constraining innovation. It is about retaining appropriate control over critical capabilities while continuing to benefit from the scale, expertise, and innovation of an increasingly interconnected digital ecosystem. Institutions that succeed will be those that treat sovereignty not as a constraint on transformation, but as an enabler of trusted innovation, resilience, and long-term strategic autonomy.





Reasserting control:

Digital sovereignty for European financial institutions

01 | Executive summary

Sovereignty – a strategic European priority for financial services

Why “European priority” does not mean one European answer

Avoiding the sovereignty trap: Speed vs control

02 | Two ways to establish an appropriate sovereignty posture: Direct control and assured oversight

Sovereignty requirements across 3 domains

Four control dials of sovereignty

03 | Sovereign FS cloud: Sovereignty control profiles

First steps: From principle to execution

04 | Turning strategy into delivery

Conclusion

Scenarios – applying sovereignty in practice

Scenario 1: Cloud-forward modernizers

05 | Scenario 2: Assurance first operators

Scenario 3: Payments and open banking participants as ecosystem trust anchors



Executive summary

European financial services institutions are accelerating cloud and AI adoption at the same time as **sovereignty expectations are rising**. Geopolitical fragmentation, increasing third-party dependency, and tighter operational resilience requirements mean that loss of control now translates directly into customer harm, market disruption, and supervisory intervention.

For financial institutions, sovereignty is **increasingly inseparable from trust**. Customers, regulators, governments, and markets now expect institutions not only to protect data, but to maintain resilient, transparent, and controllable digital operations under disruption, dependency, and geopolitical pressure. Failures in operational resilience, third-party control, or data governance are no longer experienced as technology issues; they are experienced as failures of institutional trust.

Digital sovereignty is therefore not simply a technology issue. *It is the institution's ability to retain decision authority and demonstrate control over critical services, data, and dependencies, while continuing to innovate.*

The nature of **the challenge has shifted**. Sovereignty now extends well beyond data residency to include operational control, evidence, and legal enforceability across complex dependency chains spanning cloud providers, outsourcing arrangements, and ecosystem partners. Control must be demonstrated in practice, particularly at the points of change, disruption, or cross-border exposure.

At the same time, **AI is accelerating** transformation, including unlocking long-standing mainframe modernization challenges, but it is also increasing reliance on external platforms, data, and model-driven decision-making.

In practice, **sovereignty is not challenged in a single way**. It is affected by three forces: the **speed of change**, the **complexity of the operating estate**, and the degree of **interdependence on external participants**. As organizations move faster, control can gradually erode. As estates become more complex, control can fragment. As services depend on partners, ecosystems, and shared infrastructure, control can become conditional.

Most **financial services institutions experience all three simultaneously**. Digital channels and analytics platforms operate at pace, creating exposure to control erosion. Core banking, insurance, and risk platforms sit within complex, multi-layered estates where control can fragment. Payments, open banking, and partner-driven models introduce interdependence, where outcomes rely on external participants. As a result, sovereignty must be applied differently across services, aligned to their criticality and risk profile.



The response is not a single architecture or a predefined “sovereign cloud” solution. It is to make explicit, risk-based control choices based on where control is most exposed. While the underlying control building blocks are broadly consistent, their application must vary by context, determining the level of control, governance, and evidence required across services.

To do this effectively at scale, sovereignty must be delivered as a platform capability that makes **control, policy, and evidence consistent and enforceable across the organization**. Without clear board-level direction, sovereignty fragments across competing priorities such as cost, transformation, and third-party management, leading to dependency by default rather than control by design.

The priority for boards and executive teams is to **define sovereignty ambition** and risk appetite, identify where control is most exposed, align operating models and architecture accordingly, and invest in capabilities that make control repeatable at scale. The shift is from debating sovereignty in principle to ensuring that control is sustained in practice as organizations scale, transform, and become increasingly interconnected.

Our recent industry research¹ suggests that the challenge for financial institutions is no longer recognizing sovereignty as a strategic issue but operationalizing it effectively. While 94% of European financial services boards have discussed digital sovereignty and 79% have allocated dedicated funding, only 13% of firms report having fully mapped their technology dependencies end-to-end. This highlights a growing execution gap between strategic intent and the operational visibility required to identify, govern, and reduce critical dependencies.

This paper provides a practical framework to help boards and executive teams identify where control is most at risk and take targeted action to retain it.



1. Source: Capgemini Research Institute, Digital Sovereignty: From Policy Ambition to Executive Imperative, 2026, 1,300 executives across industry, technology, and policy conducted in April 2026



Sovereignty – a strategic European priority for financial services

Digital sovereignty has become a strategic priority across Europe as the assumptions underpinning the last decade of digital transformation no longer hold, be it a stable geopolitical alignment, frictionless cross border data flows, or globally optimized technology supply chains. [The 2025 European Digital Sovereignty Summit](#) reaffirmed this direction, with commitments to reduce technological dependency, strengthen resilience, and protect strategic digital assets.



- *Europe is moving beyond regulating digital risk towards actively building sovereign digital capability. The European Technological Sovereignty Package brings together proposed legislation on cloud, AI and semiconductors with an EU Open Source Strategy, seeking to strengthen European capabilities across the technology stack and reduce strategic dependencies. This reflects a broader understanding of sovereignty that extends beyond data location to include legal and jurisdictional control, operational autonomy, technological and supply-chain dependencies, and the ability to maintain, adapt or exit critical services. The European Commission's Cloud Sovereignty Framework, already applied in its own cloud procurement, illustrates this wider, multidimensional approach.*
- *The UK is following a distinct but similarly strategic path. Its UK Compute Roadmap combines investment in national compute capacity with public-private infrastructure, support for UK AI capability, and a diverse and resilient compute ecosystem. This reflects a more pragmatic approach focused on building sovereign capability while continuing to draw on private investment and international technology ecosystems.*
- *Collectively, these developments point in the same strategic direction, but not towards a single European model. Digital sovereignty is moving from policy ambition into different combinations of infrastructure investment, procurement and operating-model decisions. For regulated institutions, the implications extend beyond compliance to resilience, trust and long-term strategic control.*



For financial services, the impact is amplified: service disruption or loss of control rapidly translates into customer harm, market impact, and supervisory intervention, as Financial Service organizations typically present:

Critical infrastructure by design: Payments, customer access to funds, identity and fraud controls, claims servicing, and market access underpin national economic stability, positioning financial services as an extension of critical national infrastructure and elevating sovereignty to a systemic, not just organizational, concern.

Deep hidden dependency chains: Cloud, identity, security tooling, payment rails, SaaS, data providers, outsourcers and fintechs form complex supply chains where concentration and jurisdictional risk can accumulate unnoticed.²

Highest trust bar: Trust depends on demonstrable control-service availability, data and system access, incident handling, and enforceable third party governance and exit-across all financial services subsectors.

In financial services, trust is the business model. Customers assume payments will clear, funds remain accessible, fraud protections operate continuously, and sensitive financial data remains protected regardless of platform, provider, or geopolitical disruption. As institutions become increasingly dependent on external cloud, SaaS, AI, and ecosystem providers, sovereignty therefore becomes more than a compliance obligation. It becomes a visible measure of institutional reliability, stewardship, and resilience.

Why “European priority” does not mean one European answer

- EU frameworks such as GDPR, NIS2 and DORA promote consistency, but national implementation, supervision and enforcement still vary. Emerging initiatives also address different dimensions: the candidate EUCS focuses on cloud cybersecurity certification, while the proposed Cloud and AI Development Act would establish a single EU-wide framework for assessing cloud and AI sovereignty. The European Commission has already applied a Cloud Sovereignty Framework in its own procurement. Institutions must therefore interpret these developments in the context of their jurisdictions, obligations and risk profiles.
- The UK’s post-Brexit path adds further complexity. The Data (Use and Access) Act 2025 amended UK data-protection law, while the Cyber Security and Resilience Bill would develop the UK’s NIS regime differently from NIS2. The lack of a directly comparable, overarching UK cloud-sovereignty framework, together with UK-specific requirements such as ring-fencing and important-business-services-based operational resilience, complicates cross-border cloud adoption and third-party governance.



2. This assessment does not consider the additional complexity introduced by crypto and digital asset ecosystems, which are outside the scope of this paper



Avoiding the sovereignty trap: Speed vs control

The largest sovereignty risk for financial institutions is not simply regulatory non-compliance. It is the gradual erosion of operational control, institutional resilience, and strategic freedom through unmanaged digital dependency. This erosion is often invisible until stress events occur (outages, cyber incidents, geopolitical disruption, provider failure, or regulatory intervention) at which point customers, regulators, and markets judge the institution on whether it retained practical control.

The alternative is to treat sovereignty as a strategic design challenge, defining the outcomes, capabilities and decision rights that must remain under organizational control, and then aligning technology, operations and suppliers accordingly.

Ignoring sovereignty has long-term consequences (Figure 1). The objective is not sovereign technology for its own sake, but a clear sovereignty posture, defining where control is essential, where dependence is acceptable, and the red lines beyond which business, regulatory or strategic risk becomes unacceptable.

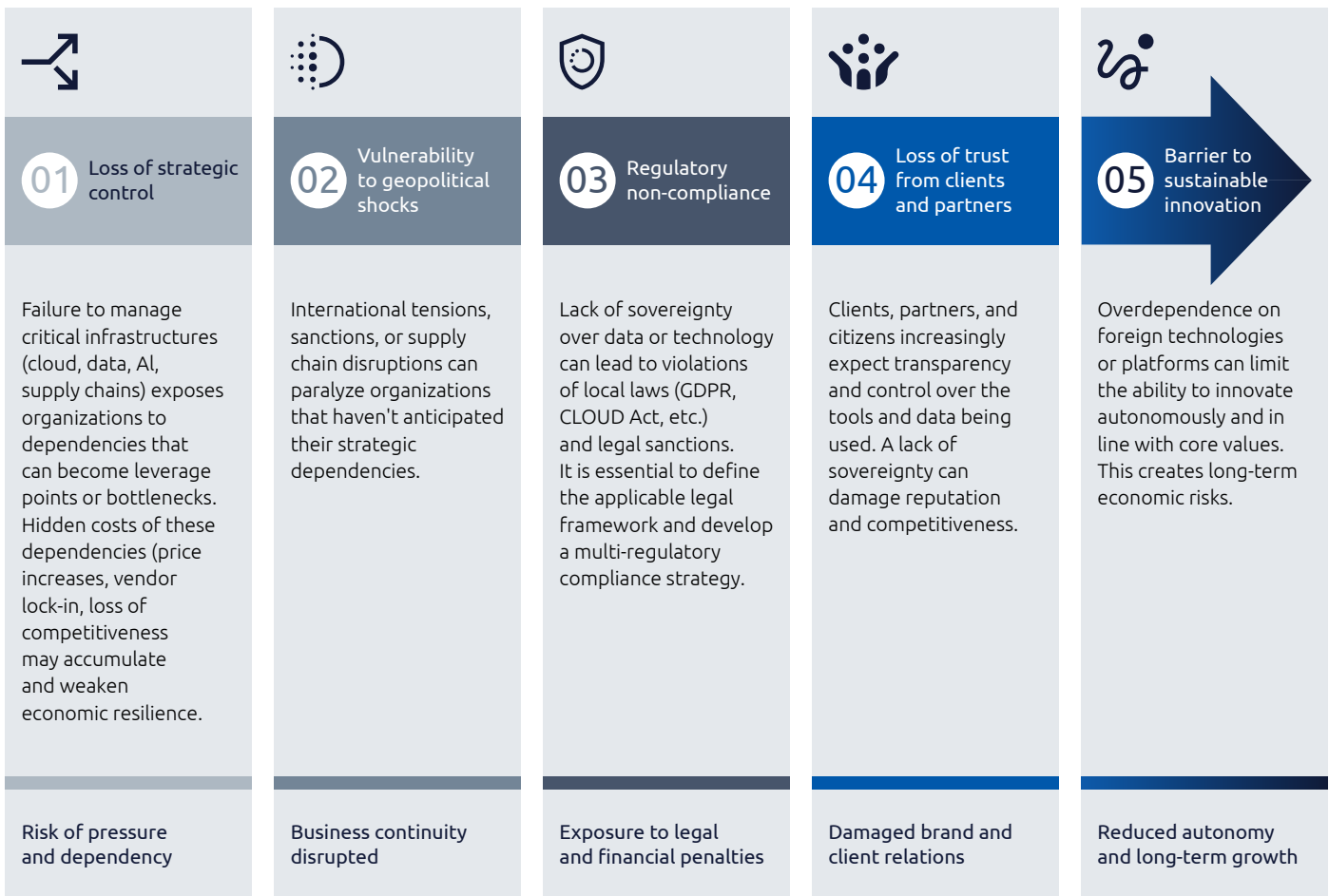


Figure 1 – Consequences of over-looking sovereignty



Two ways to establish an appropriate sovereignty posture: Direct control and assured oversight

Financial institutions increasingly recognize that sovereignty does not require complete technological independence. Our research³ shows that 79% of European financial services firms define sovereignty as resilient interdependence rather than isolation, while 61% believe complete digital sovereignty is unrealistic in today's interconnected technology ecosystem. The strategic challenge is therefore not eliminating dependency, but ensuring that critical dependencies remain transparent, governable, resilient, and aligned to the institution's risk appetite and strategic objectives.

As a result, sovereignty requirements typically resolve into two operating modes:

- **Direct control** – the institution can design, build, and enforce key decisions itself across environments, including where required within its own controlled infrastructure: identity and access rules, privileged access constraints, logging standards, security configuration, data-handling parameters, and approval of material changes that affect risk posture.
- **Assured oversight** – where parts of the service sit fully with the provider (typical for cloud and SaaS), the institution maintains sovereignty through enforceable contractual rights, transparency artifacts, auditability, and ongoing monitoring that is sufficient for internal audit and supervisory scrutiny.

In both modes, sovereignty is maintained by your ability to secure:

- **Decision rights** – the ability to direct requirements and approve or constrain material changes.
- **Access governance** – including control and evidence of privileged/provider access.
- **Evidence availability** – timely, granular logs and artifacts that the institution can use without provider interpretation.
- **Supply-chain transparency** – visibility and control over subcontractors and critical dependencies.
- **Practical exit control** – the ability to transition services or re-architect without losing governance, evidence, or continuity of control.



3. Source: Capgemini Research Institute, Digital Sovereignty: From Policy Ambition to Executive Imperative, 2026, 1,300 executives across industry, technology, and policy conducted in April 2026



Sovereignty requirements across 3 domains

Sovereignty is most keenly experienced across 3 inter-connected domains.

Data sovereignty

In financial services, data sovereignty underpins customer confidence that identity, financial behavior, and sensitive personal information remain protected from inappropriate access, opaque processing, or uncontrolled cross-border exposure.

Data sovereignty means the institution can determine, enforce and evidence where data is stored and processed (residency), who can access it (including privileged and cross-border access), and how it is protected (including encryption and key governance) under the relevant legal and security conditions.

This becomes decisive for high-sensitivity datasets such as payments and transaction records, KYC/AML and identity data, claims files, trading and portfolio data, and customer communications and servicing records.

Minimum requirements

- Maintain security appropriate to the risk, including measures such as encryption/pseudonymization and controls (e.g. control of crypto keys) that protect confidentiality, integrity and availability – with encryption applied for data at rest and in transit where appropriate, supported by effective key management.
- **Breach detection and response:** Maintain the ability to detect, investigate and respond to personal data breaches, with procedures that support timely triage and evidence capture.
- **Notification within mandated timeframes:** Notify supervisory authorities and, where required, affected individuals within mandated timeframes (sometimes within 24hrs) and keep breach records.
- **Lawful cross-border transfers and access:** Use lawful mechanisms where personal data is transferred across borders (including scenarios where overseas parties can access data remotely), and ensure protections remain effective.
- **Residency and access visibility:** Maintain sufficient visibility of processing locations (including replication, backups and DR) and access paths (including privileged/support access) to assess cross-border exposure and demonstrate compliant handling in practice.

Sovereignty uplift

- **Operational transparency of residency and handling:** Clear traceability of material data flows and locations (including inter-regional replication, backups/DR, support tooling, analytics pipelines and any model-training pathways) so the firm can evidence what happens end-to-end, not just what is contractually intended.
- **Privileged access governance (in-geo and cross-border):** The ability to constrain, approve and evidence provider/admin access to sensitive data and control planes, including where support is delivered cross-border, preventing “back-door” dependence and unmanaged transfer exposure.
- **Cryptographic assurance and evidence:** Encryption and key controls are demonstrably effective (coverage, configuration, key custody/rotation), and supporting evidence (access logs, security events, lineage) is available with sufficient detail and timeliness for audit, supervisory review and post-incident investigation without relying on provider interpretation.

Operational and technical sovereignty

Operational sovereignty directly underpins confidence in the continuity of critical financial services, particularly during operational disruption, cyber events, or large-scale platform dependency failures.

Operational and technical sovereignty means the institution can direct and verify the operation of technology services (configuration, monitoring, incident handling and change control) across internal platforms and third-party services. It becomes most visible in the services that anchor trust and regulatory outcomes, such as identity and privileged access, fraud controls, customer digital channels, claims servicing, core transaction processing, and regulatory reporting platforms.

Minimum requirements

- Maintain a sound ICT risk management framework with defined governance, controls and ownership.
- Identify, classify and report major ICT incidents, supported by timely information from third-party providers.
- Oversee third-party ICT dependencies and ensure risks are assessed, monitored and managed appropriately.
- Maintain a dependency view for critical services (including key providers and material subcontractors) sufficient to understand where operational control sits and where it is diluted.

Sovereignty uplift

- Change authority: the ability to approve, constrain or defer material service changes that affect risk posture (security baselines, identity models, logging, support access patterns), rather than being informed after the fact. In practice, this means that for control-plane services such as identity and access management, institutions must retain final authority over identity sources, MFA configuration and audit logs, rather than relying on provider defaults or discretion.
- Evidence sovereignty for operations: granular, timely operational telemetry (audit logs, configuration state, dependency information) that enables the institution to demonstrate control without provider intermediation.
- Supply-chain visibility and drift control: governance triggers for subcontractor changes and deep dependency shifts so operational control does not silently degrade over time.





Legal and jurisdictional control

Jurisdictional sovereignty ensures institutions can continue to exercise authority, fulfill obligations, and maintain customer and regulatory trust even where services, providers, and data operate across multiple legal regimes.

Legal and jurisdictional control ensures that decision rights and obligations are not merely aspirational but enforceable and anchored in the appropriate legal regime through audit rights, information rights, subcontractor controls, clear allocation of jurisdiction, and the ability to exit without undue dependency.

It is most critical where services deemed critical or important rely on a small number of dominant providers, or where supervisors require timely, direct access to evidence, data, and service governance artifacts within the appropriate legal jurisdiction. This is particularly relevant in markets characterized by provider concentration, where contractual rights may exist but are difficult to exercise in practice without credible alternatives.

Minimum requirements

- The institution retains full accountability for all risks; outsourcing does not transfer responsibility.
- Contracts provide effective rights to access information, obtain audit evidence, and enable supervisory access where required, including within the appropriate jurisdiction.
- Subcontracting is managed through transparent notification, approval, and monitoring mechanisms to ensure accountability, auditability, and evidence remain intact across the delivery chain.
- Exit strategies and defined transition plans exist for critical or important outsourced services and are capable of supporting an orderly and timely transition.
- Cross-border legal and jurisdictional exposure is understood and actively managed, including data residency, transfer requirements, localization constraints, and conflicting jurisdictional access risks.

Sovereignty uplift

- Audit and access rights are supported by pre-agreed processes, standardized evidence formats, and defined response times, ensuring they are effective in practice, not only on paper, and workable across jurisdictions.
- Subcontracting governance ensures providers cannot extend or restructure delivery chains in ways that undermine governance, auditability, or supervisory access across jurisdictions.
- Exit capability goes beyond contractual clauses, with clear data portability, defined handover processes, and continuity of governance and evidence, enabling the institution to change provider, jurisdictional footprint, or architecture without loss of control.



Four control dials of sovereignty

Sovereignty is not a binary condition. It is exercised through four control dials: **decide**, **verify**, **enforce**, and **change**. The question is not whether sovereignty exists, but how far each dial is set, with the strongest levels required for critical and important business services. The required level of control across each dial should be calibrated to the criticality of the service.

01

Can we decide?

To what extent can we set and enforce our own requirements-across data location, operations, configuration, jurisdiction, and access-without reliance on provider discretion or external legal reach?

02

Can we verify?

To what extent can we see what is happening, through timely, granular, and independent evidence across data handling, operations, and access?

03

Can we enforce?

To what extent do our legal, contractual, and technical controls hold in practice, including under cross-border or jurisdictional pressure?

04

Can we change course?

To what extent can we adapt, reconfigure, or exit if risk becomes unacceptable, without losing control, evidence, or continuity of critical services?



Sovereign FS cloud: Sovereignty control profiles

Financial services organizations need a pragmatic way to discuss “sovereign cloud” without defaulting to vendor labels or a binary “public vs private” choice. And while this paper focuses primarily on cloud, data, operational and jurisdictional sovereignty, it is important to note these sit within a wider digital sovereignty landscape incorporating AI, cyber, software, connectivity and supply-chain considerations.

In practice, sovereignty is achieved through different control profiles, applied to workloads and services based on their criticality and risk appetite (Figure 2 — Sovereign FS Control Profiles). The objective is not to move everything into a single model, but to select the appropriate level of control, assurance, and autonomy for each service.

Sovereignty control profiles

1. Provider-led control (assurance-led) – Uses mainstream cloud services while strengthening governance and controls to meet sovereignty expectations, primarily through assurance rather than full operational autonomy. Typical fit: Digital channels and customer journeys, collaboration and productivity platforms, analytics and development environments (subject to data classification).	2. Shared / sovereign control (enhanced assurance) Introduces sovereign variants and tighter operating models to increase control and transparency, particularly where regulatory scrutiny or data sensitivity is higher. Typical fit: Higher-sensitivity customer data domains, regulated data platforms, services under increased supervisory focus.	3. Institution-led control (control-led autonomy) – Applies where assurance alone is insufficient and the institution requires greater direct control over how services are operated, secured, and recovered, including jurisdictional and operational independence. Typical fit: Critical transaction processing, identity and privileged access management, high-sensitivity domains, critical or important business services where disruption would cause intolerable harm
--	---	--

Sovereignty at scale is enabled by a **platform layer** that makes control repeatable, consistent, and efficient across all deployment models, regardless of where workloads sit.

This provides the mechanisms to operationalize sovereignty through:

- Governed landing zones and standardized control environments
- Policy-as-code and embedded control frameworks

- Evidence-as-a-service to support audit and regulatory requirements
- Standard onboarding and architectural patterns
- Resilience testing and exit / transition rehearsal capabilities

This model supports geo-patriation and multi-cloud diversification by enabling institutions to distribute workloads across multiple public, sovereign, and dedicated environments to manage concentration and geopolitical exposure. A summary of current market solutions is presented in Figure 3 – Sovereign Cloud Vendor Solutions.

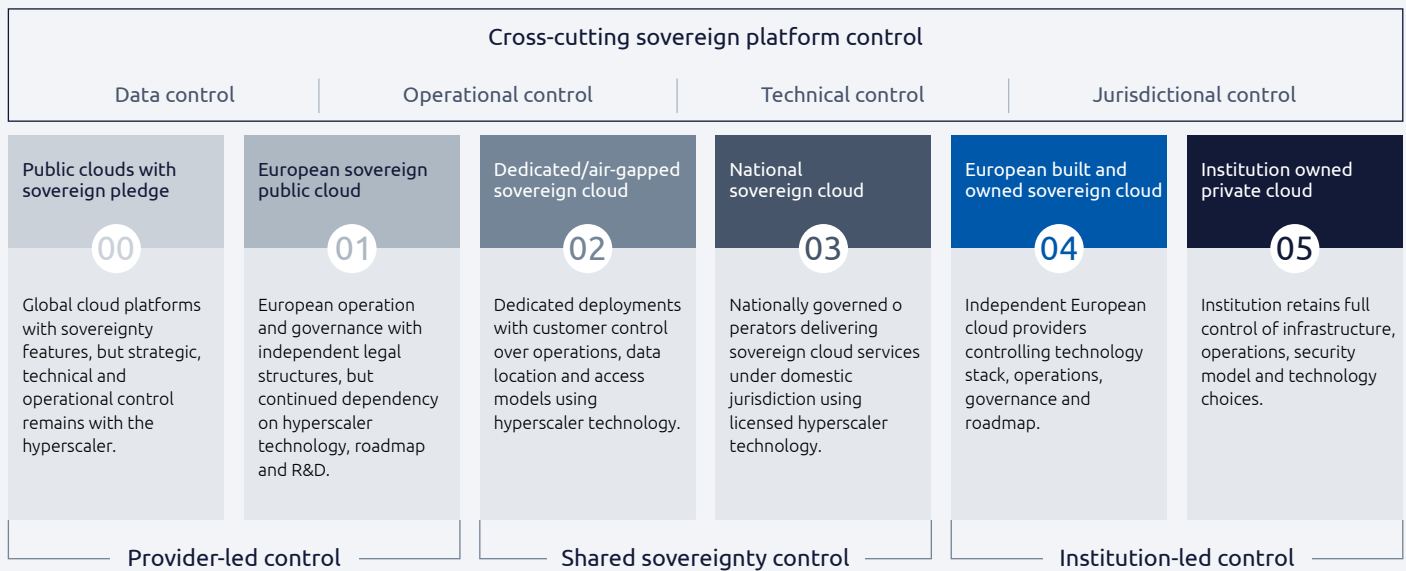


Figure 2 – Sovereign FS Control Profiles

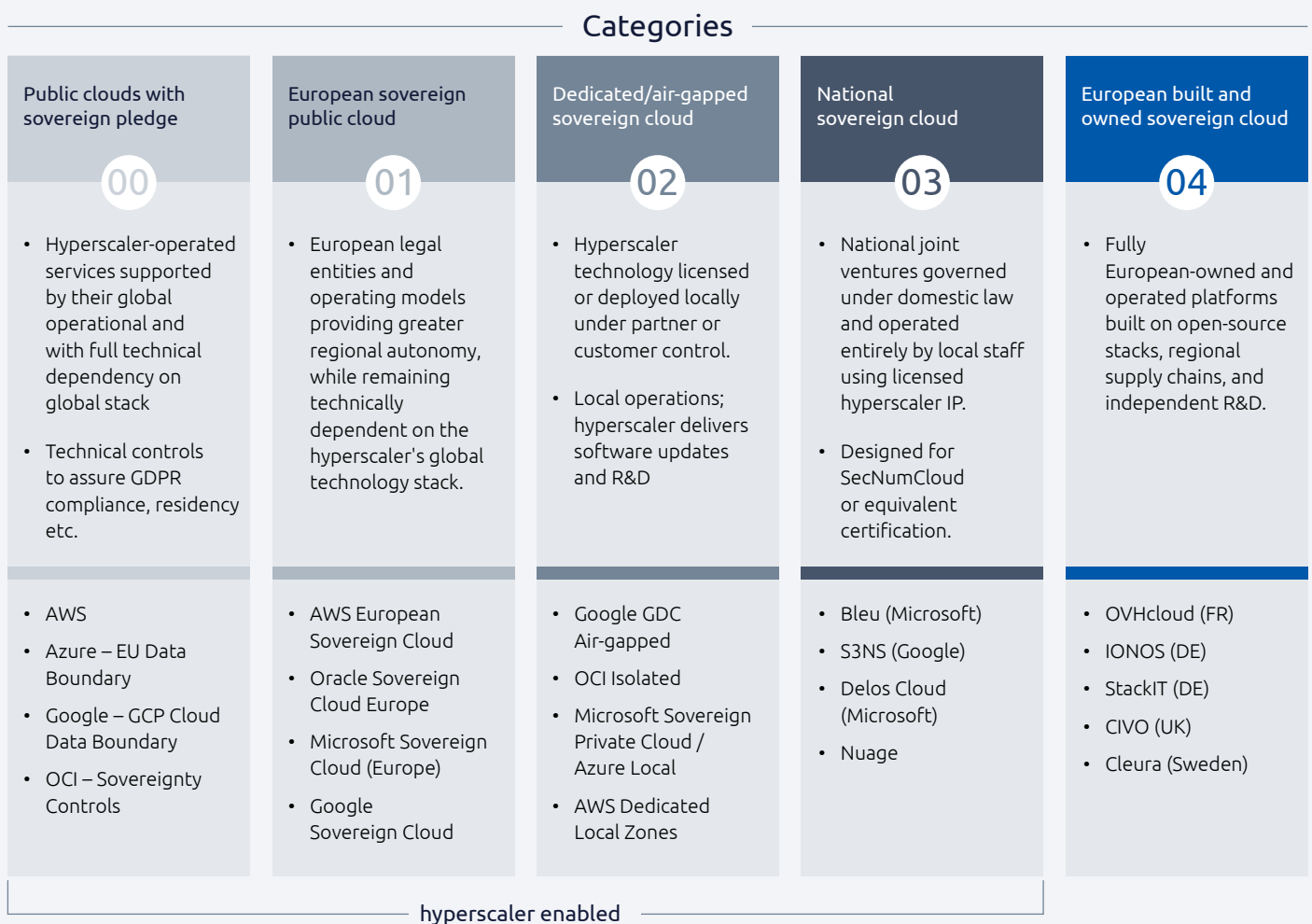


Figure 3 – Illustrative sovereign cloud market models and offerings

Illustrative market mapping based on publicly stated provider operating models and sovereignty features as at mid-2026. Placement does not constitute certification or an assessment that a service meets an institution's specific legal, regulatory or sovereignty requirements.



First steps: From principle to execution

Across EU and UK financial services, leaders are converging on four fundamental questions:

- How should sovereignty be defined and applied in practice?
- Where is strategic autonomy required, and what trade-offs are organizations prepared to make?
- How can sovereign platforms be designed, built, and operated effectively?
- How can AI, data, and digital innovation be accelerated while maintaining appropriate levels of control?

Yet despite growing clarity on the why, many organizations remain stuck between intent and execution. Leadership action is required to define where control is essential, where dependency creates value, and how innovation can be accelerated without creating unacceptable exposure. A disciplined, risk-led approach can help organizations translate sovereignty ambition into practical decisions and measurable outcomes:

Set the sovereignty ambition

Define the organization's sovereignty posture and red lines, establishing Board-level intent aligned to resilience, regulatory obligations, and strategic autonomy.

Make dependencies visible

Create transparency over critical business, technology, data and third-party dependencies, including jurisdictional and concentration risks.

Assess exposure and impact

Evaluate how disruption to critical dependencies could affect business services, customers, regulatory compliance, and strategic objectives.

Decide where control matters most

Determine where provider-led, shared, or institution-led control is appropriate, based on risk appetite, criticality, and business outcomes.

Embed sovereignty by design

Prioritize investments, operating model changes, governance, skills, and architectural capabilities required to deliver the desired sovereignty posture.

This helps ensure that investment and action are focused where they deliver the greatest reduction in material sovereignty risk, while preserving access to the innovation, scale, and capabilities that drive competitive advantage.



Figure 4 – from Ambiguity to Action – Capgemini 5 step approach



Turning strategy into delivery

The challenge is rarely selecting a single sovereign technology. It is orchestrating controls, evidence, governance and delivery consistently across providers, jurisdictions and operating models.

The five-step approach establishes the organization's sovereignty posture. The next challenge is translating that posture into execution, determining where sovereign capabilities should be consumed, where they should be retained, and how both can be combined to deliver business value.

The first execution decision is where value will be derived, whether:

- **Consuming sovereign capabilities** through provider-led and shared control models
- Building institution-led sovereign capabilities where greater autonomy is required
- Or orchestrating both in a deliberate hybrid model

In practice, leading institutions adopt a **risk-based placement across sovereignty control profiles**, rapidly identifying where **institution-led and platform-enabled capabilities** (such as standardized controls, onboarding, and continuous evidence) to:

- Accelerate change delivery
- Reduce the cost and friction of compliance
- Strengthen control, resilience, and auditability across jurisdictions

Critically, this is not solved service by service, but **systematically through a cross-cutting sovereignty platform**, which industrializes guardrails, policy enforcement, and evidence generation at scale.





Conclusion

Digital sovereignty is no longer a peripheral technology debate. It is increasingly a business, trust, and strategic resilience issue.

In financial services, customers, regulators, governments, and markets ultimately judge institutions on whether they can maintain trusted operations, protect sensitive data, and continue functioning during disruption.

Institutions that cannot demonstrate control over critical services, dependencies, and digital operations risk more than regulatory friction. They risk erosion of customer trust, reduced strategic freedom, increased systemic exposure, and weakening institutional legitimacy.

The strategic question is therefore no longer whether financial institutions should address sovereignty, but how to ensure they retain sufficient control over critical capabilities while continuing to benefit from the innovation, scale, and expertise of an increasingly interconnected digital ecosystem. The answer is not to constrain innovation or pursue sovereignty for its own sake, but to establish a clear sovereignty posture: retaining control where it matters most, accepting dependency where it creates value, and managing the trade-offs consciously.

Leading financial institutions are increasingly viewing sovereignty as a source of competitive advantage rather than simply a compliance obligation. More than half (52%) of European financial services firms now regard digital sovereignty as a competitive differentiator, reflecting a growing recognition that demonstrable control over critical services, data, and dependencies strengthens customer trust, supports operational resilience, and enhances strategic freedom in an increasingly uncertain operating environment.

The institutions that succeed will be those that treat sovereignty not as a constraint on innovation, but as an enabler of it, creating the trust, control, resilience, and strategic freedom needed to adopt new technologies with confidence and thrive in an increasingly uncertain world.



Scenarios – applying sovereignty in practice

Organizations recognize sovereignty as critical, but the challenge is not defining it but understanding where control breaks in practice.

In reality, sovereignty fails in three distinct ways:

- **Through speed**, where control erodes as change outpaces control models
- **Through complexity**, where control fragments across large, distributed estates
- **Through interdependence**, where control becomes conditional on external participants and shared infrastructure

These reflect the core forces shaping financial services today: cloud-native delivery, complex operating models, and increasingly interconnected ecosystems.

The purpose of these scenarios is to move sovereignty from principle to execution. They provide a practical way to:

- diagnose where control is most at risk
- understand how sovereignty fails in different contexts
- prioritize action based on the dominant exposure
- align control models, platform capability, and investment decisions

Most organizations will exhibit elements of all three. Different services and domains are shaped by different combinations of velocity, complexity, and interdependence. The objective is not to fit the organization into a single scenario, but to identify where each pressure is most acute and respond accordingly.

Scenario 1: Cloud-Forward Modernizers

Control must be engineered into delivery to prevent erosion as change accelerates

Scenario 2: Assurance-First Operators

Control must remain coherent and enforceable across complex, distributed estates

Scenario 3: Ecosystem Trust Anchors

Control must be enforced across organizational boundaries to sustain trust in multi-party environments

Across all three, the objective is consistent: to ensure the organization can decide, verify, enforce, and change course in practice.

What differs is the context in which control is challenged and the mechanisms required to sustain it at scale.



Scenario 1: Cloud-forward modernizers

Sovereignty through engineering, automation, and continuous assurance

This scenario applies most clearly to challenger banks, digital banks, and regulated fintechs whose operating models were built on public cloud. For these organizations, cloud is not simply a hosting choice; it is the foundation of how they deliver change, scale digital services, and operate efficiently.

In this context, sovereignty is not achieved through isolation or heavy governance overlays. It is achieved by engineering control, enforceability, and continuous evidence directly into platforms, pipelines, and operating models.

At the same time, these organizations are also among the most exposed to sovereignty risk. Their dependence on global hyperscalers, SaaS platforms, and managed services is often deepest, and without deliberate design they risk drifting into practical dependency on external providers and foreign jurisdictions.

Broad applicability across financial services

This posture applies wherever agility, automation, and standardization are strategic priorities, including:

- Retail and digital banks modernizing customer journeys and core platforms
- Specialist lenders operating API-driven distribution models
- Digitally mature insurers and wealth platforms running cloud-native estates
- Fintechs scaling into more heavily regulated environments

Across these organizations, sovereignty is tested not by whether cloud is being used, but by whether control and freedom to act are preserved over time, rather than gradually reduced as change is delivered at pace.

Why sovereignty becomes critical

In this scenario, sovereignty risk is often initially framed through privacy and regulatory compliance lenses. That is understandable: these are the most visible, codified, and auditable elements of regulation, and they align to familiar mechanisms such as policies, certifications, contractual clauses, and third-party assurance.

However, these lenses are necessary but not sufficient. They focus on whether rules have been followed, rather than whether the institution can sustain control and freedom to act in practice, particularly as change accelerates in cloud-based environments.

- Privacy asks: was data handled lawfully?
- Compliance asks: have required controls been defined and evidenced?
- Sovereignty asks: are control and freedom to act being preserved over time, or are they gradually eroding as the organization scales and changes?

This distinction becomes critical in cloud-forward operating models, where:

- Control is distributed across providers, platforms, and pipelines
- Change is continuous, automated, and high-frequency
- Evidence is often provider-generated rather than institution-controlled (or independently useable) evidence
- Dependencies accumulate across jurisdictions, services, and supply chains



In this environment, sovereignty is not tested only in design or at audit points. It is tested over time, through the cumulative effect of delivery velocity, provider dependence, architectural decisions, and operational constraints.

It begins to erode when:

- Control progressively weakens as delivery velocity increases, even if individual changes appear compliant
- Freedom to act becomes constrained by provider dependencies, contractual limitations, or jurisdictional complexity
- Evidence of control is indirect or delayed, relying on provider-generated reporting rather than institution-controlled telemetry and traceability
- Intervention becomes slower, more complex, or less certain, particularly under stress or cross-border conditions

The resulting failure mode is gradual rather than dramatic: the organization may remain compliant in principle, but over time lose the ability to exercise and evidence control with confidence when it matters most.

How sovereignty risk materializes

Common sovereignty stress events in this scenario include:

- Rapid release cycles creating unintended breaches of conduct, consumer protection, or jurisdictional expectations
- Misconfiguration or control drift affecting authentication, consent, fraud controls, or regulated customer journeys
- Hyperscaler or SaaS changes altering data processing, access paths, support models, or operational behavior with limited notice

- Regulatory scrutiny focusing on control effectiveness at the point of change, rather than on policy intent or architectural diagrams alone
- Legal, contractual, or operational constraints limiting independent intervention, escalation, recovery, or evidencing across jurisdictions

If unmanaged, these dynamics typically lead to:

- Increased supervisory friction
- Reduced ability to evidence control independently
- Heightened jurisdictional and concentration risk
- Reduced flexibility to respond to disruption or regulatory change
- Erosion of strategic autonomy as the organization scales

The core structural challenge

Cloud-forward operating models concentrate sovereignty exposure in ways that are often only partially visible:

- Control planes for identity, logging, monitoring, and security may sit outside the institution
- CI/CD pipelines can become high-privilege control paths unless explicitly governed
- Automation increases the speed and scale at which drift or misconfiguration can propagate
- SaaS and third-party services become embedded directly within regulated customer journeys
- Jurisdictional and supplier dependencies accumulate through layered services and opaque supply chains

For that reason, sovereignty cannot be treated as a retrospective compliance overlay. It must be engineered into delivery and operations by design, so that control and freedom to act do not diminish as the organization grows more digital, automated, and externally dependent.



The solution shape: engineered sovereignty for high velocity change

Design principle: preserve control as velocity increases

Cloud-forward modernizers preserve sovereignty by embedding control directly into the flow of change itself, ensuring that as change accelerates, control and freedom to act do not gradually shift to providers, platforms, or pipelines.

The primary mechanism is engineering control into the flow of change itself so that guardrails, decision authority, and evidence are produced continuously as part of delivery, rather than reconstructed after the fact.

This leads to a design where:

- control is enforced in pipelines and platforms, not only through governance
- evidence is real-time, machine-generated, and institution-controlled (or independently useable) evidence
- dependency is actively constrained as services scale and evolve

In this scenario, the sovereignty platform acts as a delivery control layer, industrializing guardrails, pipeline governance, and continuous evidence to prevent control erosion as velocity increases. The platform acts at runtime, governing pipelines, deployment, and change execution.

Key architectural patterns for cloud-forward institutions

Cloud-forward modernizers embed sovereignty through automation-led patterns that preserve speed while reducing dependency:

1. Sovereign landing zones

Institution-governed landing zones ensure identity enforcement, logging, operational control, and data boundaries are designed in from the start, rather than inherited from default cloud configurations. This may include sovereign cloud variants, region-scoped deployments, and customer-controlled encryption or key management patterns.

2. Policy-as-code guardrails

Guardrails are enforced across infrastructure, APIs, and data so that non-approved regions, services, access paths, or data flows are prevented by design rather than discovered later through review.

3. Continuous evidence generation

Telemetry, configuration state, API activity, pipeline changes, and operational actions generate real-time, audit-ready evidence in OSCAL-aligned machine-readable formats, reducing reliance on provider-generated reporting and strengthening institution-controlled (or independently useable) evidence traceability.

4. Separation of build, deploy, and operate

Pipelines, artifact repositories, and privileged administration are tightly controlled so delivery speed does not translate into unchecked authority.

5. Governed SaaS and third-party integration patterns

Identity, data handling, logging, resilience, and exit controls are standardized so external services cannot silently dilute sovereignty.

6. Selective multi-cloud or hybrid patterns

These are used deliberately where concentration or jurisdictional pressure would otherwise constrain the organization's freedom to act or ability to change course.



Shared responsibility model

A clear operating model is essential:

- Regulators set outcomes and evidence expectations
- The institution retains accountability for customer outcomes, governance of change, and continuous evidence of control
- Cloud and SaaS providers must support evidence availability, operational separation, transparency, and enforceable controls aligned to the chosen control profile
- Third parties integrate through governed patterns and operate within defined guardrails

The institution cannot outsource sovereignty. It may consume external services, but it must retain the ability to govern, intervene, and evidence control independently.

Scaling sovereignty over time

To avoid sovereignty becoming a fragmented set of point controls, institutions should mature the platform capability over time by:

- Expanding standardized guardrails and evidence services across jurisdictions
- Automating compliance evaluation and evidence packaging for audits and regulatory reviews
- Formalizing tested exit, substitution, and transition paths for key cloud and SaaS dependencies
- Extending onboarding, governance, and control patterns to ecosystem partners so growth does not dilute control
- Using the platform layer to make sovereignty controls consistent, reusable, and efficient across all control profiles

Closing implication

For cloud-forward modernizers, sovereignty is an engineering discipline; the challenge is not proving control after change, but ensuring control does not erode as change accelerates.





Scenario 2: assurance-first operators

Sovereignty through assurance, evidence, and governance at scale

This scenario applies to organizations operating large, complex estates under sustained supervisory scrutiny, where sovereignty is judged less by architectural modernity and more by the ability to demonstrate enforceable control and usable evidence at scale.

The defining characteristic is an operating reality shaped by long-lived platforms, layered delivery and outsourcing models, multiple legal entities, and persistent regulatory engagement across jurisdictions.

In these environments, sovereignty is not primarily about technology choices. It is about preventing practical dependency on provider discretion. The organization must be able to direct, verify, and enforce how services operate, even when delivery spans cloud, SaaS, identity tooling, security services, outsourced operations, and deep subcontractor networks.

Broad applicability across financial services

This posture applies wherever governance intensity, evidence burden, and third-party complexity are high, including:

- Large universal banks with heterogeneous estates
- Systemically important insurers with extensive outsourcing
- Asset and wealth managers with multi-platform, multi-admin models
- Market infrastructures and utilities subject to direct supervisory assessment

Across these organizations, sovereignty is not determined by documented controls alone, but by whether control remains enforceable and freedom to act is preserved across a complex operating chain over time.

Where sovereignty is tested

Sovereignty is not proven in architecture diagrams or control frameworks. It is revealed at the moments when control must be exercised, proven, or adapted under pressure.

These moments often coincide with supervisory scrutiny, but they also arise in day-to-day operations, incidents, and change events. Sovereignty is tested when the organization must demonstrate:

- Clear and enforceable ownership across services, providers, and legal entities
- Consistent application of controls across internal platforms and third parties
- On-demand, institution-usable evidence, without reliance on provider interpretation
- Accountability in action during incidents, remediation, transformation, or provider change

These tests expose whether control is genuinely operationalized across the estate, rather than defined in principle.

Why sovereignty becomes critical

In assurance-first environments, sovereignty risk is often approached through compliance, audit, and outsourcing lenses. These are necessary and well-established mechanisms for organizing control and engaging with regulators.



However, they are not sufficient on their own. They focus on whether obligations are defined, controls exist, and evidence can be assembled. Sovereignty goes further. It asks whether the organization can exercise and sustain control in practice, across complex and distributed delivery models.

- **Compliance asks:** have obligations been defined and evidenced?
- **Audit asks:** can controls be tested and traced?
- **Sovereignty asks:** can the organization decide, verify, enforce, and change course – without dependency or delay?

This distinction becomes critical in environments where:

- Evidence is distributed across legacy platforms, cloud services, SaaS, and outsourcers
- Accountability is shared across business units, legal entities, and third parties
- Control is exercised through layered governance rather than direct technical ownership
- Supervisory expectations extend beyond documentation to operational enforceability

In this context, sovereignty is tested during events that require rapid, coordinated control across the estate, including:

- Regulatory or audit reviews requiring rapid aggregation of evidence across claims, pricing, and outsourced services
- Conduct or customer harm incidents spanning internal teams and third-party providers
- Material outsourcing changes or subcontractor failures requiring clear accountability and intervention
- Multi-year remediation programs requiring continuous, verifiable evidence of progress
- Cross-border changes where data movement, access, and accountability must be demonstrated

In these moments, sovereignty is effectively assessed through a simple but demanding test:

- Can the organization decide, verify, enforce, and change course, without ambiguity, delay, or reliance on provider discretion?

If not, control does not fail visibly – it fragments across the estate, expressed as inconsistent evidence, unclear accountability, and practical dependence on external providers.

Focus subsector: Insurance (assurance-heavy archetype)

Insurance illustrates this challenge clearly. Large insurers often operate business-critical platforms over multi-decade horizons, while depending heavily on delegated authority and third-party delivery.

In this context, sovereignty is not primarily about hosting data correctly. It is about being able to prove control over the integrity of records, decisions, and servicing across time and across providers.

Large insurers commonly:

- Operate long-lived policy, claims, underwriting, and actuarial platforms
- Depend on TPAs, loss adjusters, data providers, SaaS platforms, and managed service partners
- Carry long-tail liabilities, making traceability and auditability essential over many years
- Span multiple legal entities and jurisdictions with overlapping regulatory regimes

Here, sovereignty is tested when organizations must demonstrate that control has remained continuous, enforceable, and attributable across the full delivery chain, not just defined at a point in time.



The core structural challenge

Assurance-first operators face sovereignty challenges driven by complexity rather than speed. Pressure arises because:

- Evidence, access control, and accountability are distributed across legacy, cloud, SaaS, and outsourced environments
- Contractual rights (audit, access, exit) are difficult to operationalize consistently
- Multiple operating models coexist, each with different control assumptions
- Legal-entity structures and technology boundaries do not align cleanly
- Provider and subcontractor dependencies introduce points where control becomes indirect or conditional

In this environment, sovereignty is achieved not by simplifying architecture, but by making complexity governable, evidenceable, and enforceable in practice.

The solution shape: Operationalized sovereignty across distributed control environments

Design principle: preserve enforceable control as complexity increases

Assurance-first operators preserve sovereignty by making control enforceable across a fragmented operating chain, ensuring that as complexity increases, control does not fragment across platforms, providers, and legal entities.

The primary mechanism is making control operationally coherent and enforceable across the estate so that governance, contractual rights, and technical controls work together in practice, not just in documentation.

This leads to a design where:

- ownership is clear and enforceable across services and entities
- evidence is consistent, aggregated, and usable without provider interpretation
- control remains executable across legacy, cloud, SaaS, and outsourced environments

In this scenario, the sovereignty platform acts as an estate control coherence layer, industrializing control mapping, evidence, and enforceability to prevent fragmentation across complex delivery chains. The platform acts across the operating chain, aligning control, evidence, and accountability across services, providers, and entities.

Key architectural and operating patterns

Assurance-first operators embed sovereignty through patterns that make control demonstrable, consistent, and enforceable:

1. Evidence sovereignty by design

Capture telemetry, audit logs, configuration state, and key decisions in formats usable without provider interpretation

2. Service-aligned control mapping

Link controls to how services actually operate (e.g. claims, underwriting, customer lifecycle)

3. Hybrid sovereignty across mixed estates

Apply consistent control outcomes across legacy, cloud, SaaS, and outsourced environments

4. Legal-entity and critical-service segmentation

Align accountability, evidence, and control to regulatory scope

5. Third-party enforceability and subcontractor transparency

Operationalize contractual rights through defined evidence, access, and escalation mechanisms

6. Repeatable assurance foundations

Use platform-based guardrails, identity baselines, and evidence services to standardize control across the estate



Shared responsibility model

The institution may distribute delivery, but must retain the ability to govern, verify, enforce, and change course independently.

- Regulators define outcomes and evidence expectations
- The institution retains accountability for control effectiveness, evidence, and third-party oversight
- Cloud and SaaS providers must enable transparency, enforceable controls, and usable evidence
- Partners and outsourcers operate within contractual and technical guardrails

Scaling sovereignty over time

To avoid fragmentation, institutions should:

- Build standardized guardrail and evidence services across the estate
- Instrument legacy and outsourced environments for consistent evidence
- Prioritize domains with the highest assurance burden
- Rehearse exit and substitution to prove the ability to change course
- Extend control and onboarding patterns across ecosystem partners

Closing implication

For assurance-first operators, sovereignty is not primarily a cloud design problem. It is a discipline of operationalized control across complexity.

As estates grow in scale and layering, sovereignty depends on ensuring that control remains enforceable, evidence remains usable, and the organization retains the ability to act, rather than allowing fragmentation to dilute practical authority.





Scenario 3: Payments and open banking participants as ecosystem trust anchors

Sovereignty through controlled interoperability, boundary enforcement, and verifiable coordination

This scenario applies to organizations that operate as trust anchors within payments and open banking ecosystems, where services sit directly in the critical path of money movement, fraud controls, consent, authentication, and regulated data exchange across a network of schemes, PSPs, banks, TPPs, and specialist partners.

In these environments, sovereignty is not only about retaining control within the organization's own estate. It is about ensuring that control remains enforceable across organizational boundaries, where outcomes depend on multiple independent participants and shared infrastructure.

The defining characteristic of this scenario is interdependence. These organizations often rely on cloud services, partner platforms, scheme rules, APIs, identity services, fraud utilities, and ecosystem participants to deliver regulated outcomes in real time. The sovereignty challenge is therefore not simply to govern internal operations, but to ensure that authority, evidence, and intervention rights remain effective across the wider operating network.

In this context, sovereignty is closely linked to trust. Trust underpins scheme participation, partner onboarding, customer confidence, and continued access to payment rails. Organizations that can demonstrate controlled interoperability, enforceable boundaries, and verifiable evidence across the ecosystem can move faster with greater confidence; those that cannot become exposed to partner discretion, opaque dependencies, and fragmented accountability.

Broad applicability across financial services

This posture applies wherever the organization must deliver regulated outcomes through an ecosystem rather than a self-contained estate, including:

- Payments institutions and PSPs supporting payment initiation, fraud decisioning, dispute handling, and settlement orchestration
- Open banking participants managing consent, tokenization, data access, and third-party connectivity at scale
- Banks operating partner-led distribution or embedded finance models where regulated journeys depend on external channels and APIs
- Market-facing utilities or shared services that provide trust-critical connectivity, authentication, or evidencing across multiple participants

Across these organizations, sovereignty is not determined only by internal control maturity. It is determined by whether control, evidence, and the ability to intervene remain effective across external interfaces and dependent participants over time.



Where sovereignty is tested

Sovereignty is not proven in API specifications, participation agreements, or ecosystem diagrams. It is revealed at the points where coordination, authority, and evidence must hold across organizational boundaries in real time. This is where interdependence becomes operationally visible.

These moments often arise when the organization must demonstrate:

- Enforceable control at the boundary between its own estate and partner, scheme, or provider environments
- Observable and governable interactions across APIs, identity flows, fraud decisions, and operational escalations
- Verifiable evidence across participants, without relying on goodwill, manual reconstruction, or provider interpretation
- The ability to isolate, constrain, or reroute dependencies when disruption, fraud, or non-compliance emerges across the network

These are the moments that expose whether sovereignty has been designed into the ecosystem model, or whether it depends on assumptions about partner behavior and provider responsiveness.

Why sovereignty becomes critical

In this scenario, sovereignty risk is often approached through resilience, fraud, or third-party connectivity lenses. Those are necessary and important, because ecosystem participation does depend on service continuity, secure integration, and effective oversight of external parties. However, they are not sufficient on their own. They do not fully address whether the organization can exercise and sustain control when outcomes depend on other actors, shared infrastructure, and cross-organizational decision paths.

- Resilience asks: can the service remain available and recover effectively?
- Third-party governance asks: are partner obligations and controls defined?
- Sovereignty asks: can the organization decide, verify, enforce, and change course across ecosystem boundaries, without becoming dependent on partner discretion or opaque provider control?

This distinction becomes critical because payments and open banking ecosystems are tightly coupled. Trust-critical services increasingly rely on cloud-based platforms, shared APIs, partner-operated components, identity and consent services, fraud analytics, and scheme-level operational dependencies. As interoperability expands, so too does the number of points where authority must be enforced and evidenced.

In this environment, sovereignty is tested when:

- A scheme-wide or ecosystem incident requires rapid, coordinated containment across multiple participants
- Fraud campaigns exploit consent journeys, API paths, or partner integration points across the network
- Control-plane or administrative actions in shared platforms affect identity, signing, access, or operational change, despite accountability remaining with the regulated institution

The organization must prove who could access what, where data was processed, and how decisions were taken across cross-border and multi-party flows

In these moments, sovereignty is assessed through a practical test:

- Can the organization enforce control beyond its own organizational boundary, verify what happened across participants, and change course without waiting on provider or partner discretion?



If not, the failure mode is not simply internal fragmentation. It is loss of coordinated control across the ecosystem, where responsibility remains with the institution, but the ability to direct and enforce outcomes becomes conditional on others.

Focus subsector: Payments and open banking

Payments and open banking illustrate this challenge clearly. These organizations sit in the critical path of money movement, authentication, fraud controls, consent, dispute handling, and regulated data exchange. Their services are inherently multi-party: outcomes depend not only on internal systems, but on counterparties, schemes, TPPs, acquirers, issuers, fraud providers, and platform partners acting in a coordinated and controlled way.

In this context, sovereignty is not primarily about where systems are hosted. It is about whether the organization can retain authority over trust-critical interactions, ensure boundaries are enforceable, and produce usable evidence across the full chain of participation.

Payments and open banking participants commonly:

- Operate regulated services such as payment initiation, account information access, consent and token management, fraud decisioning, strong customer authentication support, dispute workflows, and operational reporting
- Depend on partner connectivity, scheme rules, cloud platforms, APIs, and specialist providers to deliver outcomes
- Carry high expectations for real-time control, evidencing, and incident response across multiple independent participants
- Face cross-border legal, operational, and jurisdictional pressures where control must remain visible and enforceable

Here, sovereignty is tested when organizations must demonstrate that interoperability has not diluted authority and that trust can be sustained because boundaries, decisions, and evidence remain under effective control.

The core structural challenge

Payments and open banking participants face a sovereignty challenge driven by interdependence across organizational boundaries. The organization may remain accountable for outcomes, yet key elements of execution rely on entities it does not fully control.

Pressure rises because:

- Critical flows depend on shared interfaces, partner-operated services, and ecosystem-wide rules
- Control is exercised through protocols, interfaces, and interaction patterns, not only internal systems or contracts
- Evidence of what happened is distributed across organizations and platforms
- Provider, partner, and jurisdictional dependencies constrain independent action
- Interoperability increases points where authority becomes ambiguous under stress

For this reason, sovereignty is achieved not by reducing interdependence, but by making boundary control explicit, enforceable, and observable in practice. In this scenario, control does not sit primarily in infrastructure or governance layers, but at the points of interaction between participants; APIs, identity flows, orchestration paths, and trust services.

The solution shape

Payments and open banking participants preserve sovereignty by making interactions across the ecosystem governable, evidenced, and enforceable by design. The objective is not to eliminate interdependence, but to ensure that interdependence does not become dependency without control.



The practical design intent is to:

- Establish controlled, policy-enforced interoperability so partner connectivity is observable and restricted
- Separate run, change, and administrative authority so shared tooling cannot bypass controls
- Ensure trust-critical services operate in environments aligned to sovereignty requirements
- Make control, onboarding, and evidence repeatable across partners and jurisdictions

This aligns to a risk-based sovereignty control posture:

- Provider-led control (assurance-led) for services where governed interfaces are sufficient
- Shared / sovereign control (enhanced assurance) for trust anchors requiring visibility and control
- Institution-led control (control-led autonomy) for critical services requiring direct authority

These are supported by a cross-cutting sovereignty platform capability acting as a boundary control layer, governing interoperability, onboarding, and evidence across participants. The sovereignty platform acts as a boundary control layer, governing APIs, identity, onboarding, policy enforcement, and evidence across interactions rather than just within systems.

Key architectural and operating patterns

1. Controlled API gateway and interaction layer

All external interactions are mediated through governed API gateways and integration layers, where policy enforcement, authentication, rate limiting, and jurisdictional rules are applied consistently. This ensures that interoperability is controlled rather than implicit.

2. Identity, consent, and trust control plane

Identity, consent, authentication, and tokenization services operate as trust control planes, where authority over access, delegation, and verification remains explicit and auditable across participants.

3. Boundary-level policy enforcement

Policy-as-code is applied at interaction boundaries, not just within infrastructure, governing what partners can access, how data flows, and how decisions are executed across ecosystems.

4. Cross-participant evidence and traceability layer

Transaction traces, access logs, consent records, and decision events are captured in a way that enables end-to-end visibility across organizational boundaries, without reliance on partner reconstruction.

5. Service orchestration with controlled failover paths

Orchestration layers manage routing, failover, and degradation across participants, ensuring the organization can isolate dependencies, reroute flows, or constrain activity when disruption occurs.

6. Enforced partner onboarding and integration blueprints

Standardized onboarding patterns, integration templates, and control requirements ensure that new participants enter the ecosystem without weakening control or introducing unmanaged risk.



Shared responsibility model

- Regulators and schemes define participation rules and expectations
- The organization remains accountable for outcomes and control
- Providers must support enforceable controls and evidence
- Ecosystem partners operate within governed interfaces

The organization participates in the ecosystem but must retain the ability to govern interactions, verify behavior, enforce boundaries, and change course independently.

Scaling sovereignty over time

- Standardize onboarding and control patterns across participants
- Strengthen evidence and guardrails early
- Harden integration and gateway controls
- Rehearse substitution and rerouting
- Use platform capability to scale governance and interoperability

Closing implication

For payments and open banking participants, sovereignty is a discipline of controlling interdependence.

As ecosystems expand, sovereignty depends on ensuring that interoperability does not dilute authority. Control must remain enforceable, evidence usable across participants, and the organization must retain the ability to act independently.





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 marketleading 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



Make it real .