Futurum®

IBM

The New Rules of Digital Sovereignty: Architecture, Control, and Competitive Advantage

How MSPs and System Integrators Can Turn the Digital Sovereignty Imperative into Competitive Advantage

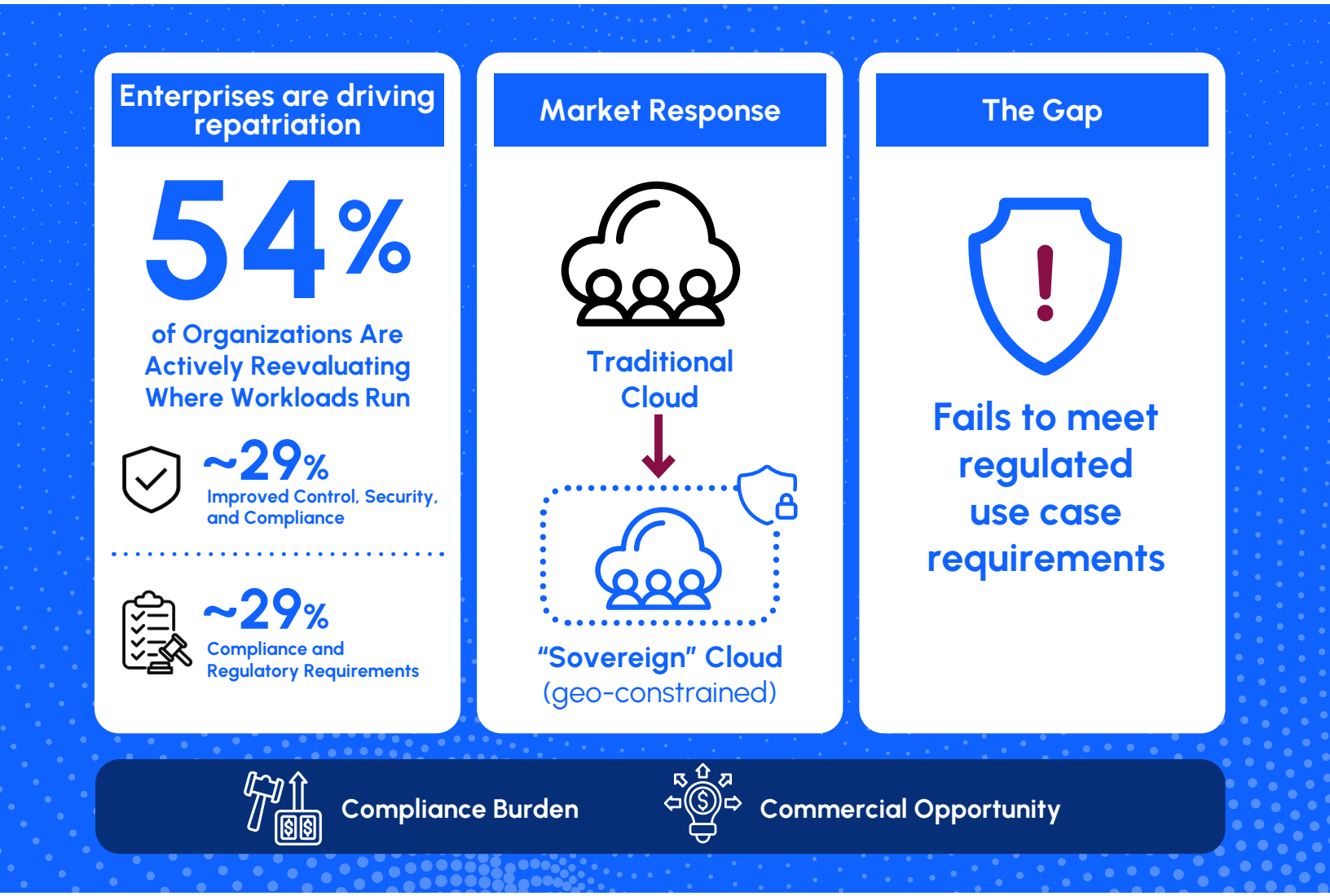
MAY 2026

The Sovereignty Imperative Is No Longer Theoretical

Digital sovereignty has moved from a niche compliance concern to a strategic priority for governments and enterprises worldwide, who are taking action to control where data can reside, who can operate infrastructure, and how AI systems are governed.

For managed service providers (MSPs) and system integrators, this shift represents both a compliance burden and a substantial commercial opportunity. According to the Futurum Research CIO Insights Survey (Q4 2025), 54% of organizations are actively reevaluating where workloads run, with improved control, security & compliance, and regulatory requirements now co-equal as the top drivers – each cited by approximately 29% of respondents. Yet the market response has been uneven (see Figure 1). Most sovereign offerings remain variations on a familiar theme: take an existing public cloud architecture, restrict it to a geographic boundary, and market it as sovereign. For service providers and integrators advising regulated enterprises and public-sector clients, this approach is increasingly insufficient.

Figure 1. Workload Repatriation Is Driven by Control and Compliance, but "Sovereign" Responses Remain Incomplete



Futurum Research, CIO Insights Survey, Q4 2025.

The Limits of Legacy Sovereign Cloud Solutions

Legacy sovereign solutions addressed the most visible requirement: data residency. By locating compute and storage within national borders, providers can satisfy regulations mandating local data retention. But this leaves deeper structural questions unanswered. Futurum identifies several persistent gaps:

Control-Plane Dependency: The operational control plane often remains managed by the hyperscaler from infrastructure outside the sovereign boundary – the defined jurisdiction under the organization's own control – exposing software updates, identity management, and orchestration decisions to extraterritorial legal reach.

Policy-Overlay Fragility: Sovereignty enforced through contractual terms or configuration policies – rather than architectural design – is inherently fragile. Policies can be overridden, misconfigured, or rendered moot by platform changes.

Vendor Lock-In as a Sovereignty Risk: If an organization cannot migrate away from a provider without prohibitive cost or disruption, the claim of sovereignty is compromised as the organization is not truly in control.

AI Governance Gaps: Legacy solutions lack mechanisms to enforce where model inference occurs, who controls training data, or how AI decision-making is logged and audited within the sovereign boundary.

Point in Time Governance: The proliferation of compliance regulations makes compliance using traditional, periodic audits unworkable. Organizations need continuous verification of their compliance posture, not just a snapshot taken once a year.

For MSPs and integrators building sovereign offerings, these gaps translate directly into risk. If the underlying platform cannot demonstrably satisfy geographic or jurisdiction-specific regulatory requirements, the service provider inherits that exposure.

Reframing Digital Sovereignty

Next-generation digital sovereignty moves beyond data residency to address the full spectrum of sovereignty, data, operational, technology, and AI-related sovereignty requiremevnts. Futurum identifies five defining principles:

Five Principles of Next-Generation Digital Sovereignty

1	**Operational Control:**	The customer or designated local operator controls the full operational stack, including the control plane, identity services, and encryption key management, not just the data layer. This must hold true even when a service provider is delivering the sovereign solution.
2	**Open and Auditable Foundations**	The software stack is built on open-source components that can be owned, improved, independently inspected, audited, and verified by the operator or designated third parties.
3	**Vendor Independence and Operational Resilience**	The platform can continue to operate without dependency on the original technology vendor – including under sanctions, supply-chain disruption, or vendor withdrawal – and organizations can migrate workloads to alternative platforms without architectural rework, i.e. no vendor lock-in.
4	**Provable Compliance**	Fragmented compliance standards increase risk of non-compliance. Sovereignty needs to be evidence-based and supply continuous evidence.
5	**Optionality in Composable Architecture**	It is unlikely that all the technology you utilize will be maintained within your sovereign boundary, so it is important to maintain the flexibility to select, replace, or remove independent components without disrupting the entire system.

These principles define the difference between offering a sovereign-labeled hosting service and delivering a platform that can withstand regulatory scrutiny and earn long-term client trust.

The Revenue Opportunity for Service Providers

For MSPs and integrators, Digital Sovereignty is not merely a compliance exercise – it is a service-creation opportunity. While US hyperscalers dominate the cloud market, local and regional providers are gaining ground as enterprises seek alternatives that keep operations under domestic jurisdiction.

Service providers meeting the next generation sovereignty criteria are positioned to capture demand across government modernization, financial services, healthcare, defense, and any enterprise operating under DORA, NIS2, or the EU AI Act. A sovereign platform enables providers to move beyond commodity infrastructure resale and offer differentiated managed services – sovereign AI hosting, compliance-as-a-service, jurisdiction-specific managed Kubernetes – that command higher margins and longer contract terms.

Evaluating Next-Generation Sovereign Cloud Platforms

Service providers evaluating next-generation platforms for their sovereign practice should assess candidates against the five principles above, plus several practical considerations:

Customer-Operated Control Plane: The operator – not the vendor – must hold direct authority over deployment, configuration, and orchestration. Vendor-managed control planes outside the sovereign boundary introduce structural weakness.

In-Boundary Identity and Key Management: Authentication, authorization, and cryptographic key storage must reside entirely within the defined jurisdiction.

Embedded Compliance Automation: Look for platforms where compliance monitoring is continuous and produces regulator-ready evidence on demand, rather than relying on periodic manual audits.

Operational Resilience under Disruption: The platform must continue operating independently even in the face of sanctions, disconnection, or vendor withdrawal.

AI Governance within the Boundary: The platform must enforce where inference runs, who controls models, and how AI decisions are logged – a regulatory requirement in multiple jurisdictions.

Deployment Speed and Multi-Tenancy: Service providers need to stand up sovereign environments quickly and serve multiple clients from a shared platform. Automation and multi-tenant architecture are essential for commercial viability.

IBM Sovereign Core: Built for Next Generation Sovereignty

IBM Sovereign Core represents a notable entry in the Digital Sovereignty category. Rather than retrofitting sovereignty controls onto an existing public cloud, IBM has designed Sovereign Core as purpose-built software for enterprises – and the service providers that support them – to build, deploy, and manage cloud-native, on-premise, and AI applications under their own authority and within chosen jurisdictions.

The architecture aligns with the next-generation sovereignty principles outlined above. Sovereign Core delivers a customer-operated control plane where the service provider or end client maintains direct operational authority without intermediation from IBM or any external vendor. Identity services, encryption keys, and access management remain within the jurisdiction boundary. Compliance capabilities are embedded in the software, enabling continuous automated compliance. On the AI front, Sovereign Core governs where inference occurs, who controls models, and how decisions are audited, including support for CPU- and GPU-based clusters within the sovereign boundary.

IBM Sovereign Core is built on an open-source, auditable foundation, enabling customers to move workloads across regions and infrastructure types. Additional components include secrets management and a compliance center for continuous compliance verification. Pre-built regulatory accelerators aligned to compliance frameworks speed time to identification of compliance risk. For service providers, the multi-tenant architecture and automation enable rapid, repeatable deployments.

From Constraint to Strategy

The transition from data sovereignty to comprehensive digital sovereignty is a market inflection point. Service providers that continue to offer sovereignty as a geographic overlay will face growing difficulty satisfying regulatory requirements and client expectations. Those that adopt platforms designed for operational sovereignty, AI governance, and structural independence are positioned to capture a growing share of enterprise IT spending.

Futurum recommends that MSPs and integrators take three steps:

1

Assess Current Offerings Against the Five Digital Sovereignty Principles:

Identify gaps in control-plane independence, AI governance, compliance evidence, and vendor survivability.

2

Evaluate Platforms with Architectural Rigor

Look beyond marketing claims to examine where the control plane resides, how keys are managed, and whether the platform can operate independently of the vendor, including in the case of service provision.

3

Engage Early with Emerging Platforms

Solutions such as IBM Sovereign Core are entering the market now. Service providers that engage early will have a head start in building differentiated sovereign offerings.

Digital sovereignty is no longer a constraint to manage. For service providers prepared to treat it as a strategic capability, it is the next major revenue frontier.

Important Information About This Report

AUTHORS

Nick Patience
Vice President & Practice Lead,
AI Platforms | The Futurum Group

PUBLISHER

Futurum Research

INQUIRIES

Contact us if you would like to discuss this report and The Futurum Group will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in context, displaying author's name, author's title, and "The Futurum Group." Non-press and non-analysts must receive prior written permission by The Futurum Group for any citations.

LICENSING

DISCLOSURES

The Futurum Group provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

ABOUT IBM

For over a century, IBM has been at the forefront of technological innovation. Beginning in the earliest days of computing, IBM has blended intelligence, innovation and science to improve business, society and the human experience.

IBM's hybrid and multi-cloud approach is designed to support workload mobility across cloud, on-premises, edge, and air-gapped environments, while addressing regulatory requirements and strengthening enterprise security. By combining open technologies, interoperable platforms, and built-in governance, IBM enables organizations to deploy and scale AI transparently, verify access, and meet regulatory obligations with confidence.

Learn more about digital sovereignty solutions at IBM http://ibm.com/sovereignty

ABOUT THE FUTURUM GROUP

The Futurum Group is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.

CONTACT INFORMATION: **The Futurum Group LLC | futurumgroup.com | (833) 722-5337**