kyndryl

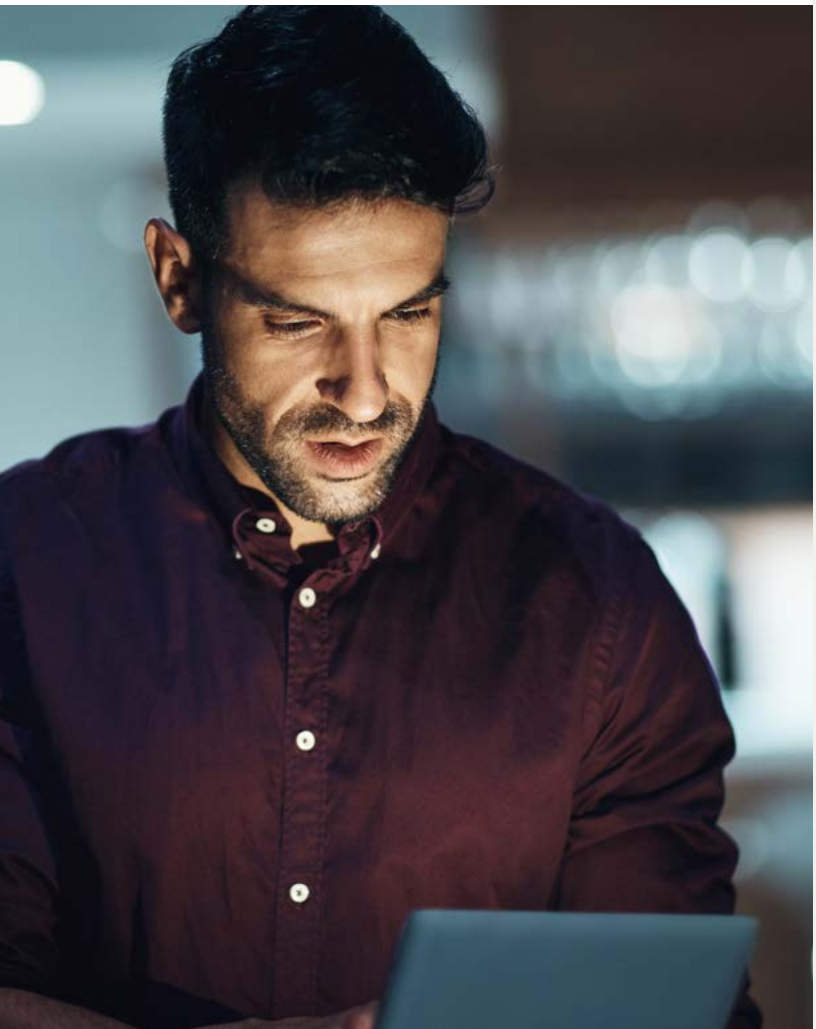
Digital sovereignty by design: Choice and control

From global integration to strategic choice

Over the past decade, assumptions underpinning globalization, trade and cross-border cooperation have been steadily re-examined. What were once considered stable foundations—open markets, integrated supply chains and shared security expectations—are now being reassessed by governments and enterprises alike. Nowhere is this shift more visible, or more consequential, than in technology.

As organizations adjusted trading partners and suppliers, their IT estates evolved into deeply interconnected global systems. Innovation flowed rapidly across borders, driven largely—though not exclusively—by ecosystems centered in the United States and China. Governance models and technical standards established by global technology providers earned wide adoption by emphasizing scale, interoperability and trust.

That model is now under strain. The same global interdependence that enabled efficiency and innovation is being reconsidered in a world shaped by heightened geopolitical competition, national security concerns, supply chain fragility and an accelerating wave of regulatory and sovereignty-driven requirements. Boards, regulators and customers are no longer asking only whether systems are secure—but who ultimately controls them.



The new digital sovereignty landscape

Organizations today are navigating competing imperatives: innovating in the age of AI, delivering resilient and always-on services, complying with increasingly local and sector-specific regulations and defending against sophisticated global threats. There are no universally agreed global standards for data privacy, security or AI governance, and regulatory requirements across jurisdictions are often inconsistent—or directly conflicting.

Digital sovereignty is not a single concept but a set of overlapping and evolving dimensions:

Data sovereignty: Where data is stored and processed, who may access it, and which legal regimes apply.

Operational sovereignty: The ability to independently operate, maintain, and recover technology systems without undue external dependency.

Technological sovereignty: The degree to which an organization's technology stack is insulated from foreign ownership, control, or influence that could enable surveillance, coercion or disruption.

As AI is operationalized at scale, control over the data, infrastructure, models, talent and tooling that underpin those capabilities becomes even more important.

Crucially, sovereignty does not require digital isolationism. Attempts to retreat into fully nationalized, end-to-end technology stacks risk fragmenting global data flows, weakening security, and undermining innovation. Digital sovereignty is better understood as **a strategic planning discipline**—one that expands choice and control while preserving the benefits of global integration where appropriate.

Sovereignty as freedom of action

Sovereignty can appear daunting because it challenges prior decisions that delivered real and measurable value. Cloud adoption, shared platforms and global tooling simplified operations and reduced cost. Reversing those decisions wholesale can reintroduce complexity, diminish resilience and slow innovation.

A control-first approach recognizes that sovereignty is rarely all or nothing. Most organizations can achieve meaningful data and operational sovereignty through deliberate design choices:

- Identifying business and mission-critical objectives
- Mapping jurisdiction-specific regulatory and contractual constraints
- Classifying data by sensitivity, criticality and risk
- Selecting architectures, controls and operational models aligned to those distinctions

Sovereignty, in this sense, is about **preserving freedom of action**—not constraining it.

Data and cloud decisions

Over the past two decades, organizations migrated data to the cloud to gain scale, speed and flexibility. Hyperscale providers invested heavily in security, resilience and continuous improvement—often detecting and remediating vulnerabilities globally faster than localized environments could respond.

Some organizations are now considering partial exits from public cloud environments to meet data localization or sovereignty requirements. In many cases, however, only narrowly defined categories of sensitive data require local residency. A blanket move away from public cloud services can undermine the very security and resiliency benefits that cloud adoption was intended to deliver—particularly for organizations deploying AI and data-intensive workloads that rely on global scale.

Sovereignty should therefore be addressed through segmentation and design, not wholesale withdrawal. Sensitive datasets may be isolated or regionally constrained, while non-sensitive workloads continue to benefit from global cloud platforms.

Sovereignty through security and control

Beyond architectural choices, sovereignty can be reinforced through advanced security and governance controls that apply regardless of where infrastructure is located:

Data vaulting enables resilient recovery by isolating protected copies of critical data—logically or physically—from production environments.

Advanced encryption and key management allow organizations to retain sovereign control over data access, even across borders.

Post quantum cryptography (PQC) addresses the emerging risk of "harvest now, decrypt later" strategies, ensuring long-term protection against future computational advances.

These measures allow organizations to meet sovereignty objectives while avoiding the false trade-off between security, performance and innovation.

Open-source software and supply chain resilience

For many organizations, open source software offers an additional lever for operational and technological sovereignty. By reducing dependence on single vendors or geopolitical supply chains, open source ecosystems can enhance transparency, resilience and long-term control.

Governments and public institutions—particularly in Europe—are increasingly viewing open source adoption as a means of reinforcing sovereignty objectives without sacrificing interoperability or security. The Austrian military, for instance, is making its own switch from Microsoft to open-source LibreOffice. The EU sees open-source technologies as having "the potential to enable greater control over digital infrastructure and to reduce [its] dependencies, ensure greater supply chain transparency and support cybersecurity vulnerability management."

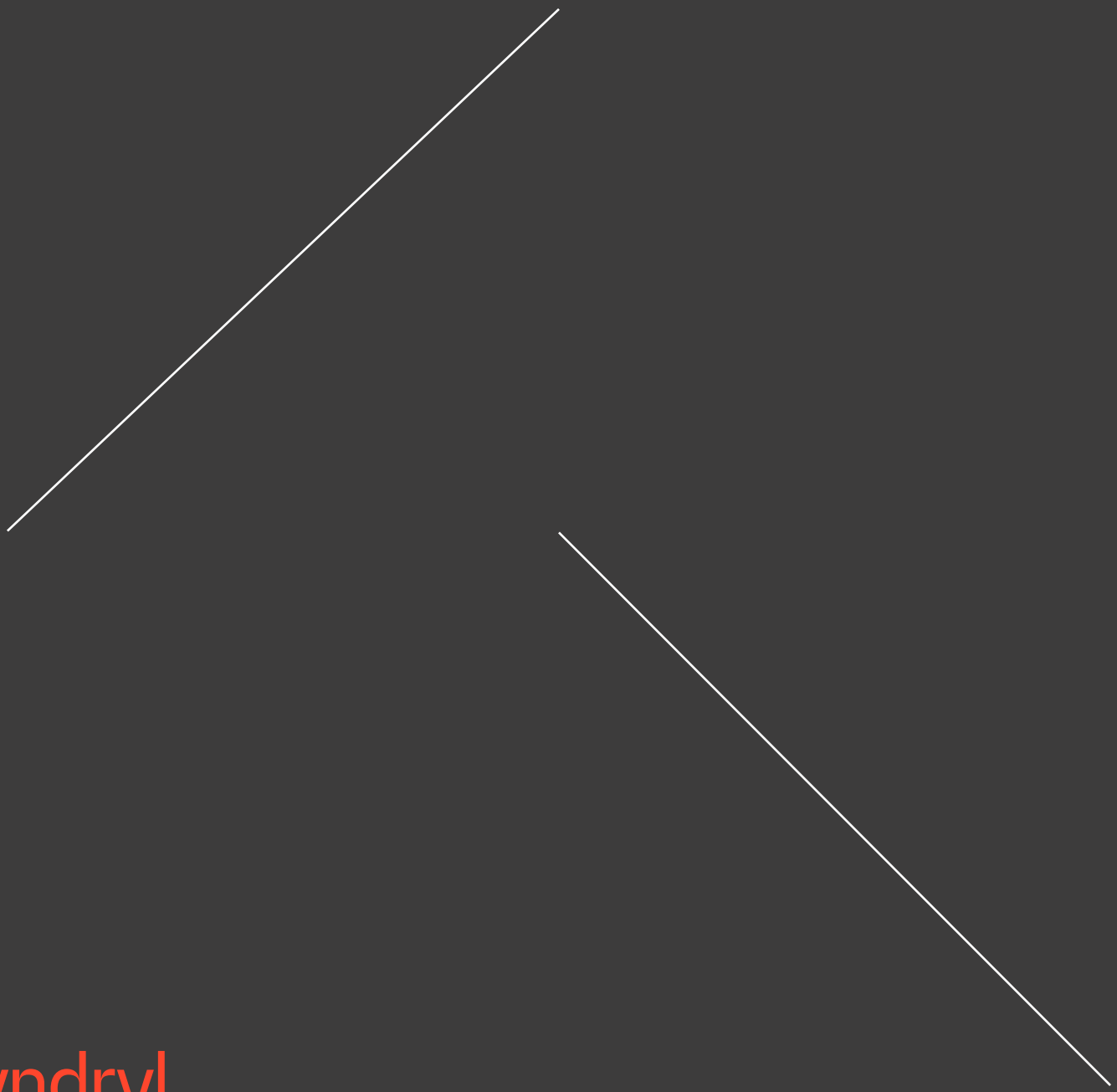
The goal is not disengagement from global technology markets, but optionalities and exit paths grounded in control.

Conclusion: Sovereignty as a design principle

Digital sovereignty is ultimately about **choice, control and adaptability**—not about retreating behind digital borders. Organizations that approach sovereignty as a foundational design principle will be better positioned to navigate geopolitical uncertainty, regulatory divergence and rapid technological change.

Paths will differ by industry, geography and risk profile. Technologies will continue to evolve, and geopolitical dynamics will remain fluid. In this environment, partner selection must be grounded in technical capability, governance maturity and disciplined security practices.

The organizations that succeed will be those that treat sovereignty not as a constraint, but as an enabler—one that allows them to innovate, operate, and grow with confidence in an increasingly complex world.



kyndryl