

DIGITAL SOVEREIGNTY

Maintaining government autonomy, resilience and competitiveness in a digital world

DXC Public

No nation can be a digital island — so what should you do?

What is digital sovereignty?

Digital sovereignty is the ability to be resilient, independent and stand on one's own feet despite changes in geopolitics, vendor policies, supply chain and other global risks.

- Applies across the **whole tech stack**, including energy supply, chips/hardware, data centers, data, AI models and digital operations
- Includes **compliance** with local laws and regulations
- Applies to **governments and other mission-critical service providers**
- Can extend to cover **national technology competence** and industrial policy
- Has become a **worldwide priority**, especially in countries that have a limited technology base

Digital capability has become the foundation of defense, security and public service delivery. So, what happens if a government cannot access vital systems or data due to forces beyond its control? Or, just as concerning: What access might other states or nonstate actors have to confidential systems and data? The risks are real.

In recent months, we have seen extraterritorial data demands, shortages in critical computer chips, state-backed cyberattacks, access to AI models cut off overnight and uncertainty over the risk of free AI models from China. The issue is that in today's highly interconnected digital world of the internet, cloud, worldwide supply chains and global IT companies, it is hard, if not impossible, to be a digital island. Indeed, being a digital island may not even be desirable, since home-sourced options, such as domestically produced infrastructure, or open-source/open-weight models, can fall a long way short of the demands of citizens and enterprises. To complicate matters, there is no single digital sovereignty lever that governments can pull. Ensuring digital sovereignty depends on vendor selection, digital engineering, contract terms, cybersecurity, compliance controls, governance and local digital capability.

To chart the right path through this complex terrain, governments need a partner with deep engineering expertise and extensive experience in the complex technology and regulatory environment of government. Likewise, a partner needs to have solutions designed to meet the particular challenges of digital sovereignty, as well as a strong partner ecosystem to bring solutions from other tech players when these are the right answer. DXC Technology helps governments to be sovereign: protecting critical services, retaining strategic choice and sustaining access to the digital capabilities on which their missions depend. Understanding three widespread misconceptions about digital sovereignty explains why these capabilities are essential.

Misconception 1: Sovereignty is just a compliance issue
Reality: It's a fundamental strategic question

The ability of a government to continue operating core services during a geopolitical disruption is not a compliance question. It is a question of strategic resilience and national capability. Put bluntly, citizens and businesses are looking to governments to make the right decisions to protect their data, their livelihoods and their security. This broader understanding of digital sovereignty is reflected in the wide range of frameworks that are applied. For example, The U.S. National Institute of Standards and Technology's Cybersecurity Framework 2.0 (NIST CSF 2.0) addresses governance, supply chain risk, incident response and recovery. ISO 22301 establishes international requirements for business continuity and organizational resilience.

Sovereignty governance has evolved beyond simple compliance checkboxes. Where organizations once approached data residency and certifications as discrete requirements, the conversation now centers on embedding sovereignty

More control does not automatically mean a higher level of sovereignty.

concerns throughout solution architecture and implementation. This more sophisticated approach requires a coherent framework that connects technical choices, governance structures and organizational capability building.

These choices belong with leaders, because they define risk appetite, accountability, budget and mission continuity. Politicians and senior executives should be fully engaged. Instead of being passive recipients of compliance and technology recommendations, they must be active participants in setting objectives, understanding trade-offs and accepting the accountability that goes with the choices made.

Misconception 2: Sovereignty means maximum control everywhere Reality: It's about making the right choice for each part of the tech stack

It is easy to assume that digital sovereignty demands complete independence: national clouds, domestically owned infrastructure and the elimination of all foreign technology dependencies. That ambition is rarely achievable, never affordable and frequently counterproductive. In a digital world, autonomy and independence depend on strong digital capability to power the economy, defend national interests and provide effective public services. Complete control over weak technology capability is not a route to meaningful sovereignty.

In addition, more control does not automatically mean a higher level of sovereignty. Consider the example of organizations pursuing maximum sovereign control by migrating entire estates to highly restricted environments. The timeline and cost of such comprehensive migrations can be prohibitive, delaying modernization and leaving organizations exposed to the risks they sought to mitigate.

Digital sovereignty is therefore not absolute. Trade-offs are required across three key priorities that often pull in different directions:

- **Control.** Tighter controls and full operational autonomy strengthen independence, but they raise costs and can limit access to advanced capabilities.
- **Capability.** Leading edge technology increasingly underpins effective defense and other public services but can come at the price of supply chain and geopolitical risks. Is the price worth paying? Can the risks be mitigated? It's not just a question of the capabilities themselves but also of how quickly they can be accessed or alternatives be brought into play.
- **Cost.** The options that bring the most control are often the most expensive and not always the most capable.

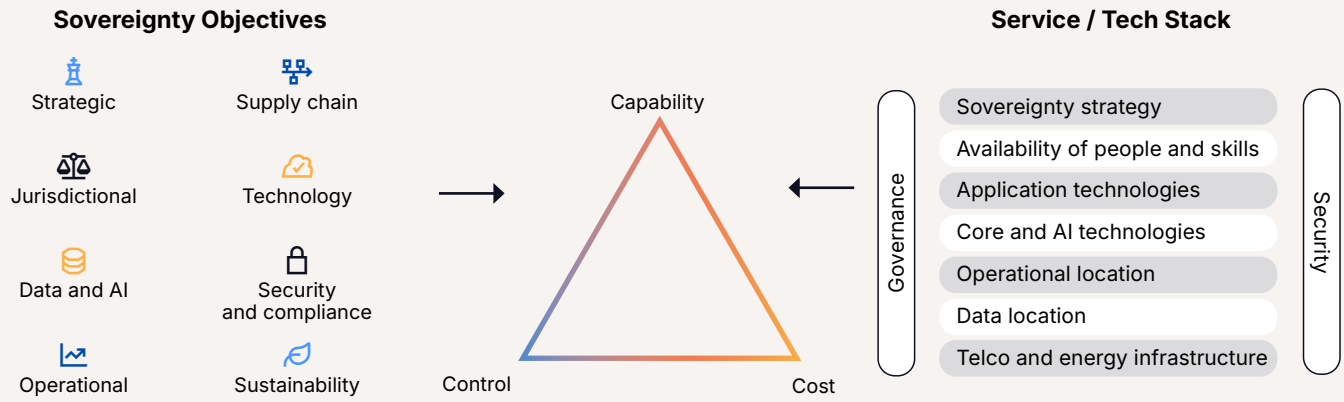
These three dimensions are interdependent: More attention to one usually comes at the expense of another, as in the traditional project triangle of cost, quality and speed. You can't have all three at once.

The optimal strategy is to weigh these three dimensions deliberately for each part of the technology estate. Depending on the technology area — its business importance, the risk of an incident and the speed with which alternatives can be brought into play — the correct balance will differ. Moreover, the balance will need to be monitored and reviewed constantly, since digital sovereignty sits at the intersection of two dynamic forces: geopolitics and technology innovation.

To help organizations adopt a structured — and auditable — approach to making these decisions, we developed the DXC Digital Sovereignty Triangle, shown in **Figure 1**. The triangle provides a leadership decision model that enables executives to make explicit, auditable trade-offs between control, capability and cost for each workload or technology domain.

Figure 1. DXC Digital Sovereignty Triangle

The DXC Digital Sovereignty Triangle provides a structured process to reach the right answer for each part of the tech stack — and an explainable audit trail for decisions.



*Example sovereignty objectives from Cloud Sovereignty Framework, European Commission Directorate-General for Digital Services, October 2025

The DXC Digital Sovereignty Triangle is applied at the workload or technology-domain level and starts by capturing sovereignty objectives, such as mission criticality, regulation, geopolitical exposure and reversibility requirements. Next, technology options, each with their own implications for control, cost and capability, are weighed against these objectives. We then record the agreed trade-offs in an auditable decision matrix that recommends the target development, hosting, sourcing and operating model. For a European public sector agency, for example, DXC recently translated sovereignty requirements into workload-level hosting decisions, comparing public cloud, sovereign cloud and private cloud against control, capability, and 5- and 7-year cost scenarios.

Misconception 3: The nationality of a technology provider is a sure guide to sovereignty
Reality: Nationality offers an easy answer, but it may not be the right answer

When assessing digital sovereignty, it is not sufficient to look at the nationality of a tech provider. Assessing sovereignty requires looking beyond nationality to the broader technology ecosystem on which a service or solution depends. For example, hardware assembled in Europe may use non-European semiconductors, which creates supply chain risks. The location of final assembly tells only part of the story. The same principle applies to cloud services. Selecting a provider

Instead of starting with the nationality or location of a supplier, start by identifying the risks that you want to protect against and then decide what you need from a supplier.

headquartered in the region may reduce certain jurisdictional risks, but it does not automatically eliminate dependency. Many sovereign cloud offerings rely on globally sourced hardware, software, AI capabilities or hyperscale infrastructure.

Nationality is not the same as capability. True digital sovereignty comes from engineered controls, operating capability and credible exit options, not from the nationality or label of a provider. As Mario Draghi highlighted in his report **The Future of European Competitiveness**, the need for domestic technology competence can be an important strategic consideration, but equally, a small domestic provider that carries a local flag may lack the scale, security capabilities and operational assurance needed to run and/or scale sovereign workloads.

Digital sovereignty is not determined by the location of a technology provider's global headquarters. It is determined by localized operational oversight, cryptographic separation, enforceable legal protections and clear jurisdictional boundaries governing how systems are operated, accessed and controlled. DXC delivers services through regional entities that are fully subject to local legislation, regulatory oversight and sovereign contractual obligations. For example, in Europe DXC can combine EU-established delivery entities, locally operated or dedicated environments, data-residency controls, appropriately vetted personnel and customer-controlled encryption-key options to address the legal, operational and technical requirements of sensitive government workloads. DXC has comparable capabilities, combined with global resilience and best practices, in other regions where digital sovereignty is a national priority, such as Australia and New Zealand, Southeast Asia, the Middle East, and Canada.

More fundamentally, before focusing on a supplier's location or nationality, it is necessary to start by assessing the technology domain in question. What are the risks to sovereignty (e.g., data exfiltration, loss of critical IP, interruption of service delivery or extrajurisdictional intervention)? These risks will vary by technology domain.

Risk mitigation can be achieved through system architecture, contract terms, security and data controls, and fallback plans to switch to alternative options. The default option of choosing a supplier simply because they are local may amount to 'sovereignty washing', addressing the appearance but not the substance of digital sovereignty, by failing to protect against the relevant risks and compromising capability unnecessarily.

Making these choices consistently requires a structured framework and a partner able to translate strategy into secure, resilient operations. With so much at stake, what do you need from a technology partner for digital sovereignty?

Critical competencies in a digital sovereignty partner

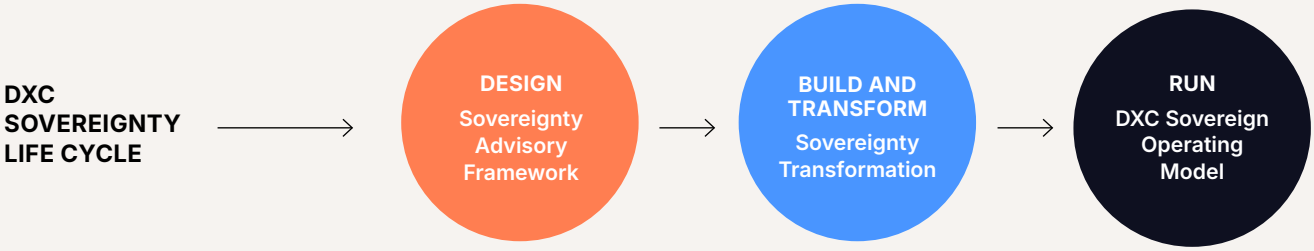
The critic H.L. Mencken famously observed: "For every complex problem there is an answer that is clear, simple and wrong." The same can be said for digital sovereignty, an inherently complex problem with few easy answers. To make the right decisions, you need to consider multiple factors: business strategy, regulation, security, procurement, IT operations and technology trends. Moreover, the cost of getting it wrong can be high. This is why you need a strong technology partner that brings deep experience and expertise across multiple domains while maintaining a neutral perspective.

DXC designs, builds and operates highly secure systems, many at the highest classification levels, for 280 public sector clients in 25 countries, supported by approximately 20,000 public sector–focused employees, with client relationships extending beyond 50 years. As a result, DXC has **deep insight into the complex technology, regulatory and business environment of government**. DXC understands how to design and operate digital sovereignty solutions to address requirements such as GDPR, ITAR, ISO 27001–aligned controls, data residency, jurisdictional access, operational continuity and credible exit options.

Sovereignty requires **deep technology expertise across the stack**: from public sector business needs and regulations to how systems are architected, where keys are held and how quickly a workload can be moved. Because DXC works across the technology life cycle from strategy and architecture to implementation and operations, our recommendations are grounded in operational reality rather than theory. We understand where sovereignty requirements introduce complexity, where trade-offs must be managed, and how to balance security, resilience, innovation, control and cost in live production environments (see **Figure 2**).

Figure 2. DXC Sovereignty Life Cycle

By operating across the life cycle, DXC is able to take on accountability for outcomes and assess trade-offs based on the full implications of decisions.

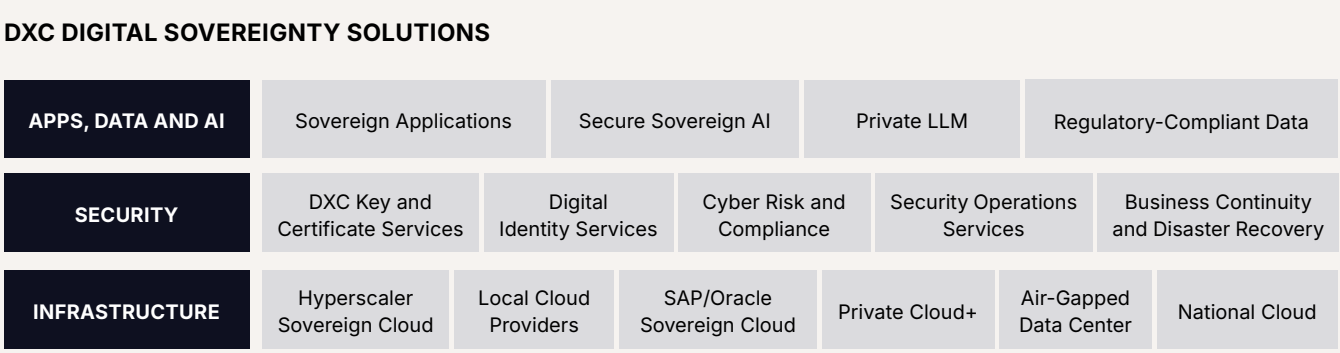


DXC's experience spans sovereign cloud adoption, mission-critical applications, secure AI platforms, enterprise technology estates, cybersecurity and managed services operations. In addition, DXC's digital sovereignty expertise is anchored in deep partnerships across the global technology ecosystem — partnerships that give us **insight into vendor solutions** while enabling us to maintain **vendor neutrality**. We can help clients objectively assess the strengths, limitations, costs and sovereignty implications of different technology choices.

Drawing on these extensive capabilities, DXC has developed a comprehensive portfolio of digital solutions, shown in **Figure 3**.

Figure 3. DXC's Digital Sovereignty Portfolio

DXC's services cover the full technology stack, providing solutions that are joined up and deliver sovereignty objectives.



DXC's end-to-end capability means we can take on complete responsibility for program delivery to meet your specific sovereignty objectives.

DXC's end-to-end sovereign capability spans the full life cycle and the complete technology estate. This means we can take on complete responsibility for program delivery to meet your specific sovereignty objectives. Equally, we can meet you where you are, supporting you at any stage in your journey to digital sovereignty:

- **Design.** The **DXC Digital Sovereignty Advisory Framework** helps organizations assess sovereignty options across technology domains, using the DXC Digital Sovereignty Triangle to evaluate trade-offs between capability, control and cost, and to select the option that is best aligned to mission requirements, risk appetite and budget. For a European public service organization, DXC developed a targeted sovereignty assessment, workload-placement model and roadmap that distinguished workloads requiring higher assurance from those that could remain in public cloud.
- **Build and transform.** Modernizing technology estates or acquiring leading edge capabilities, such as agentic AI, so that they meet demanding sovereignty objectives, are complex tasks that require highly structured and strongly governed transformation programs. **DXC Sovereignty Transformation** provides predictable delivery of complex programs across the technology stack.
- **Run.** Sovereignty solutions are only as strong as the day-to-day operations that ensure they are maintained, monitored and secured. The **DXC Sovereign Operating Model**, deployed for more than 50 clients across four continents, ensures that complex, mission-critical solutions, such as air-gapped data centers, are managed in a tightly controlled environment with dedicated secure infrastructure, local operations, security-cleared staff, controlled partner access and end-to-end governance that supports compliance and transparency.

DXC has digital sovereignty solutions for each part of the technology stack. Our customers benefit from this solutions breadth, as applications, data, security and infrastructure are intimately connected, with design choices often interdependent.

- **Applications.** DXC develops and manages applications for more than 200 clients in defense and the public sector. Our experience includes implementing and operating sovereign solutions from enterprise application providers such as SAP and Oracle. In addition, we have more than 5,000 developers with defense and national security clearances, while for some defense work we remove all business context from development tasks so they can be offshored securely to specialist technologists.
- **AI.** For agentic coding, DXC can combine the use of proprietary models from hyperscalers with on-premises models from local LLM and hosting providers to address all sovereignty concerns. For clients that require an on-premises AI capability, DXC's **Secure Sovereign AI** solution supports completely isolated networks disconnected from the public internet and protects data through hardware-based encryption and trusted execution environments. This solution was deployed for the European Space Agency to access Mistral Generative AI (see DXC's **ESA customer story**).
- **Infrastructure and cloud.** For more than 20 clients in 15 countries, DXC supports multiple sovereignty models depending on client requirements — on-premises data centers, co-located hardware, dedicated hosted environments — each chosen for greater control, security, customization or compliance. As valid as these reasons are, running your own private cloud comes with a price, carrying the full weight of life-cycle management, patching, tooling and more. For this reason, we offer **DXC Private Cloud+**, a hybrid private cloud built for enterprises and governments running sensitive and regulated workloads. Private Cloud+ is engineered as a managed private cloud environment, taking on the operational complexity for you, while delivering private cloud control, security, compliance and isolation. It combines public cloud flexibility with private cloud security, governance and control, supporting both traditional and AI workloads. Alternatively, where clients opt for sovereign cloud solutions, DXC helps organizations assess and migrate workloads to local sovereign cloud providers such as STACKIT, or to sovereign cloud solutions from global technology vendors.

DXC's commitment to digital sovereignty: Preserving operational independence and enabling strategic choice

DXC helps governments to determine the appropriate sovereignty posture for each part of their technology estate. We then help them implement that posture and make sure it remains transparent, auditable, resilient and adaptable as regulations, technologies and geopolitical risks evolve.

Our commitment is straightforward: helping governments achieve digital sovereignty in a way that protects critical services, preserves operational independence, retains strategic choice and sustains access to the digital capabilities on which their mission depends.

Authors



David Rimmer
Global Industries Leader, Consulting & Engineering Services,
DXC Technology

David Rimmer leads Global Industries within DXC's Consulting & Engineering Services business. Previously he was responsible for DXC's global public sector in the aerospace and defense industry. Throughout his 25+ year career, David has helped numerous government and defense clients around the world transform their digital operations while keeping their systems resilient and secure.



Yves Vanderbeken
DXC Fellow and Public Sector Industry Managing Partner,
DXC Technology

Yves Vanderbeken is a DXC Fellow and public sector technology strategist. He works with government leaders on AI, digital sovereignty, platform transformation and service modernization. As thought leader in Government as a Platform, he helps organizations build resilient, citizen-focused digital services.



Richard Wilkinson
Chief Technologist, Europe, Global Infrastructure Services,
DXC Technology

Richard Wilkinson is chief technologist for DXC's Global Infrastructure Services business in Europe. Based in Paris, Richard has 30 years of international experience building and leading technology and consulting teams, including in solution architecture, service transition, post-merger integration and service management. A frequent conference speaker, Richard advises leaders on digital sovereignty and agentic AI.

Learn more at

dxc.com/agentic-gov

DXC Technology (NYSE: DXC) is a leading enterprise technology and innovation partner delivering software, services, and solutions to global enterprises and public sector organizations — helping them harness AI to drive outcomes at a time of exponential change with speed. With deep expertise in Managed Infrastructure Services, Application Modernization, and Industry-Specific Software Solutions, DXC modernizes, secures, and operates some of the world's most complex technology estates. Learn more on **dxc.com**.

LinkedIn | Instagram | TikTok | YouTube

© 2026 DXC Technology Company. All rights reserved. DG_1654a-27