

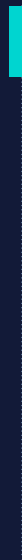
A horizontal bar with a gradient from light blue to dark blue, positioned behind the word "Digital".

Digital Sovereignty

From policy ambition to
executive imperative

Table of contents





Executive summary

In a globalized, highly connected economy, digital transformation creates a network of dependence. Amid an environment characterized by mounting geopolitical tensions, labyrinthine regulatory complexity, a mesh of extraterritorial laws, and ever more frequent and ambitious cyberattacks, the failure of a single technology provider can trigger cascading disruption around the world.

Over the past decade, organizations have optimized for speed – cloud migration, AI deployment, and digital scale – often faster than the evolution of governance and resilience models, resulting in accumulated and sometimes poorly understood dependencies. Digital sovereignty is a response to this imbalance: ensuring that speed does not undermine resilience, control, or the ability to operate under pressure. These foundations, in turn, enable faster innovation and technology adoption.

Such a delicately balanced situation has exposed critical vulnerabilities, especially in Europe, where more than 80% of digital products, services,

infrastructure, and intellectual property (IP) are imported.¹ This growing exposure is now being actively addressed at the policy level, with the European Union's recently adopted Tech Sovereignty Package – including the Cloud and AI Development Act (CADA) – marking a structural shift toward setting standards and strengthening regional control over critical digital infrastructure and capabilities.²

Digital sovereignty has now reached an immediate inflection point as AI dependency intensifies, geopolitical pressures reshape technology access and control, and the European Union's Tech Sovereignty Package accelerates the shift from policy intent to operational and strategic action.

Organizations around the world are asking urgent questions about securing and strengthening strategic autonomy, resilience, and speed to value without compromising competitiveness or stymying innovation.

In this first edition of what will become a regular series, we explore how organizations around the world are navigating these complexities. Our research reveals four key themes shaping organizational approaches to digital sovereignty:

- **Digital sovereignty has entered the mainstream as a strategic business priority**
Digital sovereignty is no longer confined to public policy debates. Increasingly, executives place it alongside core enterprise concerns such as cybersecurity, resilience, and competitiveness. In fact, 93% of organizations worldwide have discussed digital sovereignty at board level, and half have appointed, or are considering appointing, a chief sovereignty officer.
- **Digital sovereignty focuses on resilient interdependence rather than absolute independence**
Most organizations recognize that in a deeply interconnected global ecosystem, full control

Executive summary

across the tech stack is neither feasible nor desirable. Rather, they focus on maintaining strategic autonomy by selectively managing dependencies, retaining control over critical assets, and ensuring flexibility to adapt to geopolitical and regulatory shifts. Globally, 69% of organizations agree that digital sovereignty requires the capacity to choose technological dependencies. Just over half (54%) agree that they can strengthen their digital sovereignty without sacrificing competitiveness.

- **Organizations face significant technology dependency risks**

Dependency on global suppliers remains widespread across cloud, software, hardware, and connectivity. Structural constraints such as high concentration of suppliers, limited visibility beyond Tier 1 suppliers, and long switching timelines drive this dependency and increase exposure to disruption. They also limit organizations' ability to respond quickly to adverse conditions.

- **Organizations are taking a pragmatic approach to their pursuit of digital sovereignty**

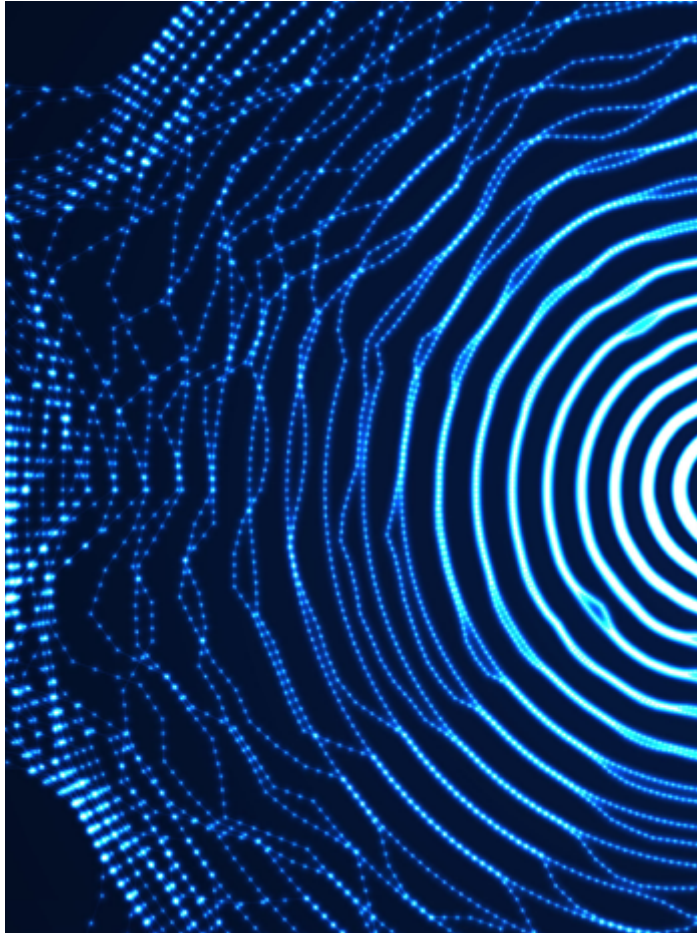
A majority (59%) of organizations agree that, in today's ecosystem structure, full digital sovereignty is unrealistic. Instead, most organizations are considering adopting hybrid models based on federated control and managed interdependence. This aligns with a minimum viable digital sovereignty approach, a pragmatic, risk-based framework that defines the smallest set of capabilities, assets, and controls that must remain under direct or assured control to safeguard critical operations.

These approaches help organizations balance control and resilience with access to global innovation, scale, and performance. Our research shows that digital sovereignty is not only about reducing risk; it also creates the trust, flexibility, and resilience needed to accelerate AI adoption, collaborate across ecosystems, and innovate with

confidence. At its core, it is about choice, control, portability, and trusted partnerships.

Overall, these findings highlight a clear shift: digital sovereignty is evolving from a policy-driven concept into a business-critical capability. While governments drive digital sovereignty through policy, investment, and ecosystem development, organizations are focusing on resilience, controllability, and managed dependencies as tangible levers within their control. To navigate this transition effectively, organizations should:

- Embrace digital sovereignty as a board-level strategic topic
- Assess exposure of critical business operations
- Prioritize interventions based on business impact and risk tolerance
- Build resilience and control into the operating model
- Foster innovation ecosystems through managed interdependence



Who should read this report and why?

This report is intended for business and technology leaders, including CIOs, CTOs, CDOs, chief data and security officers, as well as executives responsible for risk and compliance across industries. It is informed by a comprehensive global survey of 1,300 executives, complemented by in-depth interviews with leaders across industry, technology, and policy.

Our research provides unique and timely insights into how organizations are approaching digital sovereignty, including the risks, trade-offs, and strategic choices involved in balancing control, resilience, and innovation. It brings together

perspectives on dependency, governance, cost, and operating models to help organizations navigate an increasingly complex geopolitical and regulatory landscape.

As such this report is relevant to organizations seeking to strengthen resilience, reduce dependencies, and build sustainable digital sovereignty strategies.

For more details, see the research methodology at the end of the report.

How we define digital sovereignty

For the purposes of this research, 'digital sovereignty' refers to an organization's capability to be resilient, to have strategic autonomy, and be free from external interference for critical workloads across the digital value chain, including cloud, data, AI, energy, hardware, software, cybersecurity, and connectivity.

We define the tech stack as including the following dimensions:

1. **Cloud:** architecture, management, portability, reversibility, recovery, governance and control
2. **Data:** classification, storage, processing, cross-border handling, sharing, residency, and recovery
3. **AI:** AI models, platforms, deployment, compute infrastructure, access control, monitoring, and governance
4. **Energy:** the power supply for digital infrastructure
5. **Hardware:** data centers, servers, storage systems, network equipment, semiconductor components, and devices

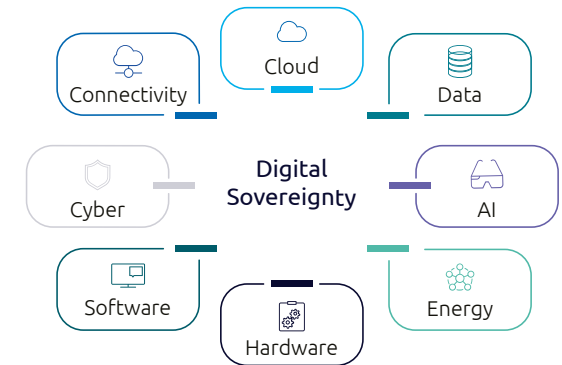
6. **Software:** operating systems, virtualization layers, middleware, databases, orchestration platforms, and applications
7. **Cybersecurity:** encryption, confidential computing, identity and access management, and incident response
8. **Connectivity:** fixed, mobile, cross-border networks including 5G/6G, private networks, fiber, and satellite

Digital sovereignty requires control across operations, data, technology, and jurisdiction to ensure resilience and compliance under external pressure.

- Operations: Control over how services are delivered and managed, including service ownership, staffing location, operational authority, and incident response
- Data: Control over how data is stored, accessed, and processed, including residency, encryption, access rights, and cross-border data flows
- Technology: Control over underlying platforms and dependencies, including portability, reversibility, platform concentration, and supply chain exposure
- Jurisdiction: Control over legal and regulatory exposure, including which laws apply, where data and operations reside, and how cross-border obligations are managed.

Figure 1.

Dimensions of the tech stack included in Capgemini's definition of digital sovereignty



Source: Capgemini.

01 | Digital sovereignty has entered the mainstream

Digital sovereignty is now a key strategic business concern

Geopolitical fragmentation and extraterritorial regulation, the acceleration of AI and concentration of technology power, and increasing exposure through globalized digital supply chains are the key structural shifts reshaping the digital landscape. Digital sovereignty is no longer a theoretical topic of discussion confined to public policy debates. Now, it is a strategic business concern alongside cybersecurity risk, resilience, and competitiveness.

47%

of executives globally view digital sovereignty as a risk-mitigation/resilience-building approach

These strategic dependencies, exacerbated by the fragile global operating environment, emphasize the criticality of digital sovereignty. Vivek Sharma, Head of Global Partner and Vendor Management at Bosch, a European software development company, says: *“Rather than simply a technical topic, we are increasingly viewing digital sovereignty as a strategic business discussion that touches business resilience, geopolitical risk, supply-chain stability, regulatory compliance, and long-term competitiveness. Put simply, it is having sufficient control and strategic autonomy over critical digital capabilities that we can operate reliably, even when conditions change.”*

Globally, 47% of executives primarily view digital sovereignty as a risk-mitigation/resilience-building approach; about a third view it as a compliance requirement; and one in five as a competitive differentiator (see Figure 2). By region, a smaller share of UK and US respondents see digital sovereignty as a competitive differentiator compared with their peers from APAC and continental Europe.

Riccardo Picca, Senior Director, Global Digital Transformation and Business Excellence at Thermo Fisher, an American life sciences company, states: *“Digital sovereignty is less about isolation and more about controlling interdependence: retaining decision rights, visibility, and resilience across critical parts of the digital value chain. In a regulated pharma environment, it spans data sovereignty, cloud and platform dependence, AI model control, manufacturing continuity, and cybersecurity for regulated operations.”*

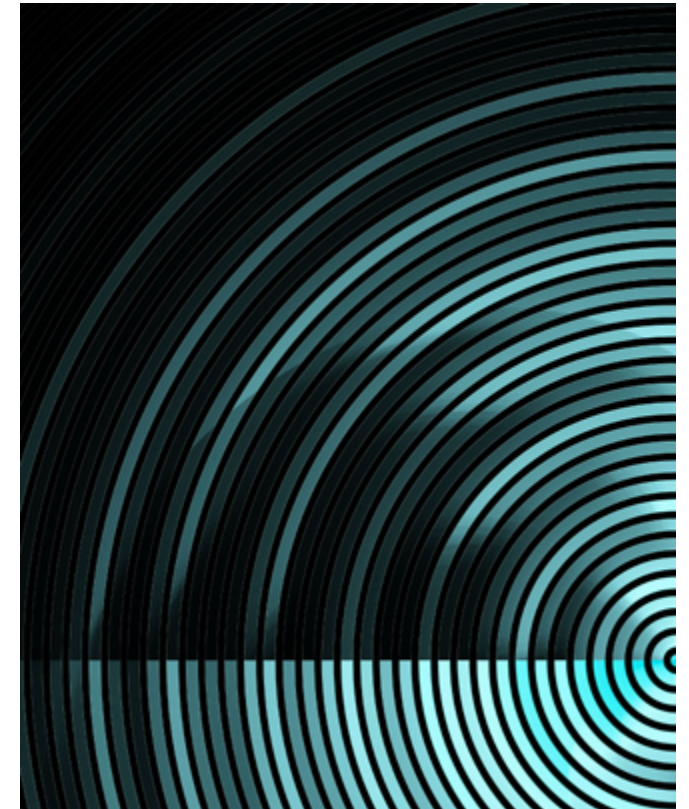
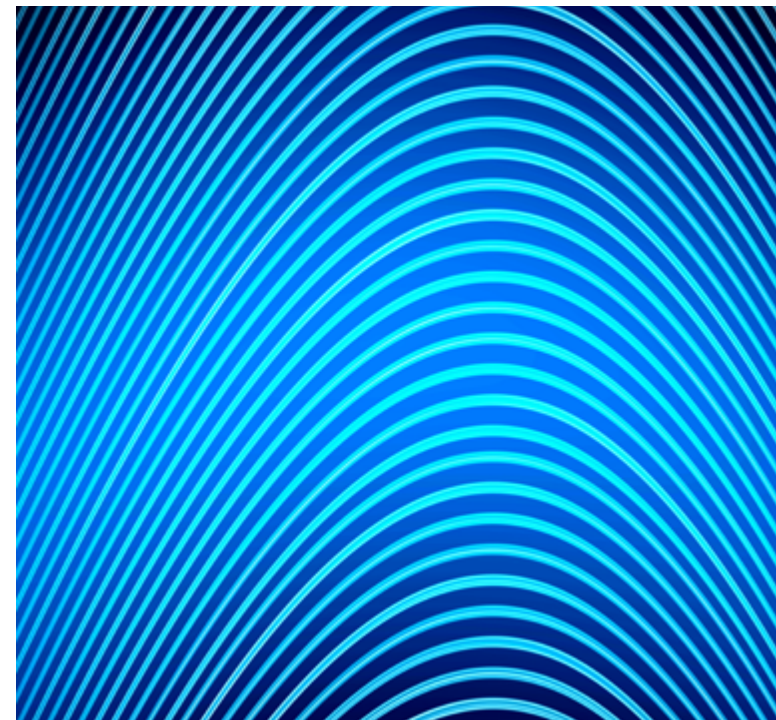
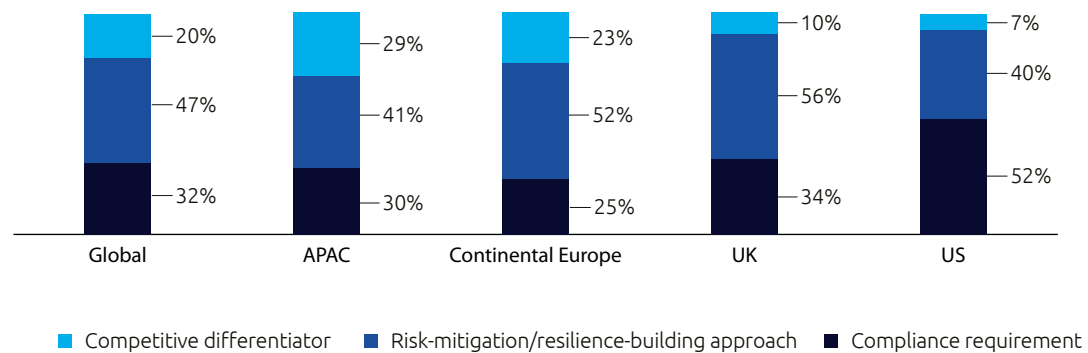


Figure 2.

47% of executives view digital sovereignty as mitigating risk and building resilience

Principal view of digital sovereignty, by region



Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.



“Digital sovereignty is no longer just a policy issue. It is a core business imperative, shaping how organizations manage risk, safeguard operations, and compete in an increasingly interdependent digital world.”

Fernando Alvarez

Chief Strategy and Development Officer, Capgemini

Digital sovereignty is no longer optional

Our research reveals that digital sovereignty is no longer a purely technical concern, but a strategic and operational topic. Three out of four organizations (76%) worldwide are highly concerned about securing critical business operations amid current geopolitical tensions (see Figure 3).

Escalating US-China technology competition and export-control measures demonstrate ways in which geopolitical developments can shape access to critical technologies. Similarly, the April 2025 blackout across Spain and Portugal demonstrated how failures in foundational infrastructure can cascade across telecommunications, transportation systems, emergency services, and other public services.³

Additionally, changes in vendor concentration and licensing can expose commercial dependency risks. For example, following Broadcom's acquisition of VMware, organizations

faced significant licensing and commercial model changes, including subscription-only models, portfolio rationalization, revised purchasing requirements, and amended renewal terms.⁴

Collectively, these events underscore the growing exposure of organizations to concentrated dependencies across the digital value chain. Reflecting these concerns, nearly two-thirds (65%) of organizations concur that excessive reliance on foreign providers poses a significant risk to digital resilience.

Bernd Meurer, Field Chief Technology Officer, Europe at BT Group, notes: *"Customers fear that foreign governments or legislation could harm their business in a political situation. They often refer to such a scenario as the 'kill switch.' Beyond that, there are sector-driven concerns in areas like health, defense, and high-tech, where data security and access risk are paramount. That is why the topic has moved from being a niche discussion into a broader executive concern about resilience and continuity."*

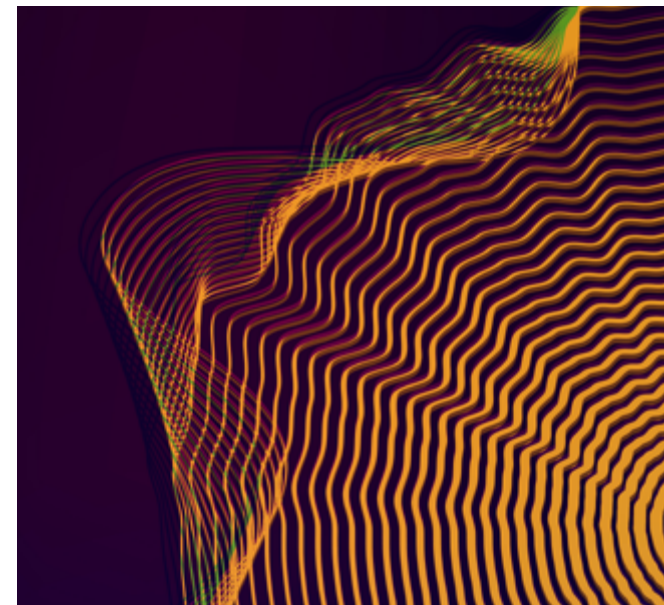
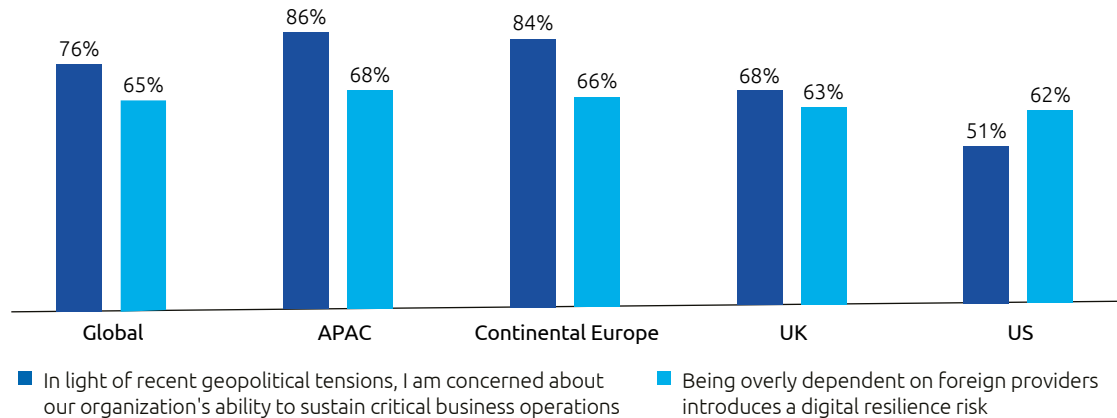


Figure 3.

76% of executives are concerned about sustaining business operations

Percentage of organizations who agree with the statements below, by region

Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

Digital sovereignty is on the boardroom agenda

Over 9 in 10 organizations worldwide, consistent across countries, regions, and industries, have discussed digital sovereignty with their boards. Among those organizations:

- 31% actively supervise it as a strategic agenda item with dedicated board governance
- 26% regularly monitor it as part of their risk portfolio
- 36% periodically review it or have ad-hoc discussions

Digital sovereignty is the top board-level priority for 44% of organizations. This increases to 59% in aerospace and defense, 57% in telecom, and 56% in financial services. Examples of key decisions that boards must make regarding digital sovereignty include acceptable dependency levels, control thresholds, and investment trade-offs.

93%

of organizations worldwide have discussed digital sovereignty with their boards

Skerdi Cerga, Chief Technology and Security Officer, Trillium Health Partners, a regional hospital system, explains: *“When data residency, privacy impact, and jurisdiction exposure are involved, decisions require cross-functional review and leadership oversight, especially when exceptions are requested.”*

Kartik Iyer, a global procurement and supply chain leader, goes further: *“Digital sovereignty is a topic of discussion at C-suite and board levels. The CTO or CIO usually leads. Decisions about vendors, supplier strategies, and operating models become strategic because they determine the level of dependency and control.”*

Governments are also making digital sovereignty a strategic priority with shared criteria. France’s High Commission for Strategy and Planning recently created the Observatory for Digital Sovereignty. The Observatory will publish data on dependence on non-sovereign digital solutions, helping to identify systemic vulnerabilities.⁵

A European government official shares: *“The lack of European digital giants has widened the GDP per capita gap with the US and undermined the ability to promote European values through technology. Independence and competitiveness are not mutually*

exclusive. The pursuit of digital sovereignty is a matter of values and long-term necessity, rather than a short-term economic calculation. We need to rebuild an ecosystem conducive to digital innovation with the necessary investment for companies to prosper.”

Most organizations have a digital sovereignty strategy in place or are planning one

The majority (79%) of organizations globally are either executing or building a strategy. An additional fifth of organizations are working towards putting a strategy in place in the next year. This data is consistent across regions (see Figure 4). Gartner suggests that, by 2030, more than 75% of organizations outside the US will have a dedicated digital sovereignty strategy – often anchored in a ‘sovereign cloud’ approach.⁶ This data is in line with our survey results for non-US organizations.

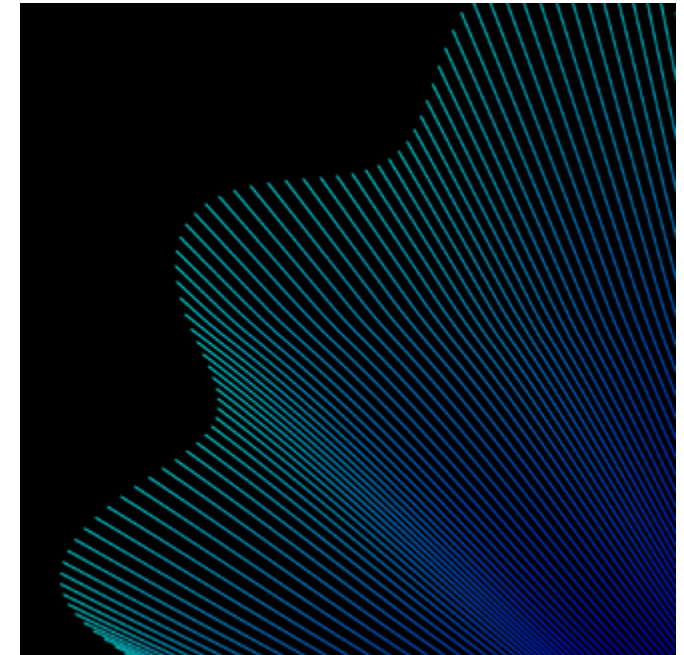
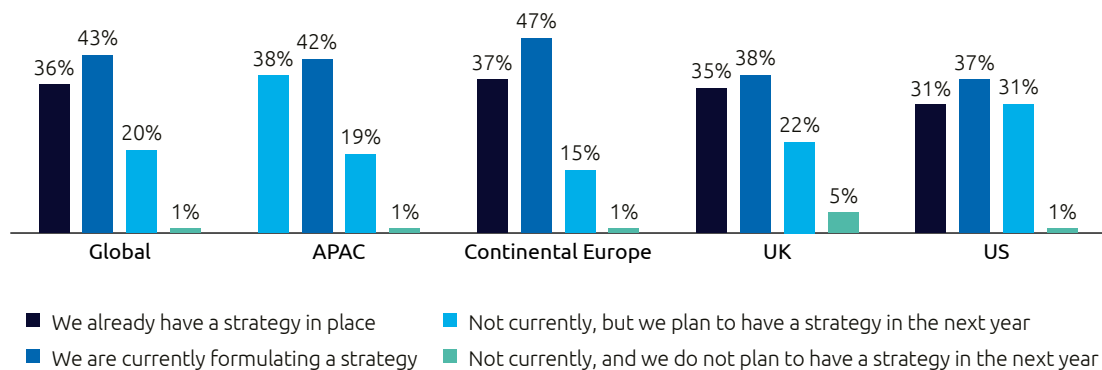


Figure 4.

Nearly eight in 10 organizations either have a strategy or are creating one

Stage of digital sovereignty strategy by region



36%

of organizations globally already have a digital sovereignty strategy in place

Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

Data, cybersecurity, and cloud are central

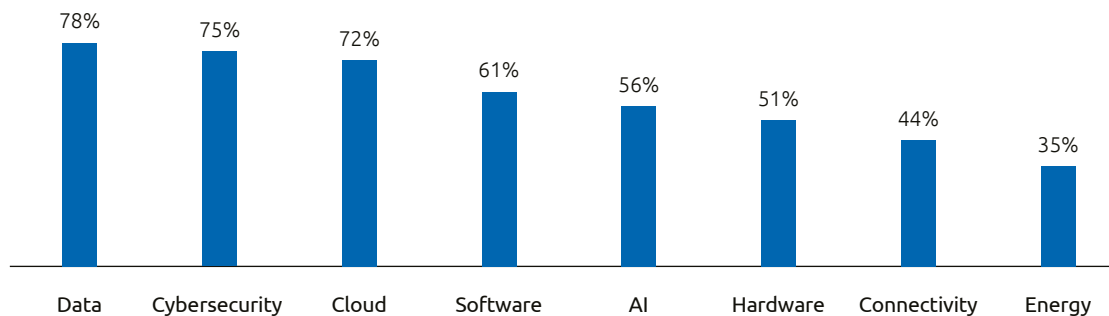
Nearly 8 in 10 organizations include data in their definition of digital sovereignty. This includes data classification, storage, processing, cross-border handling, sharing, residency, and recovery. Three quarters include cybersecurity (i.e., encryption, confidential computing, identity and access management, and incident response) and 72% encompass cloud (i.e., architecture, management, portability, reversibility, recovery, governance and control). Energy is the least considered (35%) dimension in relation to digital sovereignty (see Figure 5).

Vivek Sharma of Bosch adds: *“If you have a heavy concentration on a very small number of hyperscalers, it raises questions around portability, resilience, and strategic dependency. A close second is data and AI platforms. How the model is trained and who controls the underlying platform becomes a digital sovereignty concern.”*

Figure 5.

78% of organizations ensure data is part of their digital sovereignty approach

Percentage of organizations who consider the following tech layers when addressing digital sovereignty



Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

Around half of organizations have appointed or are considering a chief sovereignty officer

One in 10 organizations in our survey say they have already appointed a chief sovereignty officer or similar role in its C-suite, and 4 in 10 are considering it. The split is largely consistent across regions with US organizations showing slightly more urgency compared with their APAC and UK peers (46% versus 36% and 38%, respectively; see Figure 6). By sector, 50% of life sciences organizations say they are considering a chief sovereignty officer, compared with 32% among consumer products and retail organizations.

Deutsche Telekom recently created a chief sovereignty officer position with former CTO Christine Knackfuß-Nikolic taking on the role in September 2025. Her mandate is to define and

execute an organization-wide sovereignty strategy tailored to customer-specific, regulatory, and geopolitical requirements. A key focus is on developing differentiated value propositions across the portfolio to address the diverse sovereignty challenges clients face.⁷

Ferri Abolhassan, CEO of T-Systems and member of the Telekom Board of Management, highlights: *“The call for digital sovereignty is growing louder. Due to geopolitical uncertainties, more and more companies in Germany and Europe are demanding sovereign cloud solutions.”*⁸

French multinational telecom Orange has also strengthened its leadership in this domain by appointing Guillaume Poupard as Group Chief Trust Officer, effective February 2026. Reporting directly to the CEO, this role reflects Orange’s strategic prioritization of accelerating its digital sovereignty and trust strategy in a fast-evolving geopolitical context.⁹

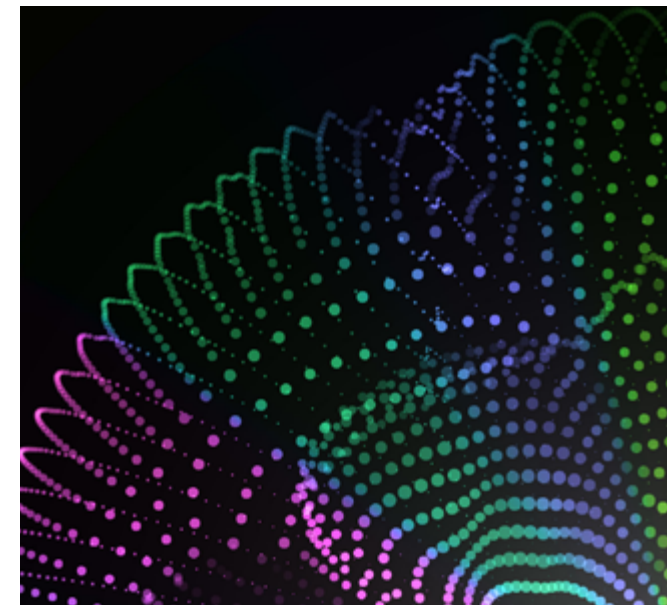
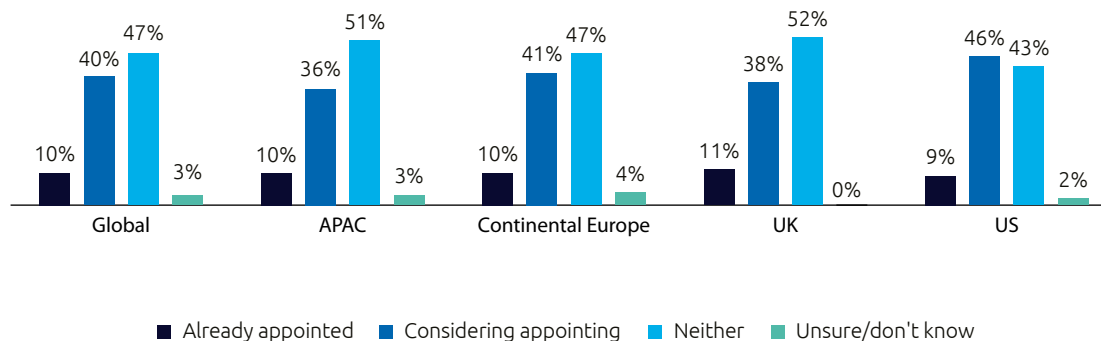


Figure 6.

Half of organizations have appointed or are considering appointing a chief sovereignty officer

Stage of appointing a chief sovereignty officer or equivalent, by region



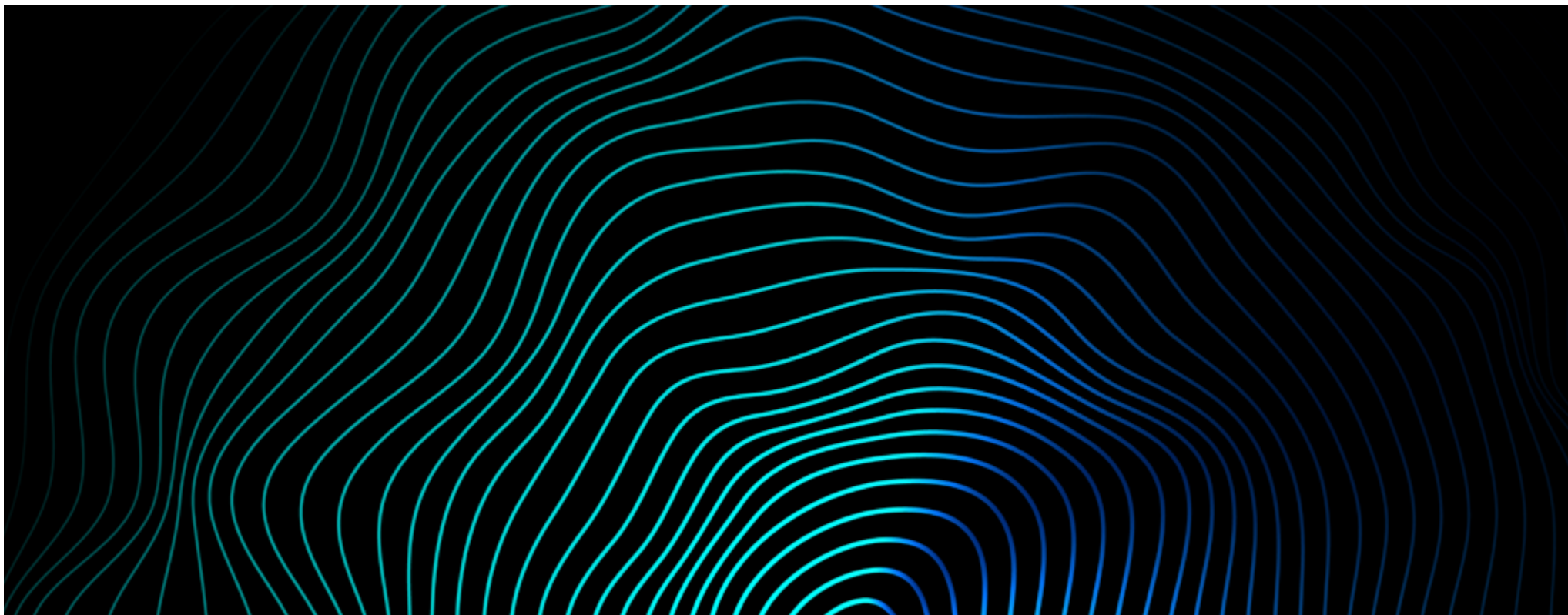
Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

Formal budgets to pursue digital sovereignty have been allocated across geographies

Globally, most (65%) organizations have allocated budget to digital sovereignty. This share is broadly consistent across regions (e.g., 68% in APAC, 66% in continental Europe, 59% in the US). The digital sovereignty budget is most commonly part of IT modernization (35%). A quarter of organizations (25%) group it with risk/compliance spend and just under a quarter (23%) have the budget as part of a dedicated investment program.

10%

of organizations worldwide have already appointed a chief sovereignty officer or equivalent





02

**Digital sovereignty means
resilient interdependence
not absolute independence**

Organizations must balance growth with control

Global providers enable scale and AI acceleration, but they also create strategic dependencies. Digital sovereignty is about careful selection and pragmatic management of dependencies to promote strategic autonomy, while sustaining resilience and competitiveness. Globally, nearly 70% of organizations agree that digital sovereignty means the capacity to choose technological dependencies and just over half (54%) agree that they can strengthen their digital sovereignty without sacrificing competitiveness (see Figure 7). Less than a third (30%) disagree that they can strengthen digital sovereignty without sacrificing competitiveness and 16% remain neutral.

A procurement leader at a global multinational automaker explains: *"The workable model is controlled interdependence: you don't build everything yourself, but you ensure no single partner is too big to fail or too powerful to leave you. That is why keeping control over encryption keys and data architecture matters, so you can unplug and move to another provider over time."*

54%

of organizations globally agree that they can strengthen digital sovereignty without sacrificing competitiveness

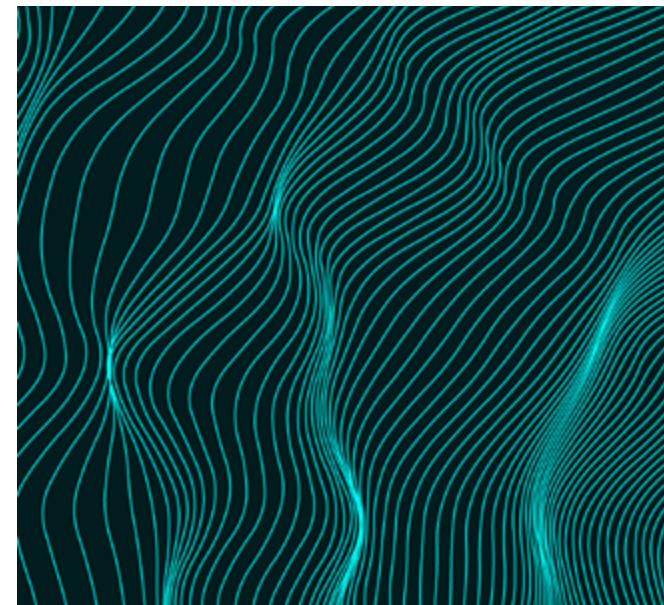
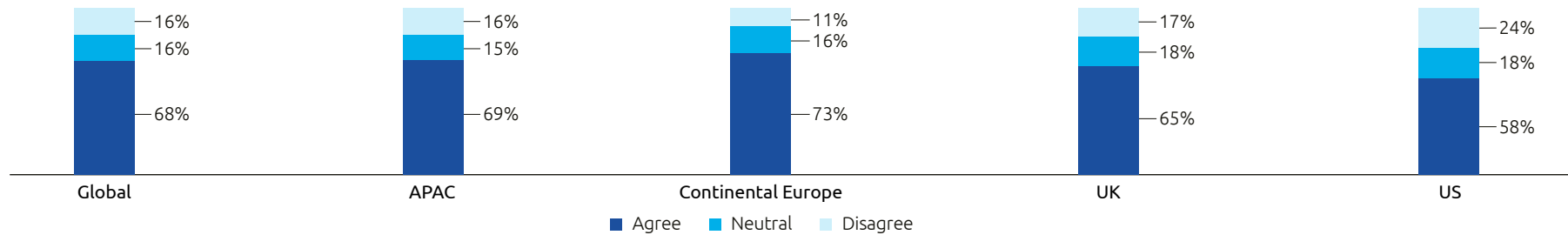


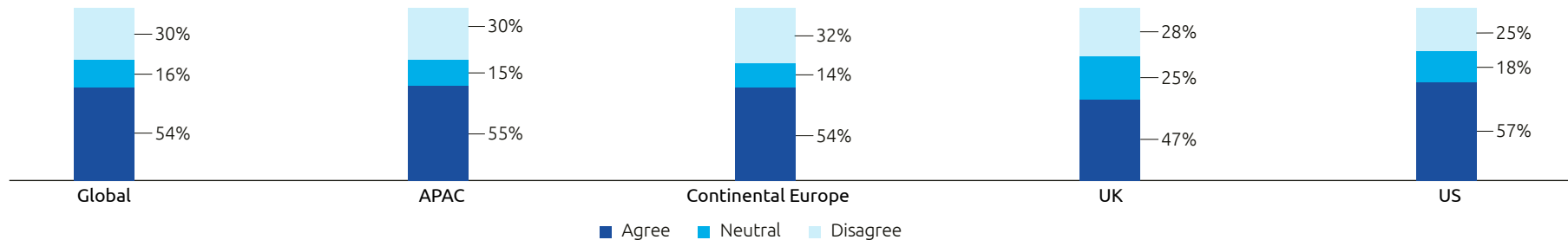
Figure 7.

Half of organizations believe digital sovereignty does not require a sacrifice of competitiveness

Percentage of organizations who agree with the statement by region: Being digitally sovereign means having the capacity to choose technological dependencies



Percentage of organizations who agree with the statement by region: Our organization can strengthen digital sovereignty without sacrificing competitiveness



Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

Digital sovereignty is not about isolation but interdependence

Sixty-seven percent of organizations agree that digital sovereignty is defined by resilient interdependence. In the US, this share drops to 50% and in continental Europe rises to 75% (see Figure 8). This approach is reflected in emerging regulatory models. For example, the EU's Cloud and AI Development Act (CADA) introduces an EU wide sovereignty framework that assesses cloud and AI services across multiple assurance levels, linking requirements to the sensitivity of use cases. Rather than mandating full technological independence, CADA adopts a risk based, industry-focused, tiered approach. Union Assurance Level (UAL) 1 to 3 allows participation of non EU controlled providers under progressively stricter conditions, while UAL 4 requires full EU control with no derogation.¹⁰

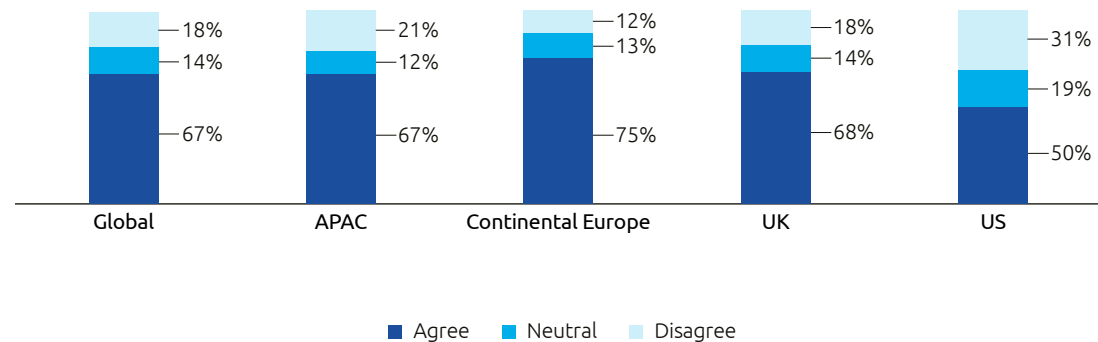
The ways in which organizations can build resilient interdependence include:

- **Multi-cloud:** diversifies dependencies across multiple providers to avoid concentration risk
- **Encryption key ownership:** ensures a provider cannot access data without authorization and reduces exposure to extraterritorial laws

Figure 8.

Most organizations agree that digital sovereignty is more about interdependence than isolation

**Percentage of organizations who agree with the statement by region:
Digital sovereignty is defined more by resilient interdependence than isolation**

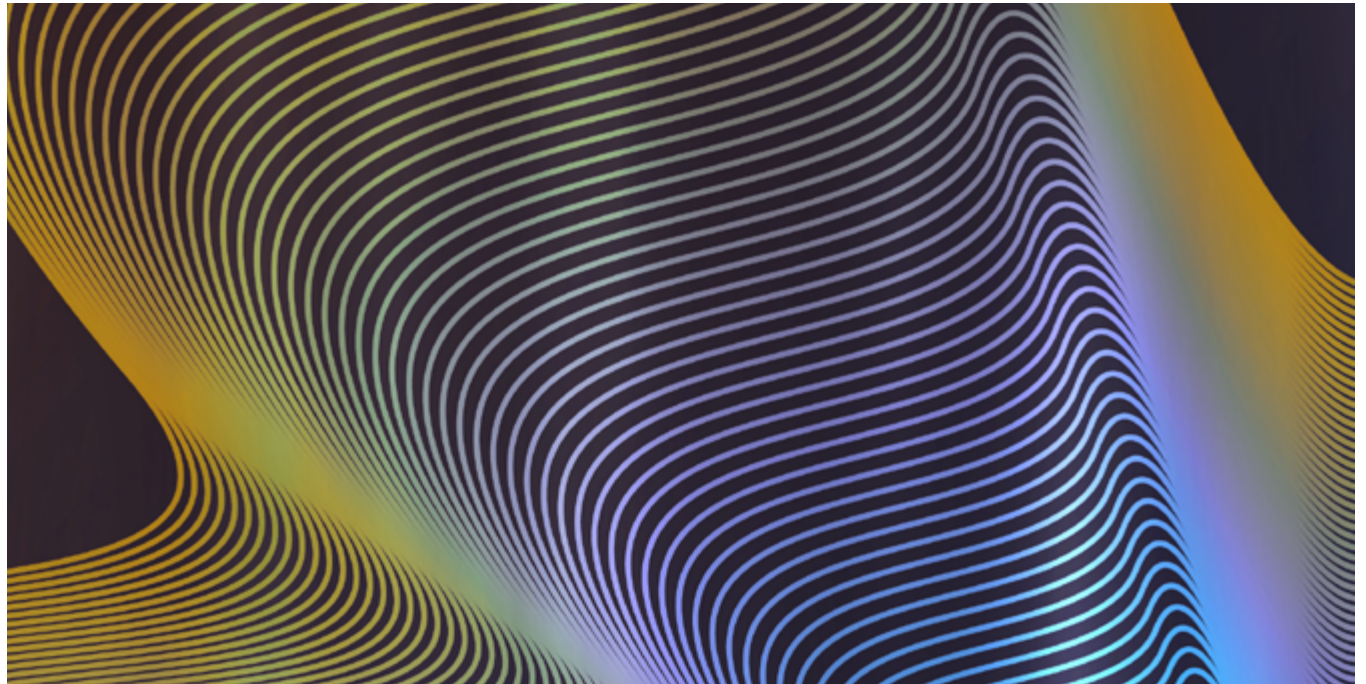


Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

- **Exit strategies:** grants the ability to migrate workloads, switch providers, maintain continuity under disruption if the dependency must be reversed
- **Local operations:** ensures compliance with national laws, reduced exposure to foreign intervention, and operational continuity.

Thermo Fisher's Picca says: *"It is important not to try to eliminate dependency; but to try to manage risk exposure. Full end-to-end digital sovereignty is neither feasible nor desirable because the ecosystem is too interconnected and globally integrated, and innovation is concentrated among a few hyperscalers and AI leaders. Replicating that internally would be extremely expensive and inefficient. The goal is managed interdependency with resilience, avoiding lock-ins in critical domains."*

Charles-Pierre Astolfi, Chief Information Officer at France's National Institute of Geographic and Forest Information (IGN), explains: *"As a public institution, we see digital sovereignty as primarily about substitutability – using solutions that can be replaced – and control over supply chains. It is fundamentally a risk management issue, including managing dependencies and controlling access to data."*





“Being sovereign means having the ability to choose your dependencies. For organizations – especially in Europe – the goal is not full autonomy, but a clear understanding of technological dependencies, so they can move from dependence to interdependence.”

Karine Brunet

Chief Operations and Delivery Officer, Capgemini

Digital sovereignty exists on a spectrum

Most (59%) organizations in our survey admit that full digital sovereignty is not a realistic goal. Twenty-eight percent of organizations believe that full digital sovereignty can be realistic and 13% remain neutral. Raquel Poncela, Director of Digital Services and Innovation at the Spanish Royal Mint, agrees: *“Digital sovereignty is synonymous with strategic autonomy. But as a provider of critical national infrastructure, including currency and digital identity services, we maintain contingency options and a spectrum of digital sovereignty for critical workloads. For example, hosting critical services or highly regulated workloads in our own data centers while remaining open to cloud solutions for non-critical workloads and processes.”*

Consider AI infrastructure where supply chains are inherently global: chips are designed in the US and manufactured in East Asia, while models are trained on datasets spanning multiple countries, and applications are deployed across jurisdictions. In this context, maintaining digital sovereignty requires moving beyond a defensive model of self-reliance toward an approach focused on orchestration, balancing national autonomy with strategic partnerships.¹¹

Operational resilience, autonomy, and risk mitigation are the dominant drivers

Organizations frame digital sovereignty largely as a pragmatic risk, resilience, and control agenda. The strongest motivators to pursue digital sovereignty today are:

- Operational resilience to geopolitical volatility and disruptions (80%)
 - A Gartner study finds that three in five of the surveyed Western European CIOs and IT leaders said geopolitical factors will increase their reliance on local or regional cloud providers.¹²
- Greater autonomy and control over data, models, and IP (76%):
 - Governments and organizations operating in highly sensitive, critical sectors prefer to retain ownership and control over core technologies, cybersecurity frameworks, and data assets.

– This push is increasingly reflected in policy. For example, the EU plans to propose stricter non-price sovereignty requirements for state tenders in sensitive sectors, potentially limiting access for non-EU hyperscalers. These measures are driven not only by concerns over the dominance of foreign technology providers but also by regulatory risks, such as the US Cloud Act, which allows authorities to access data held by US-based providers, even if it is stored overseas.¹³

- Risk mitigation and security assurance (76%)
 - Taiwan continues to dominate global chip production, accounting for over 90% of leading-edge semiconductor manufacturing.¹⁴ Its central role in the global supply chain has placed greater emphasis on its de facto autonomy. Moreover, it has made the deterrence of hostilities from Chinese against Taiwan a strategic priority for the US and its allies (this initiative is often referred to as the ‘Silicon Shield’). According to the US Commerce Secretary Howard Lutnick, the goal is to relocate up to 40% of Taiwan’s semiconductor supply chain to the US,¹⁵ although Taiwan has pushed back on the feasibility of this goal.¹⁶
 - Brussels is preparing its EU Chips Act 2.0 to boost regional semiconductor manufacturing and reduce reliance on external providers, following supply disruptions and geopolitical sensitivities around

acquisitions, including the takeover of chipmaker Nexperia by China's Wingtech.¹⁷

- Reduced dependency on foreign tech providers and infrastructure (74%)
 - Currently, three US participants, AWS, Microsoft and Google, control more than 70% of the EU cloud market.¹⁸
 - To reduce these dependencies, the European Commission is actively investing in sovereign alternatives. In April 2026, it awarded an €180 million (\$207 million) tender for sovereign cloud services to four European providers over a six-year period, as part of a broader push to reduce the dependency on non-European providers and reinforce strategic control

59%

of organizations worldwide agree that full digital sovereignty is unrealistic in today's ecosystem structure

across key technologies and infrastructure.¹⁹

- Better transparency, auditability, and accountability (74%)
 - Organizations are seeking greater visibility on how data is processed, where it resides, and how AI models are trained and governed. Jai Haridas, VP and GM, Regulated and Sovereign Cloud at Google Cloud, asserts: *"It is not enough for us to say a control exists. We need to demonstrate that it operates continuously, is actively monitored, and remains auditable."*²⁰
 - Regulations such as the EU AI Act introduce requirements around transparency, explainability, accountability, record-keeping, and human oversight for AI systems, particularly in high-risk applications.²¹

Globally, the least cited reasons for pursuing digital sovereignty are:

- Political expectations (higher in continental Europe than in the US: 57% versus 29%)
- Localized innovation (higher in continental Europe than in the US: 56% versus 34%)
- Alignment with local values, ethics, and societal priorities (higher in continental Europe than in the US: 61% versus 37%)
- National security concerns (higher in continental Europe than in the UK and the US: 65% versus 46% and 50%, respectively)

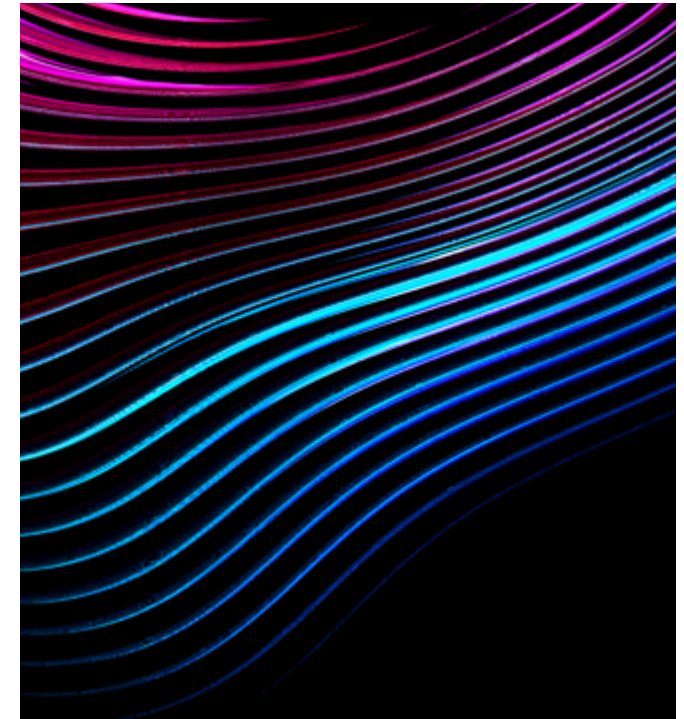
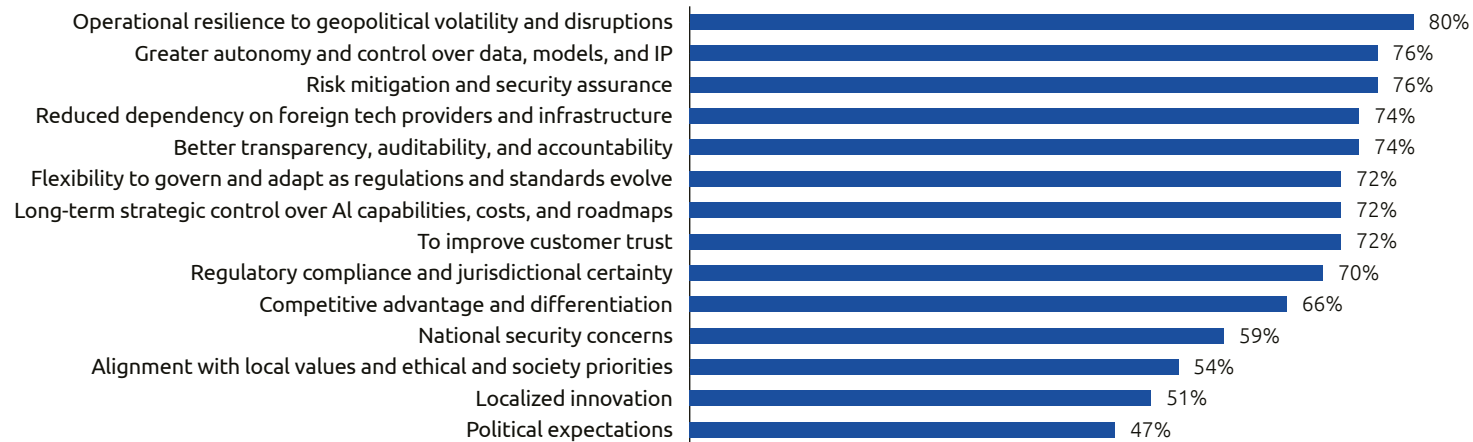


Figure 9.

Eight in 10 organizations say operational resilience is the key motivator for digital sovereignty

Percentage of organizations who are motivated to pursue digital sovereignty today for the reasons below

Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

Insights from a public sector official



Jean-Baptiste Courouble

Chief Information Officer, URSSAF (Organizations for the Collection of Social Security and Family Benefit Contributions)

URSSAF is a network of private organizations whose mandate is to collect employee and employer social security contributions that finance the general account of France's social security system, including state health insurance.

What does digital sovereignty mean for a public sector organization like yours?

"I see digital sovereignty in the same way as energy dependence. Today, energy dependency is clearly recognized as a major geopolitical issue, driving major policy decisions, such as nuclear energy in France. Digital dependency, however, has only recently been understood at the highest levels,

mostly due to geopolitical events, cyberattacks, and new data protection regulations. Also, the behavior of software vendors – especially those in monopolistic positions – reduces our freedom of choice. For URSSAF, this translates into three priorities: protecting highly sensitive data (e.g., health and income data), managing rising infrastructure and software costs, and ensuring service continuity as reliance on external and SaaS services increases."

Which dependencies matter most today?

"The most critical risk is no longer dependency itself but losing the ability to choose. The worst-case scenario is being locked into a dependency with no viable alternative. We have launched a program to formally assess and evaluate the potential to exit 'captive vendors'. It helps us decide what is feasible, what is financially justified, and what risks are mitigated. Not all exits are possible; we must sometimes accept constraints."

How are you approaching digital sovereignty in practice?

"Importantly, digital sovereignty does not mean '100% French solutions.' That is not realistic. However, we do

have a responsibility to support domestic industry. For example, the EU spends an estimated €264 billion on US cloud software services.* At the same time, Europe lacks some capabilities (e.g., chips, GPUs), so full independence is unrealistic. The approach must be pragmatic. At URSSAF, efforts focus on reducing exposure to high-risk dependencies through structured initiatives such as dependency mapping, prioritization, and ROI-based decision-making. The objective is not to eliminate dependencies, but to manage those that impact resilience, continuity, and cost trajectory."

What will determine success over the next few years?

"Three factors are critical. First, AI-related decisions will shape long-term dependency risks, making early strategic choices important. Second, achieving greater digital sovereignty requires sustained investment, often competing with business priorities. Finally, no organization can address these challenges alone; progress will depend on alliances, shared solutions, and stronger public-private collaboration. We need partners to integrate existing European solutions into a cohesive service offering. The value lies in integration and service delivery, not necessarily in inventing new products."

Source: Capgemini Research Institute interview, June 4, 2026.

*Asterès economic study, "Technological dependent on American software and cloud services: an assessment of the economic consequences in Europe," April 2025.



03

Organizations face significant technology dependency risks

When asked which layers of the technology stack pose the greatest risk to operational continuity or resilience, organizations identified cybersecurity (45%), followed closely by connectivity and AI (43% each), data (42%), and hardware (37%) (see Figure 10).

High dependency on foreign suppliers persists across the tech stack

Significant external dependencies often underpin the risks, in particular reliance on primary providers located outside the organization's home country. In our survey, 62% of organizations say their primary hardware providers are based in another country. Fifty-nine percent say the same for cybersecurity providers, 58% for connectivity, and 57% for software. They have the fewest non-domestic primary dependencies for data (36%), while 57% say their primary data providers are in their home country.

All dimensions within the tech value chain are interconnected, therefore it is not sufficient to focus only on AI or only on cloud. Organizations need to consider the dependencies across the tech stack so they do not risk over-investing in non-critical layers, or under protecting systems in which disruption would halt operations.

45%

of organizations globally said cybersecurity is the dimension of the tech stack that poses the greatest risk to operational continuity or resilience

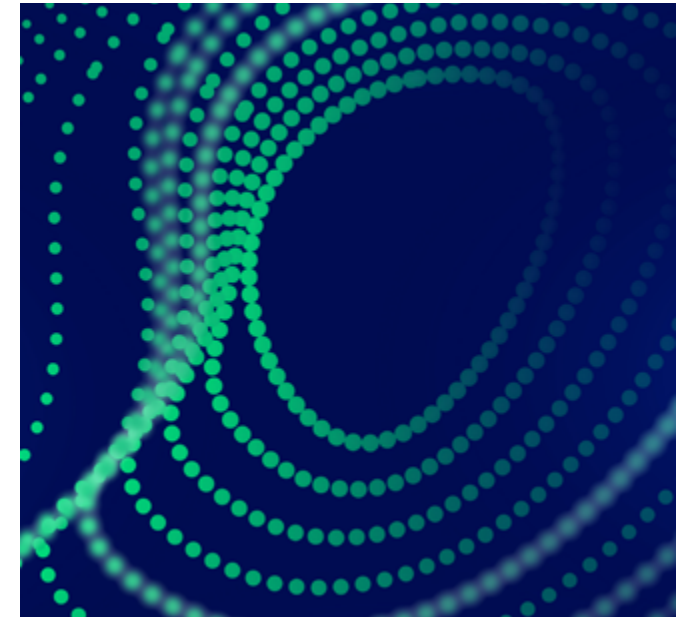
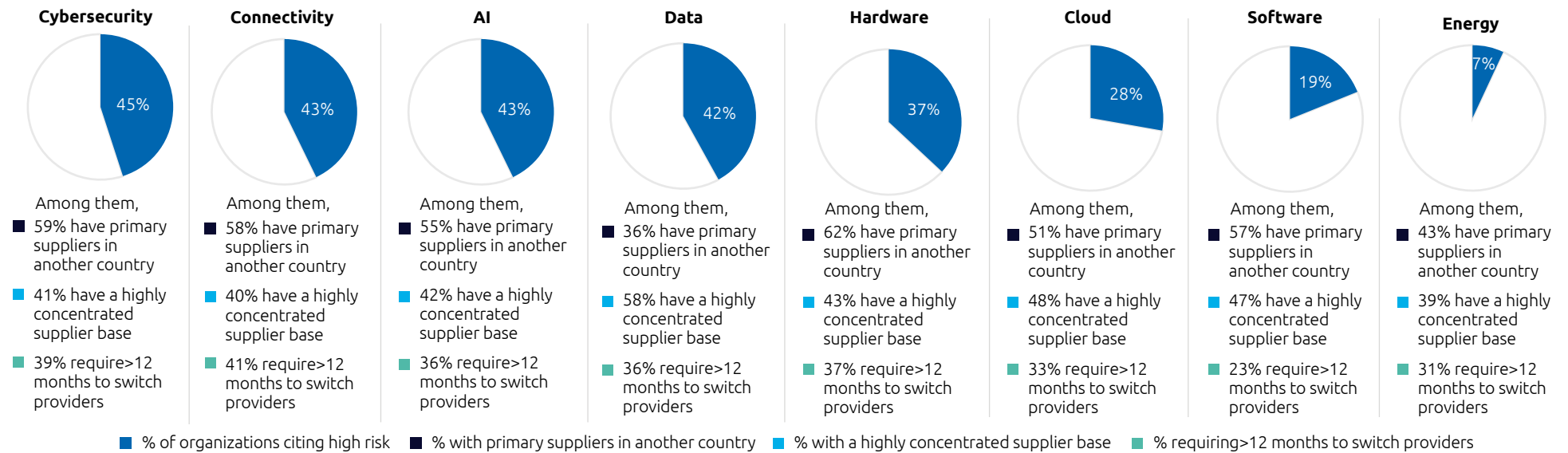


Figure 10.

Foreign dependencies, supplier concentration, and limited substitutability compound risk to operational continuity



Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

Note: For provider location, supplier concentration, and switching time, N represents the subset of respondents that identified the respective technology dimension as posing a risk to operational continuity. N = 552 for data, 368 for cloud, 560 for AI, 558 for connectivity, 583 for cybersecurity, 564 for hardware, 242 for software, and 96 for energy.

The challenge is compounded by highly concentrated supplier landscapes

Across most technology domains, organizations depend on a small number of providers, limiting optionality and increasing concentration risk. Nearly three in five (58%) report highly concentrated supplier networks for data, while nearly half report the same for cloud (48%) and software (47%). We observed similar patterns across hardware, AI, cybersecurity, connectivity, and energy.

Switching critical providers can take up to a year

When disruptions occur, dependencies are difficult to unwind. A significant 41% of organizations report that transitioning

away from a critical provider requires 3-12 months, while more than a third (36%) report more than 12 months. Only 13% say they could transition within three months. Moreover, 10% report no viable alternative provider. Connectivity, cybersecurity, and hardware emerge as the domains for which alternative providers are most difficult to find, reflecting deep operational integration and limited alternatives. Switching complexities and longer timelines mean resilience cannot be a contingency – it must be designed upfront, with portability, diversification, and exit readiness built in.

Most organizations lack end-to-end visibility of their tech supply chains

Further exacerbating the risks associated with foreign dependencies, supplier concentration, and limited substitutability is a lack of visibility across the technology

supply chain. Only 14% of organizations report end-to-end visibility into dependencies across their broader technology ecosystem (see Figure 11). This limited visibility can make it difficult to fully assess exposure, anticipate disruptions, and respond effectively. Organizations often manage increasingly complex dependency networks without a complete view of where critical vulnerabilities reside. These findings suggest that a visibility gap between technical teams and leadership is a core risk.

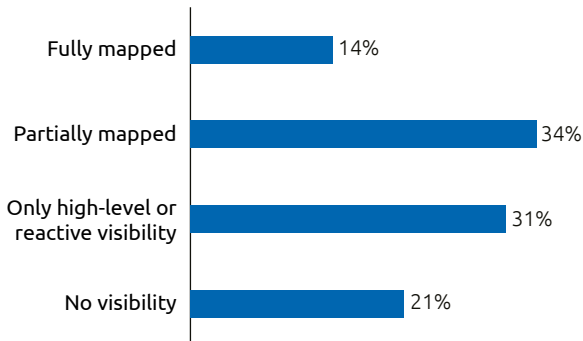
14%

of organizations worldwide report they have end-to-end visibility into dependencies across their tech supply chains

Figure 11.

Just 14% of organizations have fully mapped their dependencies

Level of real-time visibility of tech supply chains



Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.
 Definitions: Fully mapped – end-to-end visibility across all critical components, suppliers, providers, and dependencies, with continuous or near real-time risk tracking; Partially mapped – visibility for key systems or Tier-1 suppliers only, limited insight into indirect or upstream dependencies; Only high-level or reactive visibility – no comprehensive mapping; ad hoc or fragmented tracking; No visibility – little to no formal understanding of suppliers, dependencies, or risks across the value chain.

Most organizations are exposed to significant digital sovereignty risks

Since dependency risk is multidimensional and not just foreign versus domestic, we consider:

- Location of suppliers (foreign exposure)
- Concentration (single or few providers)
- Substitutability (time required to switch)

The Digital Sovereignty Index reflects the extent to which an organization relies on foreign or externally controlled supply chains; the concentration of suppliers or tech providers; and its ability to switch or substitute vendors in the event of disruption, conflict, or adverse conditions. We assessed these factors in the context of the operational criticality of each tech layer.

The Digital Sovereignty Index is expressed as a percentage that represents how close an organization is to an ideal state

of strategic control, resilience, and exposure. As highlighted in Figure 12, across the organizations in our sample, the majority (86%) are classified as having significant exposure per our index analysis. This share differs slightly across industries (ranging from 82% in life sciences and telecom to 93% in consumer goods and retail) and countries (ranging from 77% in Italy and the UK to 94% in Germany).

86%

of organizations in our global sample have significant exposure to digital sovereignty risks

Figure 12.

Most organizations are highly dependent and demonstrate weak resilience

Digital Sovereignty Index	Band	Band interpretation	Percentage of organizations
>= 80%	Close to ideal state	High control and resilience across critical layers with minimal exposure	0%
60-80%	Strong but gaps exist	Strong overall posture with some gaps that do not materially affect core areas	1%
40-60%	Moderate/mixed	Uneven maturity with noticeable gaps requiring targeted improvement	13%
<40%	Significant exposure	High dependency and weak resilience in critical areas	86%

Model inputs:

Dependency: location of primary suppliers for the eight technologies/infrastructure

Concentration: concentration of primary suppliers for the eight technologies/infrastructure

Readiness/substitutability: how quickly the organization could transition to an alternative amid disruption

Business criticality: considers which of the dimensions are critical to operational continuity (i.e., ability to sustain core business operations without significant disruption during adverse geopolitical, technological, regulatory, or supply-related events) and which dimensions have been affected by foreign or external events (e.g., sanctions, forced service withdrawals, export controls, vendor lock-in, cross-border supply disruptions) in the past 12–18 months

Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 866 executives; Capgemini Research Institute analysis.

Most organizations assess their dependencies

Of organizations in our model with significant exposure (86% of our total sample or 741 organizations):

- Two-thirds have formally assessed digital dependency risk across data, infrastructure, and technology on a regular basis.
- One-third of organizations who are significantly exposed do not undertake regular risk assessment and consequently have limited knowledge of where critical dependencies reside.

This split does vary by country and industry (see Figure 13). The highest share (80% or more) of organizations in Japan, Italy, and the Netherlands reported that they conduct regulatory risk assessments of digital dependencies. By comparison, only 46% of organizations in the US report the same. By industry, aerospace and defense and financial services see the greatest share and consumer products and retail the least.

Awareness of digital dependencies is not sufficient, organizations must have the ability to act, such as exiting dependencies without paralyzing operations.

Riccardo Picca of Thermo Fisher, says: *"There is high vendor concentration across cloud, SaaS [Software as a Service], and AI providers, with risk of losing control over data and IP. Risks include non-compliance across jurisdictions, operational disruption due to cyberattacks or provider outages, and black-box AI dependency. This makes dependency management a structural requirement."*

33%

of organizations with significant exposure do not undertake regular risk assessment

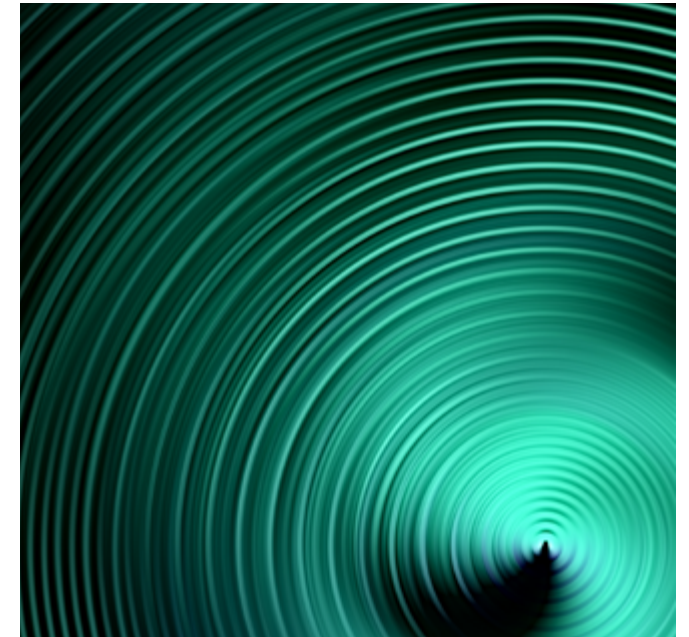
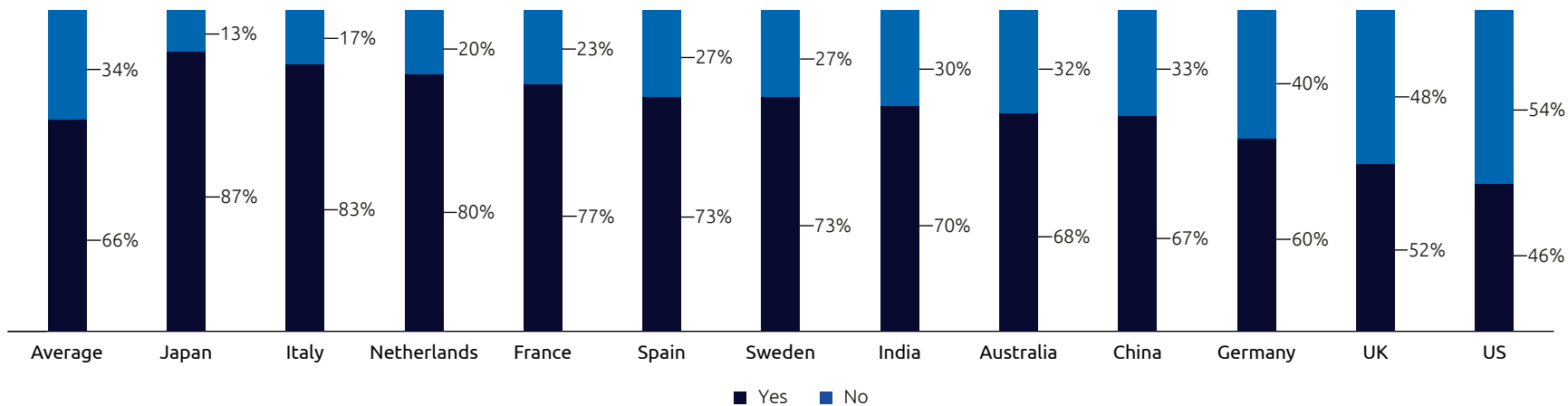


Figure 13.

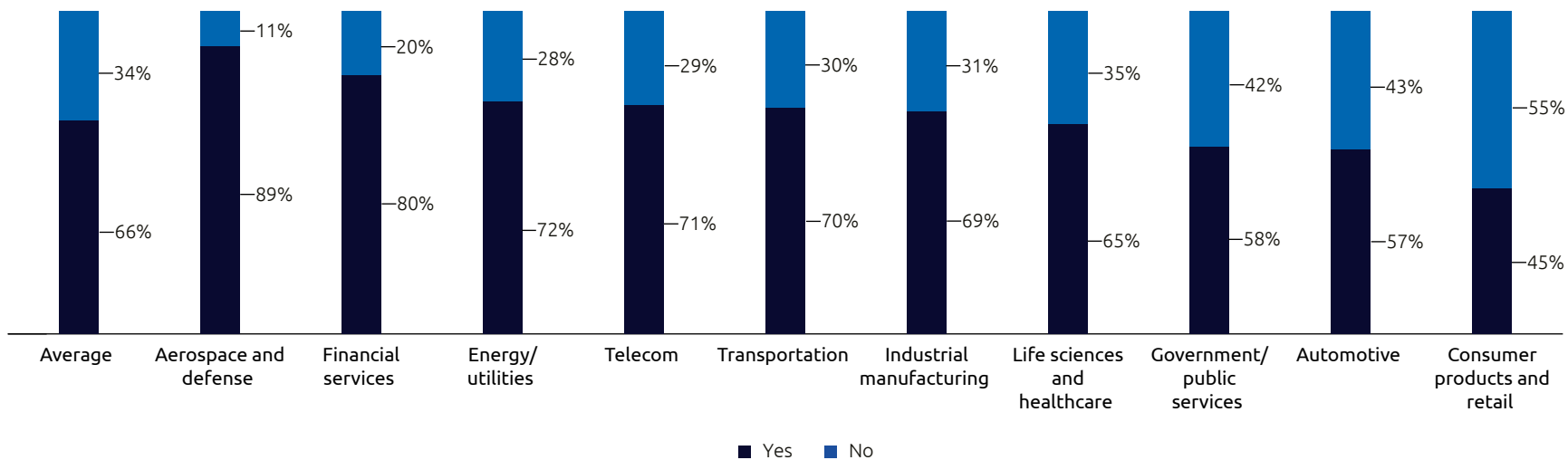
Two-thirds of organizations with significant exposure assess digital dependency risks on a regular basis

Whether organizations regularly assess the risk of its digital dependencies across data, infrastructure, and technology, by country



To be continued.

Whether organizations regularly assess the risk of its digital dependencies across data, infrastructure, and technology, by industry



Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 741 executives.



"The central challenge for organizations is not to pursue an illusion of full digital self-sufficiency, but to make clear, affordable, and strategic choices about where control matters most."

Nicolas Gaudilliere

Chief Technology Officer, Invent France

Digital sovereignty and innovation: genuine trade-off or false binary?

At its core, the control versus innovation debate is about the extent to which governments and organizations can assert control over digital assets without undermining openness, collaboration, and technological progress.

The 'control' argument emphasizes the requirement of strong control over data infrastructure, and technology to ensure security, independence, and strategic autonomy. Conversely, the 'innovation' argument is that innovation thrives in open, global, data-rich ecosystems, not in isolated or tightly controlled environments.

This issue is often incorrectly framed as a binary choice. However, as the results of this research reveal, a more nuanced digital sovereignty approach is emerging, balancing innovation and regulation. Its principles are:

- **Selective control** (risk-based digital sovereignty): Enforce strong controls only on sensitive data/workloads, allowing openness elsewhere

- **Hybrid architectures** (not isolation): Combine global cloud innovation with sovereign controls (e.g., governance, encryption, jurisdictional controls)
- **Open but regulated ecosystems**: Maintain cross-border data flows while enforcing standards for privacy, security, and competition
- **Digital sovereignty as an enabler of innovation**: Policies should actively stimulate domestic innovation ecosystems
- **Interdependence, not independence**: Recognize the necessity of global collaboration

Jai Haridas, VP and GM, Regulated and Sovereign Cloud at Google Cloud, comments: *"The supposed trade-off between sovereignty and innovation is a false choice. Choose only sovereignty and you stop innovating; choose only innovation and you lose security and control. Either extreme can put the business at risk. Organizations should be able to pick the level of sovereignty their use case requires and still innovate."*²²

When carefully designed, digital sovereignty is not restrictive but rather an enabler of innovation at scale. It operates through five key vectors:

1. **Trust**: unlocks adoption of AI and data-driven innovation
2. **Clarity**: creates clear governance and reduces regulatory uncertainty
3. **Data access**: enables secure sharing of sensitive data

4. **Resilience**: supports continuous innovation under disruption
5. **Autonomy**: allows organizations to innovate strategically and independently

The head of cloud and data at a multinational financial services company asserts that digital sovereignty can enhance customer trust and satisfaction: *"In markets where data protection is a priority, being able to prove compliance can serve as a differentiator, giving organizations a competitive advantage over less compliant peers."*

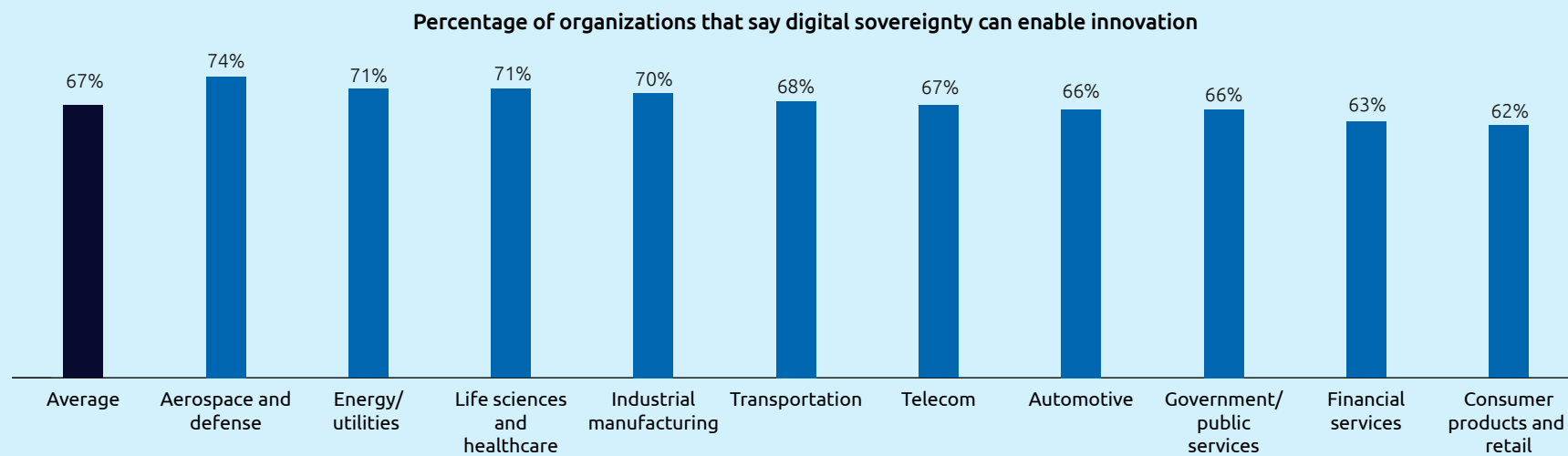
When asked which value-creation opportunities digital sovereignty can unlock, over two-thirds of organizations globally cited innovation (see Figure 14). This increases to nearly three-quarters among aerospace and defense respondents.

67%

of organizations globally believe digital sovereignty can enable innovation

Figure 14.

Most organizations believe that digital sovereignty can enable innovation



Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

04 | Organizations are pragmatic in their pursuit of digital sovereignty

Organizations prioritize AI sovereignty

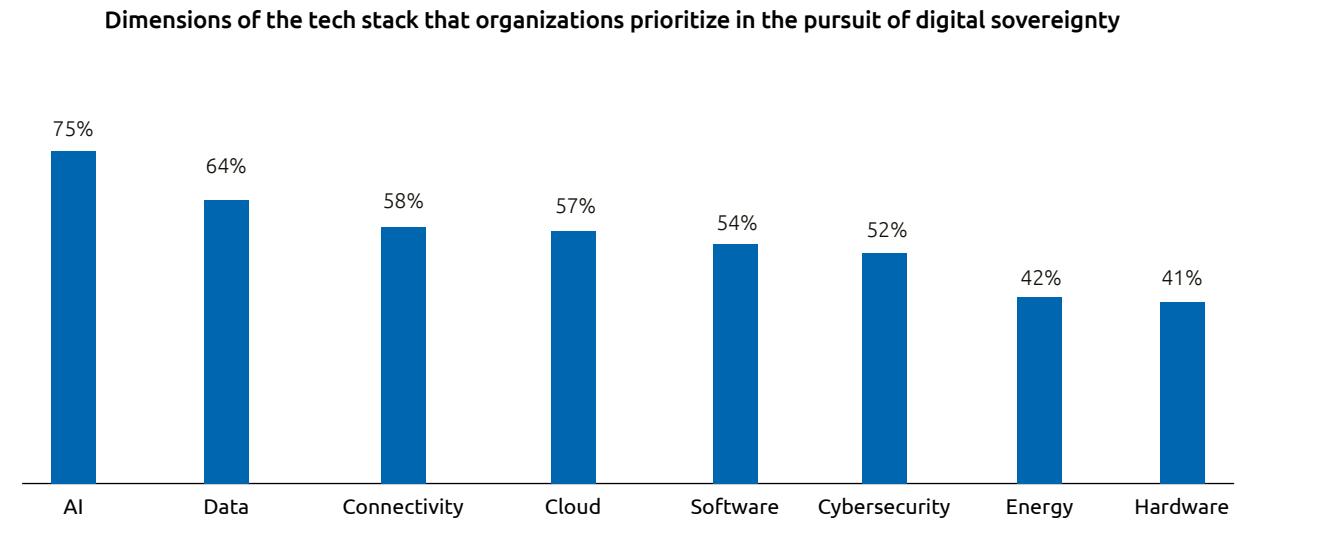
Three-quarters of organizations in our survey prioritize AI in their pursuit of digital sovereignty. This share rises to 77% in APAC (87% in China) and continental Europe and drops to 64% in the UK. The emphasis on AI sovereignty is particularly evident in sectors that manage critical infrastructure, information, or operations: aerospace and defense (82%), transportation (81%), telecom (79%), and government/public sector (76%).

Reflecting this trend, Airbus has partnered with Mistral AI to embed cutting-edge, ethical and trustworthy AI at the core of its operations and processes, while adhering to the strict security and digital sovereignty requirements of critical, highly confidential and military aerospace applications.²³ Similarly, Germany's Federal Ministry for Digitalization and State Modernization is partnering with Deutsche Telekom and SAP to develop a sovereign AI platform that provide federal, state, and municipal administrations with secure, interoperable, and scalable AI capabilities within Europe.²⁴

The second most-prioritized dimension globally (64%) is data. This share rises to 74% among APAC and French organizations and declines to 56% in the US. Hardware and energy are the least commonly prioritized dimensions among surveyed organizations (see Figure 15).

Figure 15.

75% of organizations prioritize AI for digital sovereignty



Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

The growing importance of AI sovereignty may reflect rising concerns over access to frontier AI models. Recent export controls, usage restrictions, and concentration among a small number of frontier AI providers have highlighted the strategic risks associated with dependence on external AI capabilities.²⁵ Consequently, organizations may increasingly treat access to advanced models as a sovereignty consideration alongside cloud, data, and cybersecurity.

Federated control and managed interdependence models dominate

Close to half of the organizations surveyed plan to pursue ‘federated’ control (shared control with certified local/regional partners and localized critical operations) or managed interdependent models (contractual partnerships with global providers and technical safeguards in place) across tech dimensions. About one in five prefers full sovereign control (see Figure 16). This aligns with Gartner’s estimate that sovereign cloud Infrastructure as a Service (IaaS) spending will shift 20% of current workloads from global to local cloud providers.²⁶

Hyperscalers are tailoring their offerings to meet country-specific sovereignty requirements through models such as in-country partnerships, localized operations, and customer-controlled encryption.

- Amazon Web Services (AWS) launched its European Sovereign Cloud in January 2026, an independent cloud for Europe entirely located within the EU, and physically and logically separate from other AWS regions. Technical controls, sovereign assurances, and legal protections are designed to meet the needs of European governments and enterprises for sensitive data.²⁷
- In June 2025, Microsoft expanded its sovereign cloud portfolio with new capabilities designed to help organizations meet national and regional sovereignty requirements.²⁸
 - The organization also partnered with Bleu in France and Delos Cloud in Germany to enable customers to run sensitive workloads under local regulatory frameworks.²⁹
- SAP Sovereign Cloud is another example of a platform provider developing sovereignty solutions. In March 2026, SAP launched its sovereign cloud offering in France on the Bleu platform, enabling organizations to run their critical workloads in a sovereign cloud environment designed to meet the country’s strict regulatory and security requirements.³⁰
- In May 2026, Google Cloud and Thales announced a strategic partnership to launch a new European sovereign cloud offering in Germany, designed to meet the stringent digital sovereignty and regulatory requirements of German public sector organizations and highly regulated industries. It is also designed to meet Germany’s new C3A (Criteria enabling Cloud Computing Autonomy) framework, a transparency standard published by Germany’s Federal Office for Information Security. This offering will live on dedicated infrastructure that will be managed and operated by a new German entity, which Thales will own and control.³¹
- Oracle is also accelerating sovereign tech initiatives:
 - In October 2025, Oracle and SoftBank began a collaboration to provide secure, compliant, and scalable sovereign cloud and AI services to organizations in Japan.³²
 - In November 2025, Oracle announced a major expansion of the Oracle Cloud Abu Dhabi Region with the deployment of the first Oracle Cloud Infrastructure (OCI) Supercluster powered by NVIDIA Blackwell graphics processing units (GPUs) in the Middle East. This will help customers in key regional industries (e.g., government, energy, financial services) accelerate AI adoption while meeting data sovereignty and regulatory requirements.³³

Figure 16.

Around half of organizations pursue federated control or managed interdependence models across the dimensions

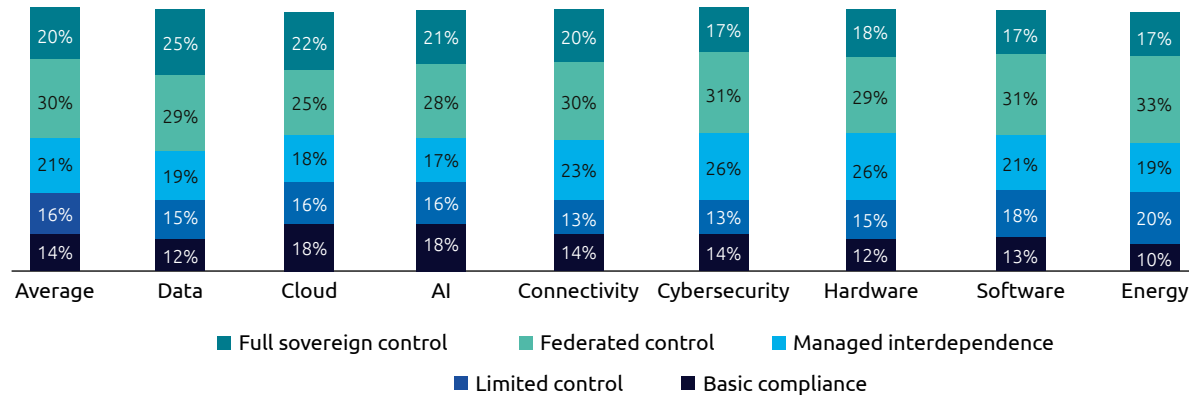
Ecosystems are essential

Most (72%) organizations agree that organizations that do not actively participate in ecosystems and/or consortia will struggle to achieve digital sovereignty. In addition, 65% of organizations agree that selective control of critical technologies, combined with strategic reliance on partners, is a more practical model than full ownership (23% disagree and 13% remain neutral). Both these sentiments are consistent across regions.

Bosch's Sharma says: *"The approach is not isolation from global ecosystems, but building trusted, balanced, resilient partnerships while maintaining strategic control over critical capabilities. We look for portability, openness, and clear governance, especially in AI and industrial IoT, where innovation happens through collaboration across companies, suppliers, startups, government institutes, and academia."*

Furthermore, 68% of organizations surveyed anticipate a combination of internal development and external collaboration in their pursuit of digital sovereignty (see Figure 17). Federated and managed models are becoming the norm because digital sovereignty outcomes increasingly depend on shared capabilities and standards, and trusted partners, rather than fully owned stacks.

Organizations' desired level of digital sovereignty across the tech stack



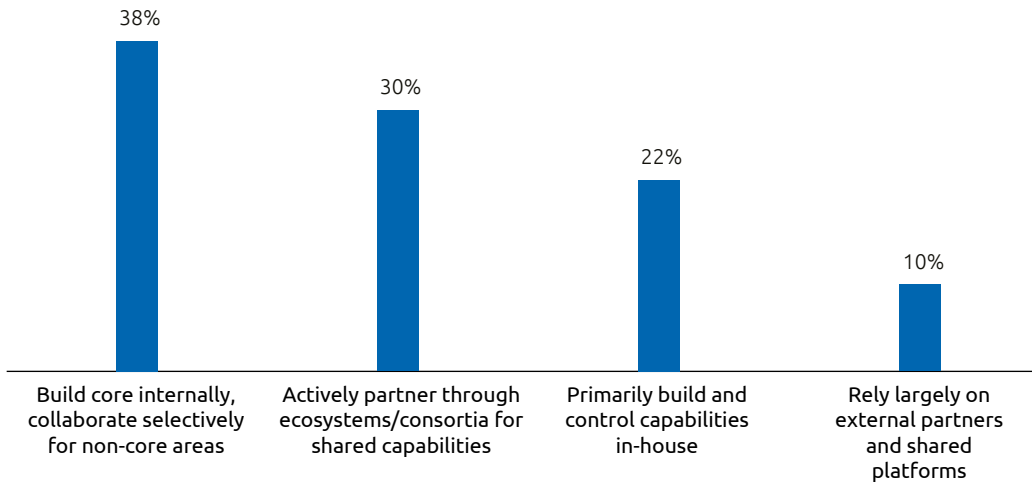
Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

Definitions: **Full sovereign control** (in-house/local; end-to-end control across the stack); **federated control** (shared control with certified local/regional partners; localized critical operations); **managed interdependence** (contractual partnerships with global providers; technical safeguards in place); **limited control** (policy-driven; selective controls applied on a case-by-case basis); **basic compliance** (only foundational security/compliance measures in place).

Figure 17.

A combined internal and collaborative approach to digital sovereignty is most popular

Percentage of organizations taking the below approaches to digital sovereignty



Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

As the premium ceiling is low, adoption will be price-sensitive

Slightly under half (49%) of organizations are willing to pay a 'digital sovereignty premium.' Of those willing to pay a premium, on average, they say they would accept a 23% price increase over current costs. There are slight variations across countries and industries:

- 43% of US organizations are willing to pay a premium versus 55% of organizations in France
- 43% of consumer goods and retail organizations are willing to pay a premium versus 58% of financial services organizations

49%

of organizations globally are willing to pay a 'digital sovereignty premium'

Bernd Meurer of BT Group explains: *“If you run on multiple platforms to get more sovereign elements, it costs more, and many customers assess what they can afford. You also lose discounts from providers when you choose multiple, and you need additional teams to run each platform. So, many say, ‘we could be more sovereign, but we cannot afford it.’”*

To add to this, the head of cloud and data at a multinational financial services company, states: *““Replicating models and services in multiple data centers to meet digital sovereignty requirements can be economically prohibitive, leading organizations to make conscious decisions about which features to offer in different markets (e.g., more conservative product offerings in regions with stricter regulations).”*

Vendor choice and performance remain non-negotiable

Nevertheless, executives are clear about the non-negotiables (i.e., what they cannot compromise in exchange for their desired level of digital sovereignty):

- Sufficient vendor choice stands out as the strongest concern (71%)

- High performance also remains a key expectation for most organizations (62%)
- Nearly half (47%) of organizations mention pace of innovation

Adoption will depend on solutions that improve control while maintaining flexibility and performance, keeping them aligned with core business priorities.

Digital sovereignty: differentiator or base requirement?

Organizations are split over the significance of digital sovereignty, although most see it as a big part of the future of business: 46% expect digital sovereignty to become a competitive differentiator, while 39% see it evolving into a regulated baseline requirement, and 15% view it as the cost of doing business (see Figure 18).

Thermo Fisher’s Picca says: *“It will become a baseline expectation, especially in regulated industries, but not uniformly across domains. Baseline will be data-residency, compliance, cybersecurity, and basic cloud governance – almost a ‘license to operate.’ Differentiation remains in how well you balance digital*

sovereignty with innovation and speed, and how effectively you scale digital sovereignty globally while complying locally.”

There are strong sectoral contrasts. For example, 62% of executives from energy and utilities and aerospace and defense industries view digital sovereignty as a competitive differentiator compared with 27% within consumer products and retail. This suggests that in some areas, especially regulated and critical environments, digital sovereignty will become essential, while in others it will become a point of difference by demonstrating stronger control, resilience, and trust. For some, digital sovereignty is transitioning from optional initiative to necessity; for others, it is a key competitive advantage.

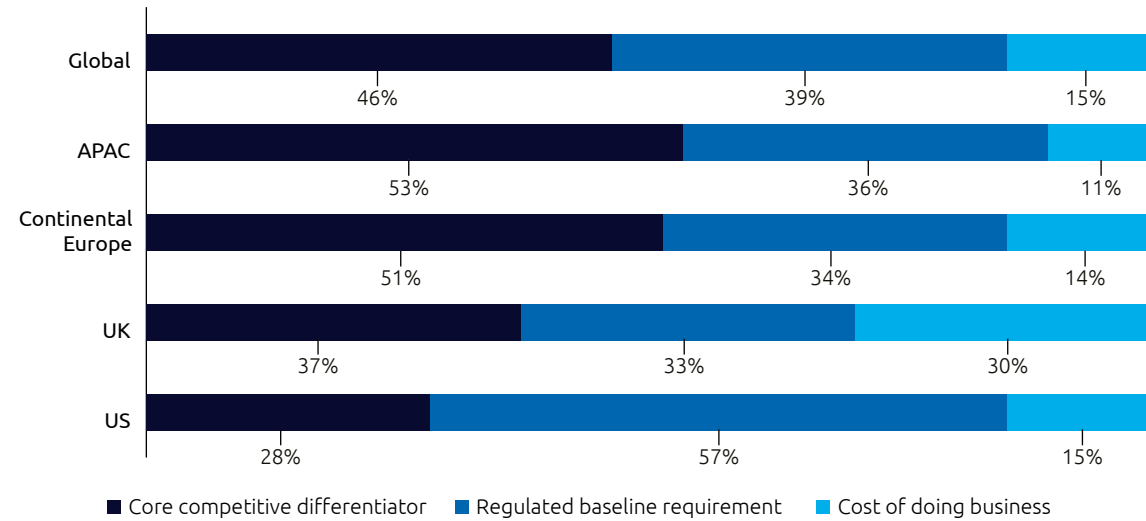
46%

of organizations worldwide expect digital sovereignty to become a competitive differentiator

Figure 18.

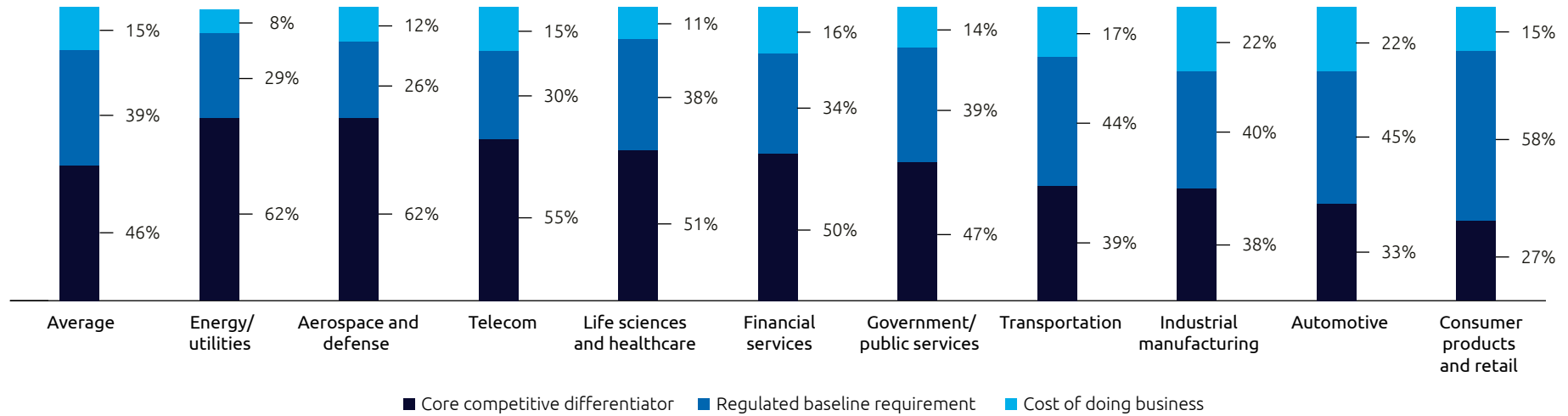
Nearly half of organizations see digital sovereignty as a competitive differentiator

Outlook for digital sovereignty, by region



To be continued.

Outlook for digital sovereignty, by industry



Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

Insights from a technology leader



Martin Merz

President Sovereign Cloud, SAP

When you hear 'digital sovereignty,' what are enterprise leaders trying to protect: resilience, autonomy, or control?

"I see digital sovereignty as a balance between freedom of choice and control. On the one hand, organizations want to use the best technology available globally. On the other hand, they need to operate within the applicable governance and regulatory frameworks of their country, particularly when national security requirements are involved. This is exactly what we see from customers and governments. Many of them wanted to move to the cloud, but regulations, particularly in areas like defense or classified environments, made that difficult. That is what drove the creation of sovereign

cloud strategies. In that sense, digital sovereignty is not just about protecting data or infrastructure; it's about enabling organizations to innovate while still maintaining compliance, control, and trust in line with national requirements. Innovation and sovereignty are not competing objectives. Organizations need both: access to the best technology available and the governance to use it responsibly.

One pragmatic way to think about this is the 'buy, build, and assemble' approach. 'Buy' means using the best technology available globally where it delivers the greatest value. 'Build' means investing in the areas where you have unique strengths. And 'assemble' is about bringing everything together under your own governance and control."

Many organizations face strong dependencies across the tech stack. What is often overlooked?

"Historically, resilience has often been underestimated. For decades, we operated in a highly globalized and interconnected world where everything functioned efficiently, and dependencies were not seen as a major issue. As a result, organizations did not prioritize security, supply chain robustness, or contingency planning to the

extent they should have. Now, the reality has changed. Digital sovereignty is fundamentally a resilience discussion. Organizations and leaders need to identify their most critical systems and business processes, define how they protect them, and establish backup scenarios – what I would call plan B and plan C. Interestingly, many organizations already had these strategies documented, often as part of compliance requirements, business continuity planning, and risk management, but they were often treated as checklist items. Today, the shift is toward making these strategies operational and actionable because the threat is real."

What is a practical approach to digital sovereignty? How should organizations decide where to build greater control versus rely on trusted partners?

"It is important to recognize that digital sovereignty is not a universal requirement. Different industries and organizations require different levels of control and different approaches depending on their risk profile and regulatory environment. The highest levels of digital sovereignty are typically required in very specific environments, such as military or intelligence, where organizations operate highly sensitive workloads.

For many other industries, such as consumer goods or manufacturing, existing cloud environments already provide strong levels of security, resilience, and performance. In some cases, organizations assume they need a sovereign solution when, in fact, their requirements can be fully met with existing cloud capabilities.

The most successful organizations are those who start, implement, learn, and refine as they go. They put systems in place, have multiple paths – plan A, B, C, test them in real-world environments, choose the combination that best fits their needs, and evolve continuously.

At SAP, we typically break this down into four key dimensions: data sovereignty, ensuring data remains within the required jurisdiction; operational sovereignty, meaning that systems are run by locally authorized and, where required, security-cleared personnel; technical sovereignty, ensuring systems are designed for resilience, transparency, and strong security controls; and legal sovereignty, ensuring systems operate under the legal jurisdiction and governance customers require. Ultimately, success lies in flexibility, diversity of options, and the ability to adapt to changing circumstances rather than aiming for a rigid, one-size-fits-all solution.”

Do you see the current regulatory direction, particularly in Europe, enabling competitiveness or adding friction to innovation?

“Regulation plays an important role, particularly when it comes to safeguarding national security and protecting critical infrastructure. Certain measures are necessary and entirely justified. However, there is a fine line between regulation and overreach. The challenge arises when regulation becomes overly restrictive, limiting access to the best technologies. If organizations are constrained in their ability to adopt innovative solutions, they risk losing competitiveness over time. The objective should be to create a regulatory environment that enables innovation while maintaining trust and appropriate safeguards. That’s why it is important to maintain freedom of choice within a trusted governance framework. Organizations should be able to choose the best technologies available while maintaining appropriate governance. Striking that balance is critical, otherwise, regulation can unintentionally slow down progress and disadvantage entire regions.”

As AI becomes more central to economic productivity, is compute capacity becoming a new form of geopolitical power?

“Yes, absolutely. AI is not just about algorithms or data; it also depends on physical infrastructure such as chips, data centers, and energy supply. Even if a region has strong technology capabilities, it still needs the physical capacity to run them. Energy availability is becoming a critical factor, and we already see regions with higher energy costs struggling to compete. Access to compute capacity is therefore becoming an increasingly important strategic capability.

At the same time, compute capacity is only one part of the equation. To translate AI into long-term competitiveness, organizations also need trusted governance over how AI is deployed, how data is managed, and under which legal and operational framework AI is used. In that sense, compute capacity, together with trusted governance and the ability to apply AI responsibly, is becoming an increasingly important factor for economic competitiveness and geopolitical influence.”

Regional perspectives on digital sovereignty

While organizations globally agree that digital sovereignty is a strategic priority, regional differences emerge in how it is perceived, prioritized, and operationalized.

Eighty-six percent of organizations in APAC and 84% in continental Europe express concern about maintaining critical operations, compared with only 68% in the US and 51% in the UK.

These differences reflect underlying structural and geopolitical realities. In Europe, the Russia–Ukraine conflict has exposed vulnerabilities across energy, supply chains, and digital ecosystems, while long-running debates around data sovereignty, digital dependency, and cross-border data transfers emphasize the importance of strategic control. Regulatory developments such as GDPR, NIS2, the EU Data Act, and the Cyber Resilience Act have further strengthened the link between operational resilience and digital sovereignty.

Similarly, organizations in APAC operate in an environment shaped by geopolitical volatility, supply-chain concentration, and regulatory fragmentation. A study by IDC reveals that more than 60% of enterprises in APAC are already experiencing moderate to significant disruption to IT operations due to evolving data privacy, cybersecurity, and AI regulations.³⁴

By contrast, many US organizations operate within a strong domestic ecosystem for cloud, AI, and enterprise software, which may reduce the perceived urgency of external dependency risks and shift attention away from operational disruption concerns.

Regional realities shape definitions of digital sovereignty

Across APAC (41%), continental Europe (52%), and the UK (56%), digital sovereignty is primarily viewed as a risk-mitigation and resilience-building approach. In contrast, a majority of US organizations (52%) view digital sovereignty primarily as a compliance requirement, compared with 40% who see it as a resilience-building approach, and just 7%

who view it as a competitive or strategic differentiator. This suggests that digital sovereignty in the US is more often framed by regulatory and governance obligations than strategic autonomy or resilience.

These differences become even more pronounced when organizations consider the future role of digital sovereignty. In APAC and continental Europe, emphasis shifts from resilience toward competitive advantage. While 41% of APAC organizations currently view digital sovereignty as a resilience-building approach, 53% expect it to become a core competitive differentiator in the future. A similar pattern is visible in continental Europe, where 51% expect digital sovereignty to evolve into a source of competitive advantage.

The US again follows a different trajectory. While only 28% of US organizations expect digital sovereignty to become a competitive differentiator, 57% believe it will become a regulated baseline requirement. Rather than a source of advantage, it is expected to become a standard operating condition driven by compliance.

The UK occupies the middle ground. While organizations today predominantly associate digital sovereignty with resilience and risk mitigation, future expectations are more evenly distributed across competitive differentiation (37%), regulatory requirements (33%), and cost of doing business (30%).

When examining motivations for pursuing digital sovereignty, two emerge more strongly in APAC and the UK than in other regions:

- Long-term control over technology capabilities, costs, and roadmaps
- The flexibility to adapt as regulations evolve

This suggests that organizations in these regions focus not only on managing current dependencies but also on preserving strategic optionality.

Approaches to achieving digital sovereignty also differ

Globally, the dominant model for achieving digital sovereignty is to build critical capabilities internally while

selectively partnering for non-core requirements. But US organizations diverge from this pattern, placing greater emphasis on ecosystem collaboration and industry partnerships to develop shared capabilities (39%), compared with 27% in APAC, 28% in continental Europe, and 25% in the UK.

US organizations are less likely to prioritize in-house capability development and direct control (16%) than organizations in APAC (24%), continental Europe (23%), and the UK (28%).

Likewise, while organizations in APAC, continental Europe, and the UK often seek greater autonomy through domestic capabilities and regulatory safeguards, US organizations place more emphasis on interoperable architecture, industry standards, and ecosystem-based models of control.

Notably, higher levels of concerned awareness do not necessarily translate into stronger preparedness. Among those organizations that have recently experienced operational disruptions due to events such as sanctions, vendor lock-in, forced technology withdrawals, or

supply-chain interruptions, 64% of US organizations report having contingency plans in place, compared with 42% globally, 37% in continental Europe, 36% in the UK, and 34% in APAC.

Overall, organizations agree on the importance of digital sovereignty, but regional priorities differ:

- Continental Europe primarily approaches digital sovereignty through resilience, strategic autonomy, and reduced dependency
- Increasingly, APAC views digital sovereignty as a mechanism for long-term strategic control and adaptability
- The UK adopts a pragmatic approach focused on operational flexibility and regulatory compliance
- The US tends to frame digital sovereignty through compliance, ecosystem participation, interoperability, and shared models of control

These differences reflect each region's position within the global technology ecosystem and reinforce that a one-size-fits-all approach to digital sovereignty is unlikely to be effective.

05

How organizations can begin their digital sovereignty journeys

1. Embrace digital sovereignty as a board-level strategic topic, not an isolated technology initiative

Treating digital sovereignty as a purely technical or compliance-driven topic risks overlooking its broader implications for business resilience, supply-chain stability, and long-term competitiveness. Rather, it must be a strategic imperative that reflects an organization's ability to maintain operational continuity, strategic autonomy, and control over critical digital capabilities amid growing geopolitical fragmentation and regulatory complexity. While many organizations have begun to address digital sovereignty through targeted initiatives such as data residency or sovereign cloud deployments, these efforts often remain fragmented and limited in scope.

The question is which digital services and systems require greater control to protect critical operations and decision rights. This makes digital sovereignty a strategic issue that should be anchored in organizational priorities, with clear ownership across business, technology, procurement, and risk functions.

To do this effectively, organizations should define governance up front: who decides where digital sovereignty is needed,

how trade-offs are evaluated, and what level of risk is acceptable in different domains. Without this, digital sovereignty efforts often remain fragmented. For example, they are limited to data residency or isolated sovereign cloud decisions, without addressing the broader dependencies that affect resilience, continuity, and strategic autonomy.

2. Assess exposure of critical business operations

Organizations should begin by identifying the business processes and services that are essential to operational continuity and then mapping the dependencies required to run them.

Many organizations today still operate with limited visibility of their dependency landscape, particularly beyond direct suppliers or Tier 1 providers. As a result, decisions are often made with incomplete information, leading to an inaccurate assessment of risk exposure.

At this early stage, organizations should undertake a structured dependency, mapping assessment of critical processes. For each business process/workload, the assessment should evaluate four dimensions:

- **Criticality to enterprise operational continuity:** the extent to which the business process or workload is

essential to maintaining operations, compliance, customer obligations, and the impact on continuity if it is disrupted.

- **Compliance-critical workloads** require controls primarily to satisfy regulatory, privacy, and sector-specific obligations.
- **Operations-critical workloads** support essential business functions and require enhanced resilience, recoverability, portability, and operational control.
- **Systemic or national-critical workloads** involve highly sensitive, classified, or strategically important functions and may require the highest levels of sovereign control.

- **Degree of concentration across technology layers:** Dependency on a limited number of providers, geographies, platforms, or supply sources, concentrating risk.
- **Ease of substitution:** The speed and effectiveness with which the dependency can be replaced, migrated, or replicated, considering exit feasibility, availability of viable alternatives, and interoperability, if access is disrupted or conditions change.
- **Exposure to regulatory, geopolitical, or supply-side disruption:** The vulnerability of the dependency to changes in regulation, export controls, sanctions, geopolitical tensions, infrastructure failures, supply shortages, or vendor-driven decisions.

Organizations should also stress-test against plausible disruption scenarios, such as loss of access to a cloud provider, restrictions on cross-border data flows, vendor lock-in, or supply chain interruptions.

This provides a comprehensive view of exposure across the technology stack and underlying decision rights. Starting here prevents organizations from moving prematurely into solutions before they understand where the real vulnerabilities lie.

3. Prioritize interventions based on business impact and risk tolerance

The next step is to decide where action is required and where exposure can be tolerated. Some dependencies are acceptable because operational impact is limited or the cost of mitigation is too high. Others, particularly those tied to critical workloads and services, sensitive data, or concentrated provider dependence, justify stronger intervention. Digital sovereignty exists on a spectrum, and control must be applied selectively to protect critical digital services.

This requires defining minimum viable digital sovereignty – the smallest set of capabilities, assets, and controls that must

remain under direct or assured control to safeguard critical operations. Rather than pursuing digital sovereignty across the entire technology landscape, organizations should focus on securing this minimum viable core.

This prioritization allows organizations to define a target posture for each domain based on risk, control needs, and economic feasibility. In practice, this means choosing where to reduce dependence, where to build alternatives, and where to continue with managed exposure. This helps organizations avoid reactive decision-making during crises and instead develop a proactive, economically grounded digital sovereignty strategy.

Organizations should also anticipate evolving regulatory baselines such as those introduced by the EU's Cloud and AI Development Act, including minimum digital sovereignty requirements for public procurement and increasing expectations around data localization, auditability, and provider control structures.

4. Build resilience and control into the target operating model

After priorities are set, organizations should translate digital sovereignty requirements into technology architecture, sourcing, and operating-model decisions. This may require full control in highly sensitive areas and federated or managed interdependence where flexibility is more a higher priority than ownership.

At this stage, organizations should embed resilience by design, and an ongoing part of process development. This includes portability, interoperability, fallback arrangements, and exit strategies. Given that switching critical providers can take months or longer, exit readiness should be treated as a core resilience capability rather than a contingency plan. Organizations must define clear triggers for exit (e.g., regulatory breaches, sustained service degradation, or heightened geopolitical risk), pre-validate alternative providers or architectural options, and maintain a realistic view of transition timelines and associated costs.

The head of cloud and data at a multinational financial services company agrees: *“Embedding digital sovereignty into organizational processes is expensive and complex. Therefore, it needs to become second nature, rather than an afterthought to avoid costly compliance failures. It is critical to have internal subject-matter experts to interpret complex and evolving regulations and translate them into actionable requirements for products and services. In addition, shifting from a reactive to a proactive approach that includes regular internal and independent audits with digital sovereignty requirements is crucial to ensure ongoing compliance.”*

5. Foster innovation ecosystems through managed interdependence

Organizations today operate within highly interconnected digital ecosystems, where dependencies across the tech

stack are both unavoidable and, in many cases, beneficial for innovation and scale. But they must strategically manage ecosystem-level dependencies to reduce concentration risk while preserving access to scale, innovation, and global capabilities.

To do so, organizations should prioritize open standards, interoperable architectures, and portable technology designs that reduce lock-in and enable greater flexibility. Building relationships with trusted local and regional technology providers, industry partners, research institutions, and sovereign cloud initiatives can further diversify dependencies while supporting innovation and resilience.

Charles-Pierre Astolfi of France’s National Institute of Geographic and Forest Information explains: *“Strengthening digital sovereignty at a national level requires both supply and demand. Organizations need to actively support domestic solutions. Creating coalitions that commit to using these solutions is essential to make investments viable and sustain the ecosystem.”*

We collaborate extensively across the public sector, including joint procurement initiatives, and with private-sector partners and open-source communities. The objective is not to act alone but to build shared capabilities. These initiatives help create alternatives to proprietary technologies and strengthen digital sovereignty collectively.”

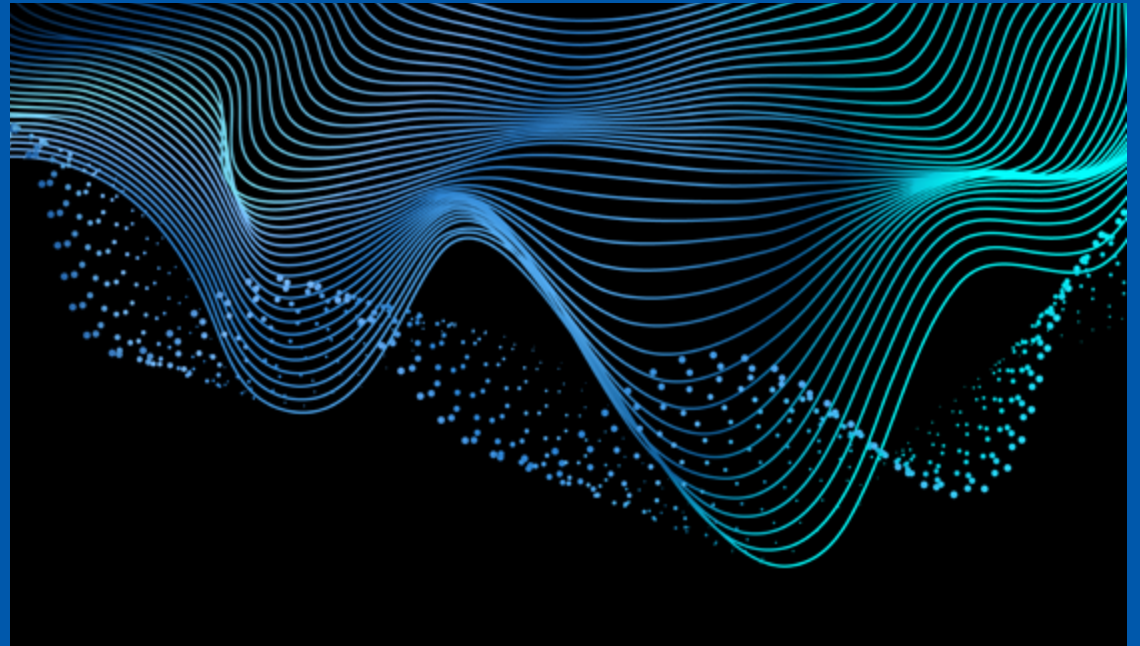
A managed interdependence approach allows organizations to retain control over critical assets and operations while continuing to benefit from the scale, innovation, and ecosystem advantages offered by global technology providers.

Conclusion

Digital sovereignty is now an operational reality for organizations worldwide. As digital ecosystems become more interconnected and geopolitical and regulatory pressures intensify, managing emerging dependencies will be critical to business resilience and long-term competitiveness. Resilience, affordability, and sustainability at AI-era speed.

Organizations are recognizing that full independence is neither feasible nor desirable. Instead, the focus is shifting to resilient interdependence: balancing control over critical assets with continued reliance on global technology ecosystems. This requires deliberate choices across technology architecture, sourcing strategies, and governance models to ensure flexibility, continuity, and strategic autonomy in the face of disruption.

Looking ahead, digital sovereignty will not be defined by isolation, but by the ability to manage complexity and make informed trade-offs. Organizations that can align control, resilience, and innovation while tapping into ecosystem partnerships will be better positioned to navigate uncertainty and sustain competitive advantage in an increasingly interdependent digital landscape.



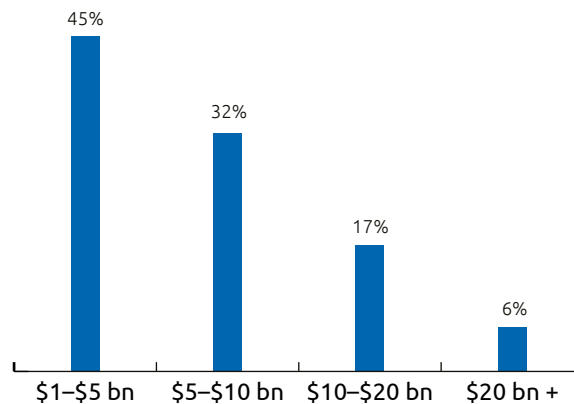
Research methodology

This publication draws on a multifaceted research program examining perceptions, maturity, and demand for digital sovereignty around the world. It included a specially commissioned online survey in April 2026 of 1,300 business and technology executives across industries at private-sector organizations with over \$1 billion in annual revenue and public-sector organizations with over \$1 billion in annual budgets.

We supplemented this quantitative research with 13 qualitative interviews with senior executives at leading global organizations. We also carried out extensive desk research.

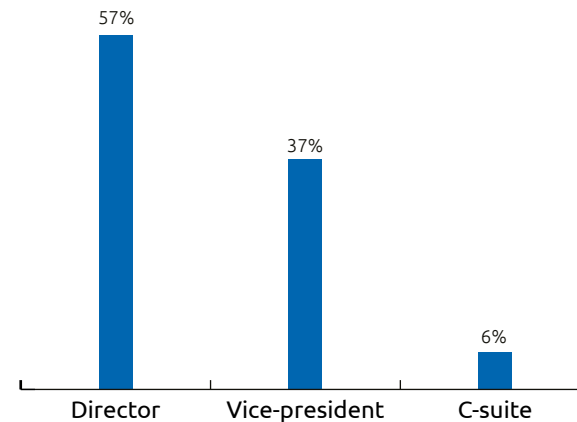
The study findings reflect the views of the interviewees and survey respondents and is intended to provide high-level guidance. Please contact one of the Capgemini experts listed at the end of the report to discuss specific implications for your organization.

Percentage of organizations, by annual revenue



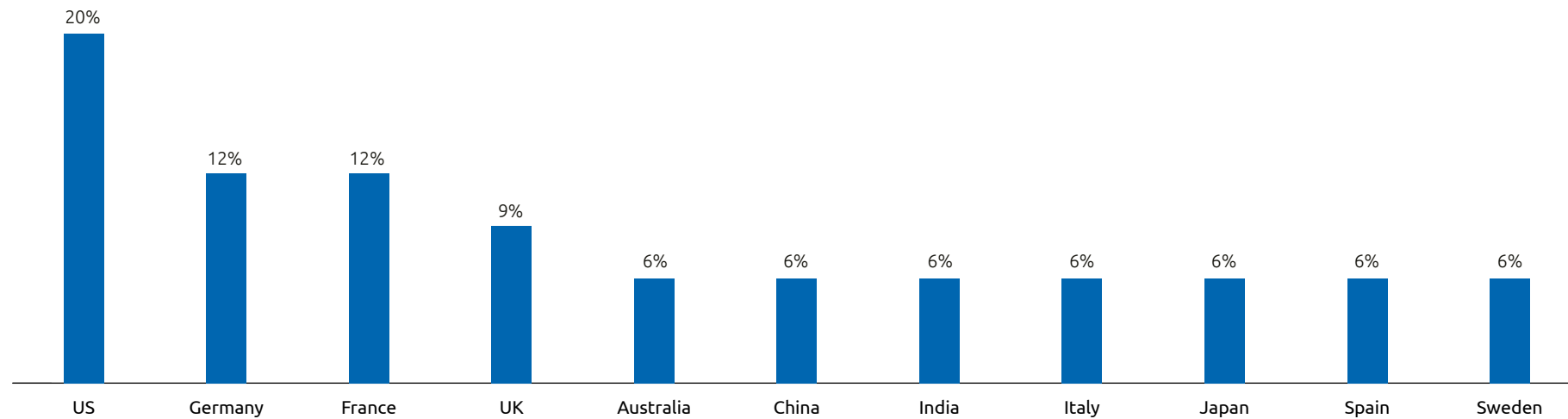
Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

Percentage of executives by job title

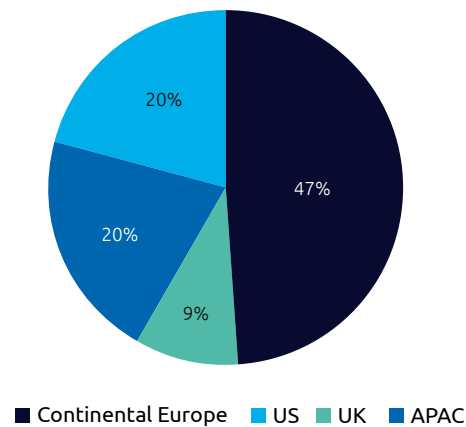


Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

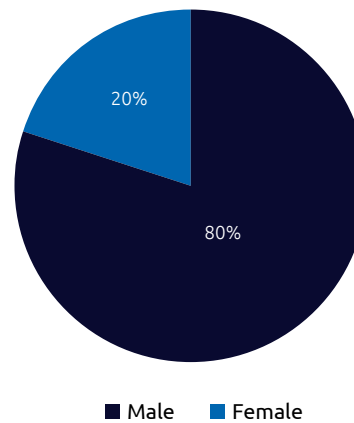
Percentage of executives by country



Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

Percentage of executives by region

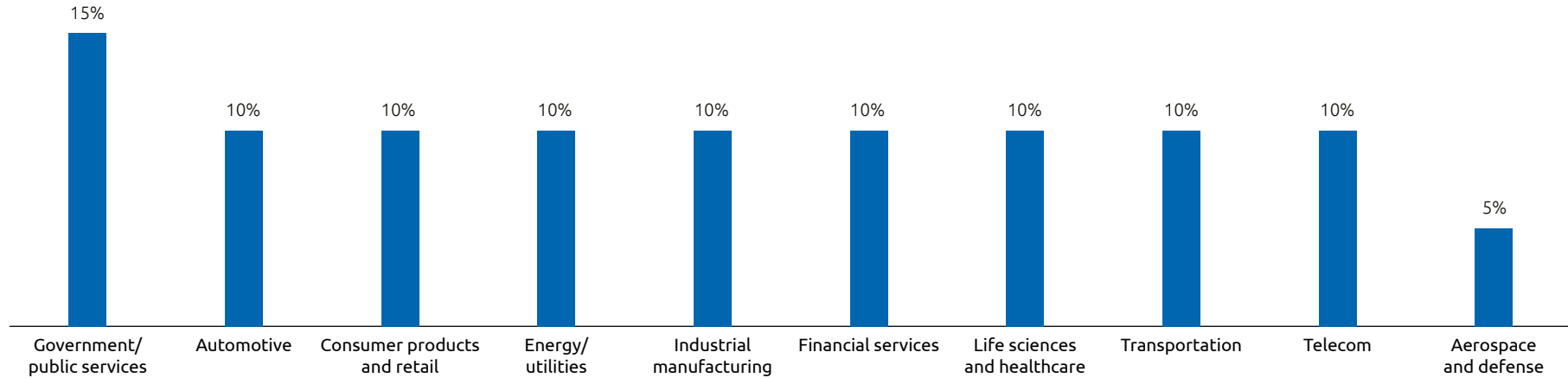
Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

Percentage of executives by gender

Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

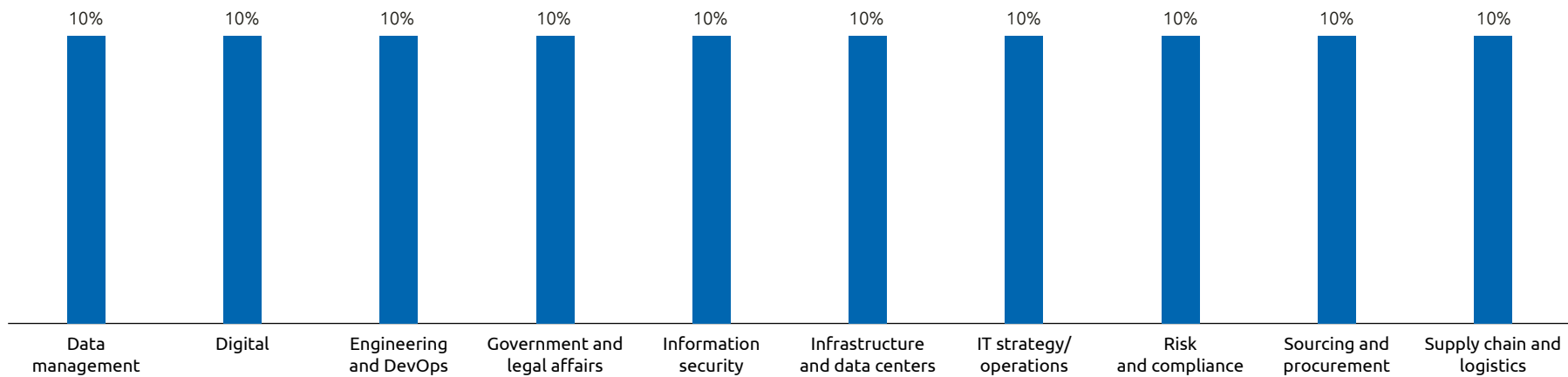


Percentage of executives by industry



Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

Percentage of executives by function



Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

References

1. The European Commission, "The future of European competitiveness," September 2024; Report on the state of the Digital Decade 2023, September 2023.
2. The European Commission, "Strengthening Europe's tech sovereignty," Website accessed June 2026.
3. Wikipedia, "2025 Iberian Peninsula blackout," accessed May 2026.
4. Claranet, "Broadcom's acquisition of VMware: effects on licensing, products, and cloud strategy," August 2025.
5. Revue Politique et Parlementaire, Thomas Courbe, "Mastering digital technology to maintain sovereignty: France's strategy to reduce our dependencies," May 2026.
6. Gartner, "Gartner survey reveals geopolitics will drive 61% of CIOs and IT leaders in Western Europe to increase reliance on local cloud providers," November 2025.
7. T-Systems, "T-Systems appoints its first Chief Sovereignty Officer," January 2025.
8. Ibid.
9. Orange, "Orange appoints Guillaume Poupard Chief Trust Officer to accelerate its sovereignty and trust strategy," December 2025.
10. The European Commission, "Strengthening Europe's tech sovereignty," Website accessed June 2026; The European Commission, "Proposal for a regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act)" June 3, 2026.
11. MIT Technology Review, "Everyone wants AI sovereignty. No one can truly have it," January 2026.
12. Gartner, "Gartner survey reveals geopolitics will drive 61% of CIOs and IT leaders in Western Europe to increase reliance on local cloud provider," November 2025.
13. Reuters, "EU cloud rules to curb Big Tech's access to strategic tenders, draft document shows," June 2026.
14. International Trade Administration, "Semiconductors including chip design for AI," December 2025.
15. CNBC, "What the U.S.-Taiwan deal means for the island's 'silicon shield'," January 2026.
16. CNBC, "'Impossible': Taiwan pushes back against Washington's 40% chip supply relocation goal," February 2026.
17. Financial Times, "EU pushes for 'tech sovereignty' to cut reliance on US," May 2026.
18. Ibid.
19. Reuters, "EU Commission awards 180 million euro cloud contract to four European providers," April 2026.
20. Capgemini Research Institute, Conversations for Tomorrow #11, "Tuning the sovereignty dial: Innovation, choice, and the future of cloud," June 2026.
21. EU Artificial Intelligence Act, "High-level summary of the AI Act," updated in May 2026.

22. Capgemini Research Institute, Conversations for Tomorrow 11, "Tuning the sovereignty dial: Innovation, choice, and the future of cloud," June 2026.
23. Airbus, "Airbus partners with Mistral AI to strengthen the use of artificial intelligence in sovereign aerospace applications," May 2026.
24. Deutsche Telekom, "Telekom to build sovereign AI platform for the German federal government," May 2026.
25. CNBC, "Trump administration's AI crackdown opens door for China to close gap," June 30, 2026; Bloomberg, "Trump's Anthropic crackdown sets off AI alarms for US allies," June 16, 2026.
26. Gartner, "Gartner says worldwide sovereign cloud IaaS spending will total \$80 billion in 2026," February 2026.
27. Amazon News, "AWS launches AWS European Sovereign Cloud and announces expansion across Europe," January 15, 2026.
28. Microsoft, "Microsoft strengthens sovereign cloud capabilities with new services," November 2025.
29. Microsoft, "Announcing comprehensive sovereign solutions empowering European organizations," June 2025.
30. SAP News Center, "SAP launches Sovereign Cloud in France in partnership with Bleu," March 19, 2026.
31. Google Cloud Press Corner, "Thales announces strategic partnership with Google Cloud to launch new sovereign cloud in Germany," May 20, 2026; Germany Federal Office for Information Security, Criteria enabling Cloud Computing Autonomy (C3A), April 27, 2026.
32. Oracle, "SoftBank Corp. accelerates Japan's AI and sovereign cloud future with Oracle Alloy," October 2025.
33. Oracle, "Oracle accelerates sovereign AI with first Supercluster deployment in the Middle East," November 2025.
34. IDC, "Over 60% of Asia/Pacific enterprises see regulatory disruption to IT Operations, says IDC," July 2025.

Authors

Meet the experts



Karine Brunet

Chief Operations and Delivery Officer
karine.brunet@capgemini.com

Karine Brunet is Chief Operations and Delivery Officer at Capgemini and a member of the Group Executive Board, roles she has held since January 2026. Previously, she was CEO of Capgemini's Cloud Infrastructure Services and before that served as COO, joining the Group Executive Committee in 2023. With a strong track record in leading large-scale transformation and infrastructure services organizations, Karine brings deep operational and technology expertise from senior roles at Vodafone, Steria, and Alcatel Group.



Nicolas Gaudilliere

Chief Technology Officer, Invent France
nicolas.gaudilliere@capgemini.com

A CentraleSupélec engineer, Nicolas started his career in the 2000s. He initially worked as a cybersecurity consultant, before helping to set up cloud service platforms for telecom operators and major integrators. In 2015, he joined Capgemini Invent as CTO to focus on the organizational and human transformations required for the implementation of numerous technological innovations such as IoT, cloud, AI, blockchain, 5G, and quantum. Nicolas previously oversaw the telco, media, and tech sectors, supporting customers in optimizing their business strategies to seize new growth opportunities, streamlining their industrial models, and expanding their technological innovation policy. Today, he oversees agentic AI for enterprise transformation and helps clients integrate AI to autonomously execute workflows, make decisions, and coordinate tasks across enterprise systems to achieve business outcomes.



Craig Suckling

Executive Vice President, Global Head of Agentic Scale
craig.suckling@capgemini.com

Craig is an Executive Vice President and Global Head of Agentic Scale. Before joining Capgemini, he was Chief Data Officer for the UK government, accountable for strategy and change agenda for data and AI, and before that global head of data and AI strategy for Amazon Web Services. Craig has held numerous other roles in the private sector, including CDO, startup founder, and advisory board member. He featured in the top 100 data and AI leaders in Europe in 2020-25, and the top 100 global data and AI leaders in 2024.



James Dunn

Director of Global Cloud and Sovereign Strategy, Cloud Infrastructure Services
james.dunn@capgemini.com

James is a technically astute and visionary leader with over 15 years of experience driving enterprise cloud transformation. He brings deep expertise in strategic sales, offering co-creation, partner ecosystem management, and technical leadership. James has successfully led global business units across cloud migration, DevOps, platform engineering, and managed services, delivering high-impact outcomes and accelerating cloud adoption at scale.

Authors

Meet the Capgemini Research Institute



Jerome Buvat

Head of the Capgemini Research Institute
jerome.buvat@capgemini.com

Jerome is the head of the Capgemini Research Institute. He works closely with industry leaders and academics to help organizations understand the business impact of emerging technologies.



Marisa Slatter

Director, Capgemini Research Institute
marisa.slatter@capgemini.com

Marisa is a Director at the Capgemini Research Institute. She collaborates with industry leaders to understand challenges and opportunities relating to emerging technologies, innovation, and sustainability.



Vaishnavee Ananth

Manager, Capgemini Research Institute
vaishnavee.a@capgemini.com

Vaishnavee is a Manager at the Capgemini Research Institute. She works closely with industry leaders and academics to inform clients about the impact of emerging technologies and evolving consumer behavior on their businesses and society.

The authors would like to thank Maarten Bal, Laura Immonen Beatty, Lukas Birn, Philipp Fürst, Brian Hammond, Stephen Hilton, Rens Huizenga, Melania Manti, Alex Marandon, Amit Patil, Tiphaine Pearson, Marc Reinhardt, Bilal Mohammad Sajid, and Tricia Stinton, Punam Chavan, Subhadra Chakraborty, Aparajita Paul, Vibha Palekar, Manish Saha, Sonali Malekar, Soumi Biswas, Surojit Majhi and Madan Dhar for their contributions to the research.

For more information, please contact:

Global

Nicolas Gaudilliere

nicolas.gaudilliere@capgemini.com

France

Guillaume Renaud

guillaume.renaud@capgemini.com

Sweden

Johan Lindh

johan.lindh@sogeti.se

Denmark

Martin Jensen

martin.jensen@capgemini.com

Norway

Gard Nordby

gard.nordby@capgemini.com

Germany

Lukas Birn

lukas.birn@capgemini.com

United Kingdom

Adam Parfitt

adam.parfitt@capgemini.com

Netherlands

Herjan van den Hengel

herjan.van.den.hengel@capgemini.com

Partner with Capgemini for Digital Sovereignty

How to mitigate digital technology risks in the face of geopolitical upheavals?

Capgemini digital sovereignty assessment

We will rapidly help you define your sovereignty objectives, assess your exposure and get actionable recommendations tailored to your market.

1.A Sovereignty assessment

Create a clear understanding on risk and a vision for a sovereignty posture for your organization

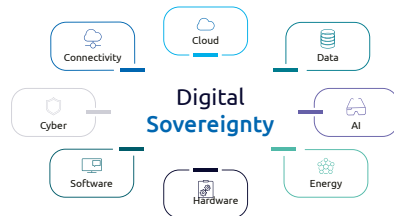
Boardroom questions answered by this assessment

- What is sovereignty for your organization?
- What is your sovereignty posture?
- What is your risk exposure?
- What is the appropriate sovereignty target state?
- What are the next steps to achieve that sovereignty level?

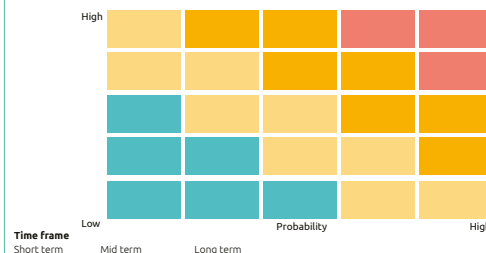
Deliverables

- Overview of relevant regulations
- Sovereign risk profile
- Sovereignty compass
- Risk mitigation scenarios including organizational impact
- High level impact on IT, TOM, budget impact

Sovereign assessment scope



Risk assessment HEAT map (example)



1.B Next steps

Begin to execute your digital sovereign strategy

Potential next deliverables*

Sovereign assessment ✓

- Cloud security, compliance and governance framework
- Infrastructure and application portfolio analysis
- Cloud vendor selection
- Target operation model
- Enterprise architecture future state
- Detailed scenarios overview
- Detailed roadmap
- Business case
- Sovereign execution plan and offer
- Data classification

More Capgemini Research Institute publications



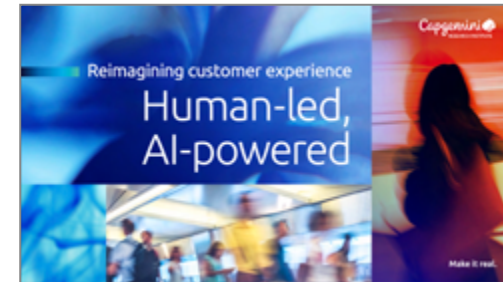
Conversations for Tomorrow #11-Digital sovereignty



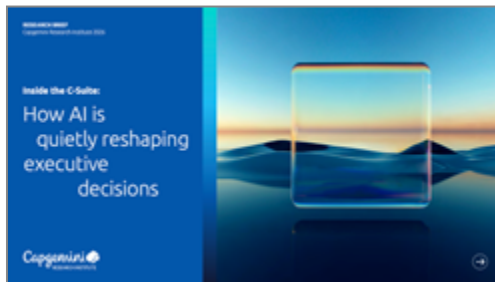
AI in robotics



Reindustrialization



AI-powered CX transformation



AI and decision-making



AI and data centers



B2B pulse for telcos

Subscribe to latest research from the Capgemini Research Institute



Receive copies of our reports by scanning the QR code or visiting

<https://www.capgemini.com/capgemini-research-institute-subscription/>

Capgemini Research Institute

Fields marked with an * are required

First Name *

Last Name *

Email *

☐ By submitting this form, I understand that my data will be processed by Capgemini as indicated above and described in the [Terms of use](#).

Submit



About Capgemini

Capgemini is an AI-powered global business and technology transformation partner, delivering tangible business value. We imagine the future of organizations and make it real with AI, technology and people. With our strong heritage of nearly 60 years, we are a responsible and diverse group of over 420,000 team members in more than 50 countries. We deliver end-to-end services and solutions with our deep industry expertise and strong partner ecosystem, leveraging our capabilities across strategy, technology, design, engineering and business operations. The Group reported 2025 global revenues of €22.5 billion.

Make it real | www.capgemini.com