Press contact:
Victoire Grux
Tel.: +33 6 04 52 16 55
E-mail: victoire.grux@capgemini.com

Most organizations say full digital sovereignty is an unrealistic goal as businesses prioritize resilience over total independence

- ***93% of organizations worldwide have discussed digital sovereignty at board level***
- ***Two thirds define digital sovereignty in terms of resilient interdependence and say selective control of critical technologies, combined with strategic partnerships, is more practical than full ownership***
- ***More than half believe they can strengthen digital sovereignty without sacrificing competitiveness***

Paris, September 8, 2026 – Sovereignty is now a boardroom priority for most organizations, but 59% of them say full digital sovereignty is not a realistic goal, according to the Capgemini Research Institute's latest report, *Digital Sovereignty: From Policy Ambition to Executive Imperative*, based on a survey of 1,300 business and technology executives. The research finds that rather than pursuing complete technological independence, organizations are taking a pragmatic approach focused on protecting critical operations, retaining control over key digital capabilities, and avoiding dependence on any single provider.

Technology dependencies leave organizations exposed
According to the report, over the past decade, organizations have accelerated cloud migration, AI adoption, and digital transformation, often faster than governance and resilience models have evolved. At the same time, they have become increasingly reliant on a small number of global technology providers, but in recent years geopolitical tensions and supply chain disruption have exposed the risks of technology concentration. Capgemini's Digital Sovereignty Index, based on an analysis of 866 organizations in the US, Europe and APAC across 5 sovereignty dimensions, shows that 86% of them have significant exposure to foreign or externally controlled supply chains.

Most organizations report heavy dependence on foreign suppliers, concentrated supplier bases, limited supply chain visibility, and lengthy switching timelines, as increasing their vulnerability to disruptions. Despite this, contingency planning remains uneven by region – just 42% of organizations that have recently experienced operational disruptions have this in place. Preparedness is highest in the US, where almost two thirds of organizations have contingency plans, compared with slightly more than a third in Europe and APAC.

Digital sovereignty climbs up the board agenda
Sovereignty is now a focus for the C-suite, with 44% of organizations ranking digital sovereignty as a board's top priority. This is translating into action, with nearly four in five organizations executing or building a strategy, while a further fifth expect to put one in place within the next year. This investment reflects mounting concern over the ability of organizations to maintain critical business operations in an increasingly uncertain geopolitical environment – more than three quarters of them are highly concerned according to the report.

Operational resilience to geopolitical volatility and disruption is the leading driver of digital sovereignty initiatives, cited by four in five respondents. AI has emerged as the area of the tech stack that organizations prioritize in the pursuit of sovereignty, with three quarters identifying it as a key focus area. A particular emphasis is evident in sectors, like aerospace and defense and transportation, that manage critical infrastructure, information, or operations.

"Today's organizations operate in highly interconnected technology ecosystems where complete independence is rarely achievable. Digital sovereignty is therefore not about full autonomy but more about ensuring organizations have a clear understanding of their technology dependencies, in order to regain the control and flexibility to manage risks," said Karine Brunet, Chief Operations and Delivery Officer at Capgemini and member of the Group Executive Board. *"This will enable them to build the best, pragmatic roadmap to meet their strategic objectives – taking into account data localization, access*

control, operations, regulatory and technology constraints. The real challenge will be to build resilience without sacrificing competitiveness, to drive innovation and long-term growth."

Despite regional nuances, most agree that it is not about complete technological independence
Although digital sovereignty has become a global business priority, organizations in different regions are pursuing alternative strategies. Across APAC (41%), continental Europe (52%), and the UK (56%), digital sovereignty is most associated with risk mitigation and resilience-building. In contrast, over half of US organizations (52%) primarily view it through a compliance lens, compared with 40% who see it as a resilience-building tool. In addition, organizations in APAC and in continental Europe express significantly more concern about maintaining critical business operations amid geopolitical uncertainty than those in the US and in the UK.

Despite these regional differences, organizations broadly agree that digital sovereignty is not about complete technological independence. Two thirds globally define digital sovereignty in terms of resilient interdependence, although this view is stronger in Europe (75%) than in the US (50%).

Organizations also differ in how they plan to achieve digital sovereignty. Globally, more than two thirds of organizations surveyed anticipate a combination of internal development and external collaboration in their pursuit of digital sovereignty. However, US organizations place greater emphasis on ecosystem collaboration and industry partnerships to develop shared capabilities, than organizations in APAC and Europe.

Visibility, vendor lock-in and cost stand in the way of digital sovereignty
Execution challenges remain. Only 14% of organizations report having end-to-end visibility into dependencies across their broader technology ecosystem, making it difficult to assess exposure to geopolitical or supplier-related risks. Another hurdle is reducing dependence on critical technology providers. More than a third (36%) of organizations report that transitioning away from a critical provider would take more than 12 months, while one in 10 say they have no viable alternative provider at all. Finally, just under half are willing to pay a 'digital sovereignty premium' (of 23% on average), which underlines the challenge of cost and competitiveness that comes with increased sovereignty requirements.

To access the full report: https://www.capgemini.com/insights/research-library/digital-sovereignty/

Methodology of the report
The Capgemini Research Institute surveyed 1,300 business and technology executives across industries at organizations with over $1 billion in annual revenue and government departments with over $1 billion in annual budget across the US, the UK, continental Europe (France, Germany, Italy, the Netherlands, Spain, Sweden) and APAC (Australia, China, India, Japan), in April 2026. The research team also interviewed 13 senior executives at leading global organizations.