

# Digital Sovereignty

From policy ambition to executive imperative

Make it real.

## Digital sovereignty has entered the mainstream

### Digital sovereignty is no longer optional



Organizations worldwide are highly *concerned about securing critical business operations* amid current geopolitical tensions

### Nearly half of organizations view it as a risk-mitigation/resilience-building approach

Principal view of digital sovereignty



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

### Digital sovereignty is on the boardroom agenda



## Digital sovereignty means resilient interdependence not absolute independence

2 in 3

organizations say so

Digital sovereignty is more about *interdependence* than isolation

7 in 10

organizations say so

Being digitally sovereign means having the *capacity to choose technological dependencies*

### Digital sovereignty exists on a spectrum

Most (59%) organizations admit that full digital sovereignty is not a realistic goal

### The strongest motivators to pursue digital sovereignty today are:



## Organizations face significant technology dependency risks



## Organizations are pragmatic in their pursuit of digital sovereignty

Across the 8 dimensions of the tech stack, *most organizations prioritize AI and data* in their pursuit of digital sovereignty

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

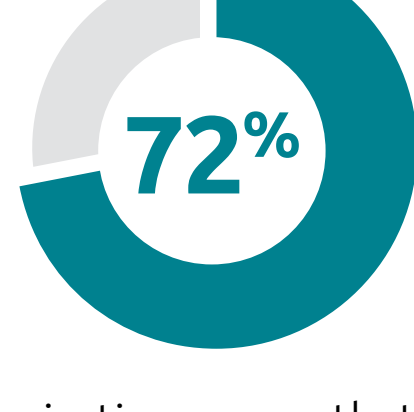
Organizations' desired level of digital sovereignty across the tech stack



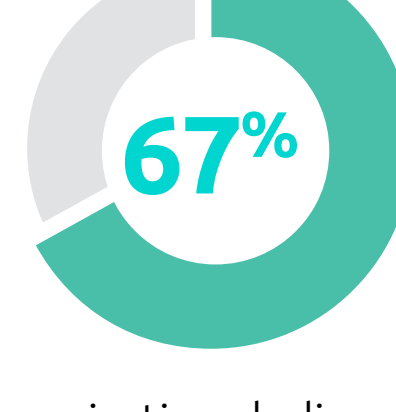
Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

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).

Most organizations are clear that they will *not compromise on vendor choice or performance* to reach their desired level of digital sovereignty



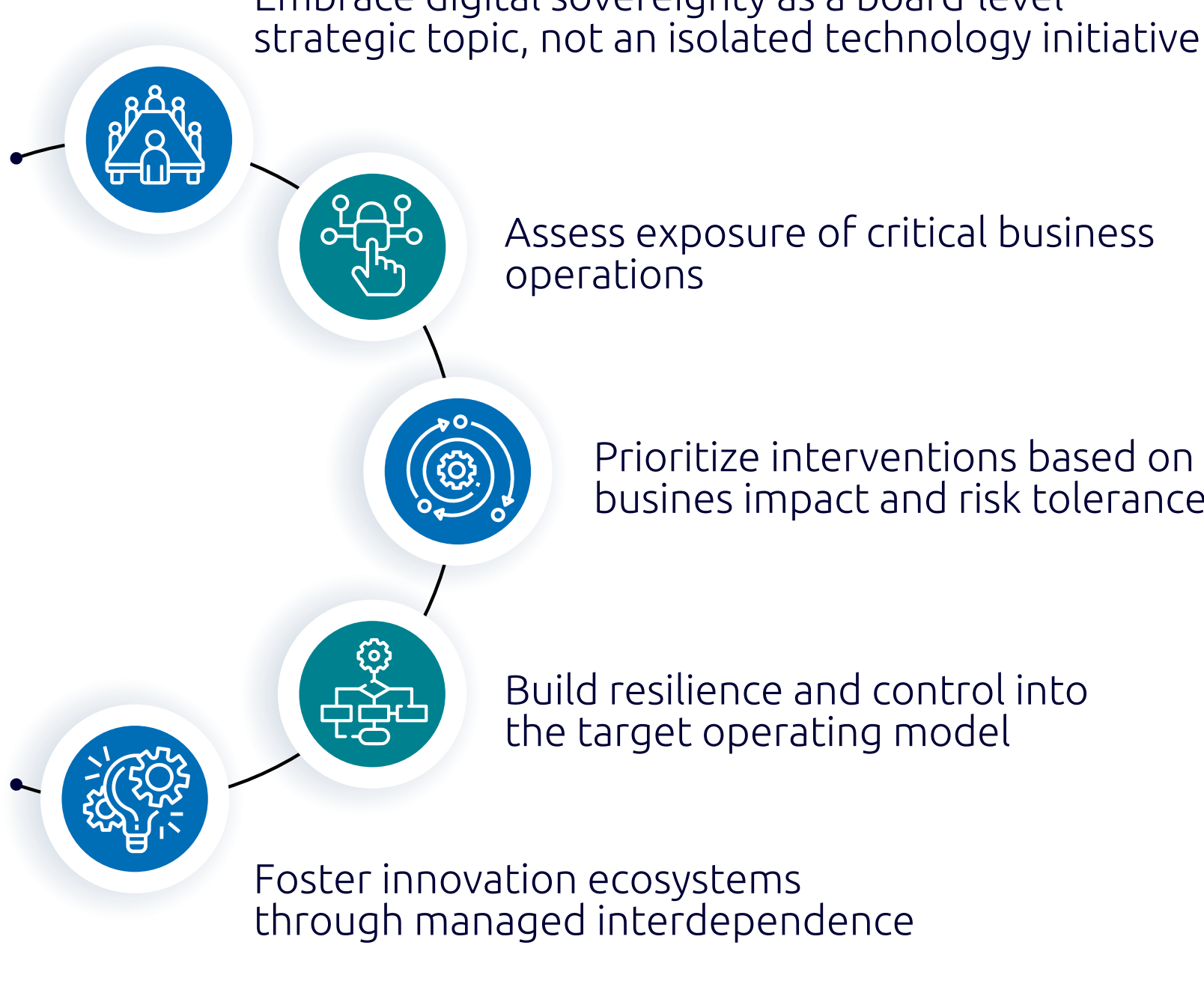
of organizations agree that active participation in ecosystems and/or consortia is essential to achieve digital sovereignty



of organizations believe that digital sovereignty can enable innovation

In the future, *nearly half of organizations 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

## How organizations can begin their digital sovereignty journeys



Download report

Subscribe to our research