

Digital Sovereignty for Governments and Enterprises

Building Resilient Technology Ecosystems on Collaboration, Innovation, and Openness

Governments have a sovereign interest in ensuring capable, resilient, and secure digital environments at home. The Business Software Alliance (BSA) urges policymakers that are pursuing digital sovereignty to focus on supply-chain resilience through frameworks grounded in collaboration, innovation, openness, and choice—not exclusion and self-isolation.

BSA members include companies from around the world that are leaders in artificial intelligence (AI), cybersecurity, cloud computing, quantum, and other breakthrough technologies. As enterprise software companies, BSA members develop and deliver trusted technologies that businesses, governments, and institutions rely on to manage sensitive data, comply with complex rules, strengthen cybersecurity, and deploy AI and other emerging technologies responsibly. Enterprise software companies are committed to the highest standards of privacy, security, reliability, and governance because they are essential conditions for customers around the world.



Resilient Digital Ecosystems Require Collaboration and Partnership.

BSA members—partners to national governments and industries in AI, quantum, cloud, and enterprise software—have made substantial, long-term investments in digital ecosystems around the world. These include operating geographically distributed cloud-computing capacity; processing data in accordance with local legal requirements; employing and training digital professionals and engineers in local markets; and collaborating with national governments

and international institutions on digital governance frameworks. Similarly, through transparent contracts, legal safeguards, and technical measures such as encryption, pseudonymization, and local data storage and processing options, BSA members can give their customers control over their data while benefiting from global innovation.

In sum, governments that choose partnership over exclusion secure access to more capable, more innovative, and more resilient technology than those that do not.



Resilient Digital Ecosystems Require Innovation and Investment From Around the World.

Digital sovereignty is grounded in investments in people, infrastructure, and innovation ecosystems—cultivating the expertise, competitive markets, and trusted technology partnerships that promote true digital capability and resilience. Blanket restrictions on foreign providers, products, or services do the opposite: they narrow the technology supply chain, raise costs, and reduce capability by depriving users of access to best-in-class solutions.



Resilient Digital Ecosystems Benefit From Global Standards and Contingency Planning Best Practices.

The concern that access to a critical service provider might become unavailable—whether due to financial failure, geopolitical disruption, or operational incident—is not a new problem, and managing it is already a mature discipline. Companies operating internationally have developed robust contingency planning best practices. Internationally recognized standards codify these approaches, including ISO and other specifications that allow enterprises to benchmark their operational readiness, redundancy, and resilience to support business continuity during disruptions, including geopolitical events.

Such standards reflect a key insight: digital resilience comes from *diversity and choice across providers and technologies*—precisely the kind of supply-chain architecture that open, competitive markets produce and that restrictive, origin-based mandates undermine.



Resilient Digital Ecosystems Require Diversity of Supply.

Resilience depends on diversity of supply, including in hybrid- and multi-cloud

environments. Conversely, a government that concentrates critical digital operations exclusively on national cloud providers has not eliminated risk—it has increased it, foreclosing the supply-chain choice that genuine resilience requires. Multi-cloud and hybrid architectures that combine providers with different capabilities and technical footprints offer more robust protection than any single-origin model.



Resilient Digital Ecosystems Are Antithetical to Arbitrary, Discriminatory, Disguised, or Unnecessary Digital Access Barriers.

Preparing for geopolitical risk events, including the possibility that access to services in one jurisdiction might be unjustifiably restricted, is already embedded in international trade rules and best practices that prohibit the application of arbitrary, discriminatory, disguised, or unnecessary restrictions on digital trade, cross-border data transfers, or continuity of access to technology. Countries should work to build on and strengthen these rules and practices.



A Policy Roadmap: How Governments Can Build Resilient Digital Ecosystems.

BSA strongly supports digital sovereignty initiatives that work with market incentives rather than against them. Constructive approaches include:

- » Commitments among allies to ensure continuity of digital services;
- » Non-discriminatory R&D grants and tax incentives for domestic digital investment;
- » Public investment in high-performance computing and digital infrastructure accessible to startups and industry;
- » Transparent, risk- and capability-based procurement criteria focused on security performance rather than provider nationality;
- » Interoperable, industry-driven standards for data-, cyber-, and supply-chain risk management that empower user choice; and
- » Early warning and consultation mechanisms between trading partners to manage cross-border service risks cooperatively.

Governments should avoid mandates that impose political mandates that impose blanket exclusions based on provider origin rather than demonstrated risk, such as prescriptive “buy domestic” mandates that undermine competition, reduce technological capacity, and limit user choice. Such mandates impede the cross-border investment and innovation that drive productivity.

THE BOTTOM LINE.

The hallmark of digital sovereignty is resilience. Resilience requires collaboration, innovation, and openness—grounded in investments in digital capacity, interoperable norms of risk management and contingency planning, and access to best-in-class technologies from around the world. These are the foundations of a trusted technology ecosystem that is resilient for the long term.