Business Software Alliance

July 2026

INDIA'S DIGITAL SOVEREIGNTY

Building Capability, Collaboration, Resilience, and Trust into India's Digital Ecosystem

Executive Summary

India is entering a new phase of its digital transformation. As artificial intelligence (**AI**), cloud computing, and cybersecurity become increasingly important to supporting economic growth and public services, questions of digital sovereignty have become both timely and consequential.

Governments around the world are seeking to strengthen the sovereignty and strength of their digital ecosystems in an increasingly complex geopolitical and cybersecurity environment.

"Digital sovereignty" should be understood as the ability to promote a digital ecosystem built on capability, collaboration, resilience, and trust. This is a particularly effective pathway to advance a sovereign ability to govern and secure, critical digital systems while maintaining access to innovation, investment, and advanced technologies.

India stands out globally as an unparalleled technology leader and pioneer. As such, India can advance its domestic interests and lead internationally by:

1. Strengthening India's **capabilities** from a digital infrastructure, innovation, and skills perspective;
2. Promoting **collaboration** on both industry-to-government and government-to-government levels;
3. Designing greater **resilience** and redundancy into digital ecosystems; and
4. Adopting measures that promote digital trust.

India's Sovereignty Opportunity

Digital sovereignty has emerged as an important policy objective for many governments. Governments are examining how to reduce supply chain and infrastructure vulnerabilities from a cyber-, economic-, and national-security perspective.

India approaches these discussions having built a strong foundation across the technology stack. Over the last decade, India has demonstrated global leadership in building digital systems at scale. Reflecting its competitive strength, India has become one of the world's leading destinations for technology investment, with global technology companies investing in infrastructure, engineering, and research capabilities across the country. These investments have helped create a vibrant ecosystem of Global Capability Centres (GCCs) that contribute to employment, skills, and technology transfer.

For India, therefore, the question is how to strengthen its digital self-empowerment and resilience while continuing to benefit from global innovation, investment, and collaboration.

Sovereign Cloud in Context

Different government workloads present different levels of sensitivity and risk. Military or other systems of national strategic importance may warrant enhanced sovereignty safeguards, while routine government functions and lower-risk workloads benefit from greater flexibility.

A risk-based approach can help ensure that sovereignty requirements remain proportionate for highly sensitive national security systems, without compromising access to secure, scalable, and innovative technologies for most workloads. Such an approach can also support continued digitization, AI adoption, competition, and efficient public service delivery

Pillar I: Strengthening Sovereignty Through Investments in Capability

Long-term sovereignty ultimately depends on capability.

India's ability to govern and secure digital systems will depend on continued investments in digital skills, cybersecurity talent, AI expertise, cloud engineering, standards development, and research and development, as well as in building relationships with like-minded countries that can offer complementary technologies in the AI value chain.

The growth of GCCs, R&D hubs, and Centres of Excellence (CoEs) provides a particularly compelling use case. These units increasingly undertake core engineering, product development, cybersecurity, AI research, and cloud operations functions. Their presence strengthens India's domestic technology capabilities while embedding Indian talent and innovation within global value chains. Similarly, India's startup ecosystem, academic institutions, and public-private partnerships all contribute to strengthening India's domestic capability.

India's global technology leadership demonstrates that digital sovereignty is grounded in digital capacity investments in people, infrastructure, and innovation ecosystems — cultivating the expertise, competitive markets, and trusted technology partnerships that promote true digital capability.
Building out digital capability is a core pillar of digital sovereignty.

Pillar II: Sovereignty Through Collaboration

Digital sovereignty is not possible without collaboration. Governments and economies that have pursued collaboration and partnership have become more technologically advanced, competitive, and secure.

Collaboration has national and international dimensions. At a national level, government bodies, the private sector, academic institutions, and technical experts each play a role in developing secure and resilient digital ecosystems. At the international level, governments should collaborate to commit that they will not weaponize digital rules against one another. This requires commitments not to impose arbitrary, discriminatory, disguised, or unnecessary restrictions on digital trade, cross-border data transfers, or

continuity of access to technology, and to support the development of internationally recognised technical standards.

India's experience demonstrates the advantages of building sovereign strength through openness, innovation, talent, and collaboration. India is not only a consumer of technology, but also an important contributor and exporter to global digital innovation, as evidenced by India's successes in its startup ecosystem, especially in B2B and enterprise services, its growing AI and cloud computing capabilities, and its leadership as a destination for GCCs, R&D centres, and CoEs. Likewise, India's leadership in international initiatives such as the Global Partnership on AI and the Global AI Impact Summit demonstrates the value of collaboration in addressing complex digital policy challenges. Similarly, India has a growing opportunity to emerge as a global leader in promoting government-to-government collaboration on digital norms under India's bilateral agreements and in multilateral fora.

Collaboration within and across governments and industries is the second pillar of digital sovereignty.

Pillar III: Building Sovereignty Through Resilience

Resilience is a core component of sovereignty. Governments need confidence that essential services can withstand and recover from disruption. Critical digital systems must continue to operate during cyber incidents, natural disasters, infrastructure shutdowns, or geopolitical disruptions. The need to manage these concerns is not new. Nor are the solutions to do so.

As governments continue to strengthen sovereign cloud requirements, greater mutual recognition of internationally accepted cloud security assurance frameworks can reduce unnecessary duplication while maintaining high levels of security. Internationally recognized standards help codify approaches that allow enterprises to benchmark their resilience in terms of operational readiness, redundancy, responsiveness, and recovery capacity during disruptions, including during geopolitical events.

Likewise, resilient hybrid- and multi-cloud architectures, hybrid deployment models, disaster recovery systems, portability requirements, and open and interoperable internationally-recognised standards can reduce single points of failure and improve continuity. Interoperable platforms and flexible architectures are essential for driving innovation, avoiding market fragmentation, and enabling organisations to adopt best-fit solutions

Such standards and business practices 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 destroy. Rather than concentrating risk in any single provider, technology stack, or infrastructure model, sovereignty frameworks should encourage architectures that support choice, continuity, and contingency planning.

Resilience — based on interoperable internationally-recognised standards and best practices — is the third pillar of digital sovereignty.

Pillar IV: Building Sovereignty Through Trust

Many sovereignty concerns are ultimately concerns about trust in relation to digital governance.

Governments' concerns regarding extraterritorial jurisdiction, lawful access to sensitive data, and continuity of critical digital services are legitimate and increasingly shared across jurisdictions. Governments need to be able to

trust that sensitive systems will remain secure, that access can be appropriately controlled, that risks are auditable, and that accountability mechanisms are effective. In this regard, trust is strengthened through a combination of technical, organizational, and legal safeguards.

These include, encryption, key management, identity and access management, auditability, transparency requirements, contractual commitments, certification frameworks, and incident response capabilities. Many sovereign cloud frameworks focus on these types of safeguards to ensure that critical systems remain under appropriate functional control and oversight.

Advances in privacy-enhancing technologies (PETs), including confidential computing, advanced encryption techniques, and secure computation methods, are expanding the range of technical options available to governments seeking to strengthen sovereignty objectives while maintaining interoperability and access to global innovation.

These increasingly sophisticated and robust technical safeguards are bolstered by government-to-government arrangements and modernized legal cooperation mechanisms.

As the fourth pillar of digital sovereignty, trust is most effectively built through a combination of legal, technical, operational, and diplomatic mechanisms.

Recommendations for India's Digital Sovereignty Framework

BSA offers the following recommendations for a future-oriented sovereignty framework built on capability, collaboration, resilience, and trust:

1. Adopt a risk-based and technology-neutral approach.
2. Promote interoperability and open, internationally recognised standards.
3. Build trust through governance, transparency, and safeguards.
4. Strengthen resilience through diversity and redundancy.
5. Preserve flexibility for routine and non-sensitive workloads.
6. Encourage capability-building through skills, innovation, and investment.
7. Promote outcome-based public procurement.
8. Institutionalize government-industry collaboration.
9. Promote competitiveness and innovation alongside sovereignty objectives.

These recommendations are aligned with sovereignty objectives that support innovation, growth, and competitiveness.

Conclusion

India's digital sovereignty journey presents a significant opportunity.

By focusing on capability, collaboration, resilience, and trust, India can strengthen digital self-empowerment while continuing to benefit from innovation, investment, and collaboration with like-minded partners.

Digital sovereignty is broader than any single technology or deployment model. It is about ensuring that India can confidently govern, secure, operate, and rely upon critical digital systems in an increasingly interconnected world.

ABOUT BSA

The Business Software Alliance (www.bsa.org) is the global trade association of the enterprise software industry, representing companies that are leaders in artificial intelligence, cybersecurity, cloud computing, quantum, and other breakthrough technologies. We work in over 20 markets in the US, Europe, and Asia, advocating for policies that build trust in technology so that every industry sector and the public can benefit from innovation.

BSA's members include: Adobe, Alteryx, Amadeus, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., TrendAI, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.