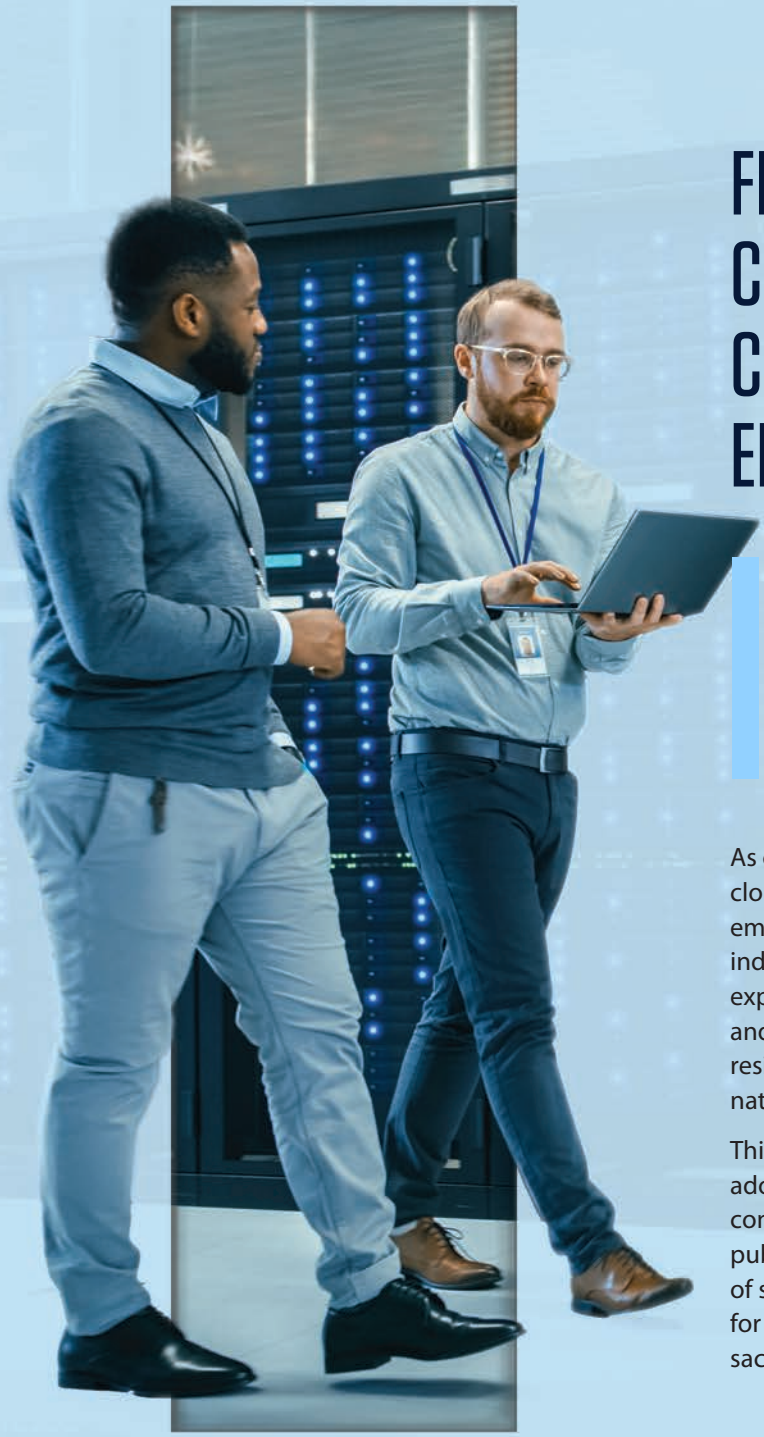
VIEWPOINT



FROM COMPLIANCE TO CONTROL: WHY SOVEREIGN CLOUD MATTERS FOR ENTERPRISES

As organizations continuously migrate critical workloads to cloud environments, the question of data sovereignty has emerged as a growing concern for governments, regulated industries, and enterprises operating across jurisdictions. The expansion of public cloud services while delivering agility and scale, has introduced complex challenges related to data residency, jurisdictional control, regulatory compliance, and national security.

This POV examines the security requirements driving the adoption of sovereign cloud architecture. It provides a comprehensive analysis of the risks inherent in non-sovereign public cloud deployments, articulates the foundational pillars of sovereign cloud security, and presents a strategic framework for organizations seeking to achieve digital sovereignty without sacrificing innovation.

Infosys
Navigate your next

Based on changing regulations like the EU's GDPR, India's DPDP Act, and industry rules such as HIPAA and PCI DSS, This POV explains that a sovereign cloud is more than compliance. It builds trust, makes systems more resilient, and strengthens the economy.

1. Industry Overview

1.1 The Rise of Cloud Computing

Cloud computing has transformed how organizations consume and deliver technology services. The global cloud infrastructure market has grown exponentially with enterprises of all sizes, relying on cloud platforms for compute, storage, data analytics, artificial intelligence, and application hosting. However, this growth has created a key challenge the need to move fast and operate globally, while still keeping data under control, following regulations, and protecting national security.

1.2 What Is a Sovereign Cloud

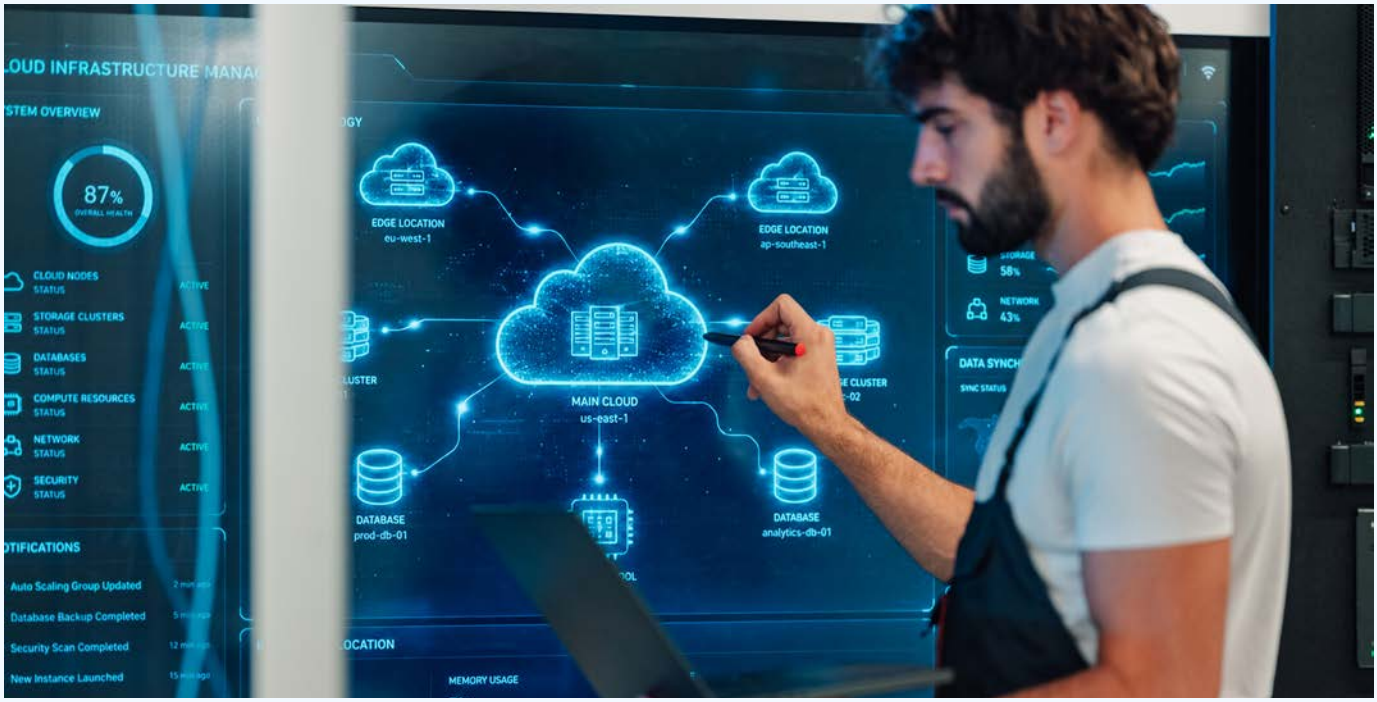
A sovereign cloud keeps data stored, processed, and accessed within the laws of the country where it operates. Unlike regular public clouds where data may move across countries and be subject to foreign laws, a sovereign cloud ensures that data is controlled only by local laws and regulations.

Sovereign cloud is especially important for organizations that handle sensitive data, such as defense agencies, public healthcare systems, financial authorities, operators of critical infrastructure, and any organization where data exposure could affect national security or competitive advantage.

1.3 Can a Standard Cloud Environment Be Transformed into a Sovereign Cloud?

Yes, a normal cloud (public cloud) can be transformed into or migrated to a sovereign cloud through a structured process. **Turning a normal cloud into a sovereign cloud requires architectural, operational, and legal changes,** not just configuration tweaks.

Data residency requires that all data, including backups, logs, and metadata, always remain within a defined country or region. Legal jurisdiction control ensures that this data is governed only by local laws, with no exposure to foreign government access or extraterritorial regulations. Access sovereignty restricts all administrative and support access to locally authorized personnel, eliminating or tightly controlling foreign access. Key and encryption control mandates that encryption keys are fully managed by the customer or a locally governed entity using local HSMs. Finally, operational independence and strong isolation ensure that cloud operations, monitoring, incident response, and infrastructure remain sovereign, secure, and isolated from multi-tenant risks.



2. Challenges and Risks of Public Cloud

While public cloud platforms offer compelling advantages in scalability, cost efficiency, and innovation velocity, they introduce significant risks that sovereign cloud architectures are specifically designed to mitigate. The following analysis details the six primary risk categories organizations face when relying on non-sovereign public cloud infrastructure.

2.1 Legal and Regulatory Non-Compliance

Organizations working across different countries must follow many different data protection and data storage laws. Regular (non-sovereign) cloud services often struggle to meet local requirements such as GDPR and India's DPDP Act. When they fail, the impact can be serious—large fines, penalties, limits on operations, or even losing the right to handle citizen data.

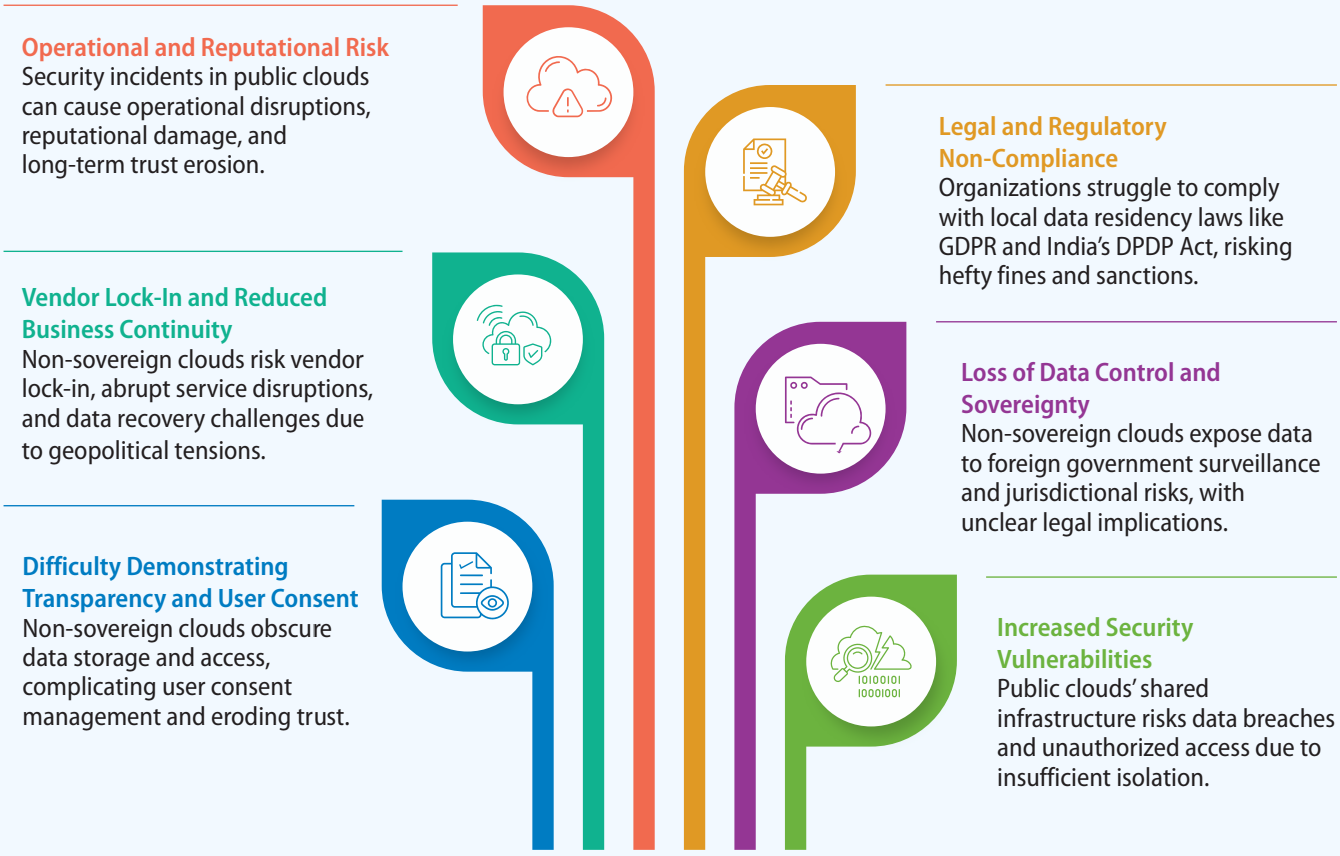
The situation is made worse by conflicting laws. For example, the U.S. CLOUD Act can require U.S. cloud providers to share data stored in other countries, which can clash with GDPR rules. This puts organizations in a difficult position, where it may be impossible to comply with all laws at the same time.

2.2 Loss of Data Control and Sovereignty

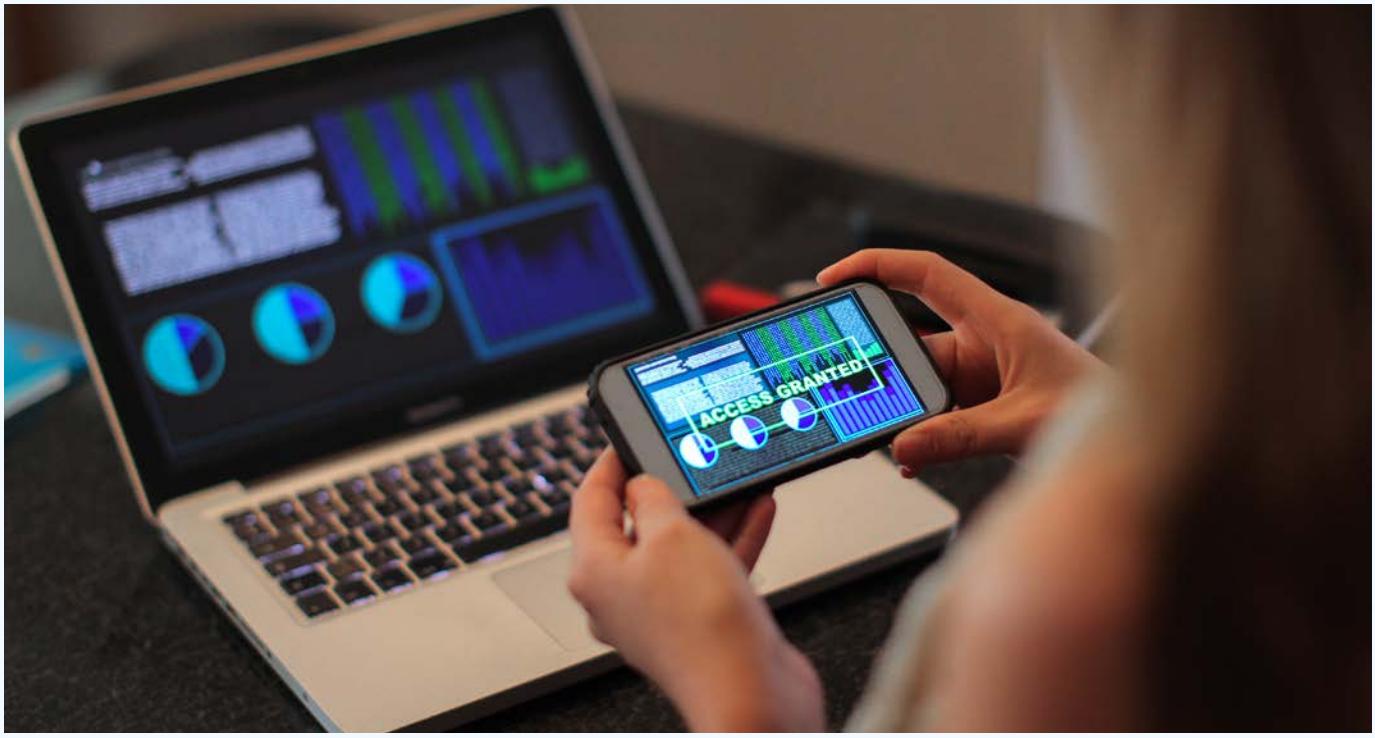
Non-sovereign clouds can expose data to foreign government access and legal risks. When data is stored in systems owned by companies from other countries, those governments may still claim legal rights over the data even if it is stored locally. This creates uncertainty for organizations about who really controls their data.

The loss of control goes beyond government access. Organizations may not fully know how their data is used, where copies are stored, who can access it, or which third parties are involved in handling the data.

Figure 1: Challenges and Risks of Public Cloud Adoption



External Document © 2026 Infosys Limited



2.3 Increased Security Vulnerabilities

Public clouds use shared systems, which can increase the risk of data breaches and unauthorized access. Because many customers share the same infrastructure, a software flaw, a configuration mistake, or a security issue in another customer's environment could expose sensitive data.

Public cloud environments also have a large attack surface. Shared hardware, common APIs, identity systems, and connected services all create possible entry points for attackers. As a result, nation-state attackers increasingly target cloud platforms because they offer access to high-value data in one place.

2.4 Operational and Reputational Risk

Security problems in public clouds can disrupt operations, harm an organization's reputation, and reduce trust over time. When a cloud provider has a breach or outage, customers feel the impact right away and often have little control over how quickly or effectively the issue is handled. Organizations cannot control the provider's response time, communication, or how problems are fixed.

Reputational risk is especially high for government agencies and healthcare organizations, where public trust is critical. A breach involving citizen data, health records, or sensitive government information can lead to long-lasting political, social, and public trust issues.

2.5 Vendor Lock-In and Reduced Business Continuity

Non-sovereign clouds risk vendor lock-in, abrupt service disruptions, and data recovery challenges due to geopolitical tensions. Proprietary APIs, data formats, and service architectures create deep dependencies that make migration costly and technically complex.

Geopolitical events can introduce sudden disruption risks. Sanctions, trade restrictions, or diplomatic conflicts may result in service suspension, data access restrictions, or forced migration timelines that organizations are unprepared for.

2.6 Difficulty Demonstrating Transparency and User Consent

Non-sovereign clouds make it hard to clearly see where data is stored and who can access it, which complicates user consent and reduces trust. Privacy laws today require organizations to clearly explain where data lives, who can access it, and why it is used. Public clouds often spread data across multiple locations and operate in ways that are not fully transparent.

This lack of transparency is especially challenging for organizations responding to GDPR data access requests, where they must clearly show what data they hold and how it is processed.

External Document © 2026 Infosys Limited

3. Key Pillars for Sovereign Cloud Adoption

Addressing the risks of non-sovereign cloud requires a structured approach built on five foundational pillars. These pillars form a comprehensive framework that enables organizations to achieve digital sovereignty while maintaining the agility and innovation benefits of cloud computing.

3.1 Compliance and Regulatory Requirements

Data Residency and Localization

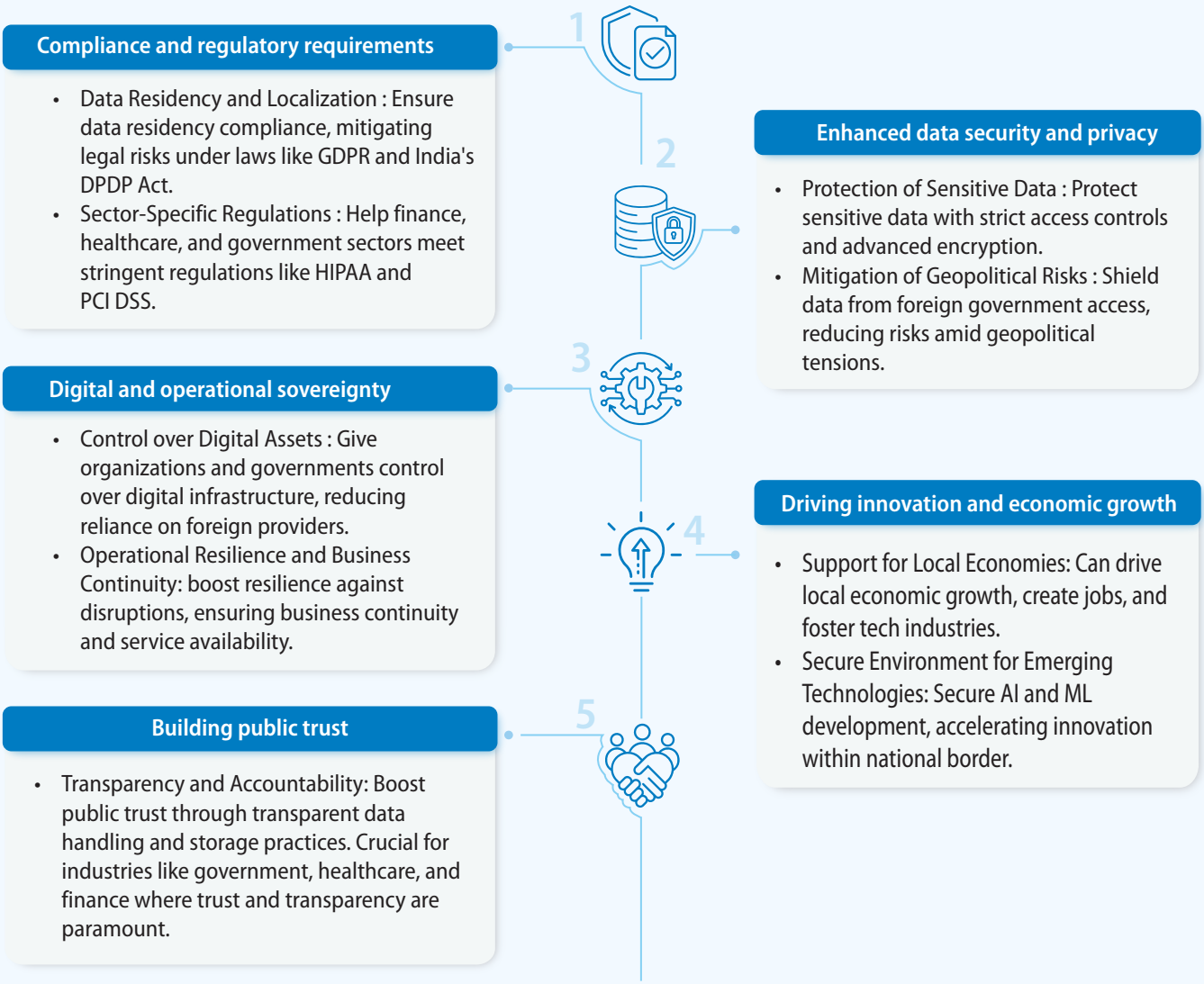
Sovereign cloud architectures ensure data stays within specific national or regional boundaries, including metadata, backups, and processing data. This helps organizations comply with regulations like GDPR and India's DPDP Act, which tightly control cross-border data transfers and reduce legal risk.

To implement this, organizations must restrict resource locations at the organizational level, deploy all infrastructure only in approved regions, and continuously monitor systems to detect any unauthorized data movement outside permitted boundaries.

Sector-Specific Regulations

Sovereign clouds must support industry-specific regulations in addition to general data protection laws. Sectors like finance, healthcare, and government face strict standards such as HIPAA and PCI DSS, which require controls like encryption, access logging, network isolation, and regular security audits.

Figure 2. Key Pillars for Sovereign Cloud Adoption



External Document © 2026 Infosys Limited

An effective sovereign cloud provides ready-made compliance profiles that map these controls to regulatory requirements, enabling compliance through automated evidence collection and continuous monitoring.

3.2 Enhanced Data Security and Privacy

Protection of Sensitive Data

Sovereign clouds protect sensitive data with strong access controls and advanced encryption. This includes customer-managed encryption keys, hardware security modules for key storage, fine-grained identity and access management with multi-factor authentication, and data classification that applies protection based on data sensitivity. Encryption must cover all stage data at rest, in transit, and in use. Technologies like confidential computing secure data even during processing by using hardware-based trusted execution environments.

Mitigation of Geopolitical Risks

Sovereign clouds protect data by ensuring infrastructure is owned, operated, and governed within the host country's legal jurisdiction. This limits exposure to foreign government access, reduces geopolitical risk, and gives organizations clarity on which laws apply to their data.

To build trust, sovereign cloud providers should publish transparency reports, undergo independent security audits, and clearly document their legal responsibilities and data handling practices.

3.3 Enhanced Data Security and Privacy

Control Over Digital Assets

Digital sovereignty gives governments and organizations control over their digital infrastructure, reducing dependence on foreign providers for critical capabilities such as data storage, computation, networking, identity systems, and application platforms. Achieving this requires investment in domestic cloud infrastructure, adoption of open-source technologies to avoid vendor lock-in, and interoperability standards that ensure data and workloads can move easily between platforms.

Operational Resilience and Business Continuity

Sovereign cloud architecture enhances resilience by reducing reliance on foreign infrastructure that could be affected by sanctions, trade restrictions, or geopolitical conflict, ensuring continued operations within national boundaries during international crises. This resilience is achieved through multi-zone and multi-region deployments within the sovereign domain, strong disaster recovery strategies, and regular resilience testing that explicitly considers geopolitical and regulatory disruption scenarios.

3.4 Driving Innovation and Economic Growth

Support for Local Economies

Sovereign cloud investments can drive local economic growth by creating jobs and strengthening domestic technology ecosystems. Building national cloud infrastructure develops local skills in areas such as cloud engineering, cybersecurity, and data science, attracting further investment and reducing reliance on foreign technology providers over time.

Secure Environment for Emerging Technologies

Sovereign cloud provides a secure environment for AI and ML development by keeping sensitive data and processing within national boundaries. This is critical for sectors like healthcare, defense, and finance, where strict control over data access, provenance, and usage is required. By offering trusted infrastructure with strong governance, sovereign clouds enable organizations to innovate with advanced technologies without compromising data sovereignty or regulatory compliance.

3.5 Building Public Trust

Transparency and Accountability

Sovereign cloud builds public trust by making data location, access, and protection clear and verifiable. This is especially critical in government, healthcare, and finance, where transparency is essential. Trust is reinforced through regular transparency reports, independent security certifications (such as ISO 27001 and SOC 2 Type II), clear data processing agreements, and simple mechanisms for individuals to exercise their data rights.

4. Key Usecases & Benefits Of Adopting Sovereign Cloud

Use cases

1. Ensuring sensitive data (e.g., personal, financial, or government data) remains within national borders to comply with regulations like GDPR (EU), CCPA (California), or India's DPDP Act.
2. Safeguarding sensitive data from unauthorized access by foreign entities or third-party cloud providers.
3. Mitigating risks of data access by foreign governments or agencies under laws like the U.S. CLOUD Act.
4. Hosting critical infrastructure systems (e.g., defense, energy, or public services) with stringent security and sovereignty requirements.
5. Reducing vulnerabilities introduced by global cloud providers with complex supply chains.
6. Supporting industries like healthcare, finance, or legal services that handle highly sensitive data requiring strict cybersecurity measures.
7. Conducting localized incident response and forensic investigations in the event of a cyberattack.
8. Mitigating risks of data access by foreign governments or agencies under laws like the U.S. CLOUD Act.
9. Protecting critical data and systems from geopolitical disruptions, such as sanctions or service restrictions by foreign providers.
10. Implementing zero-trust architectures for organizations requiring continuous verification of users and devices.

Benefits

1. Sovereign clouds store and process data in-country, reducing the risk of non-compliance with strict data protection laws. Provide audit trails and compliance certifications to meet regulatory requirements.
2. Sovereign clouds implement localized encryption, access controls, and identity management tailored to regional standards, reducing risks of data breaches or surveillance.
3. Sovereign clouds operate under local jurisdiction, limiting exposure to foreign legal requests and ensuring data remains under the control of local authorities.
4. Sovereign clouds provide isolated environments with enhanced security measures like zero-trust architecture, intrusion detection, and secure backups, ensuring operational continuity and protection against cyberattacks
5. Sovereign clouds use locally sourced hardware, software, and services, minimizing the risk of backdoors or compromised components from foreign vendors.
6. Sovereign clouds offer advanced encryption, secure multi-tenancy, and compliance with industry-specific standards (e.g., HIPAA for healthcare), ensuring data integrity and confidentiality.
7. Sovereign clouds enable faster incident response by keeping logs and forensic data within the jurisdiction, ensuring compliance with local legal frameworks and reducing reliance on foreign providers.
8. Sovereign clouds operate under local jurisdiction, limiting exposure to foreign legal requests and ensuring data remains under the control of local authorities.
9. Sovereign clouds ensure operational continuity by hosting services locally, reducing dependence on global providers that may be affected by geopolitical tensions.
10. Sovereign clouds integrate zero-trust principles like micro-segmentation, least-privilege access, and continuous monitoring, all tailored to local cybersecurity standards.

External Document © 2026 Infosys Limited

5. Security Controls Mapping

The following table maps critical security controls to the sovereign cloud pillars:

Security Domain	Control	Sovereign Cloud Benefit
Identity & Access	MFA, conditional access, privileged access management	Access governed by local identity providers and national jurisdiction
Data Encryption	CMEK (Customer Managed Encryption Keys), HSM (Hardware security module)-backed keys, confidential computing	Encryption keys never leave sovereign boundary
Network Security	VPC isolation, private connectivity, perimeter controls	Network traffic contained within national infrastructure
Logging & Monitoring	Centralized audit logs, SIEM integration, real-time alerting	All telemetry data remains sovereign; no foreign access
Compliance	Automated policy enforcement, continuous assessment	Pre-mapped to local regulatory frameworks (GDPR, DPDP, HIPAA)
Incident Response	Automated remediation, sovereign SOC operations	Response handled by cleared personnel under local jurisdiction



6. Conclusion

The move to sovereign cloud is not a short-term trend—it is a fundamental change in how countries and organizations manage their digital systems. As data becomes one of the most valuable assets today, knowing where it is stored, who can access it, and which laws apply to it is critical for national security, business stability, and public trust.

This POV shows that using non-sovereign public cloud carries growing risks. These include breaking data laws, losing control over sensitive information, security weaknesses in shared systems, business and reputation damage, dependence on a single provider, and lack of transparency. For sectors like government, healthcare, finance, and critical infrastructure, these risks are now too high to ignore.

Sovereign cloud addresses these challenges through five key areas: regulatory compliance, stronger data security, national and operational control, support for innovation and economic growth, and increased public trust. Organizations that adopt this approach can meet today's requirements while building secure, resilient systems for the future.

References

1. https://technologymagazine.com/news/gartner-governments-main-buyers-sovereign-cloud
2. https://www.gartner.com/en/documents/6952966
3. https://www.meity.gov.in/static/uploads/2026/03/a49a9e2bfb5bbd9057cf3efafda5b8d7.pdf
4. https://csrc.nist.rip/projects/cybersecurity-framework/nist-cybersecurity-framework-resource-and-overview

External Document © 2026 Infosys Limited

Author



Saurabh Sharma is a **Cyber Security Consultant** at **Infosys**, part of the Cyber Consulting and Advisory Team, focusing on cutting-edge cybersecurity solutions. With 16 years of experience, he excels in consulting, assessing, and implementing Data protection and Infrastructure Security solutions, and brings deep expertise in OT and Cloud Security.

For more information, contact askus@infosys.com

Navigate your next

© 2026 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.