Building Digital Trust:
Enabling Cloud Sovereignty through Policy and Technology

August 2025

Building Digital Trust:
Enabling Cloud Sovereignty through Policy and Technology

August 2025

Authors
Vrinda Maheshwari and Srishti Joshi

contactus@koanadvisory.com

Table of Contents

EXECUTIVE SUMMARY

Building Digital Trust: Enabling Cloud Sovereignty through Policy and Technology

Cloud computing revolutionised the information technology landscape by enabling access to computing resources over the internet with numerous benefits including scalability, agility, cost reduction, enhanced security, and resiliency. It is now a critical driver of digital transformation and economic development, with both public and private organizations increasingly adopting cloud services to drive innovation and efficiency. Government initiatives and policy support through the GI Cloud (MeghRaj) initiative, have further accelerated this adoption.

However, the rise of cloud computing has raised concerns about data control, security, and compliance, rooted in the absence of digital trust. In this context, cloud sovereignty has emerged as a strategic priority to address these concerns. Cloud sovereignty refers to the ability of a user to control their data, applications, and infrastructure within a cloud computing environment, while complying with local laws. It is a subset of digital sovereignty, which encompasses broader control over the digital infrastructure within a country's boundaries.

This report outlines the key pillars of cloud sovereignty: data residency, control and ownership of data, resiliency, security and data protection, jurisdictional control over data, and portability. Each of these pillars is crucial for ensuring that data is managed securely and in accordance with local regulations, while retaining jurisdictional and operational autonomy. Through this report, we will test our hypothesis: that existing technical controls and regulations can provide sovereignty and control to users of cloud computing. We examine how jurisdictions around the world (such as China, the EU, Australia, and the US) approach cloud governance and sovereignty and vary in their approaches, from strict state control to light-touch regulation.

We then assess India's approach to cloud sovereignty and identify how different stakeholders in the cloud ecosystem can uphold the pillars we have outlined. Cloud services in India are governed by a combination of nodal and sectoral regulations, the empanelment framework, guidelines and best practices issued by the government, and through contractual agreements. We undertake an analysis for each pillar to determine how sovereignty on the cloud is enabled through the above-mentioned mechanisms, in addition to technical controls employed by cloud providers or cloud users.

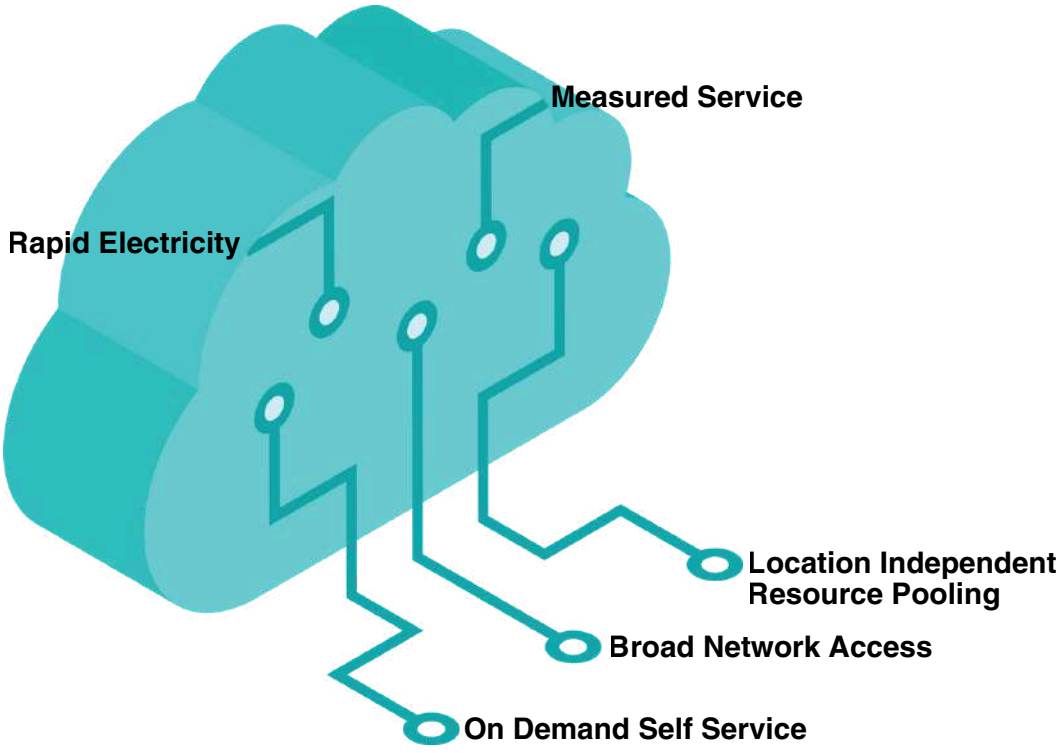
This analysis informs our recommendations for strengthening cloud sovereignty in India. These include adopting a technology-first approach, enhancing India's cloud capabilities through public-private partnerships, providing a simplified and enabling data classification framework, reinforcing jurisdictional control through Mutual Legal Assistance Treaties (MLATs), and aligning to international standards to promote portability. By implementing these measures, India can further strengthen its burgeoning cloud ecosystem - key to powering its digital economy - while retaining its digital sovereignty, thereby building digital trust.

INTRODUCTION

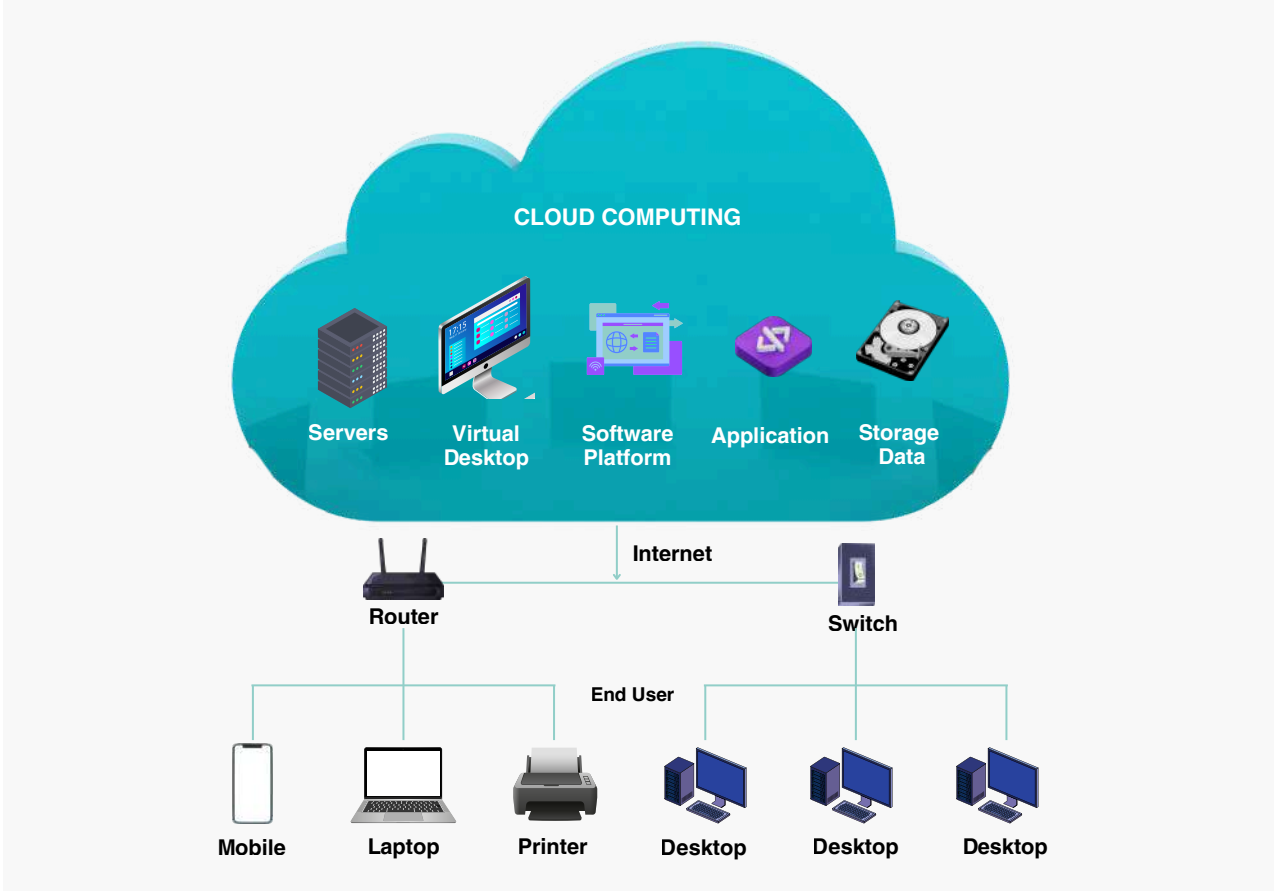
As per the National Institute of Standards and Technology (NIST), cloud computing is defined as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”[1]

At its simplest, cloud computing is a way of delivering computing resources to organisations as a utility service via a network (typically the internet) and generally scalable up and down according to user requirements. In other words, customers ‘rent’ computing resources - which can range from raw processing power and storage (servers or storage equipment) to even full software applications - from third parties when needed, instead of purchasing their own. This allows them to turn capital expenditure to operating expenditure, thus reducing their own liabilities.

CHARACTERISTICS OF CLOUD COMPUTING



CLOUD COMPUTING ARCHITECTURE



As public and private organisations increasingly adopt cloud computing, it has become a critical driver of economic development globally, revolutionising the way businesses operate, innovate, and interact with their customers. The benefits go beyond cost saving: the cloud offers scalable resources enabling organisations to adapt quickly and efficiently to changing demands and seasonal workloads, lower latency to cater to customers globally, and enhanced security and resiliency, allowing organizations to focus their resources on innovation. Additionally, the cloud enables access to IT resources and emerging technologies like AI and machine learning, providing organizations the speed and agility to accelerate innovation. Widespread adoption of cloud has accelerated the rapid growth of entrepreneurial tech businesses and start-ups.[2]

In the public sector, aligning with the objectives of the Digital India mission, the government prioritised cloud adoption and operationalised this through the GI Cloud (MeghRaj). This initiative introduced the empanelment process through which cloud service providers that follow a set of common protocols, guidelines and standards issued by the government including strict requirements of data centre facilities being located in India[3] can provide their services to government departments and public sector enterprises. The development of citizen-centric applications required scalable and flexible infrastructure with appropriate security and resiliency requirements has furthered cloud adoption.[4] For example, DigiLocker, India's digital wallet for storage and verification of documents uses cloud services to store over 900 crore documents.[5] In the private sector, the major drivers for cloud adoption have moved beyond cost and business continuity requirements to modernising data infrastructure, business growth, and collaboration and workplace productivity.

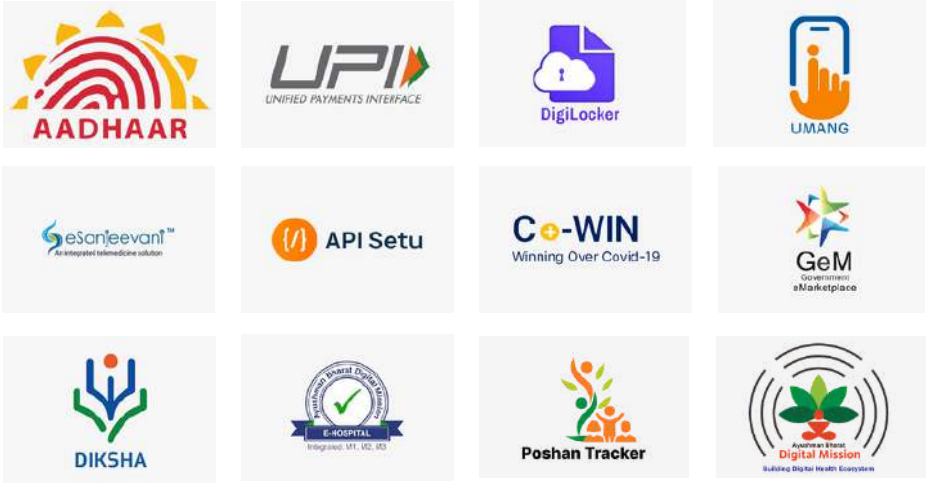
Clouds can be deployed through multiple models:

1. Private cloud: Where relevant infrastructure is owned by, or operated for the benefit of, a single large customer or a group of related entities.
2. Community cloud: Where infrastructure is owned by, or operated for, and shared among a specific group of customers with common interests, such as government agencies or financial institutions.
3. Public cloud: Where infrastructure is shared among multiple customers using the same hardware and/or software.
4. Virtual Private cloud: Where there is a logical separation of infrastructure (server, storage, network) from other offerings of the cloud service provider with strong/robust tenant isolation. Here, a secured, isolated private cloud is hosted within a public cloud, where cloud users can access and run the same functions as in an ordinary private cloud, but hosted remotely by a public cloud provider. This combines the scalability and convenience of a public cloud with the data isolation of a private cloud.
5. Hybrid cloud: Where there is a mix of on-premise, private and public cloud services with orchestration between these platforms. In some instances, certain workloads cannot easily migrate to the cloud since they need to work with local datasets, share data with on-premises applications with limited latency, or meet regulatory requirements.

India's Cloud Growth Story

The IDC estimates the Indian public cloud services market to grow to $25.5 billion by 2028,[6] driven by digital transformation, GenAI and cloud migration. As many as 80% of larger companies and 83% of mid-sized companies in India have more than a third of their data on the cloud,[7] with this number on the rise.

In the public sector, the MeghRaj initiative led over 300 government departments using cloud services,[8] and enabled the rollout of population scale governmental projects. For example, in 2021, the Ministry of Health and Family Welfare engaged MeitY to build an application to power to power its large-scale COVID-19 vaccination. To facilitate this, MeitY built and rolled out the Co-Win application on AWS cloud, through which the app was able to scale in seconds to handle user registrations, consistently support 10 million vaccinations daily, and supported peak loads delivering 25.1 million vaccinations.[9] The Open Network for Digital Commerce (ONDC), the Department for Promotion of Industry and Internal Trade's initiative to facilitate e-commerce on an open protocol network, built its architecture using Google Cloud. This provided ONDC the ability to scale from 30 transactions per month to 14 million per month one year after launching.[10]



Indicative List of Population-Scale Government Projects Rolled out on the Cloud

As the government scales digital delivery of citizen services, this expansion, along with increased adoption of AI-driven applications will require scalable, high-performance cloud infrastructure, and consequently, data centre facilities. As of 2023, India's colocation data centre capacity stands at around 977 MW, remains inadequate to keep up with growing demands.[11] For example, the United States leads in terms of installed capacity at 8201MW, followed by China with 3208MW and the UK with 1202 MW. While accounting for population and growing demand, India significantly lags. Data centre capacities in the country will need to be augmented further to meet India's growing data consumption and digitalisation needs and catch up with other comparable nations. Meeting these demands requires a collaborative and participative approach. The Indian government, cloud service providers, and industry stakeholders must work together to accelerate this growth. There is scope for international collaboration as well; for example, the recently announced U.S.-India TRUST ("Transforming the Relationship Utilizing Strategic Technology") initiative emphasises cooperation towards industry partnerships and investments in next generation data centers.[12]

As the government and private stakeholders increase digitization efforts and shift their workloads to the cloud, there may be concerns regarding the perceived loss of control over their digital assets. These concerns are rooted in the lack of digital trust, which can be strengthened by asserting sovereignty.

Sovereignty and the Cloud

An essential aspect of a country's sovereignty is its ability to control resources and people in its territory.[13] But traditional notions of sovereignty are challenged by the internet, which is inherently amorphous, decentralised and not restricted by geographical boundaries. The concept of digital sovereignty has gained currency over the past few decades as governments seek to reassert their authority over the digital sphere.[14] It can be seen as the need for control over the different layers of the internet, including physical infrastructure, the standards and rules that govern the software code, as well as the ownership and use of the underlying data.[15]

Cloud sovereignty can be thought of as a subset of digital sovereignty, where the owner asserts control over their data, applications, and account management within a cloud computing environment. It has emerged as a critical issue due to the growing reliance on cloud services to drive digital transformation and innovation. Cloud sovereignty can be understood as a composite of the following aspects:

- **Data sovereignty:** This refers to an organisation's authority over its data, including safeguarding it against unauthorised access while stored on the cloud. Some aspects of this would be access controls that limit the use to designated or permitted users, data governance based on internal policies, and adherence to any data residency regulations.
- **Operational sovereignty:** This refers to an organization's ability to maintain visibility and control over their operations in the cloud while ensuring business continuity, resiliency and regulatory compliance.
- **Technical sovereignty:** This refers to the ability of organisations to run workloads and applications on the cloud without running the risk of vendor lock-in and having the flexibility to migrate their workloads to other cloud environments if required.

Nations and organisations are increasingly concerned about who controls their data and applications and where they reside, fearing potential foreign influence, surveillance, or data breaches. This has driven the call for increased regulations and the development of localised cloud solutions in a bid to ensure data remains under the control of the user, safeguarding privacy, security, and autonomy. However, this impulse overlooks the fact that existing regulatory frameworks, technical controls and contractual agreements can

offer enforceable, real-time safeguards for cloud sovereignty to ensure data security, access control, compliance and autonomy. In this report, we will identify certain innate characteristics of cloud sovereignty, and map out how they are informed by regulations, policies, guidelines, technical controls, industry best practices and rules to varying degrees.

CHAPTER 2: DEFINING THE PILLARS OF CLOUD SOVEREIGNTY

When factoring in the different aspects of cloud sovereignty, it can be understood as constituting the following key pillars: data residency, control & ownership of data, security & data protection, resilience, and data control, ensuring jurisdictional autonomy and portability. These pillars are not exhaustive, as regulatory shifts and technological advancements will continually reshape sovereignty needs. While recognising that a flexible, adaptive approach is essential to address emerging challenges, in this section we flesh out the identified core pillars which we consider to be innate to cloud sovereignty.

1. Data Residency

Data residency refers to the geographical location of the data itself, i.e., where it is stored and whether it is subject to the laws of that region. This is often interchangeably used with data localisation, which refers to a mandate that data remains on servers within a specific location and jurisdiction, usually where it was generated. However, while data residency is rooted in ease of access and compliance, data localisation is often motivated by concerns about data privacy, security and government access to data.

In a cloud environment, consumers retain the right to choose where their data is stored with the flexibility to host data on multiple cloud locations across various geographies. Users must balance their need for agility and latency with requirements of security for their applications and their data, and compliance with regulations.[16]

2. Control & Ownership of Data

Organisations storing their data in the cloud should be able to decide where it is stored, how it is secured, and who can access it. User control over data is essential as there is a greater perception of loss of control by a cloud user in comparison to an on-premise storage solution. Thus, user autonomy and control over data is crucial to build trust in the cloud solution and mitigate concerns of loss of control or transparency.

User ownership and control of data are ensured through a combination of technical measures including encryption tools, customer-managed keys, hardware security modules (HSM), and operational measures such as robust identity and access management (IAM) systems and strong multi-factor authentication that ensures role-based access,[17] ensuring only authorised users can access their data.

3. Security & Data Protection

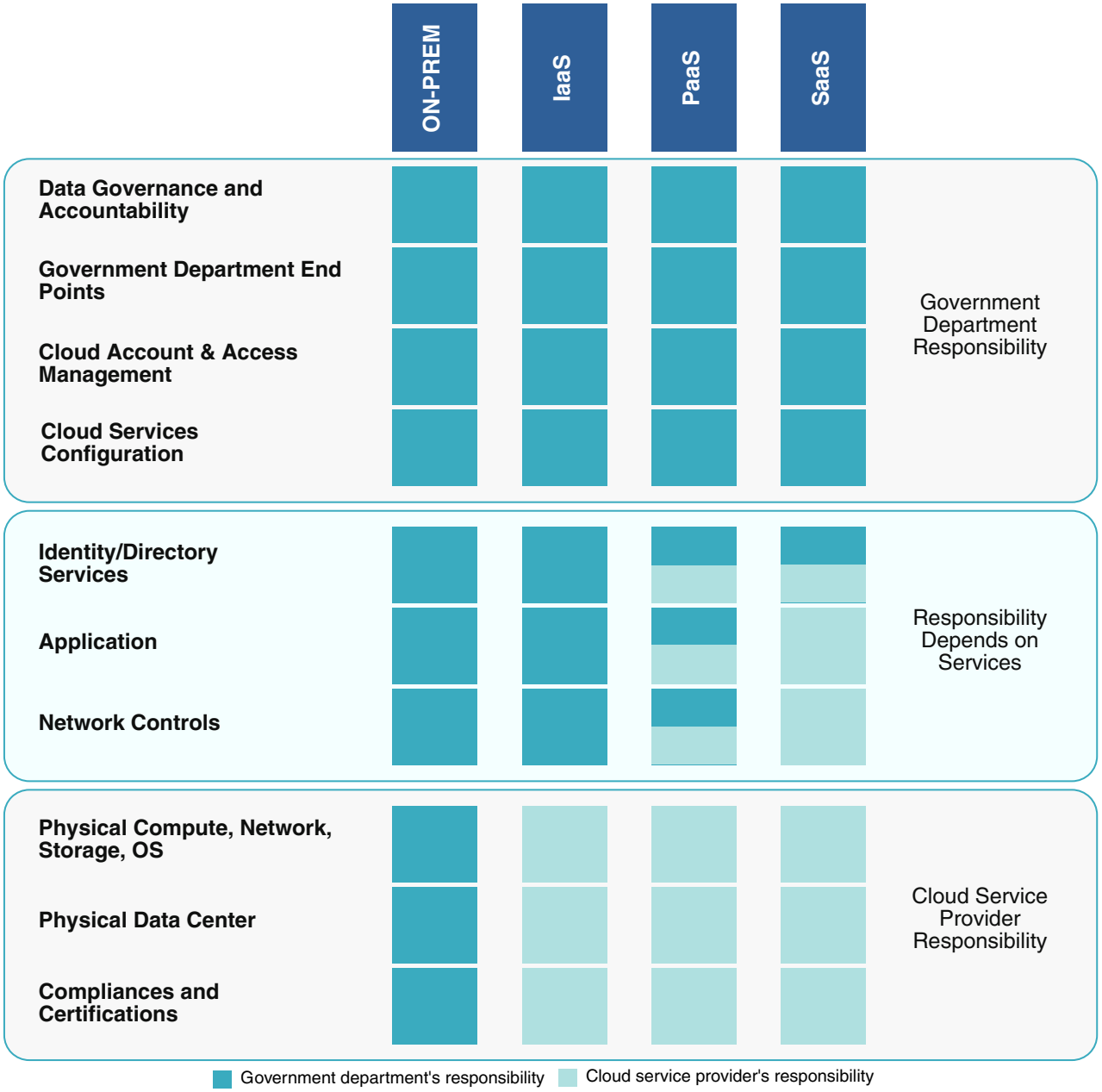
Security

As organisations (including governments) increasingly rely on cloud services to store, process, and manage business critical data, they will need to ensure their security objectives are being met. The basics of cloud security are not unique in scope as information theft, attacks and human error can occur both online and in physical networks. However, as users migrate to cloud services and incorporate cloud-based tools and

services as part of their infrastructure, in addition to the security of the cloud, new challenges concerning security may arise because of misconfigurations and poor authentication controls by the user. To ensure security, both the CSP and the customer have roles to play in securing the cloud environment.

Cloud security is a shared responsibility between the cloud service provider and user. The user has absolute ownership and control of the data and applications stored in the cloud environment and are consequently responsible for ensuring security of this aspect. The cloud service provider on the other hand is responsible for security of the cloud itself. This allocation of responsibilities recognised by MeitY[18] is the "**shared responsibility model**" which clearly defines that the CSP is responsible for the security "of" the cloud, while the customer is responsible for the security "in" the cloud. As detailed below, there is a varying degree of responsibility based on the cloud services enlisted. In all scenarios, the CSPs cannot assume responsibility of their customers data, or how their applications are used.

Example of a Shared Responsibility Model in Governmental Use of Cloud



Data Protection

The secure storage, processing and management of the data entrusted to the cloud is of paramount importance, often because of the sensitivity and volume of data being processed[19] and concerns of unauthorised access and breaches might arise. In this context, data protection laws play a critical role in safeguarding processing of personal data, preventing potential harm to data principals. Many countries have adopted general data protection and privacy laws that apply to government and private-sector activities that involve the processing of personal data. Most data protection legislations regulate processing of personal data to protect individual data principals against unauthorised collection, storage, use and dissemination of their personally identifiable information.[20] These laws generally impose conditions under which processing of personal data is legitimate and prohibits processing where it is likely to have a detrimental effect on the data principals.

3.1 Data Classification & risk-based security controls

The first step towards ensuring data protection is to classify data based on critical parameters that ensures continued innovation on the cloud while implementing appropriate security measures. Data classification refers to the identification, categorisation and labelling of data stored in cloud systems, based on its sensitivity, worth and business importance along assorted characteristics (such as data type, users, content, context, level of risk in case of disclosure, origin, and level of access). This allows for tailored protection and efficient access control to the data. Security classification, particularly of sensitive data, is crucial for safeguarding critical data and minimising risks. This exercise can be carried out by the owner of the data, which in case of the cloud environment is the cloud user. Automated tools and algorithms that use predefined rules can be used to scan and analyse data for classification of large data sets by users, following which appropriate cloud deployment models and security measures can be selected.

3.2 Identity & Access Management

Identity and Access Management (IAM) ensures only authorised individuals and systems can access sensitive data and resources, even when using third-party cloud providers. By implementing the principle of selective privileges and imposing segregation duties, IAM solutions eliminate unauthorised access and information loss/theft. IAM solutions enable organisations to manage user identities, enforce role-based access controls, and implement multi-factor authentication to prevent unauthorized access.[21] Effective IAM systems provide visibility into who accessed what data and when, supporting accountability and auditability.

3.3 Encryption

Encryption, a cybersecurity fundamental, ensures safeguarding data at rest, in transit, and in use. By converting data into an unreadable format that can only be unlocked by a unique digital key owned by the user, encryption adds a layer of security by ensuring that data remains unintelligible even if it is intercepted or accessed without authorization. Data at rest refers to information that is stored on physical or virtual storage devices, including databases, file systems, and backups. Encrypting data at rest allows organisations to retain control over their data from unauthorised access regardless of the physical location of the cloud servers. Data in transit refers to information that is being transferred from one location to another, such as between a user and a cloud service or between different cloud environments. Without adequate encryption, data in transit is vulnerable to interception, man-in-the-middle attacks, and other cyber threats. Encryption protocols such as Transport Layer Security (TLS) ensure that data is securely transmitted, maintaining confidentiality and integrity throughout its journey. To enhance protection of data in

use, a traditionally vulnerable stage in the data lifecycle, certain CSPs have developed advanced technologies and confidential computing capabilities that create isolated and secure environments to limit unauthorized exposure and enhance security even while data is being processed.

3.4 Security certifications/third party accreditations of CSPs

As a part of ensuring security "of" the cloud across geographies, CSPs rely on global security standards. Security certifications & accreditations from reputed third-party organisations like the ISO 27001, FedRAMP, GDPR, NIST 800-17,1 SOC 2, or CSA STAR reinforce trust and help users identify compliant CSPs and demonstrate that the CSP follows globally recognised security and data protection best practices. Accredited providers undergo rigorous third-party audits, offering transparency about their operations, data handling, and security measures. Additionally, sector-specific certifications such as the PCI-DSS, HIPAA/HITECH ensure security of sensitive data based on the requirements of their respective industries. Many certifications map directly to regulatory frameworks; for example, the ISO 27001 is closely correlated to (but not exactly mirrored in) the GDPR. Certifications tailored to regional laws (e.g., MeitY cloud empanelment in India[22]) ensure CSPs meet local compliance requirements, reinforcing sovereignty for regulated sectors.

3.5 Limiting Operator Access

An important aspect of achieving cloud sovereignty and trust on the cloud is limiting access of the operator of the cloud environment. As an extension of IAM mechanisms and the implementation of the principle of least privilege, this layer of control ensures that sensitive information remains under the control of the data owner rather than the CSP. This minimises the risk of unauthorised access, government overreach, or data breaches. This can be implemented through a range of technical measures such as zero-trust architectures, customer-managed encryption keys, confidential computing, and strict role-based access controls (RBAC) prevent CSPs from viewing or processing data without explicit authorisation of the user. These safeguards align with regulatory requirements, ensuring compliance with data protection laws while maintaining security, privacy, and operational control over cloud-stored data, even in multi-tenant environments.

4. Resilience

Continued access to data and infrastructure is integral to maintaining sovereignty in the cloud environment. Disruption of access to workloads can impact revenue, productivity and customer trust for cloud users. Resilience on the cloud refers to the ability to recover from infrastructure or service disruptions, to dynamically acquire computing resources to meet demand, and to mitigate disruptions, such as misconfigurations or network issues.[23] At its core, resilience refers to foreseeing disruptions to technology services and planning for both business continuity and recovery.[24]

Resilience comprises the following key elements:

- *High availability:* This refers to the ability of a system or application to remain operational and accessible with minimal downtime, even during hardware failures, network issues, or maintenance activities. It is achieved through redundant infrastructure and robust system design to ensure continuous service delivery and meet predefined uptime requirements.
- *Fault tolerance:* This refers to the ability of a system to continue operating correctly even when some of its components fail. This is achieved through mechanisms like redundancy, replication, and failover systems that ensure seamless recovery and prevent disruptions to service.[25]

- *Disaster-recovery:* This refers to strategies and processes implemented to restore systems, data, and applications to a functional state after a major disruption such as natural disasters, cyberattacks, or system failures.[26] It typically involves off-site backups, failover systems, and predefined recovery plans to minimize downtime and data loss, ensuring business continuity. Key metrics that can measure this element include mean time to recovery (MTTR), recovery time objective (RTO), and recovery point objective (RPO).

5. Jurisdictional control over data

Concerns regarding extraterritorial reach in the cloud and limitations to access to data in the cloud are addressed under this pillar. Jurisdictional control over data is fundamental to cloud sovereignty as it ensures that data generated within a nation is subject to its own laws and regulations, rather than those of foreign entities. Retaining jurisdictional control allows nations to safeguard critical information, enforce privacy laws, and ensure compliance with local standards. Typically, MLATs or similar agreements facilitate data exchange between countries.

A notable challenge arises with laws like the American Clarifying Lawful Overseas Use of Data Act (CLOUD Act),[27] which allows U.S. authorities to access data stored by U.S.-based cloud providers to investigate a crime, even if the data resides in another country. Such extraterritorial reach can conflict with local data sovereignty laws, posing significant risks to national security and privacy. (It should be noted that the CLOUD Act operates under certain very specific conditions, that is, only in criminal investigations and only with either the consent of the subject, a warrant issued by a US court or in accordance with an agreed bilateral agreement.[28] The Act also creates a framework for bilateral agreements between governments to dictate cross-border access to technology companies' data).[29]

6. Portability

Evolving needs and technological advances may demand shifts in technology service providers. Any hinderance in the ability of users to migrate in the cloud environment impacts their control, and thereby sovereignty. Portability is the ability to seamlessly move applications, data, and workloads between different cloud environments or back to on-premises systems without significant vendor lock-in. A consumer may want to migrate their workloads to leverage advantages of other cloud service providers, such as cost efficiency, innovative alternatives or more compliant providers. Portability reinforces technical sovereignty by empowering organisations to retain technical autonomy, foster competition among CSPs, and ensure service quality and cost efficiency. Portability also enhances resilience by enabling multi-cloud strategies, where workloads are distributed across providers. This reduces dependence on a single provider and mitigates risks associated with outages, geopolitical events, or policy shifts.

We argue that any cloud offering that meets the criteria listed above can be said to offer sufficient controls and sovereignty to its users over their data and applications. By addressing critical concerns such as cross-border data transfers, unauthorized access, and vendor lock-in, cloud solutions can enable organizations to assert ownership and control, and provide operational autonomy in way that supports sovereignty requirements. In the next two sections, we will look at how these pillars are implemented in the cloud ecosystem, both internationally as well as in India.

CHAPTER 3: HOW DO OTHER JURISDICTIONS TACKLE CLOUD GOVERNANCE & SOVEREIGNTY?

The widespread adoption of cloud globally has led to governments around the world prioritising efforts that will assert or enhance cloud sovereignty via existing regulatory frameworks or in some cases, specialised policies. For instance, approximately 83% of countries have put in place legislations to secure the protection of data and privacy - there are now 145 UN Member States (around ¾ of 193 total) who have adopted comprehensive data protection legislations;[30] there are around 30 countries with pending bills.[31] In this section, we map out different approaches taken by governments to enhance cloud sovereignty in their respective jurisdictions.

State Control

China approaches digital sovereignty in a state-centric manner.[32] It does not have an overarching legislation to regulate cloud but it strictly monitors data protection through an extensive legislative framework: Cybersecurity Law (CSL) (2017)[33] lays down a security framework to safeguard the collection, use and protection of personal information;[34] Data Security Law (2021) builds on CSL and adds guidelines for handling and classifying data, more stringent enforcement measures, data transfer controls and risk assessments; and Personal Information Protection Law (2021) added an additional regulatory layer.

The Chinese government has issued guiding policies on promoting the development of cloud computing through innovation, strong security capabilities, adoption of safe and reliable cloud computing practices, enhanced cloud computing abilities etc. They have also issued opinions on tackling security issues, combining cloud computing with more traditional industries to boost its use and practices to encourage research and development.[35]

In 2016, the Chinese government released draft rules to regulate cloud services for public consultation, however, this has not been implemented yet.[36] The rules sought to set up a licensing regime for cloud service operators, place restrictions on foreign investment in cloud services, prescribe reporting requirements and restrict access for foreign companies who wish to operate cloud service in China (among other measures).

Rules-based approach

The EU seeks to establish digital sovereignty through comprehensive and strict regulatory oversight; its legislative and policy frameworks prescribe extensive rules. For example, to ensure cybersecurity, policies such as the GDPR and the Data Governance Act mandate entities must put in place adequate access controls like anonymisation, pseudonymisation, encryption etc. to prevent unauthorised access or use of data. Data protection is sacrosanct to EU's concept of digital sovereignty[37] and is accounted for across all relevant regulatory or policy frameworks. The EU is currently reevaluating its approach to simplify and ease the compliance burden owing to the GDPR.[38]

A more normative approach is taken towards data classification and controls. For example, the GAIA-X labels data representing different degrees of compliance regarding factors like transparency, security, and interoperability whereas the GDPR categorises personal data based on its sensitivity. The Draft EU Cybersecurity Certification Scheme is a voluntary certification that lists internal protocols cloud services must meet while clearly demarcating responsibilities of the cloud service provider and customer.[39] The certification is in its draft stages and is yet to be published. Resilience is also addressed through multiple measures. For instance, the GDPR compels controllers and processors to ensure the availability and access to personal data in the event of a physical or technical incident, but the Data Governance Act envisions resilience and continued access to data through the lens of business insolvency.

Principle-Based Approach

Australia governs cloud through a combination of laws, policies, guidelines and frameworks aimed mostly at cybersecurity and data protection that are either industry specific or more generic at the federal or state level. These are principle-based laws that focus on the intent behind the principle, enabling greater flexibility, and are "technology neutral".[40]

Australia has also created guidelines and policies that can offer guidance to government entities in their use of cloud services. For example, the Australian Signals Directorate Cloud Computing Security Considerations[41] was created to help government agencies assess the cybersecurity risk of cloud services, and includes factors like business continuity and disaster recovery, data portability and segregation, ability to retain legal ownership of data, and protection of data (including sensitive data) from unauthorised access by third parties. More generally, frameworks such as the Information Security Manual (which delineates principles and actionable guidelines and to help organisations shield themselves from cybersecurity threats) and the Essential Eight (baseline standard to help businesses mitigate cybersecurity threats and data breaches recommended by the Australian Signals Directorate) give technical guidance and support to both private as well as government entities looking to set up any IT services and infrastructure, including cloud.

Singapore too does not have any dedicated legislation specifically addressing cloud governance. The focus is predominantly on data protection, which is governed by the Personal Data Protection Act (PDPA). The PDPA only addresses cybersecurity to the extent of data breach notifications to the Personal Data Protection Commission and affected individuals. The Cybersecurity Amendment Act requires owners and operators of computer systems involved in the provision of essential services i.e. critical information infrastructure (CII), to meet certain cybersecurity standards, ensure operational resilience, conduct risk assessment and report incidents. The Act was amended this year to include cloud computing and data service centres.[42] The Singaporean Personal Data Protection Commission has also introduced a guide to help cloud platforms implement "good practices" to secure personal data and prevent data breaches.[43]

Light touch regulation

The US stands out for its minimalist approach to rulemaking for digital or cloud sovereignty and does not explicitly endorse the concept of "digital sovereignty".[44] Its policies are usually focused on protecting American data in other jurisdictions.[45] Within the US, technology companies self-regulate and are subject to minimal state intervention,[46] in line with its "bottom-up multi-stakeholderism" approach to the internet where private sector and civil society participation are essential to internet governance.[47]

Cloud computing is mostly carried out through commercial contracts, which are a matter of state law. Additionally, data protection and security implications are governed by state-level privacy laws or federal sectoral regulations for industry-specific data. For example, the California Consumer Privacy Act (CCPA)

grants California residents' rights over their personal data, including the ability to access, delete, and opt-out of its sale. It aims to enhance transparency and accountability in how businesses handle consumer information. These regulations seem to prioritise data security and breach notification provisions rather than making sure its citizens' data remains within the country i.e. data residency.[48]

Interplay between Cloud Sovereignty and National Capabilities

Balancing innovation, sovereignty, and security remains a challenge for all nations. The U.S. favors a light-touch regulatory approach, emphasizing innovation and market-driven growth. This fosters innovation, rapid technological advances and global market leadership but can lead to inconsistent data protection standards and vulnerabilities in critical sectors. In contrast, China exercises strong state control, prioritizing national security and digital sovereignty. This ensures control over sensitive data and aligns with China's broader economic and geopolitical goals. However, it can stifle innovation due to burdensome compliance requirements and limited interoperability with global systems. This could explain the lack of globally competitive and trusted Chinese cloud companies. This will ultimately negatively impact the domestic industry. The EU adopts a middle path with GDPR and initiatives like Gaia-X, emphasizing both security and innovation. While it creates a high standard for data protection, it can increase compliance costs.

Ultimately, access to technology and capabilities must be balanced with the intention behind any national policy. Digital sovereignty should include the strengthening of domestic data infrastructure and creating conditions for development and deployment of domestic capabilities. Technological capability must be built in partnership with whoever has it, and reliance needs to be placed on the expertise and know-how of international CSPs. Countries often partner with private players in order to modernise their cloud computing infrastructure. For example, the IT Ministry launched MeghRaj 2.0, a hybrid cloud solution developed through a public private partnership, to enhance India's cloud computing capabilities and advance the nations digital transformation objectives.[49]

Different jurisdictions seek to ensure cloud sovereignty through a range of measures. However, laws alone are insufficient without technical enforcement mechanisms. Ultimately, while legal frameworks define sovereignty requirements, it is technical implementations, such as data residency controls, access restrictions, and compliance monitoring, that make sovereignty operationally enforceable in a globally interconnected cloud environment.

CHAPTER 4: GOVERNING INDIA'S CLOUD ECOSYSTEM

Evaluating Regulatory Frameworks Against Cloud Sovereignty Pillars Across Stakeholders

India's cloud first policy and MeitY empanelment framework drove the adoption of cloud services within the Government of India, while ensuring regulatory safeguards prescribed under the IT Act. MeitY has served as the nodal agency for facilitating the adoption of cloud for government functions; in 2014 NIC launched MeghRaj, the first national cloud.

The objective of the GI cloud was to optimise infrastructure utilisation, accelerate the development and deployment of eGov applications, replicate successful applications across states by avoiding any duplication, and simplify the procurement process of certified applications. The architectural vision of the GI cloud involved a set of discrete cloud computing environments spread across multiple locations, built on new or existing infrastructure, and following a set of common protocols, standards and guidelines set by the government. To implement this, the government introduced the empanelment process for private cloud companies which accounted for the gap in technical knowledge with the government and helped resolve trust issues by building in adequate regulatory and compliance requirements. India now boasts of 23 empanelled private cloud service providers. MeitY's empanelment framework for CSPs offers benefits to all stakeholders involved - the guardrails help build trust in CSPs, which then aids the government and regulated sectors to rollout services and applications on a larger scale than they otherwise would.

Governance of Cloud in India

Cloud services in India operate within a multifaceted regulatory landscape shaped by layers of governance. First and foremost, cloud services observe the principal legislations, including the IT Act as governed by MeitY, the nodal ministry for the electronics and IT industry. Cloud services engaged in regulated sectors such as banking, insurance and health, are subject to sector-specific legislations. In addition to protocols, standards and guidelines under the Empanelment Framework, MeitY has also issued cloud-specific guidelines and best practices. Furthermore, cloud service usage is bound by contractual agreements between the cloud service provider and consumer, which lay out various aspects including service-level agreements, data management and security, and compliance and legal obligations. Combined, this layered approach provides a comprehensive regulatory environment for the proliferation of cloud services in India.

1. Nodal regulation: Cloud services are required to comply with obligations under various legislations:

a. Information Technology Act, 2000: The Act prescribes obligations for data protections, cooperating with government authorities, due diligence and cyber-incident reporting. The government is looking to revamp India's digital laws, including the IT Act, through a proposed Digital India Act.
b. For conduct of businesses, like all other entities, cloud services are governed by various regulations such as the Indian Contract Act, 1872.

2. Sectoral regulations: As noted earlier, similar to IT service providers, cloud services are subject to outsourcing and cyber security requirements imposed by sectoral regulators like the RBI, IRDAI, National Health Authority, among others.

a. RBI Master Direction on Outsourcing of Information Technology Services, 2023
b. SEBI Framework for Adoption of Cloud Services
c. Information and Cybersecurity Guidelines, 2023, IRDAI
d. Circular regarding the Adoption of cloud services by intermediaries regulated by PFRDA[50]

3. Empanelment Framework: As indicated above, the government has driven cloud adoption through the 'MeghRaj' cloud computing initiative. The government regulates cloud services through their empanelment as government-approved cloud service providers. The cloud empanelment process is highly rigorous, designed to ensure only secure, reliable and compliant cloud services providers can offer services through the GI cloud. The pre-qualification criteria for empanelment requires CSPs to be registered in India with data centre facilities present within the country, adhere to the IT Act, all data is required to be stored and processed within the legal boundaries of the country, and provide various ISO certifications. CSPs are required to adhere to technical requirements including security controls and service availability, a host of legal and compliance requirements, service-level agreements requirements that entail provisions for interoperability, data portability and exit management, disaster recovery and business continuity requirements, and contractual terms and conditions to achieve empanelment for the delivery of their services. Compliance is verified through a rigorous audit conducted by the Standardization Testing and Quality Certification Directorate. Following empanelment, the CSP is also required to undergo a periodic audit for minimum security requirements and any additional requirements specified by MeitY.

4. Guidelines and Best Practices: In addition to the regulatory framework, MeitY has also issued a set of guidelines including Cloud Security Best Practices, Cloud and Disaster Recovery best practices, guidelines for Master Service Agreements and Service Level Agreements, among others.

5. Contractual Arrangements: Cloud services primarily operate on a B2B model, where businesses negotiate service-level agreements (SLAs) and contractual terms directly with cloud providers. These agreements outline compliance requirements, access restrictions, and dispute resolution mechanisms, reducing reliance on government-imposed regulations. They can demand technical safeguards such as encryption, audit logs, and customer-managed keys. This contractual flexibility allows cloud sovereignty concerns to be addressed dynamically, making prescriptive regulatory interventions less necessary in B2B cloud service relationships. These SLAs are also informed by guidelines published by MeitY mentioned above.

As discussed in Chapter 2, cloud sovereignty hinges on certain pillars that ensure control, security, and compliance within cloud computing environments. We now map out how these pillars are provided for in existing regulatory frameworks in India and further delineate the roles and responsibilities of the actors involved (that is, governments, CSPs and cloud users).

Data Residency

Government:

- MeitY's empanelment process for cloud service providers mandates that data centre facilities be present in India and requires that all storage and processing functions are carried out within the boundaries of India.[51]

- Sectoral regulation for cloud use by entities regulated by the Securities and Exchange Board of India (SEBI) mandates that "data should reside/be processed within the legal boundaries of India"[52] to ensure that access to data can be guaranteed and SEBI's right to search and seize data are not affected by the adoption of cloud services.
- The Reserve Bank of India (RBI) in 2021 directed 'payment system operators' to ensure that data related to payment systems operated by them are stored inside India within a specified period. It said that gaining 'unfettered supervisory access to data' was integral to the process of enhancing cybersecurity in India's digital payments ecosystem.[53]
- India's nodal data protection legislation - the Digital Personal Data Protection Act, 2023 (DPDP Act) makes provisions for the government to restrict the transfer of personal data to notified countries. The Draft Rules to the DPDP Act now propose that the government can specify conditions on any outbound transfers of personal data from India by either Indian or foreign businesses - thus restricting free cross-border movement of data. Additionally, large businesses processing substantial amounts of data - classified as Significant Data Fiduciaries (SDFs) - may now face a data localisation obligation for specific classes of personal and related traffic data. A government-appointed committee is proposed to notify certain categories of data which SDFs cannot transfer outside the territory of India. The Draft Rules are undergoing public consultation, and the final inclusion of the localisation mandate awaits notification.

CSPs:

- CSPs provide tools and services for compliance with data residency norms like geo-fencing, region-specific data storage, and provide preventive, detective and proactive guardrails to ensure compliance.

Cloud Users:

- As the owners of the data stored on the cloud, users should undertake data mapping to understand what data they possess, where it is located and whether there are relevant data localisation mandates. Accordingly, in line with relevant regulations, they should define necessary data residency controls, conduct regular audits, define clear data governance policies, and ensure contractual agreements with CSPs align with local laws. While CSPs provide tools for compliance, the ultimate responsibility lies with cloud users to properly configure and manage their data.

India's efforts to retain data within its borders are largely driven through the empanelment process and sector-specific legislations. While the DPDP Act has no data residency provisions, the proposed implementing rules introduce a data localisation framework, thereby awaiting further clarity. Currently, CSPs provide readily available offerings along with controls, allowing organisations to implement data residency requirements efficiently. **Current CSP offerings ensure that organizations meet the data residency requirements mandated through various government regulations and policies.**

Data Control and Ownership

Government:

- MeitY's Guidelines for Strategic Control in Outsourced Projects, 2010[54] emphasizes that the control over data and applications must be retained by the government departments/user organizations.

- MeitY Cloud Security Best Practices highlights on the importance of access control in data protection, and the need for users to ensure necessary administrative and technical controls are in place to manage data access.
- The SEBI Framework for Adoption of Cloud Services, 2023[55] stipulates that the user, in this case the FS Regulated Entity, shall retain complete ownership of all its data and logs, encryption keys, etc. residing in the cloud.

CSPs:

- CSPs enable users to have complete ownership and control of data they upload on cloud and further empower them to fine grain access control through a combination of technical and operational measures.
- CSPs have developed solutions to ensure customers retain full control and ownership of their data and applications and completely restrict operator access to customer data even during processing. Technologies like AWS Nitro and Azure Confidential Computing offload many traditional hypervisor functions to dedicated hardware, creating a secure and isolated environment where even CSPs/root users cannot have unauthorised access to customer workloads or data while in processing.[56] Such innovations are particularly relevant for industries like finance, defence, and healthcare, where compliance with stringent data sovereignty laws is mandatory.

Cloud Users:

- Research suggests that users should recognise the need for their own technical strategies rather than solely relying on the CSPs products or services.[57] Cloud users can use technical measures such as encryption tools, customer-managed keys, cloud hardware security modules[58] to enhance control over encryption keys, preventing cloud providers or unauthorised entities from accessing their data.

Cloud service delivery is architected in a manner that provides users complete control and ownership over their data and applications hosted on the cloud. The responsibility of data management rests on the cloud user, and this is emphasised by guidance provided by MeitY and SEBI.

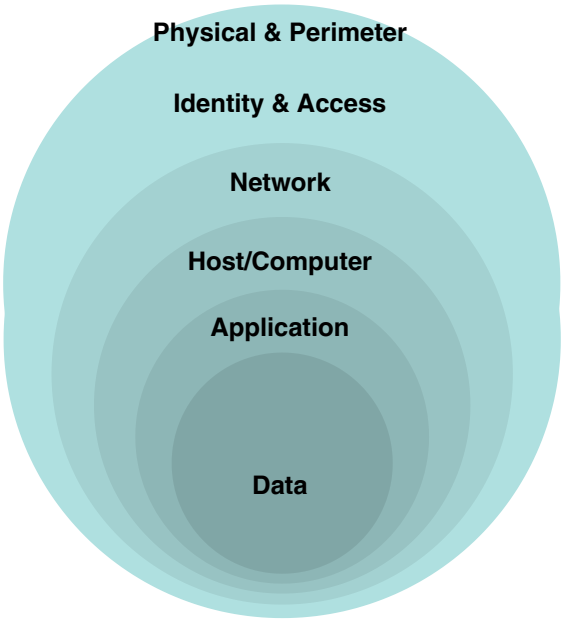
Security and Data Protection

Security:

Government:

- Regulations such as the CERT-In 2022 Directive[59] mandate enhanced security measures for cloud and other service providers and reporting of cyber incidents within prescribed timelines.
- MeitY Cloud Security Best Practices provides a shared responsibility model with distinct responsibilities of the cloud service provider and cloud user organization. While acknowledging areas of overlap in certain service delivery models, the guidance emphasizes on the government department's accountability to secure its data.
- MeitY's Guidelines on Best Practices for User Departments on Cloud Security[60] advocates for measures such as having a layered approach to security (that permeates all levels, from data to applications and

networks as well as perimeter and physical), conducting regular cloud security assessments, implementing a zero trust system (which requires stringent verification of identity for each device and person trying to access resources on a private network, regardless of their position within or outside of the network perimeter).



Layered Approach to Security, as envisaged by MeitY's Cloud Security Best Practices[61]

- The DPDP Act further includes provisions relating to reasonable security measures by service providers and reporting of personal data breaches. In addition to this, sectoral regulators provide cybersecurity guidelines for outsourcing technologies.
- The Draft DPDP Rules require data fiduciaries to ensure minimum reasonable security standards like deploying data security measures through encryption, obfuscation or masking or using virtual tokens and maintaining data backups to ensure continued data processing in case of a personal data breach.
- The RBI Master Direction on Outsourcing of Information Technology Services, 2023[62] provides a security framework highlighting shared responsibility between the user and the CSP. The user's efforts in securing their data and applications are required to be complemented by the CSP's cyber resilience controls. Common touchpoints for both parties are in ensuring continuous and regular updates of security-related software including upgrades, fixes, patches and service packs for protecting the data and application from advanced threats/ malware.
- The SEBI Framework for Adoption of Cloud Services, 2023[63] supports a shared responsibility of any function or task between CSPs and users, and mandates delineation of tasks between the two parties.

CSPs:

- CSPs provide security features to tackle security challenges that could include data encryption, identity and access management, observability and logging such that customers can ensure that their applications and data are secure on the cloud.
- CSPs provide customers the requisite security controls to secure their data based on its sensitivity and classification.
- All major CSPs provide IAM solutions with variations in architectural patterns, security frameworks and operational strategies, and allow consumers to use additional third-party solutions if needed.

- Certified CSPs provide confidence that their service aligns with national or international data sovereignty requirements. Most global cloud services have comprehensive compliance controls. For example, AWS supports 143 security standards and compliance certifications for customers to meet compliance requirements around the globe.[64]
- CSPs offer customers the option of enlisting cloud-native services or outsourcing encryption and key management systems with multiple models for different key management characteristics, and help users meet regulatory standards.

Cloud Users:

- Security in the cloud ecosystem is grounded in a shared responsibility framework, wherein the user is responsible for security "in" the cloud while the cloud service is responsible for security "of" the cloud. The user should factor in security measures while architecting applications and services. Organisations must understand these threats and acquire knowledge on how to develop defensive strategies to utilise and even operate a secure cloud network.
- Customers must ensure a "secure by design approach" while developing their applications. In the context of cloud computing, this means designing cloud systems with built-in safeguards, such as secure APIs, robust access controls, and compliance-ready configurations to pre-empt vulnerabilities.[65] By embedding security into the design, organisations can reduce risks, ensure regulatory compliance, and enhance trust in their cloud infrastructure.
- By maintaining stringent access controls, organisations can reduce the risk of data breaches and ensure compliance with data sovereignty regulations.

Data Classification:

Government:

- The Indian Governmental Cloud Selection Framework published by MeitY[66] provides guidance for security categorization that is compliant with the NIST Special Publication 800.[67] A risk assessment model is used to determine the sensitivity of data based on which suitable controls are recommended. The risk assessment model classifies data into 3 categories in addition to a separate classification for "Secret" data.
- In addition to guidelines from MeitY, industry bodies have also worked on developing data classification mechanisms. For example, the DSCI's proposed three tier categorization system[68] divides data into 3 categories (non-sensitive or public data that is unclassified and low impact; restricted or administrative data with medium impact; and finally government highly confidential data with high impact) and maps this against the MHA's Data Classification levels (Unclassified, Restricted, Confidential, Secret & Top Secret) and suggests cloud deployment models against each.

Proposed Three-Tier Categorization	Workload (Application & Data) Examples	MHA's Data Classification Level	Suggested Cloud Deployment Model
Tier 1: Non-sensitive or public data (unclassified); low impact	Open Data, Public Data, Non-Sensitive administrative information, website hosting public information	UNCLASSIFIED	Level 1: Basic Security - Cloud infrastructures in conformance with security best practices standards and guidelines (ISO 27001/17/18, and MeitY Cloud Guidelines)
Tier 2: Restricted or administrative; medium impact	Restricted matters, business or administrative data, emails, client support and CRM systems, financial records, and medical records; citizens' identity and social security data	RESTRICTED & CONFIDENTIAL	Level 2: Strong Security - Level 1 plus additional security controls, e.g., strong identity authentication (MFA), mandated data encryption, and high-availability architecture requirements.
Tier 3: Government highly confidential or above; high impact	Government documents and applications dealing with matters of international negotiations; technical matters of military nature or requiring higher protection	SECRET & TOP-SECRET	Level 3: In-Depth Protection - Level 2 plus additional security controls, e.g., encrypted private network link to the CSP's data centre or network access points, virtual network separation between departments, use of dedicated instances.

An example of a data classification framework, suggested by the Data Security Council of India

- Data classification is sometimes mandated in sector-specific legislation in India, such as in the case of the RBI Master Direction on Outsourcing of Information Technology Services, 2023, driven by the need for safeguarding customer financial information.
- Standards organisations such as ISO and NIST have also suggested certain classification methods in cases where specialised security controls must be rolled out. For example, ISO 27001 classifies data according to sensitivity and their worth, allowing it to satisfy the ISO standard's goal of avoiding unauthorised disclosure of data or alteration. Similarly, NIST's SP 800-53 standard mandates a categorization of data to assist US federal agencies in more efficiently building and managing their information technology systems. Internationally recognised associations such as the Cloud Security Alliance (CSA) have also released industry norms like the Cloud Controls Matrix,[69] which includes classification guidelines for data along parameters such type, origin, legal limitations and context.

CSPs:

- CSPs provide users with the required tools and services to implement data classification or enable cloud users to implement this through third-party mechanisms.

Cloud Users:

- As only the user is aware of the contents of their data on the cloud, it is under the remit of the user to administer appropriate classification and security controls for their data.

Data Protection:

- Data protection legislations delineate obligations expected from data fiduciaries - those who collect data from users and determines the purpose and means of processing of personal data - and data processors - those who process the data on behalf of the fiduciary. Data protection compliance obligations are laid out for data fiduciaries, since they collect data and are responsible for its protection. For instance, under the DPDP Act, data fiduciaries are expected to obtain informed consent from data principals through a notice, implement minimum security measures, intimate data breaches and erase data when requested or the purpose has been fulfilled. However, data fiduciaries through contractual arrangements may require data processors to ensure compliance with reasonable security safeguards and audits, among others. In a cloud ecosystem, CSPs function as data processors who process data as instructed by the data fiduciary (cloud users). Thus, it is important for users of cloud services to be compliant with these data protection requirements.

The policies surveyed indicate varying levels of security protections based on sectoral requirements and build on MeitY's shared responsibility model to demarcate roles and responsibilities of each stakeholder involved. Furthermore, they account for adherence to global security certifications by CSPs. However, a crucial aspect of ensuring security is the classification of data that is currently not adequately addressed in existing policies/guidelines. While the Ministry of Home Affairs has a data security classification policy in place, this may not be readily adaptable for diverse business needs in an IT/cloud environment.

Resilience

Government:

- The MeitY Empanelment Framework accounts for resilience requirements including disaster recovery and business continuity with baselines RPO and RTO requirements. Departments are advised to tailor disaster recovery requirements based on their needs. Disaster recovery is also addressed under MeitY's guidelines for SLAs, in addition to providing detailed Disaster Recovery Best Practices.[70]
- The RBI and SEBI frameworks mandate cloud users to develop and establish a robust framework for business continuity and disaster recovery in line with instructions issued by respective authorities and ensure that their IT service providers can meet their requirements.

CSPs:

- CSPs typically drive high availability and fault tolerance by developing strong infrastructure design. One example is the use of multiple isolated and physically separate zones within a geographic area, which in turn has multiple data centres and is equipped with effective power, cooling systems, physical security and is connected with redundant, ultra-low latency networks, providing resilient and scalable infrastructure. Further, redundancy is ensured by compartmentalising infrastructure and services to mitigate the effects of fires, natural calamities, or any other events.[71]
- Technological developments like "cell-based architecture" enable cloud services to provide sustained services without interruptions by employing an application design that is tolerant of failure. By offering multiple instances of the same services that are isolated from each other, consumers can continue to provide services to end users despite instances of excessive load or failure.

Cloud Users:

- Cloud users play an important role in building resilient cloud environments by ensuring their service is configured securely, encrypt data and further build resources by redundancy. It is important to remember that unlike availability and fault tolerance - which are the remit of the CSP except for on-premises cloud solutions - disaster recovery needs to be architected by the organisation as per its specific needs. Cloud users will be aware of their disaster recovery requirements and are responsible for architecting solutions while factoring in applicable regulations. However, all three requirements are defined in and met through Service-Level Agreements. Cloud users should adequately state their requirements and verify the inclusion of these requirements based on their needs. Resilience benefits of the cloud can be captured only when users design, architect and implement patterns to meet their needs, such as simplifying technology, automating functions and leveraging all the capabilities of the cloud ecosystem.[72]

The surveyed policies make efforts of fulfilling the three critical elements of a resilient cloud - high availability, fault tolerance and disaster recovery. While CSPs provide for high availability and fault tolerance by building supportive infrastructure, however, disaster recovery remains the responsibility of the user. All three elements are accounted for under contractual arrangements/SLAs.

Jurisdictional Control over Data

This pillar of cloud sovereignty primarily tackles with the access to citizen data by Law Enforcement Agencies (LEAs) from other jurisdictions and can be suitably addressed through Government intervention. For example, under the draft DPDP Rules under finalisation, it is proposed that significant data fiduciaries[73] be subject to restrictions on transfer of any personal data (and related traffic data) outside India, as identified by Government basis recommendations of a committee to be established.

Concerns regarding extra-territorial access to citizen data stemming from the CLOUD Act introduced by the US government remains a point of concern despite mechanisms under the Act for companies and the courts to reject or challenge requests for data access, if the request is believed to infringe on the privacy rights of the foreign country national. This can also be addressed by countries signing bilateral treated with the USA.

MLATs or similar agreements facilitate data exchange, and the government should consider improving such frameworks to strengthen digital sovereignty. Currently, multiple countries and regions have MLATs such as the EU-US MLAT, ASEAN MLAT, and India has over 40 MLATs.[74] When no MLAT exists, countries can also use instruments such as Letters Rogatory to seek the assistance of foreign governments for LEA access to data. However, MLATs currently lack the operational efficiency for swift and streamlined access to data. Formats for seeking data are not uniform, there exist communication gaps locally and between countries, and the process is often time consuming.[75]

Cross-border data access is provided for through MLATs. India currently lacks robust MLATs for law enforcement data access.

Portability

Government:

- The MeitY Empanelment process covers various exit management and interoperability requirements that support open-source APIs, and data portability for migration back to on-prem or to a different CSP.[76]
- The SEBI framework mandates users to implement data portability as a part for their exit strategy, while the RBI framework suggests the same as a guidance.
- Additional guidance is also provided in MeitY's Cloud Best Practices that advises user departments to factor in the issue of cloud vendor lock-in as a part of key design considerations while adopting cloud technologies. MEITY has constituted a multi-stakeholder committee to suggest a cloud interoperability and portability framework that would enable organizations to easily migrate from one cloud environment to another.[77]

CSPs:

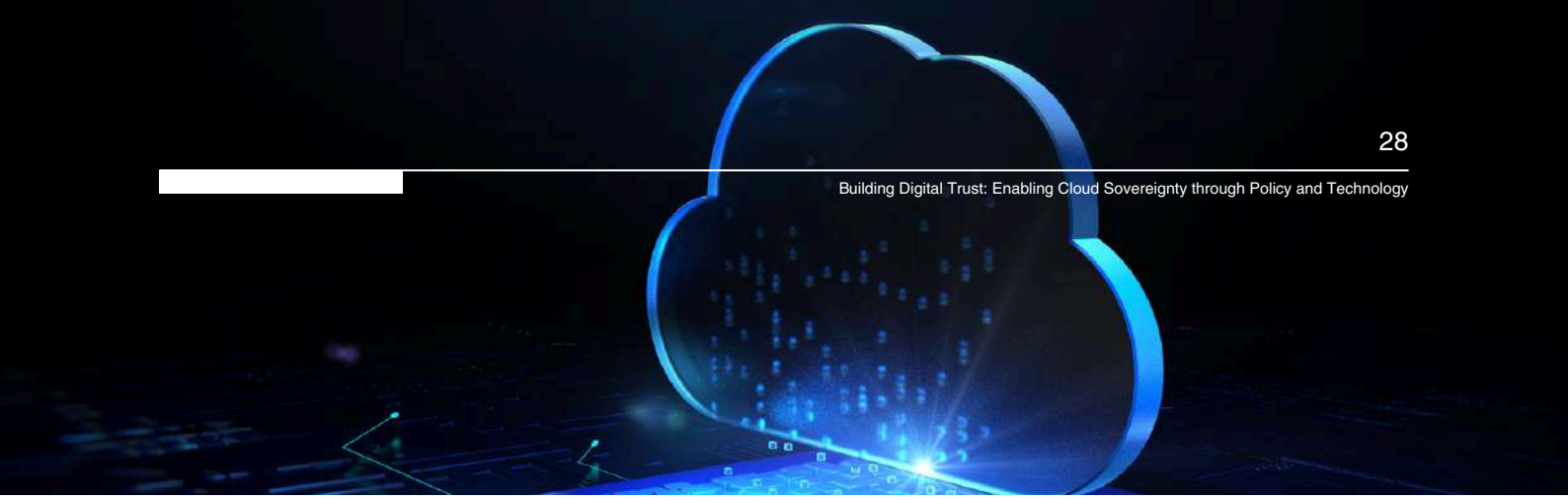
- It is a commercial imperative for a CSP to offer interoperability with innovative solutions to meet consumer demand. As customers onboard new IT tools and services, they seek suitable spaces to run each of these workloads. To compete effectively, CSPs must architect their cloud solutions to support interoperability with the customer's existing IT solutions. The flexibility to migrate across cloud environments without restrictions helps build long-term customer trust.
- CSPs can enhance portability by ensuring that migration of data from their platforms is easy - through measures like reducing egress fee (charges incurred for moving data out of a cloud) or provision of migration tools to ensure a smoother transition.
- Cloud services have been promoting portability by supporting open standards, embracing containerisation technologies like Docker and Kubernetes, developing cloud-agnostic tools, offering multi-cloud management platforms, and collaborating with industry bodies to establish common portability frameworks.
- Hyperscalers now offer free outbound data transfers to support transitioning onto a different cloud or on-premises, thereby promoting mobility and reducing vendor lock-in.

Cloud user:

- Cloud users should account for portability clauses in their contractual arrangements with CSPs.

- As the user has complete control over the data in the cloud, they can employ open source/portable formats for storing data to ensure that data can be moved on and off the cloud storage at any time.
- Further, cloud users should architect their applications to ensure portability. Mitigating against lock-in requires deployment practices and pre-planning and architecting with transience in mind.
- Some important application portability considerations include: (i) incorporating REST APIs with popular industry standards like HTTP, JSON and OAuth to abstract applications; (ii) separating business logic from application logic with clear documentation; (iii) Using container technologies to help isolate software from its environment and reduce dependencies.

Portability is accounted through contractual arrangements, as in the case of resilience. Seamless data transfer between different CSPs requires the compatible data storage formats and limited egress fee. However, while some hyperscalers can offer tools to migrate data and zero egress fees, this is not implemented by all CSPs. Also, users sometimes do not factor in portability while architecting their applications on cloud.



CHAPTER 5: CONCLUSION & RECOMMENDATIONS

Cloud services offer a secure, reliable and configurable platform for organizations to digitise, scale, innovate and adapt their services to evolving technologies. However, concerns regarding control, security and compliance, if sufficiently addressed can help realise this potential. Cloud sovereignty and digital trust are enabled through a combination of policy frameworks, technical controls offered by CSPs and contractual arrangements. International and domestic regulations - whether sectoral or nodal - touch upon the identified pillars of cloud sovereignty. For instance, regulatory frameworks such as the EU's GDPR, and India's DPDP Act and Draft Rules, account for security, data protection and access controls. Different nations enforce data and cloud sovereignty through a combination of regulatory frameworks and policy guidelines but ultimately rely on technical controls provided by CSPs and administered by cloud users to implement these mandates effectively. While policy frameworks are important, they are not enough and need to be supplemented by technical controls which can adapt to the changes in technology.

CSPs offer a wide range of technical controls such as data residency guardrails, robust IAMs, encryption with customer-managed keys, confidential computing, and zero-trust architectures to restrict unauthorised access to data and provide a secure cloud environment to their customers. These technical controls ensure adherence to legal frameworks and further cloud sovereignty principles by providing real-time, enforceable measures that can adapt dynamically. By leveraging these tools, government departments and enterprises can ensure data control, security, resilience and technical autonomy, and meet the evolving sovereignty and security requirements.

Thus, to achieve a durable foundation for cloud sovereignty, the government should prioritise efforts to further strengthen the identified foundational pillars of cloud sovereignty. Based on our analysis of existing policies and commercial offerings, we recommend the following measures to build a resilient and secure cloud ecosystem:

- ***Take a Technology-First Approach*** - While regulatory frameworks establish the foundational principles for maintaining sovereign control over technologies, it is technical controls that provide the necessary agility and adaptability to keep pace with rapidly evolving technological landscape. To effectively uphold digital sovereignty, the government must recognize and embrace the critical role of technical controls as facilitators for translating policy objectives into practical, enforceable outcomes. Technical controls on the cloud can enhance cloud sovereignty by ensuring that data and applications remain under the control of the cloud user, while securely leveraging cloud infrastructure. These measures can include data residency guardrails, encryption at rest and in transit, customer-managed keys (CMK), confidential computing, stringent IAM etc. To leverage these controls effectively, organisations should implement a layered security approach, ensuring compliance with local regulations while maintaining operational efficiency. Policies should provide simplified guidance for cloud users to implement technical controls that are outcomes driven.

Enhance India's cloud through public-private partnerships **-** In order to meet India's growing digital and cloud requirements, the government should make a proactive effort to leverage technological capabilities and infrastructure of the private cloud ecosystem. The investments by hyperscalers to enhance resiliency and reliability of their infrastructure (by architecting for high uptime) as well as maintaining the highest levels of cybersecurity can help organisations and governments meet their sovereignty and security requirements. This is evidenced in hyperscalers' support for the seamless roll-out of several e-Governance and citizen delivery projects in India. Their investments in data centers, innovation hubs, and skill development can bolster India's digital ecosystem and enhance global competitiveness.

Provide a simplified and enabling data classification framework - Cloud users need to classify their data based on sensitivity and operational impact to ensure proper implementation of security controls. However, in the absence of adequate guidance on data classification, sometimes organisations struggle to classify their data for IT environments. This ultimately hinders their adoption or migration to cloud. Existing data classification frameworks may not be easily adaptable to business requirements. Hence, a simplified data classification scheme drawing from existing frameworks such as NIST can help organisation tailor their security and privacy controls while leveraging the potential of cloud.

Reinforce Jurisdictional Control through MLATs - Jurisdictional control over data is fundamental to cloud sovereignty, as it ensures that data generated within a nation is subject to its laws and regulations rather than those of foreign entities. As indicated in Chapter 4, jurisdictional control over data is not adequately addressed through existing legislative frameworks. When sensitive data is hosted on servers outside a country's borders or by providers subject to foreign legal obligations, it creates the risk of unauthorised access or misuse, particularly in cases of conflicting legal frameworks. Retaining jurisdictional control allows nations to safeguard critical information, enforce privacy laws, and ensure compliance with local standards. Extraterritorial reach can conflict with local data sovereignty laws, posing significant risks to national security and privacy. To address this, law enforcement agencies should establish clear frameworks for cross-border data access. Governments can also build in other mechanisms to enable access to data such as bilateral and multilateral treaties. Strengthening India's mutual legal assistance treaties (MLATs) or similar agreements can facilitate lawful data sharing while respecting sovereignty.

Aligning to international standards to promote portability - Ongoing discussions among global multi-stakeholder groups such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are actively working on promoting cloud interoperability and portability to foster a more collaborative cloud ecosystem. In this context, creating local standards or mandatory requirements may inadvertently impede innovation and cross-border service delivery for local cloud service providers. However, encouraging business practices that prevent vendor lock-in such as zero egress for outward data transfers and promoting fair software licensing principles, can provide cloud users greater flexibility and control over their data while promoting a competitive cloud ecosystem.

ENDNOTES

1 "Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing", available at https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf.

2 Thomas Abell, Arndt Husar and Lim May-Ann, "Cloud Computing as a Key Enabler for Tech Startups Across Asia and the Pacific" (2021), Asian Development Bank, available at: https://www.adb.org/sites/default/files/publication/714971/sdwp-079-cloud-computing-tech-start-ups-asia-pacific.pdf.

3 Ministry of Electronics and Information Technology, "Process for Empanelment of Cloud Service Offerings of Cloud Service Providers (CSPs)", available at: https://www.ambud.meity.gov.in/assets/web_assets/Includes/files/Stepwise%20guide%20on%20empanelment%20process.pdf

4 "Assessment of Cloud Adoption in Government Sector" (2023), Nasscom, available at: https://analyticsindiamag.com/global-tech/aws-fires-up-indian-govts-digital-ambitions/

5 Government of India, "Digilocker", available at: https://www.digilocker.gov.in/

6 IDC (2024), "Cloud Adoption Accelerates in India, Driven by Digital Transformation, GenAI, and Multi-Cloud Strategies", https://www.idc.com/getdoc.jsp?containerId=prAP52965924

7 "India's Cloud and Data Revolution" (2023), FICCI & EY, available at: https://www.ey.com/content/dam/ey-unified-site/ey-com/en-in/newsroom/2023/8/documents/ey-india-cloud-and-data-revolution.pdf

8 Ministry of Information and Broadcasting, "India's Digital Revolution: Transforming Infrastructure, Governance, and Public Service" (2024), Press Information Bureau, available at: https://pib.gov.in/PressReleasePage.aspx?PRID=2082144

9 Amazon Web Service, "The Government of India powers a Population-Scale Vaccine Drive on AWS" (2022), available at: https://aws.amazon.com/solutions/case-studies/meity-gov-india-case-study/

10 Google Cloud, "ONDC: Unleashing ecommerce energy across India with Google Kubernetes Engine", available at: https://cloud.google.com/customers/ondc?hl=en

11 "Is India Building Enough to Power Its Digital Transformation" (2023), Cushman and Wakefield, available at https://cushwake.cld.bz/is-india-building-enough-to-power-its-digital-transformation/10-11/.

12 Ministry of External Affairs, "India-U.S. Joint Statement (February 13, 2025)" (2025), available at: https://www.mea.gov.in/bilateral-documents.htm?dtl/39066.

13 "Navigating Digital Sovereignty and its Impact on the Internet (2022), Internet Society, available at: https://www.internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf.

14 Julia Pohle and Thorsten Thiel, "Digital Sovereignty" (2020), available at: https://policyreview.info/concepts/digital-sovereignty.

15 Meloni Musoni and others, "Global Approaches to Digital Sovereignty" (2023), The Centre for Africa Europe Relations, available at: https://ecdpm.org/application/files/7816/8485/0476/Global-approaches-digital-sovereignty-competing-definitions-contrasting-policy-ECDPM-Discussion-Paper-344-2023.pdf.

16 Ministry of Electronics and Information Technology, "Cloud Security Best Practices", available at: https://www.ambud.meity.gov.in/assets/web_assets/Includes/files/2.%20WI3_Cloud%20Security%20Best%20Practices_06112020.pdf

17 Ibid.

18 Ministry of Electronics and Information Technology, "Cloud Security Best Practices", available at: https://www.ambud.meity.gov.in/assets/web_assets/Includes/files/2.%20WI3_Cloud%20Security%20Best%20Practices_06112020.pdf

19 Alex Tolsma, "GDPR and the Impact on Cloud Computing" (2017), Deloitte, available at: https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-update-the-impact-on-cloud-computing.html

20 Serge Gutwirth and others (eds.), "Reinventing Data Protection?" (2009), Springer, pp.3-4

21 National Security Agency, "Use Secure Cloud Identity and Access Management Practice" (2024), available at: https://media.defense.gov/2024/Mar/07/2003407866/-1/-1/0/CSI-CloudTop10-Identity-Access-Management.PDF.

22 Ministry of Electronics and Information Technology, "Inviting Application for Empanelment of Cloud Service Offerings of CSPs", available at: https://www.ambud.meity.gov.in/assets/web_assets/Includes/files/Application_Empanelment_CSPs_June_2021.pdf

23 "Is Your Cloud Resilient Enough?: What to look for in Cloud Infrastructure Design" (2024), Frost and Sullivan Whitepaper, available at: https://s3.cn-north-1.amazonaws.com.cn/aws-dam-prod/whitepapers/2024-frost-sullivan-resilient-cloud.pdf

24 Thomas Welsh and Elhadj Benkhelifa, "Perspectives on Resilience in Cloud Computing: Review and Trends" (2017), IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), available at: https://eprints.staffs.ac.uk/4420/1/8.pdf

25 ibid.

26 Milan Chauhan and Stavros Shiaeles, "An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions" (2023), MDPI AG, available at: https://www.mdpi.com/2673-8732/3/3/18

27 See generally: U.S. Department of Justice, Criminal Division, "CLOUD Act Resources", available at: https://www.justice.gov/criminal/cloud-act-resources

28 Ibid.

29 Currently, the US has bilateral agreements with the UK and Australia under the Act.

30 David Banisar, "National Comprehensive Data Protection/Privacy Laws and Bills 2025" (January 28, 2025), available at: https://ssrn.com/abstract=1951416

31 Ibid

32 Anupam Chander and Haochen Sun (eds.), “Data Sovereignty: From the Digital Silk Road to the Return of the State” (2023), Oxford Academic, pp.1-32, available at:https://academic.oup.com/book/55328/chapter/428794920

33 “Overview of China’s Cybersecurity Law” (2017), KPMG, available at: https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf

34 Which refers to data that can reveal a person’s identity such as their date of birth, identification number, biometric information, address etc.
“Overview of China’s Cybersecurity Law” (2017), KPMG, available at: https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf

35 See generally: Matthew Murphy and Fei Dang, “Cloud Computing in China” (2019), Lexology, available at: https://www.lexology.com/library/detail.aspx?g=998fe1a0-6634-41e7-a670-19ca406709e5

36 Notice on Cloud Services Business Operations Management-
Greg Pilarowski, Samuel Gintel and Lu Yue, “China to Strengthen the Regulatory Oversight of Cloud Services” (2017), Pillar Legal, available at: https://www.pillarlegalpc.com/wp-content/uploads/2024/07/Pillar-Legal-China-Regulation-Watch-China-to-Strengthen-Regulatory-Oversight-of-Cloud-Services-2017-06-16.pdf

37 Data Protection Guide for Small Business, “Data Protection benefits for you”, available at: https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-benefits-for-you_en#:~:text=Data%20protection%20is%20protected%20by,thought%20or%20freedom%20of%20assembly.

38 Suzanne Smalley, "Europe preparing to ‘ease the burden’ of landmark data privacy law", (April 8, 2025), https://therecord.media/eu-proposal-changes-gdpr-small-medium-businesses

39 European Union Agency for Cybersecurity, “Cloud Services Scheme” (2020), available at: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

40 Office of the Australian Information Commissioner, “Australian Privacy Principles”, Australian Government, available at: https://www.oaic.gov.au/privacy/australian-privacy-principles

41 Australian Signals Directorate, “Cloud Computing Security Considerations”, Australian Government, available at: https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20Cloud%20Computing%20Security%20Considerations%20%28October%202021%29.pdf. Similarly, the Protective Security Policy Framework provides guidance on how Australian government entities should assess risks associated with employing cloud resources in order to ensure security of their “people, information and assets” within Australia and overseas. The framework outlines 16 core requirements that entities must implement to achieve the government’s desired security outcomes.

42 Andy Leck and others, “Singapore: Parliament passes Cybersecurity (Amendment) Bill on 7 May 2024” (2024), Global Compliance News, available at: https://www.globalcompliancenews.com/2024/06/14/https-insightplus-bakermckenzie-com-bm-technology-media-telecommunications_1-singapore-parliament-passes-cybersecurity-amendment-bill-on-7-may-2024_052024/

43 Personal Data Protection Commission of Singapore, “Good Practices to Secure Personal Data in the Cloud Platform”, available at: https://www.pdpc.gov.sg//-/media/files/pdpc/pdf-files/other-guides/cloud-data-breach-infographic-pdf.pdf

44 Anupam Chander and Haochen Sun (eds.), “Data Sovereignty: From the Digital Silk Road to the Return of the State” (2023), Oxford Academic, pp.1-32, available at:https://academic.oup.com/book/55328/chapter/428794920

45 Meloni Musoni and others, “Global Approaches to Digital Sovereignty” (2023), The Centre for Africa Europe Relations, available at: https://ecdpm.org/application/files/7816/8485/0476/Global-approaches-digital-sovereignty-competing-definitions-contrasting-policy-ECDPM-Discussion-Paper-344-2023.pdf.

46 Anupam Chander, “Law and the Geography of Cyberspace” (2015), UC Davis Legal Studies Research Paper No. 432, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2614555

47 Anupam Chander and Haochen Sun (eds.), “Data Sovereignty: From the Digital Silk Road to the Return of the State” (2023), Oxford Academic, pp.1-32, available at:https://academic.oup.com/book/55328/chapter/428794920

48 Amy Farris, Manita Rawat and Matthew C. Mousley, “Cloud Computing in the United States” (2019), Lexology, available at: https://www.lexology.com/library/detail.aspx?g=6c9daf49-3ab7-42e1-9d63-e24741609258

49 MeitY, “MeghRaj 2.0”, available at: https://ngc.gov.in/assets/media/Service-Catalogue-Meghraj-2.0_V4.pdf

50 “Adoption of Cloud Services by intermediaries regulated by PFRSA”, Pension Fund Regulatory Development Authority, available at:https://www.pfrda.org.in/writereaddata/links/circular_compressed8cb4bcde-5f8f-465d-904a-a594184560ff.pdf

51 Pre-qualification criteria 10 in Cloud Management Office, “Stepwise Guide on Process for Empanelment of Cloud Service offerings Cloud Service Providers”, Ministry of Electronics & Information Technology, available at: https://ambud.meity.gov.in/assets/web_assets/Includes/files/Stepwise%20guide%20on%20empanelment%20process.pdf

52 Principle 3(iii) in the “Framework for Adoption of Cloud Services by SEBI Regulated Entities” (2023), Securities and Exchange Board of India, available at https://www.sebi.gov.in/legal/circulars/mar-2023/framework-for-adoption-of-cloud-services-by-sebi-regulated-entities-res-_68740.html.

53 Reserve Bank of India, “Storage of Payment System Data” (2018), available at: https://www.rbi.org.in/commonman/english/Scripts/FAQs.aspx?Id=2995 .

54 Department of Information Technology, “Guidelines for Strategic Control in Outsourced Projects” (November 16, 2010), Ministry of Electronics and Information Technology, available at: https://www.meity.gov.in/static/uploads/2024/02/Guidelines_Strategic_Control_Outsorced_Projects_251110.pdf

55 “Framework for Adoption of Cloud Services by SEBI Regulated Entities” (2023), Securities and Exchange Board of India, available at: https://www.sebi.gov.in/legal/circulars/mar-2023/framework-for-adoption-of-cloud-services-by-sebi-regulated-entities-res-_68740.html

56 Anthony Liguori, “AWS Nitro System gets independent affirmation of its confidential compute capabilities” (2023), AWS, available at: https://aws.amazon.com/blogs/compute/aws-nitro-system-gets-independent-affirmation-of-its-confidential-compute-capabilities/ and Microsoft, “Azure Cloud Computing”, available at: https://azure.microsoft.com/en-us/solutions/confidential-compute

57 Millard, p. 144

58 See generally: Iain Beveridge, “Ownership, Control and Possession: Options for Key Management on the Cloud” (2022) Cloud Security Alliance, available at: https://cloudsecurityalliance.org/blog/2022/03/24/ownership-control-and-possession-options-for-key-management-in-the-cloud.

59 Indian Computer Emergency Response Team, “Directions by CERT-In under Section 70B, Information Technology Act 2000”, available at: https://www.cert-in.org.in/Directions70B.jsp

60 Ministry of Electronics and Information Technology, “Cloud Security Best Practices”, available at: https://www.ambud.meity.gov.in/assets/web_assets/Includes/files/2.%20WI3_Cloud%20Security%20Best%20Practices_06112020.pdf

61 ibid.

62 Reserve Bank of India, “Master Direction on Outsourcing of Information Technology Services” (April 10, 2023), available at: https://rbidocs.rbi.org.in/rdocs/notification/PDFs/102MDITSERVICES56B33FD530B1433187D75CB7C06C8F70.PDF

63 “Framework for Adoption of Cloud Services by SEBI Regulated Entities” (2023), Securities and Exchange Board of India, available at: https://www.sebi.gov.in/legal/circulars/mar-2023/framework-for-adoption-of-cloud-services-by-sebi-regulated-entities-res-_68740.html

64 Amazon Web Services, “AWS Compliance”, available at: https://aws.amazon.com/compliance/

65 Robert Masse, “How to Accelerate Cloud Adoption Using Security By Design”, Deloitte, available at: https://www2.deloitte.com/ca/en/pages/insight/articles/how-to-accelerate-cloud-adoption-with-security-by-design.html.

66 Ministry of Electronics and Information Technology, “Guidelines for Procurement of Cloud Services”, available at: https://www.ambud.meity.gov.in/assets/web_assets/Includes/files/5.%20Guidelines_Procurement_Cloud%20Services_v2.2.pdf

67 The NIST SP 800 series comprises of guidelines, recommendations and technical specifications for IT cybersecurity practices for the US Federal Government that may be adopted by non-federal bodies. accessible at- https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

68 Data Security Council of India, “Security Controls Based Cloud Adoption For Government Workloads” (2021), available at: https://www.dsci.in/resource/content/security-controls-based-cloud-adoption-government-workloads.

69 “Cloud Controls Matrix” (2024), Cloud Security Alliance, available at: https://cloudsecurityalliance.org/research/cloud-controls-matrix

70 Ministry of Electronics and Information Technology, “Disaster Recovery Best Practices”, available at: https://www.ambud.meity.gov.in/assets/web_assets/Includes/files/3.%20Microsoft%20Word%20-%20WI3_DR%20Best%20Practices_28092020%20(1).pdf.

71 “Is Your Cloud Resilient Enough?: What to look for in Cloud Infrastructure Design” (2024), Frost and Sullivan Whitepaper, available at: https://s3.cn-north-1.amazonaws.com.cn/aws-dam-prod/whitepapers/2024-frost-sullivan-resilient-cloud.pdf

72 Nick Gerne and others, “The New Era of Resiliency in the Cloud” (2023), McKinsey Digital, available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-new-era-of-resiliency-in-the-cloud

73 Under India's Digital Personal Data Protection (DPDP) Act, Significant Data Fiduciaries (SDFs) are entities or classes of data fiduciaries designated by the Central Government based on factors like the volume and sensitivity of personal data they handle, and the risk they pose to data principals' rights, potential impact on the sovereignty and integrity of India etc. SDFs will be subject to stricter compliance requirements.

74 Central Bureau of Investigation, “MLATs”, available at: https://cbi.gov.in/MLATs-list

75 Faraz Sagar, Sara Sundaram, and Pragati Sharma, "Understanding Cross Border Legal Assistance", (October 29, 2020), https://corporate.cyrilamarchandblogs.com/2020/10/understanding-cross-border-legal-assistance/

76 Ministry of Electronics and Information Technology, “Inviting Application for Empanelment of Cloud Service Offerings of Cloud Service Providers” (2024), available at: https://ambud.meity.gov.in/assets/web_assets/Includes/files/Application_Empanelment_CSPs_March_2024.pdf.

77 Ministry of Electronics and IT, “Annual Report 2024-45”, accessible at: https://www.meity.gov.in/static/uploads/2024/12/10fcadec462c330211502fed3d24ea83.pdf


KOMN