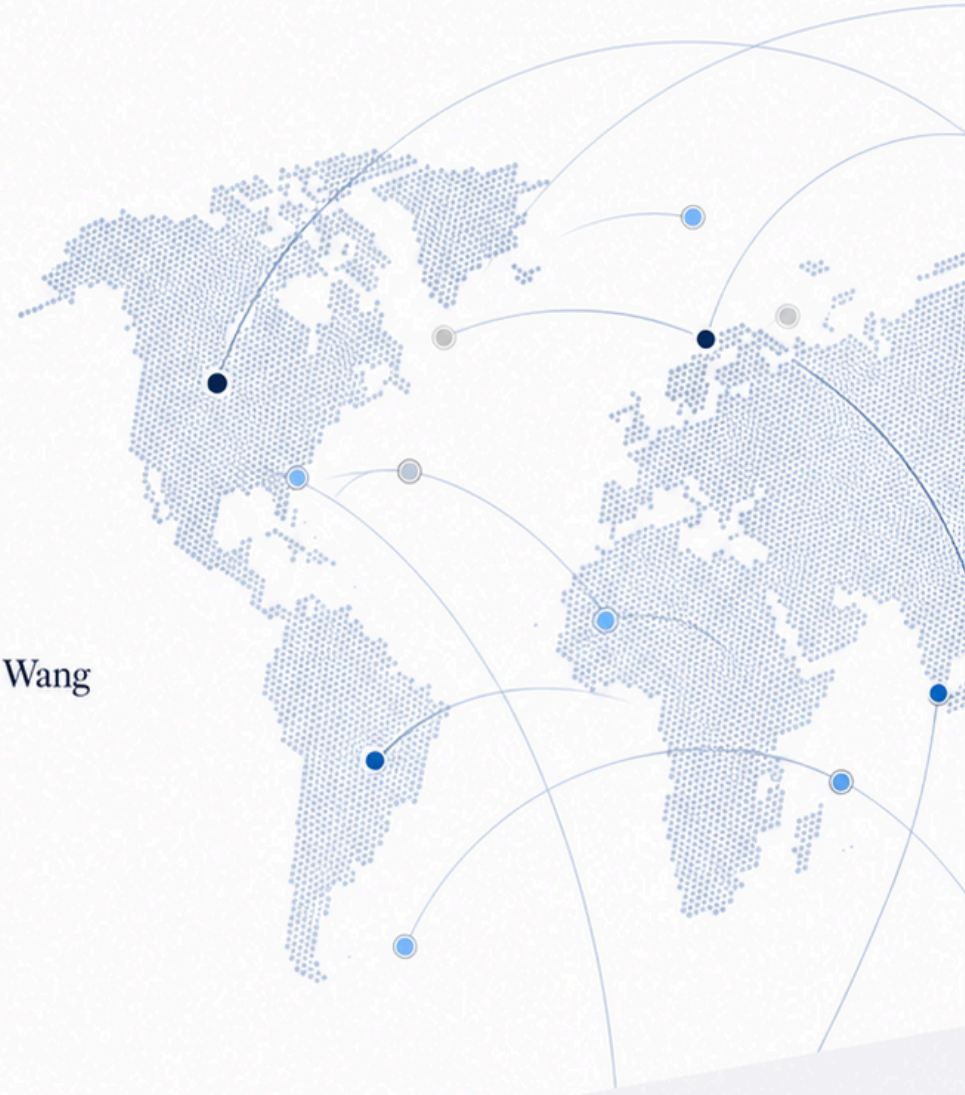
Deglobalization

EFFECTS ON ENTERPRISE TECHNOLOGY



PRODUCED FOR:

JPMorgan Chase & Co

PRODUCED BY:

Arnav Sahai | Ethan Sheinker |
Kankon Sen | Kylee Zhou |
Sofia Marrero | Wei Gan | Xiaoke Wang

FACULTY ADVISOR:

Professor Sydney Jones

JPMC

COLUMBIA | SIPA
School of International and Public Affairs

MAY 2026

Disclaimer

This report was produced for JPMorgan Chase & Co as a graduate school consulting project at Columbia University's School of International and Public Affairs. The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of JPMorgan Chase & Co.

Table of Content

Executive Summary

While JPMorgan Chase operates across dozens of markets globally, this assessment focuses on three jurisdictions where technology sovereignty regimes have become structurally incompatible with global operating models. The European Union, India, and the People's Republic of China have each implemented divergent sovereignty frameworks shaped by US-China strategic competition, national political agendas, and the treatment of data as a national resource. The incompatibility of these regimes complicates the firm's capacity to apply a "lowest common denominator" approach guiding global compliance policies and cybersecurity controls. Moreover, building separate sovereign stacks to satisfy each jurisdiction's mandates incurs substantial capital costs, fragments operational resilience, and compounds the firm's competitive disadvantage relative to domestic competitors, which are unconstrained by global presence. JPMC is compelled to walk a tightrope of maintaining market access to strategic financial markets while bearing acceptable risk.

The underlying logic of the report's proposed recommendations is to use JPMC's legal, technical, and policy resources to translate abstract sovereignty constraints into measurable capital allocation choices in plausible contingencies, balancing financial gains against the risks of non-compliance.

1. **Third-Party Risk:** Implement sovereign risk rating for EU supplies and establish a technology risk taxonomy to quantify outsourcing decisions against capital expenditure.

2. **Regulatory Conflict:** Improve coordination among HQ and regional controls and compliance teams to support preparedness protocols for conflicting-sovereignty scenarios, and standardize Hong Kong-based operations to PRC compliance standards to mitigate risks associated with the Hong Kong National Security Law.

3. **Business Continuity:** Identify regulatory risk thresholds, especially where regulatory compliance costs outweigh market access gains, and build a separate China stack.

4. **Data Localization:** Within India, formally grant the resident director veto power to prevent breaches of Indian judicial authority, run a parallel intellectual property track to

mitigate exposure of proprietary intellectual property in the PRC market, and activate sovereign Artificial Intelligence nodes in India.

Geopolitical tensions will likely intensify rather than stabilize, exacerbating the current challenges of maintaining compliance across three incompatible regimes, requiring a legally sound, technically cost-effective, and compliant policy to manage complexity and minimize risk.

1. Introduction

Globalization has enabled the integration of international financial markets, supported by multilateral diplomatic frameworks and globally interoperable cyber infrastructure that align national interests, promoting economic stability and disincentivizing intra-state armed conflict. However, contemporary geopolitical forces have undermined the efficiency-by-design model. COVID-19 compelled firms to recalibrate resilience strategies, moving away from efficiency by designing supply chains around friendly vendors within geopolitical blocs. US-China strategic competition is shaping the pace and deployment of emerging technologies, which is further fragmenting diplomatic blocs. Moreover, "global swing states" constrained by their political interests are redefining technology, data, cloud, and AI sovereignty regimes, increasingly treating data as a national resource rather than a commercial asset.

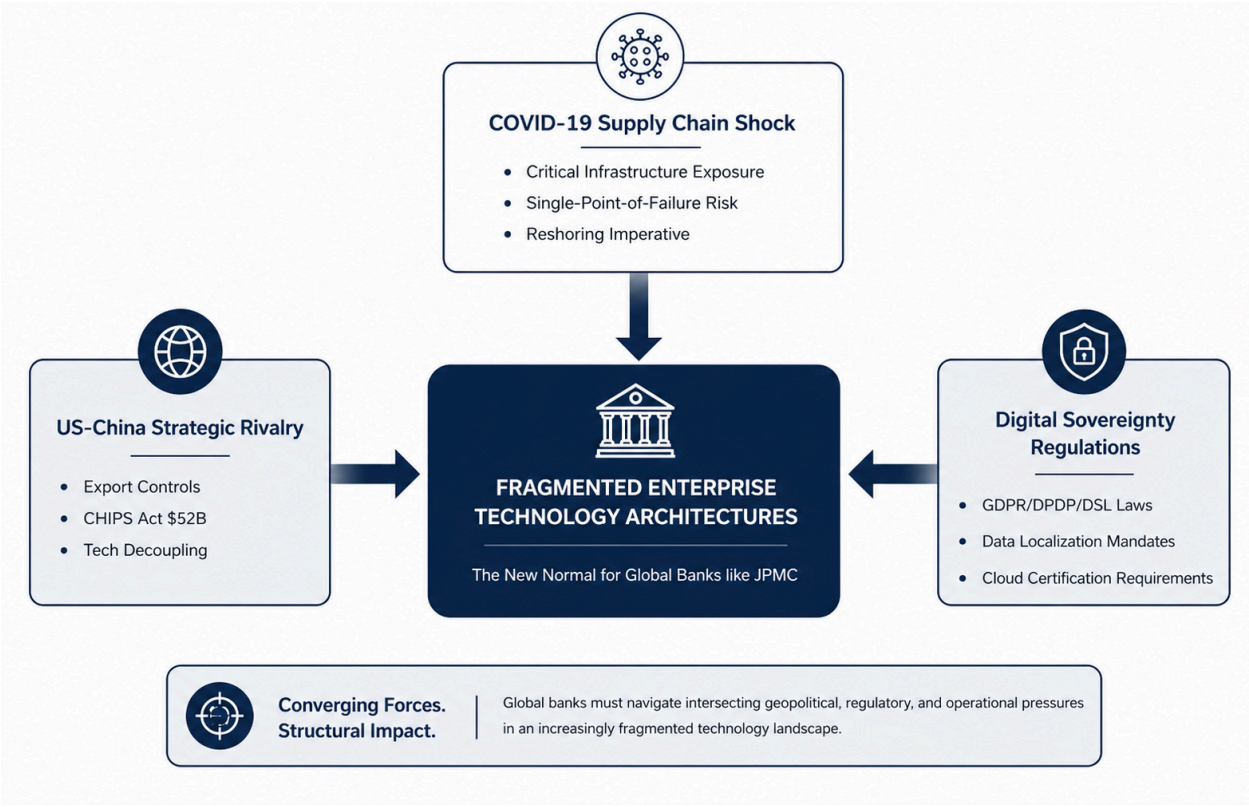


Figure 1: Converging Forces of Deglobalization

However, regulatory regimes are informed by territorial sovereignty, which does not reflect how international technology and cyber infrastructure are built and deployed. Financial services are

uniquely impacted as they're incentivized to maintain global operations, which further stabilizes international markets, yet are pulled in several directions to comply with gradually more stringent regulations, undermining their ability to maintain business continuity in strategic markets.

Unwinding the globalized digital infrastructure creates cascading second-order effects. Operational tensions arise between maintaining a globally relevant policy and adhering to localized regulations in strategic markets. Vendor constraints compound risk as data, cloud, AI, and technology sovereignty regimes favoring domestic suppliers limit the reliable third-party vendor supply, creating vendor lock-in and concentrating third-party risk. Thus, cyber compromise of a limited set of vendors could potentially disrupt critical banking functions in strategic financial markets. The mosaic of national regulations designed to serve national interests is globally incohesive because compliance in one jurisdiction creates a breach of another.

At the client's request, this report evaluates the regulatory environments of the EU, India, and the PRC regarding data, cloud, AI, and technology sovereignty, their macro-drivers, and implications for JPMC's business operations. Analysis focuses on how prominent regulations affect the firm's ability to deploy a globally consistent policy amid an increasingly fragmented regulatory landscape. Thematically categorized risks and recommendations address how JPMC can manage tensions across high-value jurisdictions while remaining resilient to geopolitical and cyber risks, and maintaining business continuity in an unpredictable period.

The technological enablers of globalization that aided JPMC in expanding into new markets are now regulatory burdens that JPMC is obliged to manage to maintain access to markets. These global challenges manifest differently across jurisdictions. Thus, JPMC should adjust to these new realities to ensure its operations are resilient to geopolitical and cyber risks while maintaining business continuity in an increasingly unpredictable period.

2. Methodology

Through semi-structured field interviews with experts in cyber regulations, cloud service providers, cyber vendor services, and AI governance professionals, we have consolidated insights into the fragmentation of digital sovereignty regulations affecting the global financial services industry. A review of regulatory and industry literature helped shape recommendations on JPMC's ability to manage conflicting regulatory pressures in strategic markets.

In an effort to clarify terminology with varying definitions, we have compiled a lexicon of terms that will be used frequently throughout this paper.

- **AI Sovereignty:** A state's authority to govern the development, training, deployment, and auditing of AI systems within its borders.
- **Bring Your Own Key (BYOK)**: A key management approach in which a firm retains custody of its own encryption keys on locally controlled hardware, rather than delegating that control to a cloud provider. In sovereignty contexts, BYOK creates a technical veto against foreign access requests by requiring decryption to engage the local control plane.
- **Cloud and Infrastructure Sovereignty:** An extension of data sovereignty to servers, control planes, and encryption keys, requiring that compute and storage governance remain under the legal and operational control of the host state.
- **Concentration Risk:** The degree to which a bank's cloud computing power is concentrated among a small number of providers, within a single provider's facilities, or shared with other financial institutions on common infrastructure. Higher concentration means greater systemic exposure.
- **Cost Center:** An organizational function that supports operations but does not generate revenue.
- **Critical Information Infrastructure Operator (CIIO):** A designation under China's Cybersecurity Law applied to organizations whose systems, if disrupted or compromised, would cause serious harm to national security, the national economy, or public welfare. Financial institutions operating in China (including foreign banks) are classified as CIIOs

and are subject to the most stringent data localization, vendor certification, and cybersecurity audit obligations under Chinese law.

- **Cyber Risk:** A subcategory of operational risk of financial loss, damage, or business disruption resulting from the failure, breach, or outage of a firm's technological systems.

- **Data Sovereignty:** The principle that data generated within a jurisdiction is governed by that jurisdiction's laws, regardless of where it is stored or processed. It is the foundation of the EU's General Data Protection Regulation (GDPR), PRC's Personal Information Protection Law (PIPL), and India's Digital Personal Data Protection (DPDP) Act.

- **Digital Sovereignty:** The ability of states or regional blocs to independently develop, control, regulate, and fund digital technologies such as cloud, AI, semiconductors, and communications infrastructure. In this report, it is treated as a governance and architecture issue rather than merely a political slogan.
- **Operational Risk:** The risk of loss from the breakdown of internal procedures, people, or systems. It is the residual risk after accounting for financial risks, and the category within which most sovereignty-related technology failures fall.
- **Lack of Substitutability:** Narrowing of viable vendors through sovereignty mandates that displace market selection with regulatory requirements, leaving only compliant suppliers as viable alternatives.
- **Legal Deadlock**: A condition in which full compliance with one jurisdiction's legal obligations creates a breach in another jurisdiction.
- **Modular Sovereignty Architecture:** The strategic model proposed in this report, in which distinct but governed architecture tiers serve different regulatory jurisdictions.
- **Necessity Doctrine**: One of the Cyberspace Administration of China's principles that companies exporting personal information from China must justify *why* the transfer is necessary — proving the data, the volume, and the recipients are all essential to the stated business purpose, with vague or precautionary justifications grounds for rejection
- **Sovereign Cell:** A self-contained, jurisdiction-specific operating unit in which data storage, encryption key custody, governance authority, and technical administration are all localized within a single national boundary. Emphasizes operational autonomy and the ability to

function independently of a firm's global core during regulatory audits or geopolitical disruptions.

- **Sovereign Cloud:** Cloud infrastructure designed to comply with a jurisdiction's legal, technical, and operational sovereignty requirements, typically including local hosting, local key management, and legal shielding from foreign access requests.
- **Sovereign Stack:** A jurisdiction-specific architecture encompassing data, cloud, and AI workloads built to satisfy a given market's sovereignty requirements as a coherent whole.
- **Vendor Lock-In**: The operational and financial dependency that arises when a firm's architecture, workflows, or compliance posture becomes so tied to a specific provider that switching carries prohibitive cost or risk. Sovereignty mandates can accelerate lock-in by narrowing the pool of compliant vendors.

3. Regional Analysis

As firms navigate a fragmenting global landscape, they must reconcile distinct regulatory philosophies governing how data is protected, stored, and audited. While financial firms aim for a unified global operational standard, the divergence between strategic jurisdictions forces a pivot toward localized compliance architectures. This report addresses three key jurisdictions: the European Union, India, and China. These are jurisdictions that represent fundamentally different logics of sovereignty. The EU pursues rights-based sovereignty by protecting citizens. India demands autonomy, while also promoting interoperability with the US technology ecosystem and European regulations. And the PRC requires direct state oversight while investing in domestic production to spur economic growth. These divergent logics create cascading tension across JPMC's legal, policy, and technical teams, requiring the firm to navigate legal conflicts that cannot be fully reconciled but can only be managed.

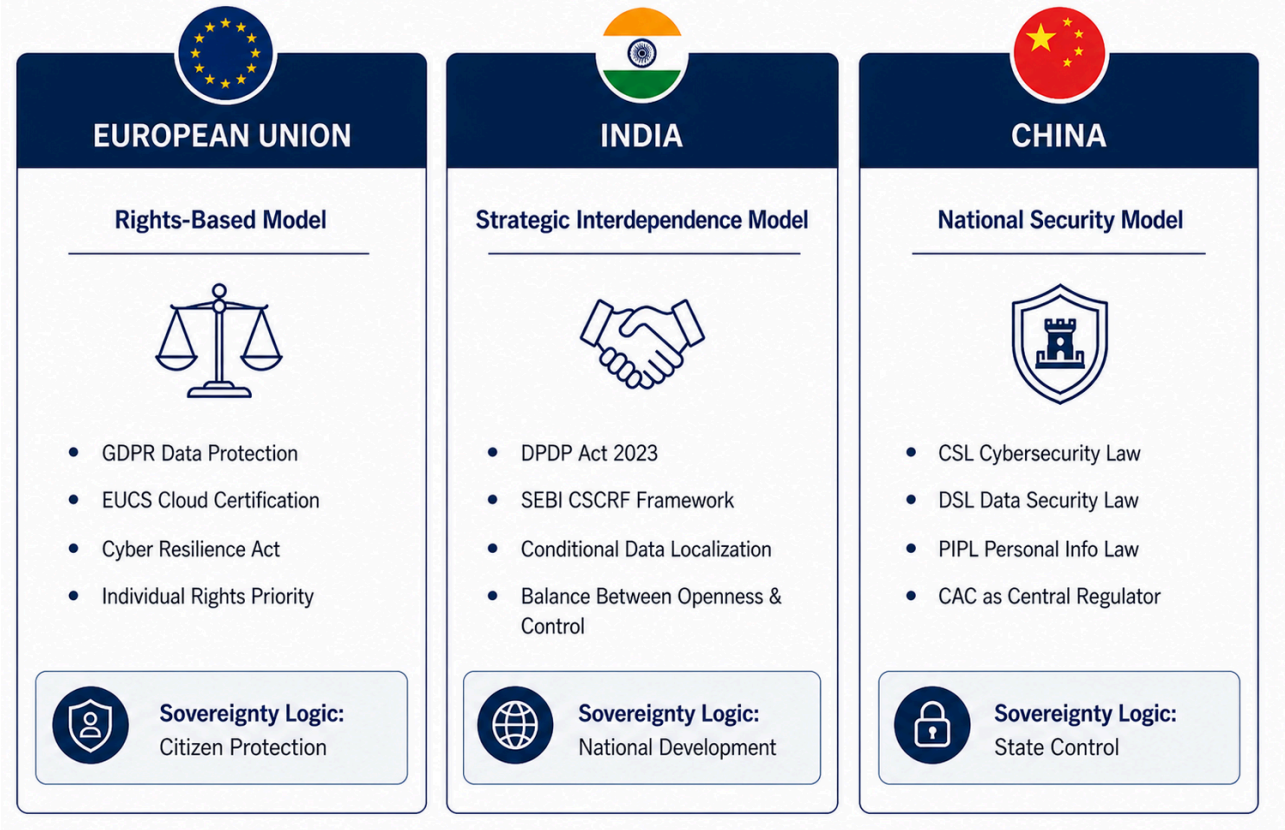


Figure 3: Jurisdictional Regulatory Logic by Region

Figure 4: Global Data Localization Regulation Timeline

3.1 European Union

To protect its citizens and economy, the EU is implementing a proactive regulatory framework designed to secure digital sovereignty and reduce reliance on foreign technological infrastructure. However, the effectiveness of this framework depends on the balance between EU supranational authority and the national policy autonomy of member states, whose divergent security and economic objectives frequently shape the regulatory landscape. The European regulatory environment prioritizes technological strategic autonomy, supply chain accountability, and data protection.

3.1.1 European Union Regulatory Landscape

- Cyber Resilience Act (CRA)
    - In force since December 2024, with main obligations fully applicable by December 2027
- Cloud and AI Development Act (CADA)
    - Scheduled for proposal in the first quarter of 2026
- General Data Protection Regulation (GDPR)
    - Published in 2016 and fully applied in 2018
- European Cloud Services Scheme (EUCS)
    - Drafted in December 2020, yet to be applied

Cyber Resilience Act (CRA)

The CRA is the first EU regulation to establish mandatory cybersecurity requirements for "Products with Digital Elements" sold in the EU.[1] The CRA requires all software and hardware products to meet cybersecurity standards at every stage of the value chain. The regulatory approach allocates legal liability to manufacturers, importers, and distributors rather than end users, requiring that products maintain security throughout their operational lifecycle. All products subject to the CRA must bear the CE marking (Conformité Européenne), serving as the manufacturer's declaration that the product complies with relevant EU legal requirements for safety, health, and environmental protection.[2] Specifically, it requires the manufacturer to

[1] *European Commission*, "Cyber Resilience Act," 2024.
[2] *European Commission*, "CE Marking," official website, accessed April 4, 2026.

conduct a conformity assessment, establish a detailed technical file, and issue an EU Declaration of Conformity. Products without CE marking are prohibited from sale or service within the EU single market.

The regulation ensures that Europe's critical infrastructure, including its financial systems, does not rely on foreign technologies with opaque security standards outside EU regulatory oversight. Consequently, any manufacturers, importers, and distributors of software and hardware with digital elements wishing to access the EU market must transparently disclose security designs and vulnerability management mechanisms, thereby strengthening the EU's control over the digital supply chain.

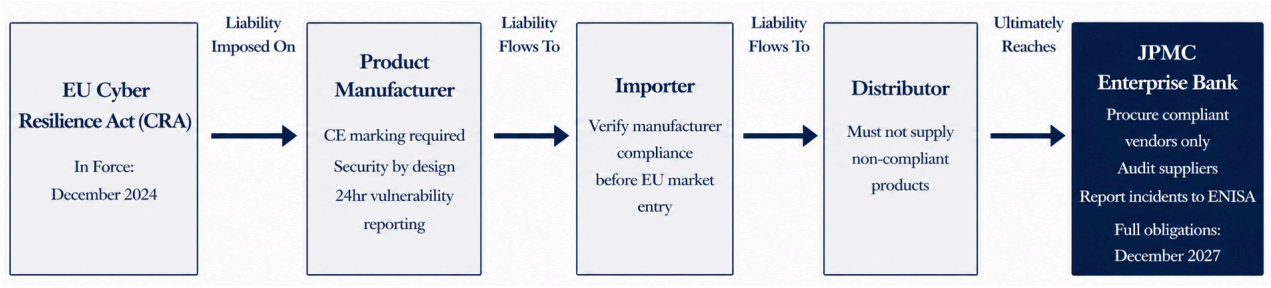


Figure 5: CRA Compliance Liability Cascade

Cloud and AI Development Act (CADA)

CADA represents the EU's industrial policy objective to establish global competitiveness in independent computing infrastructure. The act addresses Europe's shortage of high-performance computing capacity by expanding data center investments and supporting secure, sovereign cloud infrastructure.[3] These measures are designed to close the capacity gap for AI development and ensure the long-term sustainability of Europe's open digital ecosystem. Although primarily an industrial stimulus, CADA's mandates may be integrated into public procurement frameworks, potentially extending sovereign infrastructure requirements to systemically important private entities like JPMC. The potential inclusion of CADA within public procurement scopes could compel JPMC to prioritize EU-based sovereign infrastructure.

General Data Protection Regulation (GDPR)

[3]*European Commission*, "Cloud and AI Development Act: Impact on Europe's Open Data Future," data.europa.eu, October 23, 2024.

The GDPR was designed to protect individuals' rights to privacy and data protection within the EU.[4] It enforces strict rules on how data can be processed, stored, and transferred, especially across borders. Organizations must protect data and report breaches to the Data Protection Authority (DPA) within 72 hours. Non-compliance can result in fines up to €20 million or 4% of global annual turnover.[5]

European Cloud Services Scheme (EUCS)

EUC is a framework established under the EU Cybersecurity Act designed to create unified cybersecurity certification standards for cloud services across the EU.[6] Its primary purpose is to establish a horizontal, unified certification for cloud services across the EU, replacing disparate national standards to facilitate the internal market and increase the security of cloud services. Unlike binding law, the EUCS functions as a technical and organizational benchmark with three levels of assurance: Basic, Substantial, and High. As of March 2024, the most stringent sovereignty mandates, the requirement for non-EU companies to form joint ventures, were removed from the baseline requirements for the High assurance level due to the criticism from European banks, clearing houses, insurance groups, and some startups.[7]

However, implementing the EUCS still faces many difficulties because EU member states have divergent policy priorities. The political debate over the EUCS has divided the European Union into two main groups: the sovereignty-focused group, led by France and Italy, and the market-oriented group, led by Germany, the Netherlands, and Ireland.[8]

The group led by France and Italy supports the inclusion of sovereignty mandates, the requirements for EU-based headquarters, local data processing, and corporate independence from non-EU parent companies, for three reasons:

[4] *Intersoft Consulting*, "General Data Protection Regulation (GDPR)," Accessed May 4, 2026.
[5] *Intersoft Consulting*, "Fines / Penalties," General Data Protection Regulation (GDPR), Accessed May 4, 2026.
[6] *European Union Agency for Cybersecurity (ENISA)*, "EUCS – Cloud Service Candidate Cybersecurity Certification Scheme," August 2023.
[7] Yun Chee Foo, "EU Drops Sovereignty Requirements for Cybersecurity Certification Scheme, Document Shows," *Reuters*, April 3, 2024.
[8] "EUCS: A Future European Security Standard?" *Oodrive Blog*, Accessed May 4, 2026.

1. These nations aim to achieve strategic autonomy by reducing their reliance on American and Chinese technology. This independence ensures that Europe maintains political control over its digital future.[9]
2. The group argues that technical tools like encryption are not enough to block the U.S. CLOUD Act. Instead, they believe only legal ownership can truly protect European data from foreign access.[10]
3. These countries view cloud infrastructure as a critical utility for national security, balancing local control with global collaboration to safeguard data, boost innovation, and ensure long-term competitiveness.

Therefore, these countries want core financial systems to be managed only by companies with their headquarters and operations located within the EU.

Ireland and Germany lead the group opposing strict sovereignty rules.[11] This group argues that technical security standards should be prioritized over political and sovereign obligations.[12] These countries argue that advanced encryption and strict auditing provide better data protection than rules about company ownership or headquarters location. Additionally, Europe maintains a huge trade deficit, €109 billion in 2023, with the United States in the technology and services sectors, and the deficit is growing.[13] Also, US service sectors, such as financial and IT, make up a third of European Union imports.[14]

[9]Hartmann,Théophane. "France Launches Bid to Cut Europe's Tech Dependence." *Euractiv*, , Accessed May 4, 2026.
[10]Theodore Christakis, "European Cybersecurity Regulation Takes a Sovereign Turn," *Cross-Border Data Forum*, July 11, 2023.
[11]"EUCS: A Future European Security Standard?" *Oodrive Blog*, Accessed May 4, 2026.
[12]Global Data Alliance. "GDA Leads Cross-Industry Call to Adopt Technical and Functional EU Cyber Certification Scheme (EUCS)." April 11, 2024.
[13]*European Commission*, "United States," EU trade relationships, accessed April 4, 2026.
[14]"Why Trump's Tariffs Could Push Europe to Target US Tech Services," *Euronews*, February 10, 2025.

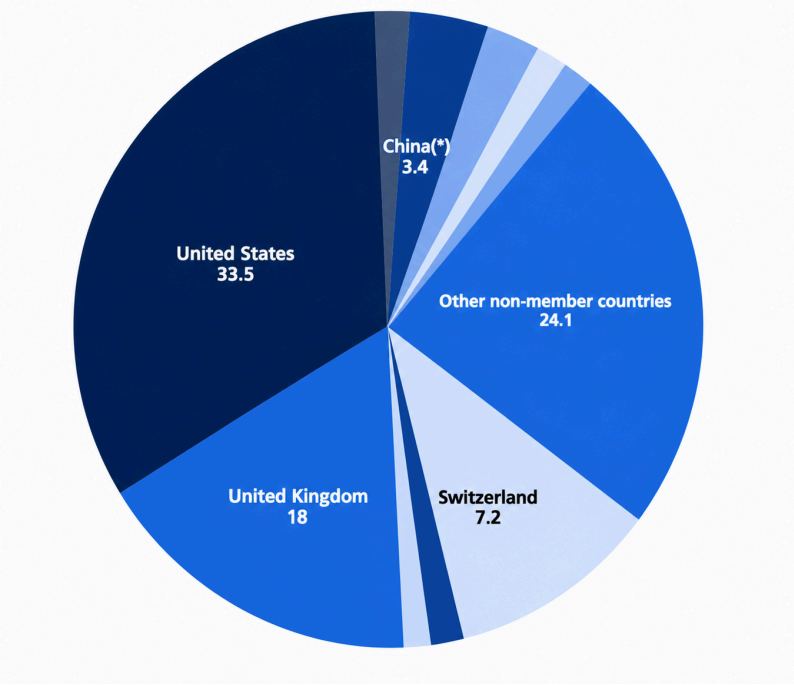


Figure 6: US Services as Share of European Union Imports

These nations fear that imposing strict sovereignty rules could lead to trade retaliation from Washington, damaging the European economy and global financial stability. From an economic standpoint, these countries' considerations are very pragmatic. According to the Center for European Policy Analysis (CEPA), prioritizing digital sovereignty could cost the EU approximately €3.6 trillion, including Opportunity Cost and direct investment in Semiconductor Infrastructure, Software Stack, Cloud and AI, Services Layer, etc., as the graph below shows, over a decade, an amount exceeding France's entire annual economic output and representing roughly 20% of Europe's 2025 GDP.[15]

[15]Kenneth Propp, "Digital Sovereignty: Can Europe Afford It?" *Center for European Policy Analysis (CEPA)*, December 20, 2023.

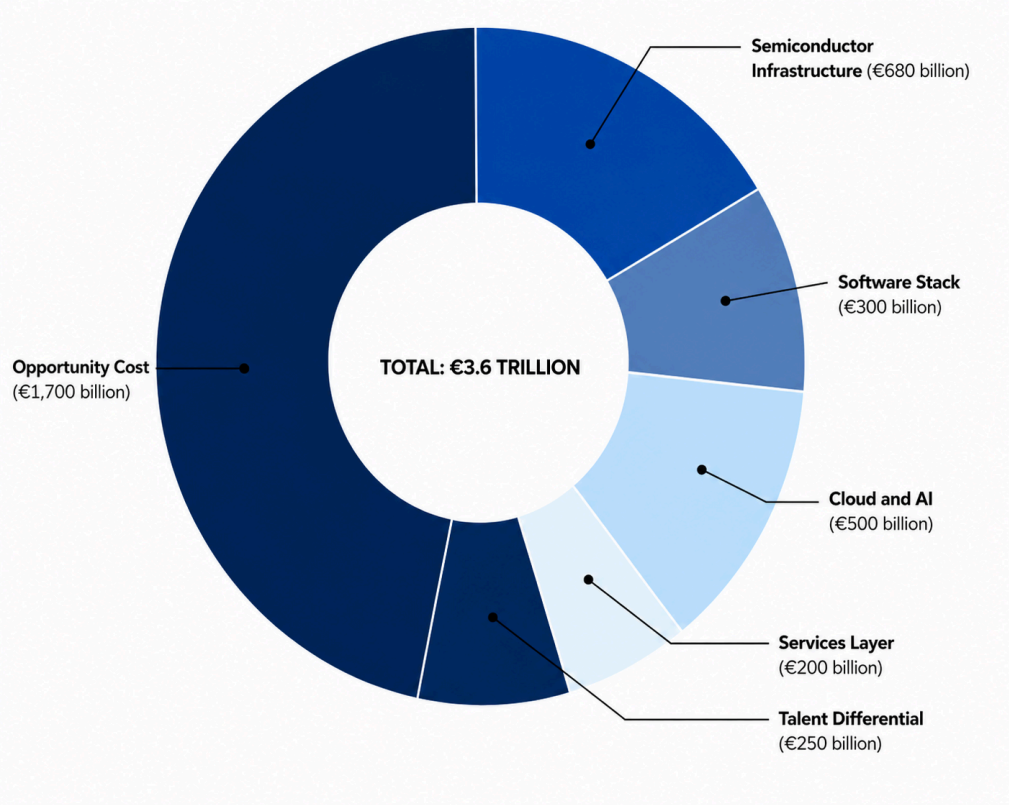


Figure 7. The Prohibitive Cost of European Digital Sovereignty

The EUCS will likely evolve into a tiered framework where strict sovereignty requirements are optional add-ons rather than mandatory rules for all high-security services. This trend allows the European Union to maintain high technical security while avoiding market isolation, trade conflicts with the United States, and astronomical expenses.

3.1.2 Drivers of the EU Model

To understand the future trajectory of the European regulatory environment, it is necessary to examine the three primary drivers behind these mandates.

1. Strategic Autonomy
2. Correction of Systemic Market Failures
3. Resolution of Jurisdictional Conflicts

Pursuit of Strategic Autonomy

The primary driver is the pursuit of "Strategic Autonomy," which seeks to establish an independent technological framework to reduce over-reliance on non-EU tech giants.[16] In the context of deglobalization, technological dependence is viewed as a national security vulnerability. Through these mandates, the EU aims to secure its digital ecosystem, ensuring unilateral control amid political volatility, trade frictions, or technical blockades.

Correct Market Failure

Caused by information asymmetry and negative externalities in the digital product market, the overcorrection of market failures attempts to address two structural inefficiencies.[17]

1. **Information Asymmetry:** Users cannot accurately assess the security risks of digital products, while manufacturers lack the incentive to disclose them.
2. **Negative Externalities:** Manufacturers prioritize speed to market over safety because the end-user, rather than the producer, bears the financial burden of a breach.

The market failure in the global digital supply chain is prompting the EU to use regulation to restructure the liability framework by mandating that manufacturers responsible for security throughout a product's lifecycle raise digital component safety standards.

Resolution of Jurisdictional Conflicts

Addressing the "legal deadlock" between jurisdictions, specifically, the conflict between the extraterritorial mandates of foreign laws, such as the U.S. CLOUD Act, and the EU's GDPR. By establishing sovereign certification standards such as EUCS, the EU aims to provide multinational institutions with technical and legal "shields" to ensure sensitive financial and personal data remains protected from foreign government interference, surveillance, or unauthorized extraction without EU judicial consent, thereby closing existing sovereign regulatory gaps.

[16]Maria Madiega, "Digital Sovereignty for Europe," *European Parliamentary Research Service*, July 2020.
[17]European Commission, "Commission Staff Working Document: Impact Assessment Report," *EUR-Lex*, September 15, 2022.

3.1.3 Implications for JPMC

For JPMC, the shift toward European digital sovereignty results in a legal deadlock over data access, direct liability for software security, and the mandatory decoupling of its global infrastructure to meet conflicting EU national standards.

Banks are compelled to clearly stipulate in contracts that data stored in Europe is strictly protected by EU law. For JPMC and peer banks, this creates a scenario where compliance with one jurisdiction necessitates a violation of the other. If JPMC complies with a U.S. subpoena for European data, it directly violates the GDPR, exposing the bank to regulatory fines of up to 4% of its global annual revenue.[18]

Under the EU Cyber Resilience Act, JPMC is required to conduct mandatory security access assessments on its digital products used in its European operations to ensure that all hardware and software systems bear the CE mark.[19] This mandate generates several direct operational impacts and systemic risks:

- CRA requires JPMC to ensure all utilized digital systems meet a five-year lifecycle maintenance requirement, including mandatory security updates and vulnerability disclosures, creating an administrative and technical burden to audit and verify that every component in its tech stack remains compliant throughout its operational life.
- The high financial and technical costs of mandatory security assessments pose a barrier to entry for small-scale and startup suppliers. The inability of smaller vendors to bear compliance costs may force JPMC to consolidate its technology spend among a few large-scale global providers, increasing vendor lock-in and reducing the bank's access to specialized innovation. The high cost of implementation is also reflected in insights from a CISO at a cloud service provider (CSP) firm, who highlighted that the final stages of implementation can significantly increase the cost of compliance-related investments.
- If JPMC's current suppliers fail to obtain or maintain the CE mark, the bank faces the immediate risk of being required to replace them. The sudden transition away from non-compliant vendors poses a significant threat to business continuity. Furthermore, this

[18] *Intersoft Consulting*, "Fines / Penalties" General Data Protection Regulation (GDPR), Accessed May 4, 2026.
[19] *European Commission*, "CE Marking," official website, accessed April 4, 2026.

exacerbates tech fragmentation, making firms less resilient to cyber compromise and subsequent recovery.

Compliance serves as a mandatory market-entry threshold, steering JPMC's procurement toward large providers capable of absorbing high regulatory costs. While these mandates aim to provide national-to-continental autonomy, the high technical and financial burdens of the CRA create significant barriers for European startups and small and medium-sized enterprises. This dynamic forces vendor consolidation and increases lock-in with dominant firms. Ultimately, promoting sovereign-specific models marginalizes local vendors who lack the scale to compete, prioritizing legal conformity over innovation speed and technical performance.

The proposed implementation of the EUCS is not uniform, as Member States have divergent interpretations of its "sovereignty requirements." The core conflict lies in whether a Member State mandates Sovereignty Requirements as part of the EUCS High-level certification:

- JPMC in France: France is the leading advocate for strict sovereignty mandates. For JPMC's operations in France, the EUCS "High" level would likely include requirements for immunity to non-EU laws.[20] If EUCS is implemented at the "High" level, JPMC may be prohibited from using cloud services provided by the U.S.-headquartered firms unless they operate through a local joint venture or an EU-owned entity. This could lead to a technical decoupling from JPMC's global U.S. infrastructure, increasing complexity in global data synchronization, and potentially causing service latency in the French market.

- JPMC in Germany: Germany prioritizes technical security standards over political ownership rules.[21] For JPMC's operations in Germany, the EUCS focus remains on encryption, auditing, and resilience. JPMC can likely continue utilizing global U.S. cloud providers, provided they meet stringent EUCS requirements for data localization and technical transparency. If primary-choice vendors fail to meet the specific technical certifications required under the EUCS framework, JPMC would be compelled to execute a mandatory and costly vendor replacement to maintain its license to operate.

[20]Hartmann,Théophane. "France Launches Bid to Cut Europe's Tech Dependence." *Euractiv*, , accessed April 25, 2026.
[21]*European Commission*, "United States," EU trade relationships, accessed April 25, 2026.

To mitigate the jurisdictional friction arising from the EU's sovereignty mandates, leading non-EU CSPs introduced institutional innovations. AWS European Sovereign Cloud developed a physically and logically isolated environment designed to satisfy EUCS "High" assurance requirements for data residency, operational autonomy, and immunity from extraterritorial legal mandates. For JPMC, such sovereign-by-design solutions present a potential pathway to mitigate the EU legal deadlock. By deploying an isolated European infrastructure, JPMC could maintain its global technology stack while adhering to stringent data localization requirements. However, this approach trades operational complexity and vendor lock-in for regulatory compliance, requiring JPMC to evaluate whether the cost of dedicated European infrastructure is offset by the ability to preserve global integration elsewhere.

Regardless of both scenarios, Europe's current deficit in indigenous cloud capacity jeopardizes the validity of the regulation. Moreover, because SaaS platforms are augmented to US CSP products, the decoupling of US CSP hardware can have secondary effects on software licensing vendors, further exacerbating vendor-lock-in and associated third-party risks. Regardless of the country, the EUCS "High" assurance level mandates that JPMC's cloud providers undergo rigorous independent auditing and implement localized encryption management.

The European Union is projected to spend approximately €3.6 trillion over the next decade to prioritize its digital sovereignty.[22] For JPMC, such massive public and private expenditures could translate into increased operational costs in Europe through higher taxes or inflated prices for technical services. However, this financial commitment does not guarantee immediate technological parity. J. Michael Daniel, President and CEO of the Cyber Threat Alliance, observes that developing domestic foundations, such as operating systems, is a multi-decade challenge that regulators often underestimate; even persistent efforts in other major economies have yet to produce viable replacements for established U.S. systems. A GW professor notes that technical realities take precedence over four-year political cycles. Since world-leading compute infrastructure cannot be built within a single term, these physical constraints act as a structural limit on the pace of strategic autonomy. For JPMC, being forced into an immature or fragmented local ecosystem could lead to a significant slowdown in innovation and a widening gap in technical performance relative to its global operations.

[22]Kenneth Propp, "Digital Sovereignty: Can Europe Afford It?" *CEPA*, December 20, 2023.

3.2 India

3.2.1 India's Regulatory Landscape

India has emerged as an architect in digital governance that neither pursues extreme open extraterritorial access nor digital isolation. A paradox defines this model. India seeks deep integration with the global technology economy while simultaneously demanding veto power over the jurisdiction of data and infrastructure within its borders. For financial institutions, understanding this philosophy is critical, as it highlights conflicting regulatory tensions that should be addressed before adopting a lowest-common-denominator approach.

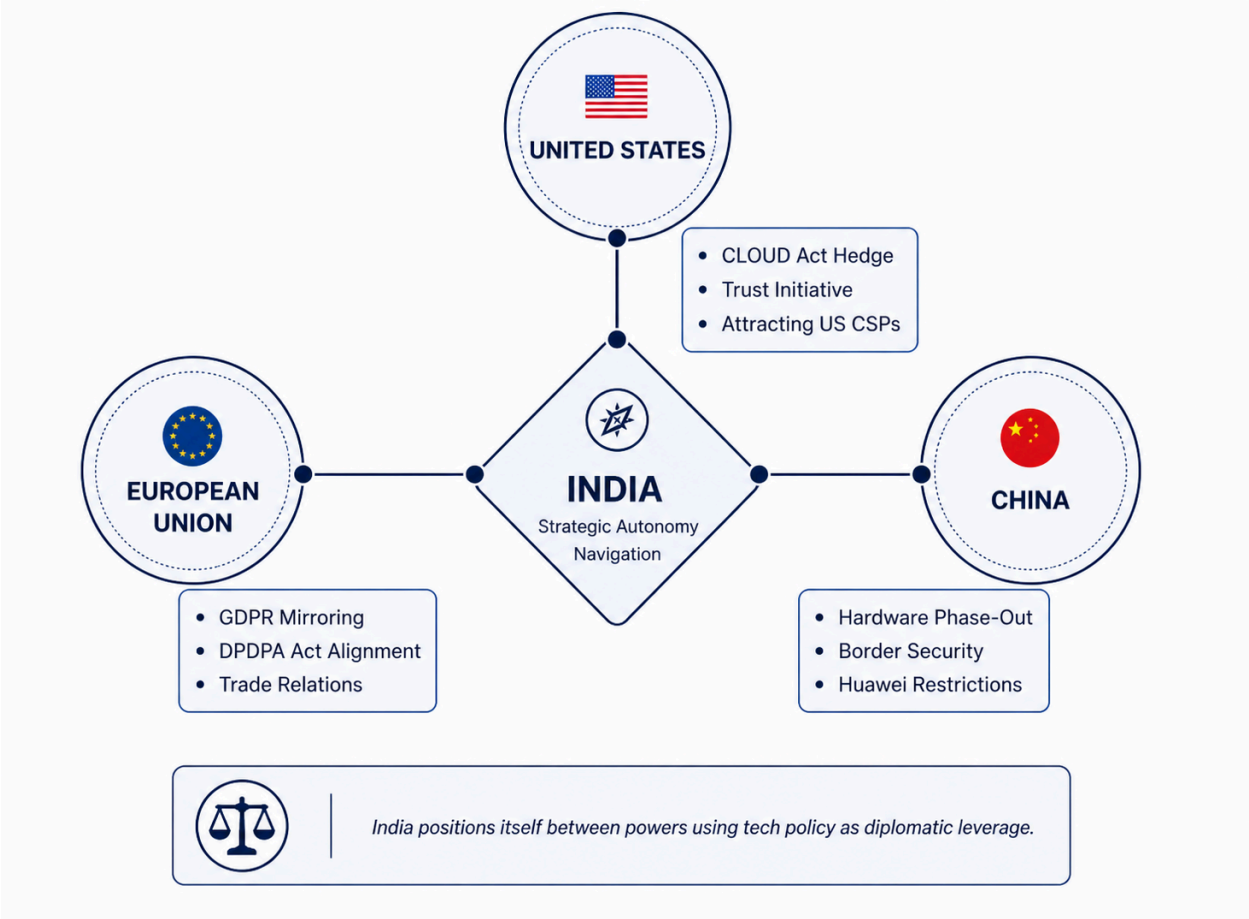


Figure 8. India's Geopolitical Triangle: Balancing the US, the EU, and China

The Geopolitical Triangle: Balancing the US, EU, and China - India's digital sovereignty agenda reflects domestic political aims and a foreign policy tool used to navigate its relationships with the world's three largest tech blocs, the United States, the EU, and the PRC.

- **The United States:** India views‑the US as an indispensable partner for hardware and innovation. Although India seeks access to American semiconductors and AI expertise and attracts US CSPs to operate in India, the CLOUD Act's jurisdictional reach compels India to hedge against Washington by mandating that data and decryption keys remain in Indian jurisdiction. These regulations attempt to neutralize foreign subpoenas, ensuring that the final word on Indian data rests in New Delhi.[23]
- **The European Union:** India has adopted a strategy of regulatory mirroring with Brussels. By aligning its Digital Personal Data Protection (DPDP) Act with the EU's GDPR, it strives for data adequacy. This enables financial institutions to move data between Frankfurt and Bangalore with minimal legal friction. The goal is to be viewed as a democratic data safe-haven.[24]
- **China:** Following the 2020 border tensions, India imposed partial restrictions on Chinese hardware and software from its financial command center, some of which are being phased out more recently.[25] For financial institutions, this necessitates a shift in supply chains towards local operations, reinforcing the need for a custom local stack built on Western hardware whilst maintaining local Indian control.

Broader Goals: Beyond Data Localization

India's ambitions extend beyond data residency. The government's goal is to build Digital Public Infrastructure (DPI), a state-backed foundation for the entire digital economy (e.g., Unified Payments Interface (UPI) for payments, Aadhaar for identity).

Relevance for Financial Institutions: The "Sovereign Cell" Concept

India's strategic interdependence model necessitates a shift from a centralized global hub to a sovereign cell architecture. Because sovereignty in India is an active requirement, the government expects banks not just to store data locally but also to participate in the Indian stack using local standards. This creates a lock-in effect: once a bank integrates with India's DPI, the

[23]Clarifying Lawful Overseas Use of Data (CLOUD) Act, 18 U.S.C. § 2523 (2018).
[24]Digital Personal Data Protection Act (DPDPA), No. 22 of 2023, Gazette of India, August 11, 2023.
[25] Nikunj Ohri and Sarita Chaganti Singh, "India Eases Curbs on Chinese Equipment Imports for Power, Coal as Projects Delayed, Sources Say," Reuters, February 18, 20.

cost of moving those operations elsewhere becomes prohibitively high, locking the institution into the Indian sovereign ecosystem.

In a traditional hub-and-spoke model, a global bank's security and data protocols are managed from a central location (e.g., New York or London). India's model breaks this by requiring local administrative authority. As a SIPA professor noted in his interview, this can lead to highly manual, localized requirements, citing historical examples in which banks had to have employees physically present in-country to "click accept" on trades to meet local jurisdictional mandates.

Expert Insights: The Trade-offs of Fragmentation

The move toward strategic interdependence carries operational risks that should be accounted for against the benefits of market access:

- **The "Fragmented Defense" Risk:** A SIPA professor warns of a "Live Globally, Die Locally" scenario. So while financial institutions operate as a global entity in good times, India's sovereign stack is designed to allow regulators to "ring-fence" the bank in bad times. This fragmentation can impact a global firm's ability to see and respond to cyber threats across its entire network, as the local Indian stack may not be able to engage with telemetry data from the rest of the world.
- **The Economic "Race to the Middle":** Professor Evan Wolff observes that while laws are easy to read, they are "hard to apply" to shared compute environments. For instance, if a financial institution builds a completely separate India-only stack, it may reach a point where the operation is "no longer economically competitive" due to the investment required to access that market. Institutions should find the middle way, such as building enough local infrastructure to satisfy the RBI, while maintaining enough global connectivity to preserve the economies of scale that a multinational bank requires.

3.2.2 Drivers of India's Model

India has shifted digital sovereignty from a theoretical policy debate to a binding operational requirement for banks' operations in India.

India's sovereign stack rests on three legally binding regulatory anchors that financial institutions must address concurrently. The RBI Master Direction on Outsourcing of IT Services governs audit access and operational oversight over material IT service providers. The Digital Personal Data Protection Act (DPDPA) sets the consent architecture and data processing baseline, mirroring the EU's GDPR while adding India-specific Consent Manager requirements. And the Securities and Exchange Board of India's Cybersecurity and Cyber Resilience Framework (SEBI CSCRF) establishes governance accountability for capital markets participants, most notably through its Resident Designated Director mandate, which places personal legal liability on an India-resident board member for technical outages. The Pax Silica Declaration and the 2047 Tax Holiday operate alongside these as commercial accelerants rather than statutory mandates; the three legal anchors define the operational floor.

April 10th Reserve Bank of India (RBI) Deadline

The catalyst for technical realignment was the April 10, 2026, RBI Master Direction deadline. This mandates that all regulated entities ensure unfettered audit access and the RBI's right to inspection across all material IT service providers.

- **Operational Trigger:** Financial institutions can no longer rely on global assurance reports from U.S. hyperscalers because the **RBI Master Direction on Outsourcing of IT Services** (effective from 2023, with strict 2026 deadlines) mandates a shift from third-party certification to direct, verifiable oversight. Financial service firms must provide a physical or virtual path for Indian regulators to audit the specific hardware and databases housing Indian client data.
- **Exit Strategy Mandate:** For vendors unable to meet these localized audit standards, the financial institution is now legally required to have a documented exit strategy to bring those functions in-house or transition to a local provider by the April 10th cutoff.[26]

The RBI's 'unfettered right to audit' is not merely a compliance check, but a pillar of digital sovereignty. Unlike standard global audits that rely on periodic third-party reports (e.g., SOC2), India's mandate requires **real-time, granular visibility into the system's operational**

[26] Reserve Bank of India (RBI), "Master Direction – Outsourcing of Information Technology Services," RBI/2023-24/102, updated April 2026.

command. By ensuring that the RBI can inspect the internal logic of a global firm's algorithms and data flows without permission from the firm's foreign headquarters, India effectively domesticates the firm's authority. This prevents 'jurisdictional shielding,' where a firm might otherwise cite foreign privacy laws or U.S. court orders to deny a local regulator access to its own domestic infrastructure.

Pax Silica and the TRUST Initiative

The Pax Silica Declaration (February 20, 2026) provides the carrot in these circumstances. This multilateral trade deal, coupled with the US-India Transforming the Relationship Utilizing Strategic Technology (TRUST) Initiative, eases previous data localization tensions. Specifically, the trade deal does so by enabling hardware swap, whereby India has agreed to grant "Trusted Node" status to multinational firms that localize their data, in exchange for prioritized, unrestricted access to next-generation U.S. AI silicon chips (e.g., NVIDIA B200S).

- **Significance for JPMC:** This creates a trusted Silicon corridor, allowing financial institutions to import hardware into Bangalore that would normally be restricted under U.S. export controls, provided the command center (the administrative keys and authority) remains within Indian jurisdiction.[27]

However, Pax Silica does not carry the same legal weight as the RBI Master Direction, the DPDPA, or the Securities and Exchange Board of India (SEBI) Cybersecurity and Cyber Resilience Framework (CSCRF) because it is a multilateral declaration rather than codified domestic law. Its effect on JPMC is reflected by the trade and licensing mechanisms it enables, primarily export control easements and "Trusted Node" designations, rather than through direct statutory force. Thus, Pax Silica is best interpreted as the political vehicle through which domestic obligations become commercially survivable for global firms, not as a source of obligation in itself.

Fiscal and Legal Anchors: DPDPA and the 2047 Tax Holiday

[27] *Pax Silica Declaration on Multilateral Semiconductor Integration*, Joint Statement by the U.S. Department of Commerce and India's Ministry of Electronics and Information Technology, February 20, 2026.

India's long-term goal is to make the sovereign stack economically viable through two primary pillars:

- **2047 Tax Holiday:** Introduced in the Union Budget 2026-27, this fiscal incentive offers a tax holiday until 2047 for global firms that establish their regional sovereign AI hubs in India.[28] This turns the high cost of redundant local infrastructure into a 20-year capital efficiency play for financial institutions. Practically speaking, this 2047 Tax Holiday can then be the "carrot" that makes the RBI's April 10 deadline more palatable. It turns a regulatory divorce from global systems into a 20-year business case for making India a primary, independent node in firms' global network.[29]
- **DPDPA-EU Mirroring:** The Digital Personal Data Protection (DPDP) Act is being implemented with an eye toward regulatory handshaking. By mirroring the EU's GDPR, India is positioning itself as a democratic data safe-haven. However, it adds the Consent Manager framework, a localized technical requirement that financial institutions must integrate into their global customer-facing APIs. This means that a standard GDPR compliant interface is insufficient for the Indian market; firms must build bespoke API layers to facilitate the state-mandated consent architecture, turning a legal alignment into a unique engineering requirement that complicates the simpler goal of a unified global customer experience.[30]

Expert Insights: Application Difficulties

Regulatory drivers are forcing a shift in how financial institutions manage their liabilities. Professor Wolff emphasizes that while the laws are clear, they are "hard to apply" to shared compute environments. He warns that as SEBI's Resident Director mandate sharpens, it places personal legal liability on an India-based board member for technical outages.

[28] Press Information Bureau, "Union Budget 2026-27 Tax Holiday Till 2047," *Government of India*, November 19 2025.
[29] *Government of India Ministry of Finance*, "Union Budget 2026-27: Incentives for Sovereign AI and Data Infrastructure," Part B, Section 12, February 1, 2026.
[30] Ministry of Electronics and Information Technology, *Digital Personal Data Protection (DPDP) Rules, 2024*, Rule 5: Technical Specifications for Consent Managersdomestically developed.domestically developed.

3.2.3 Implications for JPMC

The regulatory requirements in India have moved from policy discussions to a set of immediate operational constraints. For JPMC, this requires a fundamental shift in how the firm manages its local technical stack and its legal accountability.

Although Indian indigenous technical capacity is mature, it lacks key components that US hyperscalers rely on. Yotta Data Services emerged as the most credible domestic challenger at the cloud infrastructure layer, with its Shakti Cloud offering localized NVIDIA H100 capacity under full Indian custody[31]. CtrlS, ESDS, Tata Communications, and Reliance Jio Cloud Services round out the Infrastructure as a Service (IaaS) layer[32], while Zoho has built a domestically developed SaaS suite that several Indian banks have adopted for non-core workloads.[33]

However, the depth across the full enterprise stack, such as sovereign-grade AI/ML platforms, global threat intelligence feeds, and the financial services-specific tooling JPMC currently receives from AWS and Azure, does not yet exist domestically at scale.[34] For JPMC, wholesale substitution for Zoho or Yotta is currently not feasible, requiring a hybrid approach in which a US hyperscaler operates an India-resident sovereign region with local key custody and Indian-administered audit controls[35], supplemented by domestic providers for workloads where regulatory pressure or cost favors them.

Transitioning to Trusted Node Status

The primary implication of the Pax Silica and TRUST initiatives is the requirement for JPMC to redefine its India data centers as trusted nodes.[36]

---

[31] *NVIDIA*, "Yotta Built India's First Sovereign AI Infrastructure With Shakti Cloud," NVIDIA Customer Stories, accessed May 4, 2026.
[32] Varghese Pappachan, "How Cloud Computing is Becoming a Reality in India," *Digital First Magazine*, September 23, 2020.
[33] Larry Dignan, "Zoho Just Delivered the Best SaaS Defense vs. AI," *Constellation Research*, February 18, 2026.
[34] Paula Rooney, "JPMorgan Chase Builds Ambitious AI Foundation on AWS," *CIO*, December 4, 2024; ESDS Software Solution, "Sovereign Cloud & Data Residency for India: The Future of Trusted Digital Infrastructure," *ESDS Knowledgebase*, November 24, 2025.
[35] *Amazon Web Services*, "AWS Digital Sovereignty," accessed May 4, 2026.
[36] *Pax Silica Declaration on Multilateral Semiconductor Integration*, February 20, 2026, Section 4.2 (Trusted Node Certification).

- **Operational Shift:** This status allows financial institutions to bypass previous bottlenecks and import advanced AI hardware (e.g., high-end American semiconductors and rack-scale supercomputing systems that were previously subject to strict export controls or domestic protectionist import licenses) directly into India. However, firms must demonstrate that the data processed remains within the local Indian jurisdictional corridor when deploying shared compute environments.
- **The Sovereign Stack:** For JPMC, this necessitates deploying a portable stack in Bangalore that can operate independently of the global core during regulatory audits.

Sovereign Key Management (BYOK)

To resolve the conflict between the U.S. CLOUD Act and Indian jurisdictional mandates, financial institutions should implement Bring Your Own Key (BYOK) protocols.[37]

- **Jurisdictional Partitioning:** By hosting encryption keys on Indian-soil Hardware Security Modules (HSMs), financial institutions create a technical veto. Even if a U.S. court issues a warrant for data access, the firm cannot provide the decrypted data without engaging the local Indian command center.[38]
- **Regulatory Alignment:** This satisfies the RBI's demand for local control while technically insulating the global firm from the legal double jeopardy of conflicting warrants.

Board-Level Liability and the Resident Director

- The SEBI CSCRF framework introduces a significant shift in corporate governance by mandating a Resident Designated Director with personal legal accountability.[39] This is a deliberate "jurisdictional anchor." By placing a specific individual's freedom at stake, India ensures that JPMC's global headquarters cannot prioritize New York-led technical updates over New Delhi-led regulations.

---

[37] Ministry of Electronics and Information Technology (MeitY), *Technical Standards for Sovereign Encryption and Key Management*, Advisory No. 4/2025.
[38] *United States v. Microsoft Corp.* (The CLOUD Act), 18 U.S.C. § 2523, as interpreted under the India-US TRUST Initiative Reciprocity Framework (2026).
[39] Securities and Exchange Board of India (SEBI), *Cybersecurity and Cyber Resilience Framework (CSCRF)*, 2023 (Revised 2026). *Note: The Resident Designated Director serves as a jurisdictional anchor, ensuring local legal accountability for global technical decisions.*

- **Resident Veto:** For JPMC, this means the India-based leadership has formal veto authorities over global system updates. This does not prevent foreign jurisdictions from making laws. Still, it ensures that, when laws conflict, the firm's local operations default to Indian requirements, thereby protecting the Resident Director from personal statutory liability.

3.3 China

3.3.1 China's Regulatory Landscape

China's regulatory environment treats data and technology infrastructure as national security assets and is shaped by three foundational laws:

- Cybersecurity Law (CSL)
- Data Security Law (DSL)
- Personal Information Protection Law (PIPL)

These are primarily administered by the Cyberspace Administration of China (CAC), alongside sector-specific rules issued by China's financial regulators and the industrial direction set by the 15th Five-Year Plan (FYP).[40] The driving unified logic across all of these instruments is that data generated in China should be stored, processed, and governed in China, on infrastructure that the Chinese state can inspect and audit.

The Cybersecurity Law (CSL)

Designates financial institutions, as Critical Information Infrastructure Operators (CIIOs), and requires them to use "secure and controllable" (i.e., domestically certified) hardware, software, cloud services, and AI models.[41] The 2026 amendments eliminated the "warning and rectification" grace period, introduced immediate fines of up to roughly $1.4 million for serious breaches, and extended the law's reach to any overseas activity deemed to harm China's cybersecurity.[42] The amended CSL also embeds business continuity into compliance, as under Articles 35 and 36, CIIOs must ensure their infrastructure can support "stable and continuous operation of business," maintain disaster recovery backups of critical systems, and run regular cybersecurity emergency drills.[43] This turns continuity from a best practice into a documented compliance obligation.

---

[40] Jihong Chen. "Data Protection & Privacy 2025: China." Chambers Practice Guides. *Chambers and Partners*. March 10, 2026.

[41] DigiChina, trans., "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," *DigiChina,* Stanford University, June 29, 2018.

[42] *Cybersecurity Law of the People's Republic of China*, amended October 28, 2025, effective January 1. 2026.; AmCham China, *Analysis of China's Evolving Data Security Framework* (Beijing: American Chamber of Commerce in China, November 2025).

[43] Herbert Smith Freehills Kramer, "China's Revised Cybersecurity Law: Key Changes," November 2025.

The Data Security Law (DSL)

Classifies all data as general, important, or national core, with the strictest handling, including export prohibition, for the upper tiers. Under the national standard, a dataset is graded at the level of its most sensitive component. Furthermore, the quantitative scale of the data impacts grading parameters, meaning sharing even general data can trigger a full CAC assessment once aggregated to sufficient volume.[44] Its most consequential provision for global banks is Article 36, which prohibits any organization in China from sharing China-stored data with a foreign court, regulator, or law-enforcement agency without prior approval from Chinese authorities.[45]

The Personal Information Protection Law (PIPL)

Requires explicit consent and impact assessments for handling personal data and restricts cross-border transfers to three tightly regulated pathways:

1. Security assessment by the CAC
2. Standard contract
3. Certification

Exports are subject to security assessment by the CAC. Non-compliance can attract fines up to 5% of annual revenue and personal liability for responsible officers.[46]

Sector-specific financial rules are often layered on top of the three foundational laws. The National Financial Regulatory Administration (NFRA) requires 20 days' advance notice before banks share bulk-sensitive data with affiliates and operates its own four-tier data classification. The People's Bank of China (PBOC) operates a parallel five-tier grading system for payments and credit data. Both frameworks prohibit the use of public cloud for core financial systems and require encryption using Chinese SM series standards, functionally equivalent but not interoperable with Western AES/RSA. [47] The Ministry of Public Security's (MPS) Multi-Level

[44]National Information Security Standardization Technical Committee (TC260), *Data Security Technology — Rules for Data Classification and Grading*, GB/T 43697-2024 (effective October 1, 2024).
[45]"Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)," DigiChina, Stanford University, June 29, 2021.
[46] "Translation: Personal Information Protection Law of the People's Republic of China (Effective Nov. 1, 2021)," *DigiChina*, Stanford University, August 20, 202.,
[47]National Financial Regulatory Administration (NFRA), *Banking and Insurance Institutions Data Security Management Measures* (Beijing: NFRA, December 27, 2024), effective March 1, 2025.;People's Bank of China (PBOC), *Administrative Measures for Data Security in the Business Areas of the People's Bank of China* (Beijing: PBOC, May 1, 2025), effective June 30, 2025.; National Financial Professional Standardization Technical

Protection Scheme 2.0 (MLPS 2.0) classifies information systems on a five-tier impact scale. Financial institutions designated as CIIOs occupy Level 3 or higher, mandating annual third-party security assessments, network segregation, SM-series cryptography standards, and in-country disaster recovery with no cross-border failover.[48]

Volume thresholds create a second, size-driven layer of constraint that foreign banks actively manage operations around. The Network Data Security Management Regulations and CAC outbound transfer rules require security assessment and annual compliance audits whenever an organization processes personal information for more than 1 million individuals, holds any "important data," or transfers "personal information" of more than 100,000 individuals (or sensitive PI of 10,000 individuals) across borders.[49] Crossing the 1 million-individual threshold reclassifies a firm as a "large-scale personal information processor," triggering mandatory appointment of a Personal Information Protection Officer, periodic impact assessments, and CAC security assessment for any cross-border transfer regardless of volume — step-changing compliance posture in a way that forces architectural and headcount investment that cannot easily be reversed.[50]

Additionally, Professor Wolff highlighted that there has never been a distinction between commercial and national security data in China. For global firms, operational standards should be prepared, "not for plausible deniability, but to be able to operate in-country without running afoul of the stricter laws." This absence of distinction means the entire regulatory framework is read through a national security lens rather than a commercial compliance one.

Committee, *Financial Application Specification of Cloud Computing Technology*, JR/T 0166–0168–2020 (October 16, 2020).; Office of State Commercial Administration (OSCCA), *SM Series Cryptographic Algorithms* (including GB/T 32918 [SM2], GB/T 32905 [SM3], and GB/T 32907 [SM4]).

[48]MLPS 2.0 / Level 3+ requirements: Standardization Administration of China & Ministry of Public Security.

[49]State Council of the People's Republic of China, *Regulations on Network Data Security Management* (Beijing: State Council, September 30, 2024), effective January 1, 2025.

[50]State Council of the People's Republic of China, *Regulations on Network Data Security Management* [网络数据安全管理条例], Decree No. 790 (Beijing: State Council, September 30, 2024), arts. 13–15, effective January 1, 2025.;Cyberspace Administration of China (CAC), *Guidance on the Security Management of Cross-border Data Transfers and Large-Scale Processing* (Beijing: CAC, January 30, 2026).

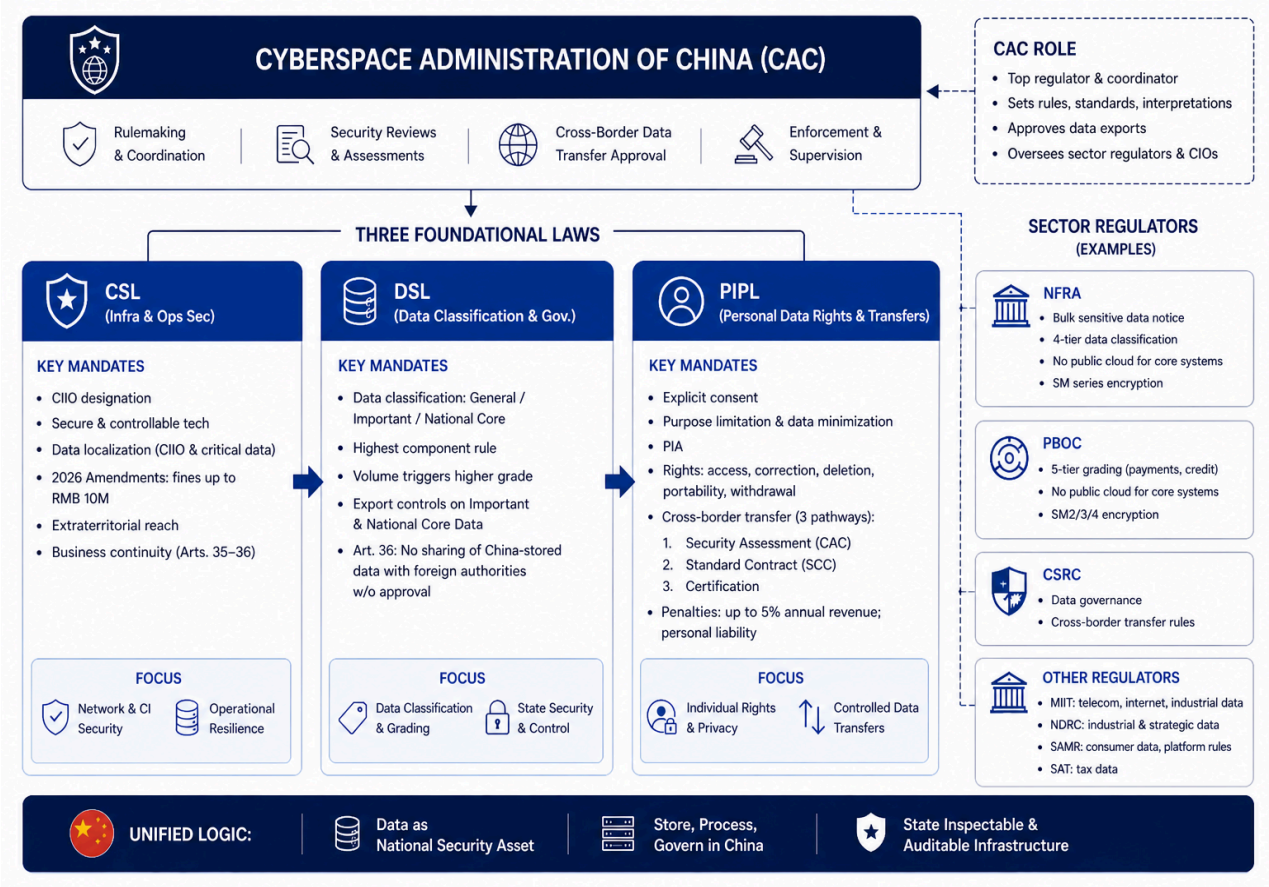


Figure 9. China's Three-Law Data Regulatory Landscape

3.3.2 Drivers for China's Model

China's regulatory architecture is the product of two reinforcing drivers: the Sino-American strategic relationship and a dual-track domestic approach that pursues frontier innovation while tightening state control over the indigenous technology stack.

US–China Strategic Competition

The US and China pursue divergent technological strategies reflecting their distinct governance systems and policy aims. The United States prioritizes technological leadership as a strategic asset, directing roughly $52 billion through the CHIPS Act into domestic semiconductor manufacturing and R&D, while imposing export controls on advanced AI chips and fabrication

equipment from October 2022.[51] China's 15th Five-Year Plan mandates domestic substitution: a 50% domestic-equipment rule for chip fabrication, a ban on foreign AI accelerators in state-funded data centers, and a 70% self-sufficiency target by 2030.[52] Once Beijing concluded that access to frontier US technology could be cut off at any time, the regulatory calculus shifted from *managing* foreign technology dependence to *eliminating* it. Restrictive regulation becomes the policy lever that forces this elimination on a defined timeline. This logic is also self-perpetuating: each new US export control gives Chinese regulators political cover to extend localization mandates further, and each new Chinese localization mandate gives US policymakers justification for additional controls.

This divergence creates a cascade of geopolitical effects. "Global swing states" are increasingly hedging between the two powers, mixing US, Chinese, and European technologies to avoid over-reliance on any single source, as J. Michael Daniel, President and CEO of the Cyber Threat Alliance, put it. However, this strategic hedging produces a fragmented landscape in which financial firms navigate varying degrees of local technology substitutability across strategic markets. The export control regime itself becomes self-reinforcing, providing China with political justification to demand full technological autonomy, driving regulatory tightening that is unlikely to ease, regardless of improvements in trade relations. The same expert described the dynamic as "missile gap logic" — the gap created by export controls puts domestic pressure on Beijing to pour state capital into indigenous chips and to strengthen procurement regulations.

The Dual-Track Approach

China's AI policy pursues two contradictory objectives: global technology leadership and stringent state-level visibility into the development and deployment of emerging technologies.

The 15th Five-Year Plan's "AI+" Action Plan commits state investment to domestic AI compute, such as GPUs, data centers, and a national "computing power network," while the Algorithm Filing System requires companies to register recommendation, generative, and deep-synthesis

[51]Bureau of Industry and Security, Department of Commerce, *Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputing and Semiconductor End Use; Entity List Modification*, 87 Fed. Reg. 62186 (October 13, 2022).
[52]CHIPS and Science Act of 2022, Pub. L. No. 117-167, 136 Stat. 1366 (2022).; Central Committee of the Communist Party of China, "The 15th Five-Year Plan for National Economic and Social Development and the Long-Range Objectives Through the Year 2035," *Beijing: Xinhua News Agency*, March 2026.

models alongside training data sourcing and intended use with the CAC before deployment.[53] The AI Safety Governance Framework 2.0 operationalizes this dual objective through pre-deployment security assessments, training-data provenance audits, mandatory watermarking of AI-generated content, and certified domestic infrastructure requirements.[54] Because Beijing refuses to trade off either objective, each new capability initiative triggers parallel expansion of registration, assessment, and certification requirements.

This produces a regulatory apparatus that grows more layered and sometimes internally inconsistent over time. Because Beijing refuses to trade off either capability or visibility, regulation becomes the only instrument that can deliver both — enabling innovation through subsidies and compute access while constraining it through filings and audits in the same motion. Each new capability initiative, therefore, triggers a parallel expansion of registration, assessment, and certification requirements, producing a regulatory apparatus that grows more layered and sometimes internally inconsistent over time, with no equilibrium point at which it stabilizes.

3.3.3 Implications for JPMC

The regulatory architecture and macro drivers described above translate into three cascading implications for JPMC, each operating across the firm's legal, policy, and technical functions, and narrowing the set of strategic choices still available.

1. China needs to be carved out from the firm's global operating model
2. Technical fragmentation compounds resilience risk
3. Structural regulatory conflicts and intellectual property exposure cannot be fully reconciled, only managed.

Compelled Departure from the "Lowest Common Denominator"

[53]Central Committee of the Communist Party of China, "The 15th Five-Year Plan for National Economic and Social Development and the Long-Range Objectives Through the Year 2035," *Beijing: Xinhua News Agency*, March 2026.;Liu Peilin, et al. "15th Five-Year Plan (2026-2030), AI+ Action Plan Provisions." *Caixin Global*. November 7, 2025 .;State Council of the People's Republic of China, *Opinions on Deepening the Implementation of the 'Artificial Intelligence +' Action* [关于深入实施"人工智能+"行动的意见] (Beijing: State Council, September 24, 2025).

[54]Cyberspace Administration of China (CAC), *AI Safety Governance Framework V2.0* [人工智能安全治理框架 V2.0] (Beijing: CAC, September 15, 2025).

Global financial institutions like JPMC typically pursue a "common denominator" approach to multi-jurisdictional operations by designing policies to meet the most stringent regulatory requirements, so that all operations comply by default. However, China's regulatory environment compels financial firms to design policy carve-outs due to indigenous technology mandates and data export restrictions.[55] In China, JPMC may need to operate subsidiary entities with distinct policy controls, technical stacks, vendor relationships, in-country data residency, and state-controlled infrastructure. Financial data generated in China must remain in China and be processed on infrastructure that the Chinese state can inspect and audit, making China a "data island."

However, the data island creates a second-order consequence. A China-resident data lake accumulates transaction, client, market, and risk data that is valuable for serving the onshore book but is legally fenced off from JPMC's global platforms. For the headquarters, this regulatory boundary produces a structural information lag. Group risk, treasury, and anti-money laundering (AML) functions lose real-time visibility into the China book and must instead rely on aggregated, lagged, or regulator-approved extracts. This erosion of the consolidated risk insight undermines the operating model that JPMC's global architecture is built to support.

These implications extend to Hong Kong via the Greater Bay Area Standard Contract and the National Security Law of Hong Kong, which prohibits Hong Kong recipients of PRC-origin data from transferring that data overseas without first satisfying the original export requirements, and expands the PRC's enforcement power over to Hong Kong.[56] This closes off Hong Kong as a usable transit point for global operations. Because rules can shift in interpretation without warning, JPMC should adopt a defensive posture: protecting intellectual property and minimizing exposure rather than testing regulatory boundaries.

Technical Fragmentation and Resilience Risk

---

[55]Arendse Huld, "Revisions to China's Cybersecurity Law: Strengthened Oversight and Alignment with Emerging Technologies," *China Briefing*, Dezan Shira & Associates, November 12, 2025.
[56]Cyberspace Administration of China, Innovation, Technology and Industry Bureau, and Office of the Government Chief Information Officer, *Standard Contract for Cross-Boundary Flow of Personal Information Within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong)*, effective December 13, 2023.;Bryan Cave Leighton Paisner, "GBA Standard Contract to Promote Cross-Border Data Flow," *BCLP Insights*, January 15, 2024.; *The Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region*, June 30, 2020, Instrument A406.

The data island mandates local processing while the carve-out mandates local autonomy. Additionally, AI training data and deployed models are treated as regulated infrastructure. All of this forces JPMC's China stack to diverge permanently from its global footprint as every layer of the China stack evolves on its own trajectory. This creates escalating resilience risks. Every separate stack is an additional attack surface to defend, a distinct vendor governance requirement, and an architectural seam where incidents can propagate.

Critically, Chinese enforcement does not require a breach to attach liability and hefty fines. The 2026 CSL amendments eliminated the prior "warning and rectification" period, so immediate fines of up to RMB 10 million (approximately $1.4 million) can now be imposed for a single serious incident, with additional PIPL penalties of up to 5% of annual revenue and personal liability for responsible officers. Moreover, the MLPS 2.0 reinforces resilience through compliance obligations. A failed security assessment, an undocumented emergency drill, or an unreported architectural change triggers MPS sanctions and CIIO decertification. Preparedness gaps are independently actionable violations. Compliance with resilience documentation is a binding requirement, not best practice.[57]

To maintain business continuity and demonstrate operational resilience, policy teams design controls that hold the data island architecture in place while meeting the business continuity obligations that regulators now treat as binding compliance requirements. Technical teams implement, document, and continuously audit those controls at a defensible cost, despite the substantial capital expenditure required to build the China stack in the first place. Any technical failure requires notification and subsequent regulatory inspection, regardless of the underlying cause.[58]As an expert in cyber resilience and semiconductor policy observed, Chinese enforcement operates through "a national security lens, an economic protection lens, and a

[57]*Cybersecurity Law of the People's Republic of China* [中华人民共和国网络安全法], amended October 28, 2025, effective January 1, 2026.;Cyberspace Administration of China (CAC), *Administrative Measures for Reporting National Cybersecurity Incidents* [国家网络安全事件报告管理办法] (Beijing: CAC, September 11, 2025), effective November 1, 2025.;Arendse Huld, "China Cybersecurity Law Amendment in Effect January 1, 2026," *China Briefing*, Dezan Shira & Associates, November 12, 2025.;Mayer Brown, "CSL Amendments Analysis: Tiered Penalties and Extraterritorial Reach," Kennedy, Gabriela and Wong, Koanna K.C., "China Finalises Amendments to the Cybersecurity Law What Businesses Need to Know Before 1 January 2026. *Mayer Brown* December 15, 2025.";Klea Legal. "China Data Laws in 2026: What's Changed and What Your Business Needs to Do." February 10, 2026..

[58]Deloitte, *TMT Predictions 2026: The AI Gap Narrows but Persists* (Deloitte Touche Tohmatsu Limited, December 2025).; Bain & Company, *Technology Report 2025: Tech's Most Valuable and Globally Fragmented Tech* (Bain & Company, October 2025).

political control lens, all of which expand the definition of risk," citing HSBC as a case where inadequate resilience likely drove subsequent regulatory tightening as the issue was not a breach, but a failure to demonstrate preparedness.

Ownership liberalization has compounded tech fragmentation, undermining JPMC's operational resilience in PRC operations. For instance, JPMC's asset management, futures, and securities branches entered the PRC market as joint-ventures in 2004, 2007, and 2011 through the Sino-Foreign joint-venture structure mandates.[59] As equity caps were progressively lifted, the firm converted each to wholly-foreign-owned status. Futures achieved 100% foreign ownership in June 2020, securities in August 2021, and asset management in January 2023.[60] However, ownership liberalization has not translated into vendor liberalization, as JPMC bears the capital and headcount costs of these entities while constrained to a narrower set of domestically approved vendors.

JPMC's preferred global vendors have mitigated their PRC operations due to intellectual property disclosure requirements. This narrows the vendor pool to domestic hyperscalers, foreign clouds operated through licensed Chinese partners, carrier-neutral data centers, MPS-certified domestic financial vendors, and domestic server CPUs that use the SM encryption standard. JPMC controls none of these vendors. Most are procured only at a Chinese scale, creating isolated vendor relationships disconnected from global operations.

Therefore, to prepare for foreseeable resilience challenges, JPMC should budget for divergence as a structural feature of operating in China, not a transitional one.

Structural Regulatory Conflict

Significant elements of China's regulatory regime are in direct, deliberate conflict with US legal obligations, as JPMC also faces. DSL Article 36, interpreted as a response to the US CLOUD Act, prohibits any organization in China from sharing China-stored data with a foreign court,

[59] "About Us: Corporate Information," J.P. Morgan China, accessed May 4, 2026.
[60] JPMorgan Chase & Co., "J.P. Morgan Futures Becomes First Wholly Foreign-Owned Futures Company in China," press release, June 18, 2020.; JPMorgan Chase & Co., "J.P. Morgan Receives Approval from the China Securities Regulatory Commission for Registration of Full Ownership of J.P. Morgan Securities (China) Company Limited," press release, August 6, 2021.; J.P. Morgan Asset Management, "J.P. Morgan Asset Management Receives Regulatory Approval for 100% Ownership of China Joint Venture," *PR Newswire*, January 19, 2023.

regulator, or law enforcement agency without prior approval from Chinese authorities.[61] This is a legal deadlock in which full compliance with one law mandates non-compliance with the other.

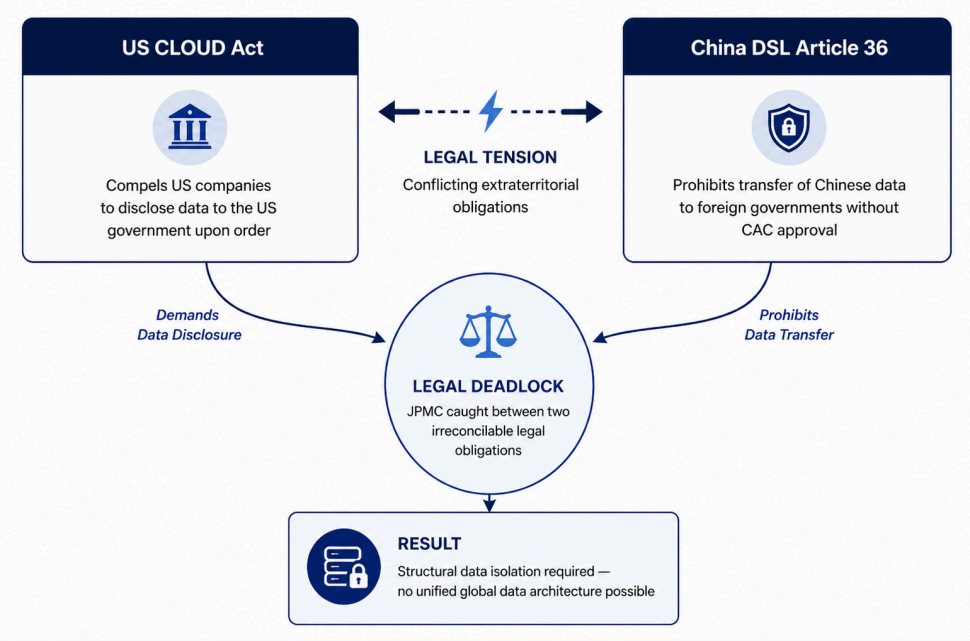


Figure 10: CLOUD Act vs. DSL Article 36 Legal Deadlock

A second structural difficulty compounds the first and further narrows the firm's options. In China, the line between commercial and state data is functionally absent, because the state does not separate industry from national security. This drives the most consequential strategic question facing foreign firms: whether the intellectual property exposure of operating in China can be mitigated enough to justify staying. For a global bank, intellectual property comprises a variety of revenue-generating assets. These include proprietary trading algorithms, derivatives pricing engines, AML machine-learning models, and other material non-public information. Once these assets are exposed through audit, vendor source-code escrow, party-member reporting channels, or the CAC's pre-deployment AI assessment, they become reverse-engineerable by domestic competitors.

A cyber resilience expert observed that the structural exposure then compounds to domestic clones within four to five years. This timeline illustrates the operational risk of maintaining intellectual property-intensive operations in a jurisdiction where regulatory disclosure

[61] Clarifying Lawful Overseas Use of Data (CLOUD) Act, 18 U.S.C. § 2713 (2018).;*Data Security Law of the People's Republic of China* [中华人民共和国数据安全法] (promulgated by the Standing Comm. Nat'l People's Cong., June 10, 2021, effective Sept. 1, 2021), art. 36.; Ross, Lester. "China Promulgates Data Security Law." *WhilmerHale.* June 15, 2021.

mechanisms serve as de facto vehicles for technology transfer. Professor Wolff emphasized this point and suggested that firms might exit markets with high compliance costs rather than operate at a competitive disadvantage.

These conflicts are difficult to resolve because, as a GW professor observed, sovereignty mandates in their current form do not reflect how data and cyberspace function. The operational consequence is sustained pressure across all three JPMC functions. Legal teams continually assess how to avoid contradictions. Policy teams are compelled to carefully apply global banking policy while remaining aware of "local nuances in local regulations," as the GW professor framed it. Technical teams must understand how each regulatory provision actually manifests in the function of their capabilities. None of these tensions is new in itself. These tensions are not new, but the escalating stringency of PRC sovereignty measures narrows the operational discretion available to financial institutions.

4. Regional Sovereignty Risk Matrix

The following matrix synthesizes the regional analysis from Sections 3.1, 3.2, and 3.3, mapping key risk and compliance dimensions across the European Union, India, and the People's Republic of China. Each cell reflects the dominant regulatory logic, operational constraint, or JPMC action required within that jurisdiction.

Matrix Subcategories

The matrix evaluates JPMC's risk exposure across 7 subcategories, each representing a distinct dimension of sovereignty-driven operational or legal risk:

1. **Regulatory Conflict** — How each jurisdiction defines and enforces its foundational data, cloud, AI, and cyber sovereignty frameworks, creating conflict with others.
2. **Data Localization** — Requirements to store financial, personal, or sensitive data within national borders.
3. **Cloud Architecture** — Sovereign cloud requirements and restrictions on the use of foreign cloud infrastructure and hyperscalers.
4. **Third-Party Risk** — Restrictions on foreign vendors, exit strategy obligations, and domestic vendor preference mandates.
5. **AI Governance** — Classification, explainability, and oversight requirements for AI and algorithmic systems used in financial services.
6. **Business Continuity / Resilience** — Disaster recovery (DR) infrastructure requirements, Recovery Time Objectives (RTOs), and cross-border failover restrictions.
7. **Audit & Inspection Rights** — Government rights to audit, inspect, or demand real-time access to financial institutions' systems and data.

Subcategory	European Union	India	China	JPMC Risk Exposure
1. Regulatory Conflict	Rights-based sovereignty; GDPR, CRA, EUCS. Member-state variation (FR strict, DE technical).	Strategic interdependence: RBI, DPDP Act, SEBI. April 10, 2026, compliance deadline.	National security supremacy; CSL, DSL, PIPL, 15th Five-Year Plan. Party-state control.	Three incompatible sovereignty regimes require parallel compliance programs, costing hundreds of millions annually; no unified governance model. [CRITICAL]
2. Data Localization	Sector-specific mandates; financial data residency required for critical personal data.	Strict localization for financial & payments data; RBI mandates local storage.	Mandatory local storage for all important data; cross-border movement requires CAC approval.	Mandatory separate data stores in India and China significantly increase TCO. RBI barred Mastercard/AmEx for non-compliance; the same risk applies to JPMC. [HIGH]
3. Cloud Architecture	EUCS Tier 3 certification; local audit trails.	Sovereign Cell Architecture with a local governance board; local HSMs are mandatory.	Ring-fenced domestic stack; no global integration for classified systems; local data centers only.	Three incompatible sovereign cloud architectures are required simultaneously, creating cross-border latency and heavy capital expenditure; the existing multi-cloud strategy requires redesign. [HIGH]
4. Third-Party Risk	CRA vendor conformity requirements; mandatory exit strategies; annual vendor risk reviews.	RBI cloud outsourcing guidelines, vendor lock-in restrictions, and domestic vendor preference.	Domestic vendors mandated for critical infrastructure; use of foreign vendors restricted.	Hyperscaler reliance conflicts with China/India domestic vendor mandates; CRA enforces direct software liability and supply chain risks. [HIGH]
5. AI Governance	EU AI Act; high-risk classification for financial AI; explainability & human oversight mandatory.	SEBI algorithmic trading rules; AI model documentation required; no comprehensive AI law yet.	15th Five-Year Plan projects domestic AI; foreign AI models are subject to CAC security review.	China's domestic AI rules require separate pipelines and may require retraining proprietary models. [HIGH]
6. Business Continuity / Resilience	NIS2 Directive: information communication technology resilience & incident reporting[62]; 4-hour initial notification for significant incidents; annual penetration testing.	RBI Business Continuity Policy; 2-hour RTO for payment systems; local DR sites required.	MLPS 2.0 resilience requirements; DR within China mandatory; no cross-border failover.	Incompatible RTO targets and China's cross-border failover ban force standalone resilience investment per jurisdiction, multiplying DR costs. [HIGH]

[62] "The NIS2 Directive," *European Commission*, accessed May 4, 2026.

7. Audit & Inspection Rights	DPAs and national competent authorities; on-site audits possible; GDPR Art. 58 & NIS2 Art. 32 supervisory & audit powers over ICT systems.	RBI on-site inspections; data audit trails required; real-time reporting obligations.	CAC and MPS have broad inspection authority; a security assessment is mandatory before data export.	CAC/MPS unannounced inspection rights expose JPMC data to intelligence risk; a single incident triggers simultaneous EU/India/China investigations requiring three incompatible audit formats. [HIGH]

5. Recommendations

The regional analysis across sections and the cross-jurisdictional risk matrix reveal a pattern of escalating regulatory constraints that compounds operational friction across JPMC's legal, policy, and technical functions. Given regional constraints and their implications for JPMC's global operations, this assessment proposes recommendations organized around four thematic areas: third-party risk, regulatory conflicts, business continuity, and data localization. These recommendations address both jurisdictional-specific challenges and cross-cutting global risks.

Each recommendation acknowledges both the operational necessity of compliance with sovereignty mandates and the associated cost burden. The assessment, therefore, presents each recommendation with explicit trade-offs. The intent is not to eliminate the tension between global operations and local compliance, but to provide JPMC with actionable starting points to translate abstract sovereignty constraints into measurable, defensible capital-allocation choices.

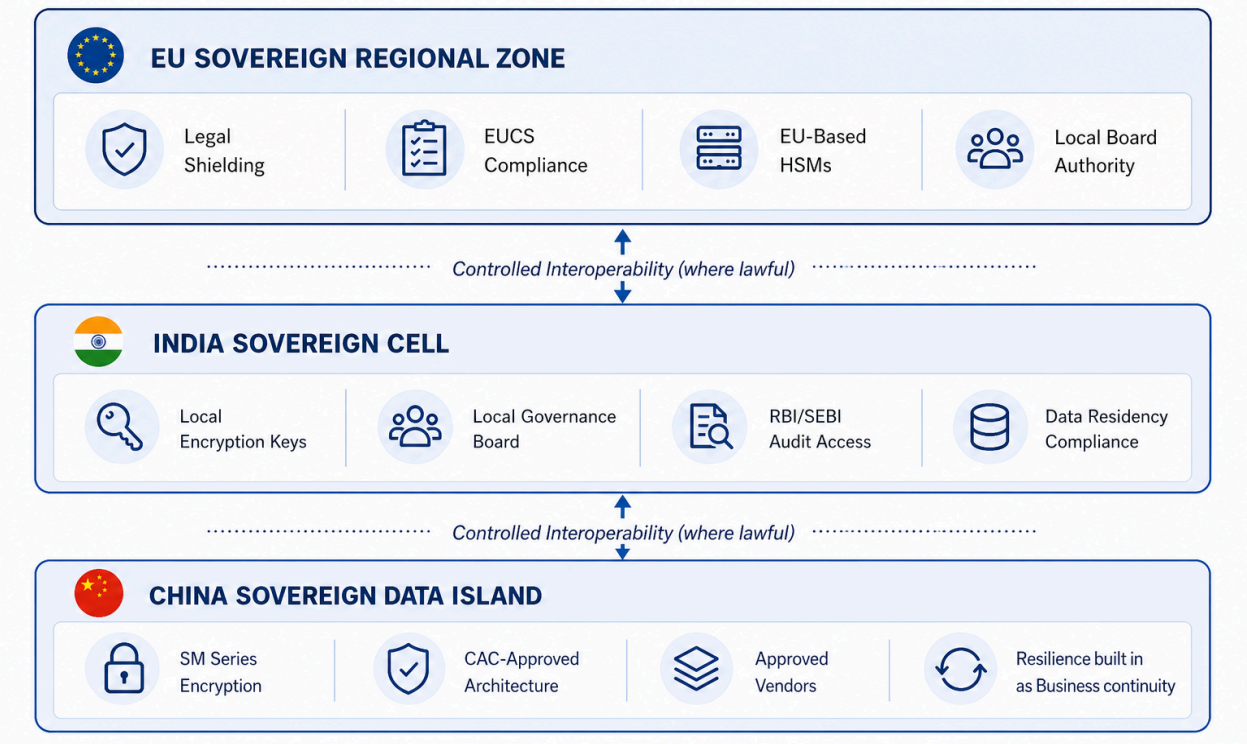


Figure 11: JPMC Modular Sovereignty Architecture

5.1 Third- Party Risk

1. **Implement "sovereign risk ratings" for EU market suppliers to mitigate systemic operational risks arising from supply chain disruptions.**

Pros	• Enhances resilience by evaluating third-party risk based on exposure to sanctions or regulatory divergence • Aligns with the EU Cloud Framework Sovereignty Assessment guide, ensuring the bank's risk posture remains proactive and credible with regional regulators
Cons	• Violates the principle of technology neutrality • Compliance-favored vendor ratings risk favors non-competitive European vendors over superior global alternatives. • Risk advisory doesn't adequately address exposure as effectively as controls (if JPMC uniformly views high-risk vendor compliance costs as too steep)

An advisory risk rating informs JPMC's third-party risk management strategies without forcing exclusions when vendor options are limited. The cons potentially favor European vendors, the pros calibrate these compliance gains accordingly without compelling vendor lock-in to non-competitive European vendors.

2. **Establish a technology-sovereignty risk taxonomy to identify opportunities to outsource regulatory burden to qualified third-party providers at a cost-effective price.**

Pros	• Enables outsourcing strategies that reduce capital expenditure and internal operational burden • Provides legal exposure frameworks for third-party vendors to guide decision-making • Informs decision-making on balancing telemetry capabilities with financial and legal risk mitigation

Cons	• Requires updates when sovereignty mandates change • Potential model bias risks vendor lock-in • Telemetry and direct control of audits are difficult to quantify

The taxonomy quantifies the relationship between regulatory risk exposure and operational cost, identifying functions where internal control and telemetry justify investment against those where trusted third-party management maintains risk parity. This taxonomy is applicable to jurisdiction-specific and global third-party risk management frameworks.

5.2 Regulatory Conflict

1. **Standardize Hong Kong-based operations to PRC compliance standards to mitigate legal risks under the National Security Law**

Pros	• Mitigates National Security Law enforcement risk • Reduces compliance complexity across dual regulatory requirements • Maintains Hong Kong as the regional operational HQ and capital hub, and signals compliance with PRC governance
Cons	• Creates a compliance precedent that encourages Beijing to raise regulatory demands progressively • Undermines Hong Kong's competitiveness for attracting regional talent and investment • Compliance policies are less effective than technical measures (data segmentation, access controls) in mitigating data sovereignty exposure

A compliance standardization function serves JPMC by incorporating the lowest common denominator across China-related operations. Although the cons are substantial and could put JPMC's Asia Pacific HQ operations in a prisoner's dilemma with its competitors, the pros shield JPMC from high-leverage legal liabilities.

2. **Improve coordination among global and regional controls and compliance teams to support preparedness and response protocols for conflicting-sovereignty scenarios.**

Pros	• Supporting measures (TTX) reveal underlying risks between conflicting mandates • Reduces legal exposure and response latency to law-enforcement demands • Creates audit trails for regulators • Reduces ad-hoc legal review costs on each request
Cons	• Conflicting mandates may be impossible to reconcile • Requires legal and compliance investment • Risks of being perceived as a "cost center" • Requires executive buy-in to implement long-term

Synchronized coordination between global and regional controls and compliance teams helps inform how JPMC should operate amid sovereignty-related legal conflicts among diverging sovereignty regimes. This aligns with all three regulators' expectations while reducing uncertainty in incident response. Although some conflicts cannot be eliminated, preparedness measures reduce the risk of human error.

5.3 Business Continuity

1. **Build a separate China technology stack on domestic infrastructure using Chinese encryption standards and deploy separate AI models trained on Chinese data.**

Pros	• Reduces risk of infrastructure seizure or operational shutdowns • Mitigates Cyber Security and Infrastructure Security Agency sanctions risk on US-origin IT technologies (Executive Order 14177)[63]
Cons	• High capital expenditure • Operationally complex • Reduces resilience by increasing endpoint attack surface and associated vulnerabilities • Restricts vendor choice to Chinese-only solutions, increasing switching costs and internal tech fragmentation • Difficult to revert without regulatory and reputational damage

[63] Office of the Press Secretary, "Statement on the Executive Order Strengthening the Cybersecurity of the United States Financial Sector," *Daily Compilation of Presidential Documents*, 2025, DCPD-202500168, March 12, 2025.

An investment in jurisdiction-specific technology infrastructure serves JPMC by converting data separation into a permanent operating model rather than a temporary compliance measure. Although the cons run counter to resilience standards and entail high capital expenditure, the financial benefits of maintaining access to the Chinese financial market are worth the expense.

2. **Identify regulatory risk thresholds for when regulatory compliance costs outweigh market access gains.**

Pros	• Provides early warning to re-prioritize global resources • Reduces the impact of the sunk-cost fallacy from locking capital into low-Return on Investment markets • Gives indicators on regulatory creep
Cons	• Compliance thresholds risk being undermined by growth targets • Risks perception of worst-case scenario planning, inflating risk estimates, and leading to resource over-allocation • Market access has assets that are difficult to quantify

A risk threshold serves JPMC by converting abstract sovereignty constraints into measurable capital-allocation choices. Although the cons reflect organizational tensions that bias teams associated with "profit generators" and against "cost centers." However, the pros empower controls and compliance teams to provide quantifiable evidence, shielding firms from the sunk-cost fallacy of locking capital into low-ROI markets. Furthermore, these risk thresholds are applicable for regulatory and geopolitical associated risks.

5.4 Data Localization

1. **Run two parallel intellectual property tracks: develop China-specific datasets, models, and algorithms for deployment on the China stack, and keep global proprietary intellectual property out of the China perimeter entirely.**

Pros	• Shields the global intellectual property from PRC disclosure mechanisms • Complies with CAC without sacrificing global competitive advantage

	• Resolves the DSL Article 36 / CLOUD Act deadlock at the intellectual property layer • Preserves China's market access
Cons	• The China subsidiary may be commercially weaker than domestic competitors and international competitors using global intellectual property • Requires significant compliance, technology, and investment costs for effective enforcement

Intellectual property separation controls shield JPMC's global portfolio from China's disclosure mechanisms. This satisfies CAC requirements while preserving market access and mitigating the risk of regulatory conflicts between the DSL Article 36/CLOUD Act conflict. However, Chinese subsidiaries may not be as competitive as domestic banks and global firms willing to use global intellectual property in the PRC market.

2. **Formally grant the Resident Director veto power over global "operational command center" changes to prevent jurisdictional breaches.**

Pros	• Creates credible, auditable governance • Strengthens regulator confidence in local oversight
Cons	• Operational bottleneck if exercised frequently • Potential CTO/CIO tension

A governance accountability function serves JPMC by converting statutory liability into enforceable authority. This aligns with SEBI CSCRF's personal director accountability while creating defensible escalation paths. Although centralized control is operationally cleaner, veto power is necessary to satisfy local governance requirements.

3. **Activate Sovereign AI Nodes: Leverage Pax Silica to deploy localized AI training clusters, ensuring models meet "Explainability" requirements.**

Pros	• Positions JPMC ahead of explainability mandates • Local training reduces cross-border exposure

Cons	• High capital expenditure • Pax Silica dependency • Explainability standards still in flux

A strategic infrastructure investment serves JPMC by building compliance-ready AI capabilities before regulatory requirements solidify. This aligns with India's sovereign technology trajectory while reducing data transfer risk. Although relying on global AI models reduces upfront costs, it exposes the organization to evolving explainability standards that may not align with local governance.

6. Conclusion

The technological enablers of globalization have become regulatory constraints. The examination of incompatible European Union, Indian, and Chinese sovereignty regimes challenges the applicability of the "lowest-common-denominator" compliance model due to legal conflicts between incohesive sovereignty regimes. Furthermore, sovereign cells built exclusively on indigenous technology are not viable. The capital expenditure required is substantial. Indigenous technical capacity in observed jurisdictions is suboptimal, limiting substitutability among vendors. Simultaneously, tech fragmentation reduces the cyber resilience that sovereignty regulations demand.

Across the EU, India, and PRC, three incompatible sovereignty regimes define the regulatory terrain that JPMC is compelled to comply with. The EU pursues rights-based sovereignty through legal and technical shielding, escalating compliance costs. India demands local control over contracts, encryption keys, and governance roles, converting data accountability into immediate board-level obligations. China requires ring-fenced local stacks, restricted data flows, domestic vendor lock-in, and state-filed AI models. Implementing these regimes surfaces tension between legal, policy, and technical teams that strive for a lowest-common-denominator approach, while struggling to satisfy legal conflicts among nationally influenced by sovereignty regimes that develop an incohesive set of tectonic plates. The result is not three versions of the same operating model, but three structurally incompatible ones JPMC sustains simultaneously.

Geopolitical tensions will intensify, not stabilize. Further technology restrictions, data localization mandates, and vendor exclusions are probable. JPMC's ability to remain operational across strategic markets depends on how its legal, compliance, and controls teams manage these paradoxes.

7. Bibliography

Amazon Web Services. “AWS Digital Sovereignty.” Accessed May 4, 2026. https://aws.amazon.com/compliance/digital-sovereignty/

AmCham China. “Analysis of China's Evolving Data Security Framework.” November 2025. https://www.amchamchina.org/insights/

Bain & Company. Technology Report 2025. https://www.bain.com/insights/topics/technology-report/

BDO India. Union Budget 2026-27: Technology Sector Highlights. BDO India, February 3, 2026.

Bryan Cave Leighton Paisner. “GBA Standard Contract to Promote Cross-Border Data Flow.” 2024. https://www.bclplaw.com/en-US/events-insights-news/gba-standard-contract-to-promote-cross-border-data-flow.html

CHIPS and Science Act of 2022, Public Law 117-167; 15th Five-Year Plan (2026-2030). https://www.congress.gov/bill/117th-congress/house-bill/4346

Clarifying Lawful Overseas Use of Data (CLOUD) Act, 18 U.S.C. Sec. 2523 (2018). https://www.congress.gov/bill/115th-congress/senate-bill/2383/text

Cyberspace Administration of China (CAC). AI Safety Governance Framework 2.0. 2023. https://www.cac.gov.cn/2025-09/15/c_1759653448369123.htm

Deloitte. “Navigating Technology Sovereignty.” TMT Predictions 2026. https://www.deloitte.com/lk/en/Industries/tmt/perspectives/tmt-predictions.html

Digital Personal Data Protection Act (DPDPA), No. 22 of 2023, Gazette of India, August 11, 2023. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

Dignan, Larry. “Zoho Just Delivered the Best SaaS Defense vs. AI.” Constellation Research. February 18, 2026. https://www.constellationr.com/insights/news/zoho-just-delivered-best-saas-defense-vs-ai.

ESDS Software Solution. “Sovereign Cloud & Data Residency for India: The Future of Trusted Digital Infrastructure.” *ESDS Knowledgebase*. November 24, 2025. https://www.esds.co.in/kb/sovereign-cloud-data-residency-for-india/.

European Commission. “CE Marking.” Official website, accessed April 4, 2026. https://single-market-economy.ec.europa.eu/single-market/ce-marking_en

European Commission. “Cloud and AI Development Act: Impact on Europe's Open Data Future.” data.europa.EU, October 23, 2024. https://data.europa.eu/en/news-events/news/cloud-and-ai-development-act-impact-europes-open-data-future

European Commission. “Commission Staff Working Document: Impact Assessment Report.” EUR-Lex, September 15, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022SC0263

European Commission. “Cyber Resilience Act.” 2024. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

European Commission. “United States.” EU Trade Relationships, accessed April 4, 2026. https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/united-states_en

European Union Agency for Cybersecurity (ENISA). “EUCS - Cloud Service Candidate Cybersecurity Certification Scheme.” ENISA, December 22 2020. https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

Foo, Yun Chee. “EU Drops Sovereignty Requirements for Cybersecurity Certification Scheme, Document Shows.” *Reuters*, April 3, 2024. https://www.reuters.com/technology/eu-drops-sovereignty-requirements-cybersecurity-certification-scheme-document-2024-04-03/

GB/T 43697-2024. “Data Security Technology - Rules for Data Classification and Grading.” TC260, effective October 1, 2024. https://www.tc260.org.cn/front/postDetail.html?id=20240905143846

Geffray, Maxime.“EUCS: A Future European Security Standard?” *Oodrive Blog*, https://www.oodrive.com/blog/security/eucs-european-security-standard/

Gillin, Paul. “A Close Look at JPMorgan's Aggressive Cloud Migration.” *SiliconANGLE*, July 27, 2024. https://siliconangle.com/2024/07/27/close-look-jpmorgans-aggressive-cloud-migration/.

Global Data Alliance. “GDA Leads Cross-Industry Call to Adopt Technical and Functional EU Cyber Certification Scheme (EUCS).” April 11, 2024. https://globaldataalliance.org/resource/cross-border-data-transfers-and-the-draft-eu-cloud-services-cybersecurity-certification-scheme-eucs

Government of India, Ministry of Finance. “Union Budget 2026-27: Incentives for Sovereign AI and Data Infrastructure.” Part B, Section 12, February 1, 2026. https://www.indiabudget.gov.in/

Hartmann,Théophane. “France Launches Bid to Cut Europe's Tech Dependence.” *Euractiv*, Accessed May 4, 2026. https://www.euractiv.com/section/tech/news/france-launches-bid-to-cut-europes-tech-dependence

Herbert Smith Freehills Kramer. "China's Revised Cybersecurity Law: Key Changes." November 2025. https://www.herbertsmithfreehills.com/notes/tmt/2025-posts/china-cybersecurity-law-revised

Huld, Arendse “China Clarifies Cross-Border Data Transfer Rules: Key Takeaways from Official Q&A (I).” *China Briefing,* Dezan Shira & Associates. April 18, 2025. https://www.china-briefing.com/news/china-clarifies-cross-border-data-transfer-rules-official-qa/

Huld, Arendse. “China Cybersecurity Law Amendment in Effect.” *China Briefing*. Dezan Shira & Associates. November 5, 2025. https://www.china-briefing.com/news/china-cybersecurity-law-amendment/

Huld, Arendse. "Revisions to China's Cybersecurity Law: Strengthened Oversight and Alignment with Emerging Technologies." *China Briefing,* Dezan Shira & Associates, November 5, 2025. https://www.china-briefing.com/news/chinas-data-security-framework-compliance-for-fies/

Intersoft Consulting. "Fines / Penalties." General Data Protection Regulation (GDPR), Accessed May 4, 2026. https://gdpr-info.eu/issues/fines-penalties/

Intersoft Consulting. "General Data Protection Regulation (GDPR)." Accessed May 4, 2026. https://gdpr-info.eu/

Jihong Chen. “Data Protection & Privacy 2025: China.” Chambers Practice Guides. *Chambers and Partners*. March 10, 2026. https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2026/china

Kennedy, Gabriela and Wong, Koanna K.C., “China Finalises Amendments to the Cybersecurity Law What Businesses Need to Know Before 1 January 2026. *Mayer Brown* December 15, 2025.”https://www.mayerbrown.com/en/insights/publications/2025/12/china-finalises-amendments-to-the-cybersecurity-law-what-businesses-need-to-know-before-1-january-2026

Klea Legal. “China Data Laws in 2026: What’s Changed and What Your Business Needs to Do.” February 10, 2026. https://klealegal.com/newsroom/china-data-laws-2026-key-changes

Liu Peilin, et al. “15th Five-Year Plan (2026-2030), AI+ Action Plan Provisions.” *Caixin Global*. November 7, 2025
https://www.caixinglobal.com/2025-11-15/china-unveils-ai-plus-strategy-for-15th-five-year-plan

Madiega, Maria. “Digital Sovereignty for Europe.” European Parliamentary Research Service, July 2020. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)651992

Ministry of Electronics and Information Technology. Digital Personal Data Protection (DPDP) Rules, 2024, Rule 5: Technical Specifications for Consent Managers.
https://www.meity.gov.in/data-protection-framework

Ministry of Electronics and Information Technology (MeitY). Technical Standards for Sovereign Encryption and Key Management, Advisory No. 4/2025. https://www.meity.gov.in/

National Financial Regulatory Administration. Measures for Data Security Management of Banking and Insurance Institutions [《银行保险机构数据安全管理办法》]. Issued December 27, 2024. https://www.nfra.gov.cn/

NVIDIA. “Yotta Built India's First Sovereign AI Infrastructure With Shakti Cloud.” NVIDIA Customer Stories. Accessed May 4, 2026.
https://www.nvidia.com/en-us/case-studies/yotta-built-india-sovereign-ai-infrastructure-shakti-cloud/

Ohri, Nikunj, and Sarita Chaganti Singh. “India Eases Curbs on Chinese Equipment Imports for Power, Coal as Projects Delayed, Sources Say.” *Reuters*, February 18, 2026.
https://www.reuters.com/sustainability/climate-energy/india-eases-curbs-chinese-equipment-imports-power-coal-projects-delayed-sources-2026-02-18/

Pappachan, Varghese. “How Cloud Computing is Becoming a Reality in India.” Digital First Magazine, September 23, 2020.
https://www.digitalfirstmagazine.com/how-cloud-computing-is-becoming-a-reality-in-india/

Pax Silica Declaration on Multilateral Semiconductor Integration. Joint Statement by the U.S. Department of Commerce and India's Ministry of Electronics and Information Technology, February 20, 2026. https://www.state.gov/pax-silica

People's Bank of China. Administrative Measures for Data Security in the Business Areas of the People's Bank of China [《中国人民银行业务领域数据安全管理办法》]. Issued May 1, 2025; effective June 30, 2025. http://www.pbc.gov.cn/tiaofasi/144941/144957/5702602/index.html

People's Bank of China. Financial Application Specification of Cloud Computing Technology — Technical Architecture [JR/T 0166-2020]. https://www.codeofchina.com/

Press Information Bureau. "Union Budget 2026-27: Tax Holiday Till 2047." Government of India, November 19, 2025. https://pib.gov.in/PressReleasePage.aspx?PRID=2084545

Propp, Kenneth. "European Cybersecurity Regulation Takes a Sovereign Turn." *Cross-Border Data Forum*, September 13, 2023. https://www.crossborderdataforum.org/european-cybersecurity-regulation-takes-a-sovereign-turn

Lundblad, Nicklas. "Digital Sovereignty: Can Europe Afford It?" *Center for European Policy Analysis (CEPA)*, October 29, 2025. https://cepa.org/article/digital-sovereignty-can-europe-afford-it

Reserve Bank of India (RBI). "Master Direction - Outsourcing of Information Technology Services." RBI/2023-24/102, updated April 2026. https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12664

Rooney, Paula. "JPMorgan Chase Builds Ambitious AI Foundation on AWS." CIO, December 4, 2024. https://www.cio.com/article/3616622/jpmorgan-chase-builds-ambitious-ai-foundation-on-aws.html

Ross, Lester. "China Promulgates Data Security Law." *WhilmerHale.* June 15, 2021. https://www.wilmerhale.com/en/insights/client-alerts/20210615-china-promulgates-data-security-law#

Securities and Exchange Board of India (SEBI). Cybersecurity and Cyber Resilience Framework (CSCRF), 2023 (Revised 2026). https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html

"Sovereign AI: Why Nations are Treating Compute as Critical Infrastructure." *RAISE Summit*, February 13, 2026. https://www.raisesummit.com/post/sovereign-ai-compute-critical-infrastructure

Standard Contract for Cross-Boundary Flow of Personal Information Within the Greater Bay Area, effective December 13, 2023. https://www.info.gov.hk/gia/general/202312/13/P2023121300134.htm

Stormacq, Sébastien."Opening the AWS European Sovereign Cloud." *AWS News Blog.* January 14, 2026. https://aws.amazon.com/cn/blogs/aws/opening-the-aws-european-sovereign-cloud/

State Cryptography Administration of China (OSCCA). SM-Series Commercial Cryptographic Algorithm Standards [GM/T 0002-2012, GM/T 0003-2012, GM/T 0004-2012]. Beijing: State Cryptography Administration. 2012.
https://www.codeofchina.com/standard/GMT0002-2012.html

"Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)." *DigiChina*, Stanford University, June 29, 2018.
https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017

"Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)." *DigiChina*, Stanford University, June 29, 2021.
https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china-effective-sept-1-2021

"Translation: Personal Information Protection Law of the People's Republic of China (Effective Nov. 1, 2021)." *DigiChina*, Stanford University, August 20, 2021.
https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021

U.S. Department of Commerce, Bureau of Industry and Security. Advanced Computing and Semiconductor Manufacturing Export Controls, October 7, 2022 (updated October 2023 and December 2024).
https://www.bis.gov/press-release/bis-updated-public-information-page-export-controls-imposed-advanced-computing-semiconductor

Utho. "Top 10 Cloud Service Providers in India for 2026." *Utho*. November 1, 2025.
https://utho.com/blog/top-cloud-service-providers-in-india/

"Why Trump's Tariffs Could Push Europe to Target US Tech Services." *Euronews*, February 10, 2025.
https://www.euronews.com/next/2025/02/10/why-trumps-tariffs-could-push-europe-to-target-us-tech-services

Zhang, Laney. "China: Amended Cybersecurity Law Takes Effect." *Library of Congress.* January 8, 2026.
https://www.loc.gov/item/global-legal-monitor/2026-01-08/china-amended-cybersecurity-law-takes-effect/

Deglobalization

EFFECTS ON ENTERPRISE TECHNOLOGY

THANK YOU

We extend our gratitude to all contributors and reviewers whose insights and expertise made this research possible.

THESIS

> *In a fragmented world, compliant global operations require architecting for divergence, not convergence*

JPMC

COLUMBIA | SIPA
School of International and Public Affairs

MAY 2026