



CHINA BRIEFING

From Dezan Shira & Associates

Issue 209 • October 2025 | www.china-briefing.com

Data Compliance in China: A Roadmap for Foreign Investors

Navigating Trends in China's Data Compliance Regime Pg 04

Building a Future-Proof Data Compliance Framework Pg 10

Six Data Compliance Hotspots for 2025 and Beyond Pg 15

Introduction



ADAM LIVERMORE

Partner
Dezan Shira & Associates

In today's digital economy, data has become a decisive resource – fueling innovation, enabling smarter decision-making, and shaping competitive advantage. As the value of data has grown, so too has the sophistication of China's regulatory approach. What began with the establishment of cornerstone laws has evolved into a comprehensive compliance regime marked by detailed implementation rules and increasingly consistent enforcement. For companies operating in China, data compliance is no longer a matter of choice but an imperative task.

For foreign-invested enterprises, the stakes are even higher. Data localization rules, cross-border transfer restrictions, and evolving definitions of "personal information" and "important data" create unique challenges for businesses that depend on global data flows. At the same time, China's regulatory logic differs in key respects from frameworks like the EU's GDPR, making direct transplantation of global compliance models ineffective.

Yet these challenges also present opportunities. A well-structured, future-proofing data compliance framework not only reduces regulatory risk but can enhance operational efficiency, build trust with regulators and partners, and even strengthen global credibility.

This issue of *China Briefing Magazine* takes both a strategic and practical perspective. We unpack the legal foundations, track recent legislative and enforcement trends, and provide actionable insights for building compliance systems that are locally attuned yet globally aligned.

Designed for business leaders, compliance officers, legal teams, and IT decision-makers, we hope this publication equips you with the clarity and tools to both manage compliance risks and transform them into drivers of

With kind regards,

Adam Livermore



DEZAN SHIRA & ASSOCIATES
www.dezshira.com



ASIA BRIEFING
www.asiabriefing.com



ASEAN BRIEFING
www.aseanbriefing.com



CHINA BRIEFING
www.china-briefing.com



INDIA BRIEFING
www.india-briefing.com



VIETNAM BRIEFING
www.vietnam-briefing.com



MIDDLE EAST BRIEFING
www.middleeastbriefing.com

Credits

Publisher - Asia Briefing
Media Ltd.

Editor - Qian Zhou

Contributors - Tony Tang
and Arendse Huld

Designer - Miguel Enrico
Anciano

Data Compliance in China: A Roadmap for Foreign Investors

Contents

Navigating Trends in China’s Data
Compliance Regime

Pg 04

Building a Future-Proof Data
Compliance Framework

Pg 10

Six Data Compliance Hotspots
for 2025 and Beyond

Pg 15

Annual Subscription

China Briefing Magazine is published four
times a year. To subscribe, please visit www.asiabriefing.com/store. And please explore
the clickable resources below.



Strategic Advisory and Commentary
info@dezshira.com



Professional Services
www.dezshira.com/services



Asiapedia
www.dezshira.com/library



Legal, Tax, Accounting News
www.china-briefing.com/news



Magazines, Guides, Reports
www.asiabriefing.com/store



Podcast and Webinar
[www.dezshira.com/library/
search?type=podcast&language](http://www.dezshira.com/library/search?type=podcast&language)



Reference

China Briefing and related
titles are produced by Asia Briefing
Ltd., a wholly owned subsidiary
of Dezan Shira Group. Content
is provided by Dezan Shira &
Associates.

No liability may be accepted
for any of the contents of this
publication. Readers are strongly
advised to seek professional
advice when actively looking to
implement suggestions made
within this publication.

For queries regarding the content
of this magazine, please contact:
editor@asiabriefing.com

All materials and contents
© 2025 Asia Briefing Ltd.

Asia Briefing Ltd. Unit 507, 5/F,
Chinachem Golden Plaza, 77
Mody Road, Tsim Sha Tsui East
Kowloon, Hong Kong.

Follow Us

Connect with us for the latest news,
events and insights across Asia.



Like *China Briefing*
on Facebook



Follow *China Briefing*
on Twitter



Connect with *Dezan Shira
& Associates* on LinkedIn



View *Dezan Shira &
Associates* on Youtube



Scan the QR code to follow
us on WeChat and gain
access to the latest investor
news and resources



Navigating Trends in China's Data Compliance Regime

Alongside China's digital transformation, the country's data compliance regulatory environment has matured rapidly, evolving from foundational legislation to strict and consistent enforcement. For foreign-invested enterprises operating in China, building a data governance framework that is compliant, efficient, and globally coordinated has been inseparable from business continuity and long-term competitiveness.



Qian Zhou
Manager
China Briefing
Author



Tony Tang
Manager, IT Service
Dezan Shira & Associates
Contributor

In a landmark move that sent ripples across the international business community, Chinese regulators publicly penalized French luxury brand Dior for unlawful cross-border data transfers – marking the first time a foreign company has been formally sanctioned under China's Personal Information Protection Law (PIPL).

The September 2025 announcement followed a data breach earlier this year and revealed Dior's failure to obtain regulatory approval, inform users, or implement adequate security safeguards before exporting personal information to its headquarters in France. While no financial penalty was disclosed, the case serves as a clear signal: China's data compliance regime is entering a new era of assertive enforcement.

This development underlines the urgency for foreign-invested enterprises (FIEs) to reassess their data governance strategies. As China continues to refine its regulatory framework – introducing mandatory compliance audits, expanding enforcement

mechanisms, and refining cross-border data transfer rules – companies must move beyond reactive compliance and build systems that are resilient, scalable, and aligned with both local and global standards.

In this chapter, we provide a structured overview of China's evolving data compliance landscape and examine the key legislative developments and enforcement trends.

Supporting regulations and guidelines are becoming more robust

China's data governance framework has evolved rapidly beyond its three foundational laws – the *Cybersecurity Law* (CSL), *Data Security Law* (DSL), and *Personal Information Protection Law* (PIPL) – with a growing body of supporting regulations, national standards, and official guidelines that clarify and operationalize compliance obligations for businesses.

For example, the cross-border data transfer (CBDT) mechanisms that are of high concern to FIEs have become more structured and diversified. The release of the *Measures for Security Assessment of Data Export, Standard Contract Measures for Personal Information Export, and Certification Guidelines for Personal Information Protection* have clarified the three main pathways for lawful outbound data transfers. These instruments are further complemented by ongoing Q&A, manuals, and guideline publications from the Cyberspace Administration of China (CAC), which provide practical guidance and case-based interpretations to help enterprises navigate the approval and filing processes.

Compliance audits are another area where abstract requirements are becoming concrete. While Article 54 of the PIPL established audit obligations, practical details only emerged recently. In February 2025, the CAC issued the *Measures for the Administration of Compliance Audits on Personal Information Protection*, effective May 1, along with guidelines specifying the scope of review. Then in May 2025, the National Information Security Standardization Technical Committee (TC260) released standardized audit procedures and guidance on selecting external auditors. Together, these measures transform compliance audits into structured, enforceable practices with clear expectations.

Sector-specific regulations are also emerging to address industry-specific risks. Regulatory authorities have issued tailored compliance requirements for sectors such as finance, healthcare, and automotive.

These rules often include stricter data localization mandates, enhanced security protocols, and reporting obligations for data breaches or transfers involving “important data.”

Despite the overall robustness, the pace and scope of rulemaking have varied across regions and industries, resulting in a fragmented landscape. Acknowledging these inconsistencies, regulators have begun efforts to harmonize the system. A key milestone is the *Regulations on Network Data Security Management*, issued in September 2024 and effective January 1, 2025. This regulation consolidates and aligns overlapping provisions of the CSL, DSL, and PIPL, providing clearer definitions, unified enforcement mechanisms, and a more integrated compliance structure, marking a shift toward greater consistency and predictability in China’s data governance regime.

Overall, China’s data compliance legal architecture is maturing into a more actionable and increasingly coherent system. While the regulatory environment remains dynamic, the direction is clear: China is building a multi-layered governance model that emphasizes accountability, transparency, and risk mitigation. For foreign enterprises, this means shifting from ad hoc compliance to strategic, system-wide governance that aligns with both local mandates and global standards.

Cross-border data governance shifts toward flexibility and lawful enablement

China’s regulatory approach to cross-border data flows is transitioning from blanket control toward a more refined and enterprise-aware model. This shift reflects a growing emphasis on proportional enforcement and practical accommodation of business needs, especially for FIEs.

In the early stages of implementation, some local regulators adopted overly rigid practices, such as blanket requirements for security assessments or broad interpretations of “important data,” which

created uncertainty and discouraged legitimate data transfers. These practices not only raised compliance costs but also became a friction point in China's business environment.

Since 2023, regulators, including the CAC and the Ministry of Commerce (MOFCOM), have actively engaged with foreign businesses through consultation meetings, seeking feedback on issues like data localization, outbound transfer procedures, and compliance burdens. These dialogues have informed a more pragmatic regulatory posture, with authorities now emphasizing that "secure and controllable" does not mean "prohibited". The policy goal is to mitigate risks, such as national security threats and personal data misuse, while enabling lawful and necessary data flows that support commercial operations, research collaboration, and internal management.

This shift is clearly reflected in the *Regulations to Promote and Standardize Cross-Border Data Flows* released in March 2024, which formalize a more balanced and transparent framework. Pilot Free Trade Zones have gone further by adopting negative list models, clarifying the types of data that can be freely exported within certain industries.

Several foreign enterprises have successfully completed security assessments or standard contract filings, providing reference cases that enhance industry confidence and demonstrate the feasibility of compliant data transfers under the evolving regime.

Enforcement authorities get more coordinated and specialized

Another trend in China's data compliance regime is that the country continues to strengthen

its collaborative enforcement model for data governance, characterized by a multi-agency framework that combines strategic oversight, sectoral expertise, and criminal enforcement. This system – led by the CAC, supported by industry regulators, and backed by the Ministry of Public Security (MPS) – is evolving toward greater precision and specialization:

- The CAC remains the central authority, overseeing personal information protection, cross-border data transfers, and the implementation of key compliance mechanisms such as security assessments, standard contracts, and certification.
- The Ministry of Industry and Information Technology (MIIT) plays a critical role in supervising data security within specific industries, particularly telecom, internet services, and industrial platforms.
- The MPS serves as the enforcement backbone for criminal violations, targeting illegal data transactions, personal information abuse, and black-market data operations. Its role is increasingly important in tracing data breaches and prosecuting offenders under criminal law.
- The newly established National Data Administration (NDA) is tasked with building the data market, overseeing data classification and grading, and regulating public data transactions. Its enforcement scope includes compliance in data trading and public data operations.
- Other agencies, such as the State Administration for Market Regulation (SAMR), focus on consumer protection and unfair data-driven practices, including exploitative algorithms, misleading app behavior, and misuse of user profiling. Meanwhile, the China Cybersecurity Review and Certification and Market Regulation Big Data Center (CCRC) is responsible for establishing a data compliance qualification system, covering both personnel and enterprise qualifications.

- Sector-specific regulators in finance, healthcare, and transportation are also stepping up enforcement around sensitive industry data, privacy protection, and cross-border transfers.

This coordinated enforcement system reflects a broader trend: China is moving toward granular, risk-based, and sector-sensitive data governance, with clearer responsibilities and more professionalized enforcement teams. For foreign enterprises, this means navigating a landscape where compliance expectations are increasingly tailored to industry context and operational risk, requiring not only legal awareness but also strategic coordination across internal functions.

Enforcement grows tougher and more case-driven

China’s data compliance enforcement is entering a more mature and assertive phase, where rules are no longer theoretical – they are being actively applied, tested, and refined through real-world cases and coordinated regulatory actions. Authorities are shifting from symbolic oversight to substantive enforcement, with a clear focus on high-risk scenarios and sector-specific vulnerabilities.

For example, for CBDT, regulators have started penalizing failures to submit, misrepresent, or fulfill contractual obligations, such as in the Dior case.

China’s Data Compliance Authorities		
Agency	Core responsibilities	2025 enforcement focus
CAC	Central regulator for data security and personal information protection; leads implementation of outbound data transfer mechanisms (security assessments, standard contracts, certifications)	- Cross-border data compliance (security assessments, standard contracts, certifications) - Personal information protection (compliance audits, user rights, sensitive data handling) - Identification of important data and inter-agency coordination
MIIT	Oversees data security in industrial, telecom, and internet sectors; focuses on secure data collection, transmission, and storage	- Industrial internet data, telecom user data, and app-based personal data collection - Data security systems, log retention, and technical safeguards in telecom and internet enterprises
MPS	Investigates and prosecutes data-related crimes, including illegal data trading and personal information abuse	- Criminal offenses involving personal data - Black-market data trading, breach tracing, and criminal enforcement - Whether the enterprise has obtained consent for processing personal information. (We see this as a sign that the MPS is beginning to actively check for compliance.)
NDA	Develops the data factor market; oversees data classification, grading, and data transaction compliance	- Implementation of data classification and grading systems - Compliance in public data operations and data trading
SAMR	Protects consumer rights and addresses unfair data-driven practices	- App user rights (e.g., auto-renewals, algorithmic discrimination, profiling abuse) - Unfair competition and consumer fraud in enterprise data use

China's Data Compliance Authorities

Agency	Core responsibilities	2025 enforcement focus
CCRC	Introduces qualification programs for both entities and individuals	- Qualification frameworks to ensure data compliance - Certifications for cybersecurity-related products, services, systems, and personnel
Sectoral regulators	Enforces data compliance within specific industries	- Identification and protection of industry-specific important data - Cross-border transfers, privacy protection, and incident response

Similarly, personal information protection is moving beyond formalistic privacy policies toward functional accountability. Joint inspections and audits, often triggered by user complaints, are targeting vague disclosures, ineffective consent mechanisms, and poor responsiveness to data subject requests. The protection of important and core data is also gaining traction, with enforcement now examining whether companies have established internal data catalogs, implemented encryption and access controls, and restricted outbound transfers.

Incident response is another area of heightened scrutiny. The newly released *Management Measures for National Cybersecurity Incident Reporting* have put forward strict requirements for the incident response time and response mechanism of enterprises. Companies are expected to report breaches promptly, notify affected individuals, and demonstrate effective containment and remediation. Delays or omissions in reporting are increasingly met with penalties, reflecting a regulatory emphasis on transparency and accountability. Finally, compliance audits and internal governance are evolving from checkbox exercises to performance-based evaluations. Regulators now assess not just the existence of policies, but their implementation quality, staff training, and executive responsibility.

The release of typical cases, such as the Guangzhou Internet Court's ruling against a multinational hotel group for unlawful data transfers and inadequate user rights handling in September 2024, illustrates how judicial enforcement is reinforcing administrative oversight and setting precedents for future compliance expectations.

Together, these trends show that enforcement under China's data compliance regime is becoming more detailed and responsive to real-world risks. As China advances its national data compliance system, enforcement will become more precise, more actionable, and better aligned with balancing compliance costs and regulatory requirements. For foreign enterprises, this means building systems that can withstand scrutiny, adapting to evolving standards, and earning regulatory trust.

Key takeaways: From passive compliance to proactive governance

For many FIEs, data compliance in China has long been viewed as a defensive exercise – meeting minimum requirements to avoid penalties. However, the maturing enforcement environment and rising expectations from regulators, partners, and consumers mean that “passive compliance” is



RELATED READING

Cybersecurity Incident Reporting in China - New Rules in Effect November 1, 2025

September 25, 2025

Starting November 1, 2025, companies operating in China must comply with the *National Cybersecurity Incident Reporting Management Measures*, which establish standardized procedures for reporting cybersecurity incidents. These rules aim to strengthen early warning systems, improve incident response, and enhance national cybersecurity oversight.

The Measures apply to network operators, including businesses, public institutions, and service platforms. Incidents such as data breaches, ransomware attacks, and system failures that disrupt operations or affect public interests must be reported to local cybersecurity authorities within one hour of detection, followed by detailed updates as investigations progress.

The Measures introduce graded reporting requirements based on incident severity and require companies to implement internal protocols for incident classification, escalation, and resolution.

For foreign companies, the new rules highlight the importance of timely and accurate reporting. Non-compliance may result in significant fines and reputational risks. By setting unified standards, the Measures help businesses navigate previously fragmented requirements under China's broader cybersecurity and data protection framework.

[READ MORE](#)

no longer sufficient. The next frontier is “proactive governance,” where compliance is embedded into corporate strategy and becomes a driver of trust, efficiency, and competitive advantage.

This shift requires companies to go beyond paperwork and checklists. Leading practices include building cross-functional governance structures, integrating compliance into product design and customer experience, and leveraging compliance technology to enhance monitoring and reporting. It also involves fostering a compliance-aware culture across departments, ensuring that data governance is not siloed but embedded in daily operations. By proactively identifying risks, engaging with regulators, and aligning with global standards, companies can turn compliance from a cost center into a strategic asset and part of their corporate culture.

Ultimately, treating data compliance as a strategic asset rather than a regulatory burden allows enterprises to differentiate themselves in the market. In a business environment where reputation, transparency, and security are paramount, firms that embrace proactive governance will be better positioned to win stakeholder trust, attract high-value partnerships, and achieve sustainable growth in China. 🇨🇳



CYBERSECURITY & COMPLIANCE ADVISORY

With support from our in-house legal, HR, finance, and IT specialists, Dezan Shira & Associates helps clients strengthen defenses, prepare for audits, and build privacy programs that transform data compliance from a risk into a competitive advantage. Get in touch with our local experts to schedule a consultation: china@dezshira.com.

[EXPLORE MORE](#)



Building a Future-Proof Data Compliance Framework

Building a future-proof data compliance framework requires more than awareness – it demands strategic governance, adaptive methods, and a culture that evolves with China’s shifting regulations and global standards.



Qian Zhou
Manager
China Briefing
Author



Tony Tang
Manager, IT Service
Dezan Shira & Associates
Contributor

An effective data compliance framework is the foundation for sustainable and secure operations in China’s increasingly regulated digital environment. This chapter outlines a practical pathway for FIEs to establish a future-ready governance model – one that addresses common compliance challenges and integrates regulatory obligations with operational agility and long-term resilience.

Common data compliance challenges faced by FIEs

Beyond the regulatory complexity and enforcement trends discussed in Chapter 1, foreign companies operating in China face a distinct set of challenges rooted in operational fragmentation, technological misalignment, and legislative divergence.

These issues rarely occur in isolation; they often intersect and amplify one another, creating systemic risks that hinder sustainable compliance.

Divergence between global and Chinese regulatory logics

In today’s globalized digital economy, many FIEs in China face the complex reality of “multi-jurisdictional compliance,” where global standards like the European Union’s *General Data Protection Regulation* (GDPR) must coexist with China’s distinct regulatory framework.

While GDPR is often regarded as the global “gold standard” for data protection – emphasizing individual rights, transparency, and harmonized enforcement – China’s data governance system, built on the PIPL, CSL, and DSL, reflects a different legislative philosophy. It prioritizes data sovereignty, national security, and development interests, resulting in a fragmented yet deeply protective compliance landscape.

Moreover, China’s regulatory logic is more sector-specific and layered. Sensitive data categories, such as minors’ information, biometric data, and core

national data, are subject to heightened scrutiny. Industry-specific rules in finance, healthcare, and automotive further complicate compliance.

These differences are not merely academic; they create practical friction for FIEs. Compliance strategies designed for GDPR cannot be directly transplanted into China. For example, a data transfer activity that complies with the GDPR may still violate China's filing and declaration requirements if it exceeds the personal information volume threshold.

Similarly, centralized data storage outside China may trigger localization obligations and security assessments under the PIPL.

For FIEs, these divergences mean that global compliance frameworks must be localized – not just translated but re-engineered to align with Chinese legal expectations. Failure to do so can result in enforcement actions, reputational damage, and operational disruptions.

Internal compliance capacity gaps

Another persistent challenge for FIEs in China is the absence of a centralized and locally responsive compliance function. Instead of a unified structure, responsibilities are often scattered across legal, IT, HR, and operational teams, lacking integrated oversight and strategic coordination. This siloed approach results in:

- Inconsistent execution of compliance policies across departments.
- Lagging responses to regulatory developments and enforcement actions.
- Weak documentation practices and limited audit preparedness, increasing exposure during inspections.

Without a coherent governance framework, compliance efforts tend to be reactive and fragmented, leaving organizations vulnerable to regulatory scrutiny and ill-equipped to adapt as legal requirements evolve.

Lack of continuous monitoring and operational mechanisms

As discussed, China's data compliance is not a one-time obligation but a dynamic, ongoing discipline, shaped by frequent legal updates, industry-specific mandates, and active regulatory enforcement. Yet many FIEs continue to rely on ad hoc responses, addressing issues only after they surface rather than embedding preventive mechanisms.

This deficiency often stems from the lack of essential operational infrastructure, including:

- Real-time monitoring capabilities to identify data risks and policy breaches as they occur.
- Structured incident response protocols that enable swift and coordinated action during investigations or breaches.
- Centralized compliance dashboards offering visibility into data flows, audit status, and emerging risk indicators.

In the absence of these tools, compliance remains disjointed and susceptible to disruption. More critically, the failure to implement proactive governance systems undermines credibility with regulators and erodes stakeholder trust, particularly in an environment where transparency, accountability, and readiness are under increasing scrutiny.

To build a resilient compliance posture, FIEs must integrate these operational capabilities into daily workflows, enabling predictive risk management,

automated reporting, and continuous refinement of their data governance practices.

Misalignment between technology systems and legal requirements

Due to cost constraints, global infrastructure dependencies, and limited local expertise, many FIEs continue to rely on legacy IT infrastructures that fall short of meeting China's evolving data compliance standards. Common deficiencies include:

- Insufficient encryption protocols and lack of pseudonymization measures to protect sensitive data.
- Fragmented or manual consent management processes, which fail to meet the PIPL's explicit consent requirements.
- Missing or incomplete audit trails, limiting traceability and accountability during inspections.

Closing this gap requires a strategic overhaul of digital systems, including modernization of core platforms, integration with locally compliant technologies, and alignment with regulatory mandates.

This transformation is not merely technical; it is foundational to enabling scalable, transparent, and legally sound data governance in China.

Pillars of a resilient data compliance framework

To effectively navigate China's complex regulatory environment, FIEs must establish a data compliance framework that is strategically structured, operationally scalable, and responsive to legal and technological change. A resilient framework rests on four interdependent pillars.

1. Governance and accountability

A robust compliance framework begins with clear governance. Key actions include:

- Establish a data governance committee comprising legal, IT, HR, risk, and business leaders.
- Appoint a data protection officer (DPO) as mandated by laws and regulations.
- Define reporting lines to both China leadership and global compliance teams.

This structure ensures accountability, facilitates cross-functional collaboration, and enables strategic oversight.

2. Policies and procedures

Establishing robust internal policies and procedures is essential for translating legal obligations into consistent, operational practice. Well-designed policies provide clarity, consistency, and enforceability, enabling teams to act decisively and compliantly in day-to-day operations. They also create a documented framework that supports audit readiness, internal accountability, and regulatory engagement.

Critically, policies must meet the compliance requirements of China, while remaining aligned with global governance standards. Moreover, they should be reviewed and refined regularly to stay responsive to legal updates, enforcement trends, and operational changes, ensuring that compliance remains a living, adaptive function.

3. Risk management and controls

Effective data compliance requires proactive risk identification and mitigation across the data lifecycle. Enterprises should implement internal controls,

such as access restrictions, encryption, incident response protocols, and regular risk assessments. These measures help reduce exposure to regulatory penalties, prevent data breaches, and ensure operational resilience.

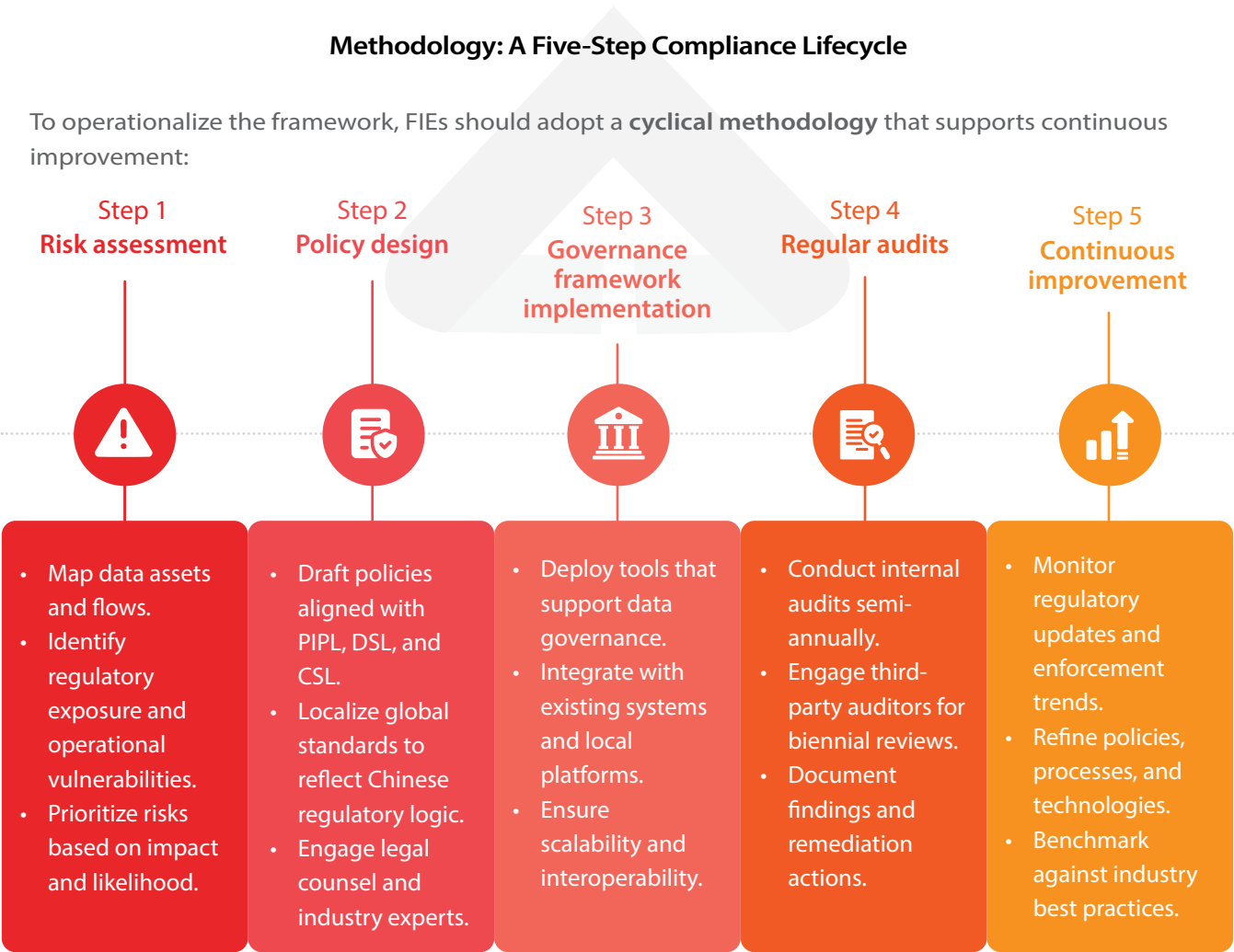
By embedding risk management into daily operations, companies can respond swiftly to emerging threats, maintain audit readiness, and demonstrate a strong compliance posture to regulators and stakeholders.

4. Culture and awareness

Last but not the least, for data compliance to be truly effective, it must be woven into the fabric of the

organization, not treated as a standalone function. This means fostering a culture where compliance is understood, valued, and practiced at every level. Key enablers include:

- Ongoing training to ensure employees are familiar with data protection principles and their responsibilities under Chinese law.
- Visible leadership support, with senior executives actively promoting compliance as a strategic priority.
- Ethical standards and internal values that encourage responsible data handling and transparency in decision-making.



This lifecycle ensures that compliance evolves with the business and regulatory landscape.

A strong compliance culture helps minimize human error, strengthens internal accountability, and builds lasting trust with regulators, partners, and customers.

Global perspective: Harmonizing HQ and local requirements

For FIEs who have to align global data governance frameworks with China's distinct regulatory environment, a dual-track strategy that respects both corporate standards and local legal mandates can help.

Regulatory mapping

The first step is regulatory mapping: conducting a comparative analysis of frameworks such as the EU's GDPR and China's PIPL to identify areas of alignment, divergence, and gaps that require localization. This analysis helps organizations understand where global policies can be applied directly and where adjustments are necessary to meet Chinese legal expectations.

Modular frameworks

To operationalize this alignment, companies should adopt modular compliance frameworks that allow for local customization without fragmenting global consistency. For instance, global templates for privacy notices can be adapted with localized language and consent mechanisms, while global data classification models can be adjusted to reflect China's sensitivity tiers.

Local expertise and engagement

Engaging local expertise is also critical. Partnering with Chinese legal advisors, consultants, and industry associations can help clarify regulatory

ambiguities, facilitate interactions with relevant authorities, and anticipate enforcement trends.

Dual reporting structures

Finally, establishing dual reporting structures, where compliance officers report both to local leadership and global governance teams, ensures that the organization remains responsive to local developments while maintaining alignment with overarching corporate standards.

This integrated approach enables multinational enterprises to navigate China's regulatory landscape with confidence, ensuring both legal compliance and operational coherence.

Key takeaway

Building a future-proof data compliance framework in China demands strategic governance, localized policies, and technology-driven adaptability. For FIEs, aligning global and Chinese standards, closing internal capacity gaps, and embedding a compliance culture are essential to ensuring resilience, regulatory trust, and sustainable operations in China's rapidly evolving digital and data landscape. 



VIRTUAL CIO & INTERIM IT OPERATIONAL MANAGEMENT

Dezan Shira & Associates' virtual CIO services help businesses drive digital transformation, strengthen internal processes, and ensure secure, compliant IT operations aligned with corporate objectives. Get in touch with our local experts to schedule a consultation: china@dezshira.com.

[EXPLORE MORE](#)



Six Data Compliance Hotspots for 2025 and Beyond

In China's fast-changing data compliance landscape, businesses must move beyond isolated and reactive fixes. They must take a focused, strategic approach, directing compliance efforts where regulatory attention is greatest.



Qian Zhou
Manager
China Briefing
Author



Tony Tang
Manager, IT Service
Dezan Shira & Associates
Contributor

Data compliance is no longer a back-office function – it is a strategic imperative shaping market access, investor confidence, and business continuity for FIEs in China.

This chapter highlights six key data compliance priorities for FIEs in 2025 and beyond.

Rather than covering every regulation, it offers a practical framework to identify critical areas, understand their impact, and respond effectively. Each topic includes a concise overview of regulatory context, operational requirements, common missteps, and actionable recommendations.

Through this chapter, we aim to help decision-makers build a clear roadmap for strategic prioritization, resource allocation, and resilient governance aligned with both Chinese regulatory expectations and global standards.

Data classification and grading: The foundation of compliance

Effective data governance begins with knowing what data you have, how sensitive it is, and how it should be managed. Under China's DSL, enterprises are required to classify data based on its level of importance, forming the basis for a hierarchical protection system.

This process involves two distinct but interconnected dimensions:

- Data classification – refers to categorizing data by its industry sector (such as finance, healthcare, energy) and business attributes (such as business function, data subject, processing stage).
- Data grading – involves assessing the sensitivity, regulatory implications, and potential impact of the data, typically resulting in categories such as general data, important data, and core data.

This foundational step reinforces nearly all subsequent compliance activities, including CDBT, access control, storage strategies, and security measures.

Without a clear understanding of data types and their associated risks, enterprises risk misapplying controls, overlooking regulatory obligations, and exposing themselves to enforcement actions.

A structured approach typically involves five steps: identification, planning, classification and grading, labeling, and control implementation.

Yet many companies still struggle with this process. Common issues include a lack of visibility in data assets, unclear definitions of data importance, insufficient staff awareness, and technical safeguards that fail to cover the full data lifecycle.

In some cases, the absence of important data identification has led to non-compliant transfers

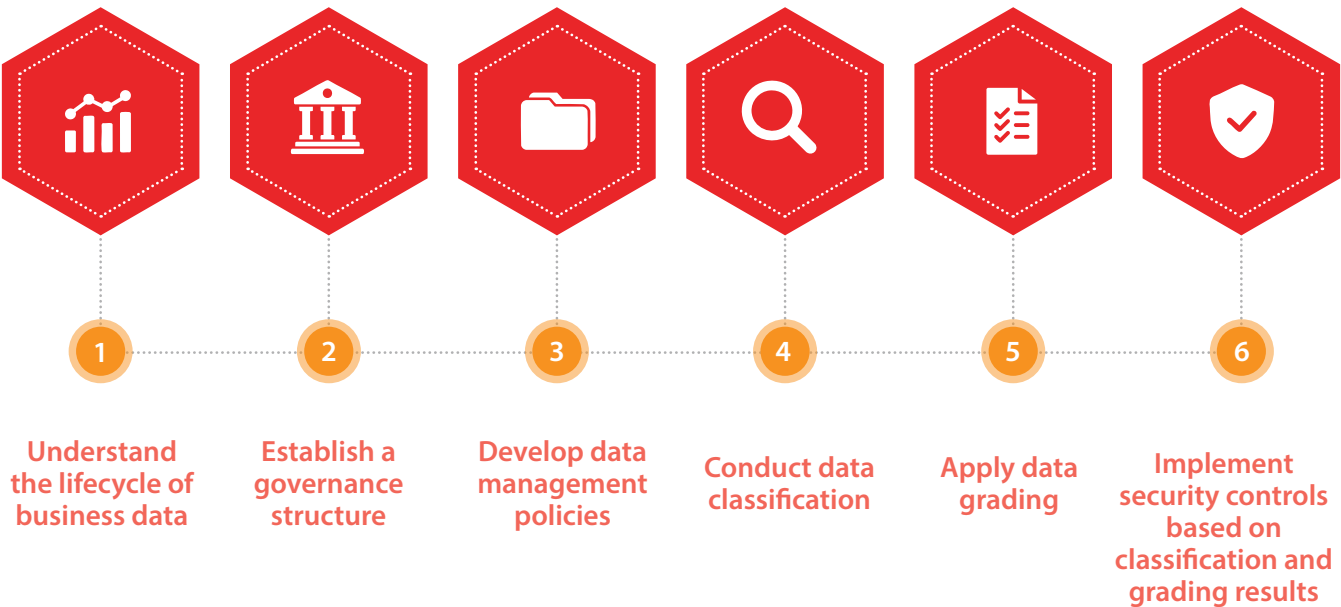
or usage, while classification outcomes are not consistently linked to actual control measures.

To address these gaps, enterprises should begin by building a comprehensive data asset inventory, mapping data types to business scenarios. Classification and grading standards should be aligned with China’s DSL, PIPL, and relevant technical specifications.

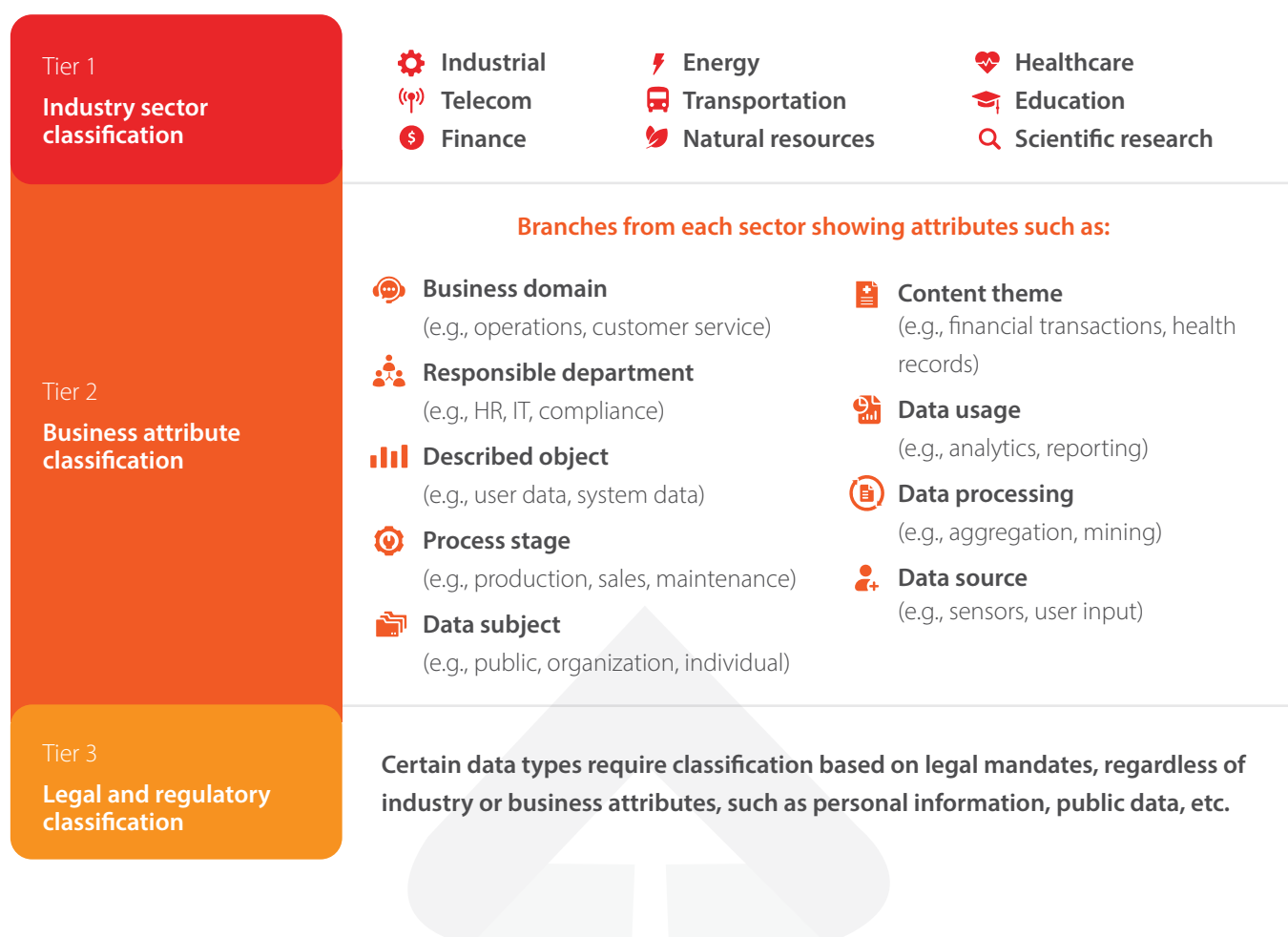
Crucially, classification and results must be operationalized, informing access permissions, storage protocols, and outbound data assessments.

By treating data classification and grading not as a one-time exercise but as a dynamic governance process, companies can lay a solid foundation for compliance, reduce regulatory risk, and enable more precise, scalable data management.

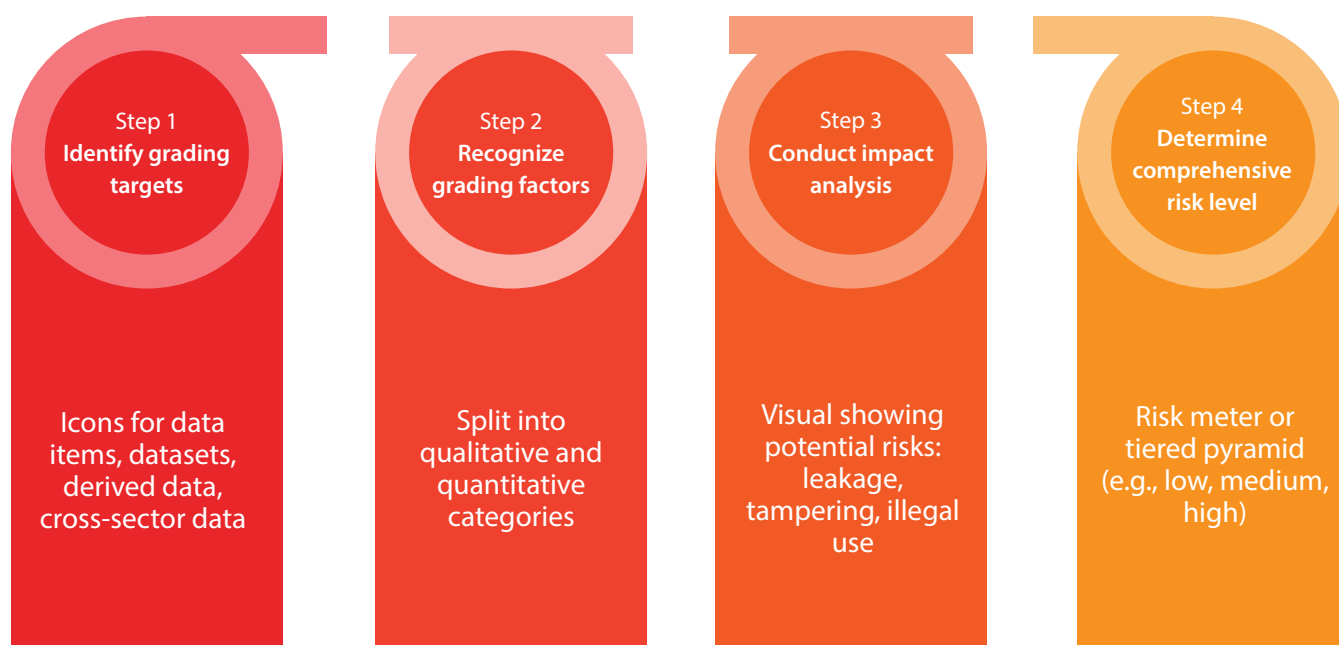
How Data Classification and Grading Works



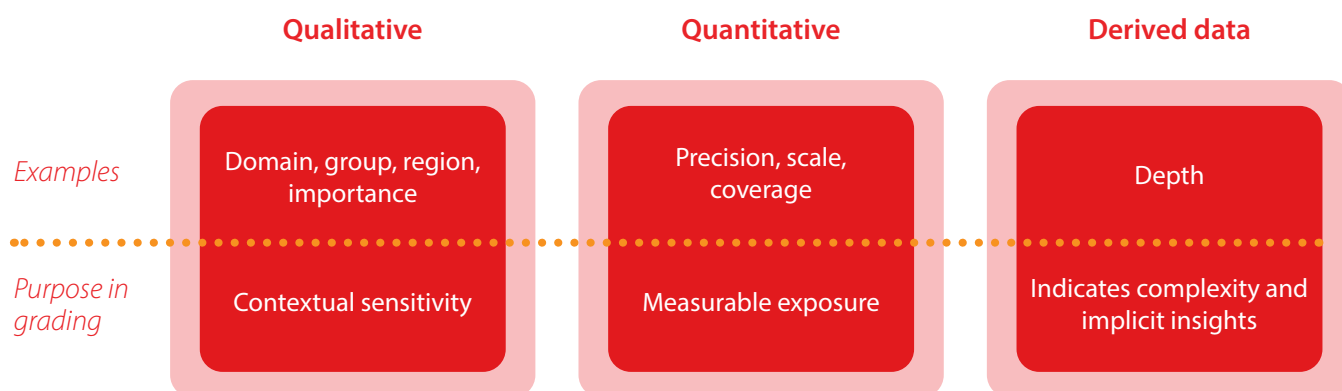
1. Three-tier data classification framework



2. The four-step grading process



3. Grading factors overview



Consent management: The cornerstone of personal information protection

Under China's PIPL, the lawful processing of personal information hinges on obtaining valid user consent. This consent must be informed, explicit, and specific, and in certain scenarios – such as the handling of sensitive personal information, third party sharing, or cross-border transfers – separate consent is required.

Consent management is a dynamic compliance obligation that must reflect the evolving nature of data use. This requirement applies across a wide range of operational contexts, including mobile apps, websites, offline forms, third-party data sharing, and employee data processing.

Yet many enterprises still fall short in execution. Common issues include pre-ticked boxes, bundled consent mechanisms, failure to distinguish between different data uses, and outdated authorization flows that do not reflect changes in business practices. Additionally, privacy policies are often vague or overly technical, and user requests to access, delete, or withdraw consent are not handled promptly or transparently.

To address these gaps, enterprises should implement layered, scenario-based consent mechanisms along with a consent review policy. Regular reviews should be conducted to ensure that personal information processing activities remain consistent with the original consent, especially when business

Consent Management Requirement Under the PIPL

Circumstance	Consent requirement
Processing general personal information	Yes, with limited exceptions permitted by law
Processing sensitive personal information	Yes, separate consent is required
Providing personal information to other processors	Yes, separate consent is required
Providing personal information to overseas parties	Yes, separate consent is required

changes affect how data is used. Privacy policies and authorization flows should also be reviewed periodically to ensure they stay accurate, transparent, and compliant. Crucially, companies must establish robust user rights response systems, including clear procedures for handling data access and deletion requests.

By treating consent not as a formality but as a living part of the user experience and compliance architecture, enterprises can build trust, reduce regulatory risk, and align with both legal obligations and user expectations.

PIPIA: A prerequisite for high-risk processing activities

Under China’s PIPL, conducting a personal information protection impact assessment (PIPIA) is a legal prerequisite for high-stakes personal information processing activities. These include processing sensitive personal information, using personal data for automated decision-making, entrusting or sharing personal data with third parties, publicly disclosing personal information, and transferring personal data overseas, and so on.

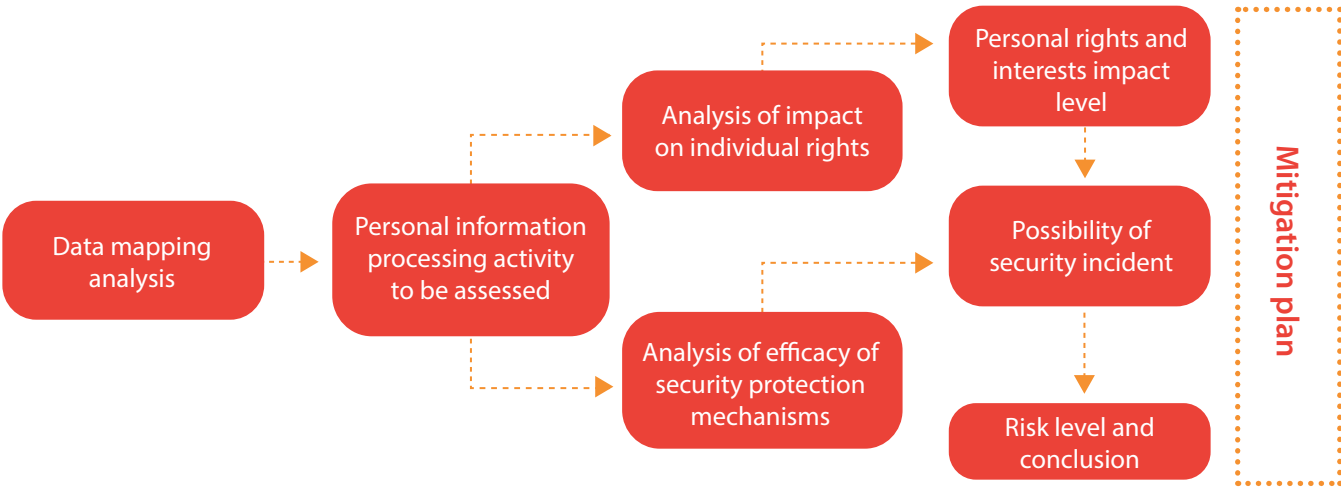
Nevertheless, the law also includes a catch-all clause – “other activities that may have a significant impact on individual rights” – which, while not clearly defined, signals a wide scope of applicability.

Given this ambiguity, a fully compliant approach recommends conducting a PIPIA for all personal information processing activities, regardless of perceived risk level. More than a compliance formality, PIPIA serves as a proactive risk management tool that enhances transparency, strengthens internal controls, and helps enterprises demonstrate accountability.

A robust PIPIA should include several core elements: a clear statement of processing purpose and legal basis, a comprehensive inventory of data activities, an assessment of potential risks (such as unauthorized access, misuse, or leakage), and corresponding mitigation measures. The goal is to ensure that all legal conditions for processing personal information are met before any data activity begins.

Despite its importance, many enterprises still struggle with implementation. Common issues include failing to compile a complete data activity inventory, relying

Personal Information Security Impact Assessment Workflow



Source: Guidance for personal information security impact assessment (GB/T 39335-2020)

solely on IT system reviews without business context, conducting superficial assessments that overlook real risks, and lacking documentation or follow-up mechanisms to support regulatory inquiries.

To address these challenges, companies should establish and maintain a detailed register of personal information processing activities, covering both internal and external data flows.

The assessment process should be standardized and cross-functional, engaging legal, technical, and business teams to ensure that evaluations are both comprehensive and actionable.

Importantly, PIPIA should not be treated as a one-time exercise but as a living process that evolves with changes in data use, business models, and regulatory expectations.

By embedding PIPIA into the organization’s data governance framework, enterprises can not only meet legal obligations but also build a culture of responsible data stewardship that supports long-term compliance resilience.

CBDT: A Critical threshold for multinational enterprises

For multinational companies operating in China, cross-border data transfers (CBDT) are often essential to daily operations – whether for internal reporting, global coordination, or cloud-based services. However, despite ongoing regulatory refinements and increased responsiveness to investor concerns (as discussed in Chapters 1 and 2), the transfer of data collected or generated within China to overseas entities (including headquarters, affiliates, or third-party service providers) remains subject to strict legal supervisions under the CSL, DSL, PIPL, and associated implementing regulations.

China’s regulatory framework outlines three main pathways for lawful data export: security assessment, standard contract filing, and certification. Choosing the correct path depends on the nature of the data, the volume involved, the sensitivity level, and the location. Non-compliance, such as failing to file, misclassifying data, or breaching contractual obligations, can result in regulatory interviews, mandatory rectification, and administrative penalties.

Personal Information Export Volume Thresholds for CBDT Compliance Procedures

Required procedure	Current regulation
No procedures required	Cumulative since January 1 of the current year: < 100,000 (normal PI)
PI protection certification or standard contract signing and filing	Cumulative since January 1 of the current year: ≥ 100,000 (normal PI) and < 1,000,000 (normal PI); or < 10,000 (sensitive PI)
Security assessment by CAC	Cumulative since January 1 of the current year: ≥ 1,000,000 (normal PI); or ≥ 10,000 (sensitive PI)

**PI = personal information; "< 100,000 (normal PI)" refers to processing non-sensitive personal information of fewer than 100,000 individuals.*
*** Critical information infrastructure operators (CIIOs) must still undergo a security assessment, regardless of the type or volume of data they export.*
**** There are several additional circumstances in which a company may be exempt from undergoing compliance procedures even if they exceed the thresholds.*

Despite growing clarity in the rules, many enterprises still face challenges in execution. Common issues include failing to identify all outbound data scenarios (especially indirect transfers via APIs or cloud platforms), uncertainty around filing standards, and lack of preparedness in documentation and risk assessment. These gaps not only increase compliance risk but also delay business operations.

To navigate this landscape, companies should begin with a comprehensive mapping of cross-border data flows, including hidden or embedded transfer mechanisms. They must then determine the appropriate compliance pathway, such as using the standard contract route for non-sensitive personal information, and prepare supporting materials, including data export lists, impact assessments, and legal agreements. Proactive engagement with regulators and internal coordination across legal, IT, and business teams is essential to ensure smooth execution.

PIP compliance audit: A mandatory legal obligation

A personal information protection compliance audit (PIP compliance audit or PIP audit) in China is a legally mandated process that evaluates whether an organization's personal information processing activities comply with the country's data protection laws, primarily the PIPL and related regulations.

As discussed in Chapter 1, the release of the Measures for the Administration of Compliance Audits on Personal Information Protection (effective May 1, 2025) and corresponding guidelines from TC260, such as the PIP Compliance Audit Requirements, has transformed the PIP compliance audits into enforceable obligations.

The audit requirement applies broadly but is especially critical for entities processing large volumes of personal information. Companies handling the personal information records of over 10 million people must conduct audits at least once every two years, while those processing between one and 10 million records are advised to audit every three to four years. Even smaller processors are encouraged to audit every five years, reflecting regulators' intent to embed compliance culture across all data handlers.

Beyond regulatory compliance, audits serve as a strategic tool for risk management. They help organizations identify gaps in data handling practices, assess exposure to legal and reputational risks, and implement corrective measures.

High-risk scenarios, such as employee data processing, customer profiling, app and website data collection, cross-border transfers, third-party sharing, automated decision-making, and biometric data use, require particular scrutiny.

Despite clear legal mandates, many enterprises struggle with execution.

Common pitfalls include treating audits as a box-ticking exercise, difficulties in collecting accurate evidence, failure to prioritize high-risk activities, neglecting documentation requirements, and poor coordination between legal, IT, and business teams.

To address these issues, companies should:

- Establish a regular audit schedule aligned with data processing scale and risk level.
- Focus on high-risk activities, ensuring that sensitive and complex data flows are thoroughly reviewed.
- Engage professional institutions when internal

capacity is insufficient, especially in cases involving regulatory scrutiny or large-scale processing.

- Document findings and remediation efforts, maintaining a clear audit trail to support regulatory inquiries.
- Report to authorities when required, demonstrating transparency and proactive compliance.

By embedding compliance audits into the organization's data governance framework, enterprises not only fulfill legal obligations but also build a resilient foundation for long-term data stewardship.

Frequency of the PIP Compliance Audit

Processor type	Audit frequency	Regulatory basis	Notes
Handles >10 million individuals' personal information	At least once every 2 years	<i>PIP Compliance Audit Management Measures, Article 4</i>	Mandatory
Handles >1 million but ≤10 million individuals' personal information	At least once every 3–4 years , based on risk, volume, and business scale	<i>PIP Compliance Audit Requirements, Section 4.2.4</i>	Recommended
Handles ≤1 million individuals' personal information	At least once every 5 years , based on risk, volume, and business scale	<i>PIP Compliance Audit Requirements, Section 4.2.4</i>	Recommended
Handles minors' personal information	Annually , conducted internally or by a professional institution	<i>Regulation on the Protection of Minors in Cyberspace, Article 37</i>	Mandatory

PIPIA vs. PIP Compliance Audit

PIPIA

Frequency:

Every 1 to 3 years

Method:

Risk assessment

Purpose:

To evaluate and control risks before conducting high-risk personal information processing activities.

PIP audit

Frequency:

Every 1 to 5 years

Method:

Evidence collection

Purpose:

To verify that technical and organizational measures are in place and compliant with legal requirements.

Shared features

- Both generate a gap analysis report requiring rectification before project completion.
- Final reports must be archived for future regulatory inspection.

In an era of increasing regulatory enforcement and scrutiny, robust audit practices are indispensable for maintaining trust and operational integrity.

Important data and localization: Sector-specific compliance obligations

China's data governance regime imposes heightened requirements on the handling of "important data" – a category distinct from personal information and defined by its potential impact on national security, economic stability, or public interest. Industries such as automotive, healthcare, finance, and telecommunications are particularly affected, with sector-specific rules mandating local storage and, in some cases, prohibiting cross-border transfers.

The stakes are high: unauthorized export or leakage of important data can trigger severe regulatory penalties and reputational damage. For example, automotive data involving geographic and traffic information must be stored locally and undergo security assessments before any outbound transmission. Similarly, financial institutions face strict controls over customer transaction data and risk models.

Despite the clear risks, many enterprises struggle with compliance. Common issues include:

- Overlooking industry-specific data localization rules, such as those issued by MIIT or local Free Trade Zones.
- Misclassifying important data as general business data, leading to inadvertent cross-border transfers or insecure processing.

To mitigate these risks, companies should:

- Closely monitor regulatory updates from both national and local authorities, including sectoral guidelines and pilot zone policies.

- Conduct internal data mapping exercises to identify whether any datasets fall under the "important data" category.
- Plan data infrastructure accordingly, including localized storage solutions and CBDT strategies that incorporate security assessments, government filings, operational safeguards, and legal documentation where required.

While not all companies are subject to these rules, those operating in regulated sectors or handling data with potential national relevance must treat localization as a strategic compliance priority. Proactive planning not only ensures legal conformity but also positions enterprises to navigate China's increasingly complex data environment with confidence.

Key takeaway

In China's rapidly evolving data compliance landscape, addressing isolated regulatory issues is no longer sufficient. Enterprises must adopt a structured, strategic approach – one that identifies areas of intensifying regulatory scrutiny and prioritizes compliance efforts where they matter most, starting with the key areas introduced in this chapter. 

DATA PRIVACY AND COMPLIANCE



Dezan Shira & Associates offers tailored data compliance services, including data asset mapping, privacy policy drafting, outbound data transfer strategy, and PIA evaluation support. Our experts help design consent flows, review compliance documents, and guide standard contract filings – ensuring your business meets China's evolving regulatory requirements with confidence and precision. Get in touch with our local experts to schedule a consultation: china@dezshira.com.

EXPLORE MORE



DEZAN SHIRA & ASSOCIATES

Your Partner for Growth in Asia

Are you making changes to your operations in Asia?

Get started by speaking to our professionals today

Accounting | Audit and Financial Review | Business Advisory | Business Intelligence
Corporate Establishment and Governance | Due Diligence | HR and Payroll | Mergers
and Acquisitions | Outbound Direct Investment | Risk Management | Tax | Technology

Our Offices in China

Hong Kong SAR

hongkong@dezshira.com

Guangzhou

guangzhou@dezshira.com

Qingdao

qingdao@dezshira.com

Tianjin

tianjin@dezshira.com

Beijing

beijing@dezshira.com

Haikou

hainan@dezshira.com

Shanghai

shanghai@dezshira.com

Dalian

dalian@dezshira.com

Hangzhou

hangzhou@dezshira.com

Shenzhen

shenzhen@dezshira.com

Ningbo

ningbo@dezshira.com

Suzhou

suzhou@dezshira.com

Zhongshan

zhongshan@dezshira.com

Our Offices in Asia

INDIA

Delhi

delhi@dezshira.com

Mumbai

mumbai@dezshira.com

Bengaluru

bengaluru@dezshira.com

VIETNAM

Ho Chi Minh City

hcmc@dezshira.com

Hanoi

hanoi@dezshira.com

Da Nang

danang@dezshira.com

INDONESIA

Jakarta

indonesia@dezshira.com

SINGAPORE

singapore@dezshira.com

MALAYSIA

malaysia@dezshira.com

THAILAND

thailand@dezshira.com

THE PHILIPPINES

philippines@dezshira.com

China · Hong Kong SAR · Australia · Bangladesh · Cambodia · Dubai UAE · Germany · India · Indonesia · Italy · Japan
Malaysia · Mongolia · Nepal · Singapore · South Korea · Sri Lanka · Thailand · The Philippines · United States · Vietnam

www.dezshira.com



Asiapedia™

