Deloitte.
Digital

Strategies for Data Compliance in China

October 2024

MAKING AN IMPACT THAT MATTERS since 1845

Contents

Executive Summary

Target Audience for this White Paper

This paper is appropriate for medium to large corporations with significant business in the Chinese mainland, or plans to expand business in the Chinese mainland.

Corporations and the Chinese Market

The Chinese mainland offers substantial business opportunities for multinational corporations. It is the second largest economy in the world by nominal GDP and first by purchasing power parity. China's GDP grew at 5.2% in 2023 [1] Business cases are often made on total addressable market or on market growth, and China is a leader in both.

However, there are also business risks associated with the Chinese market—among them, recent data laws and regulations. The Cybersecurity Law was passed in 2017, followed by the Data Security Law,[2] and the Personal Information Protection Law in 2021.[3] These laws significantly changed the nature of doing business in China. Regulatory trends continue to become more stringent and complex at an increasing speed, including semi-annual reviews by the Cyberspace Administration of China.

Multinational companies are challenged to comply with these regulations in a timely manner. Enterprise IT projects can be significantly longer than the semi-annual periods of regulatory updates. In that time, companies are expected to:

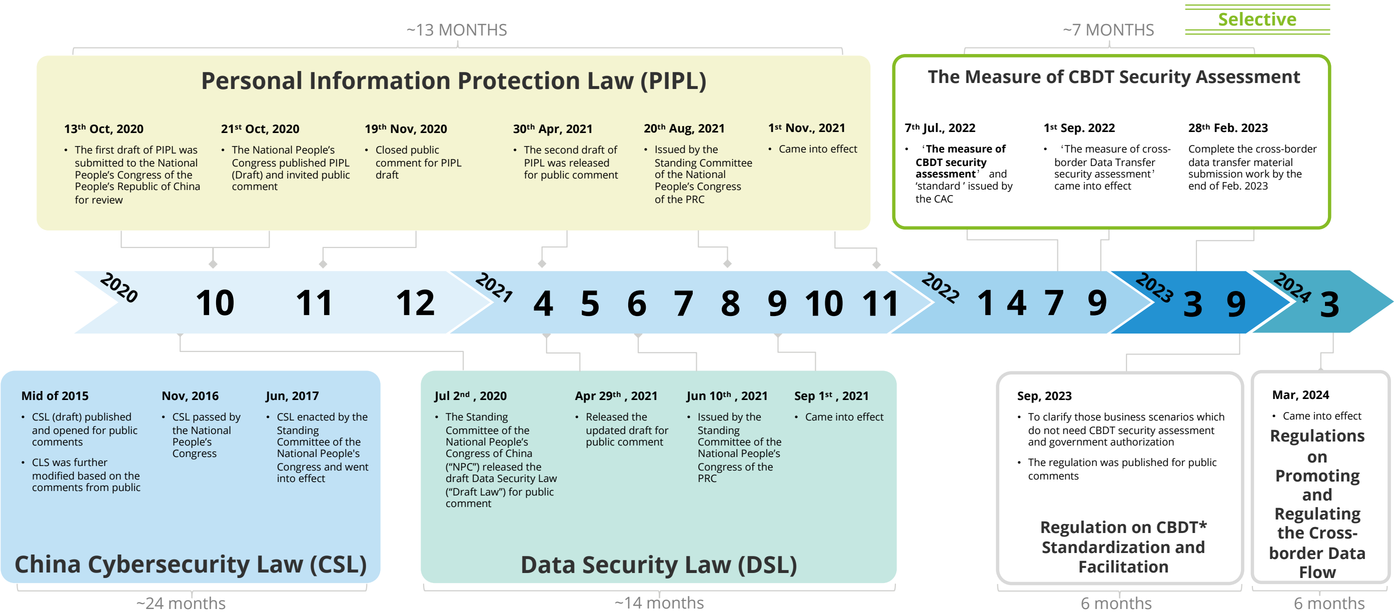
- Classify all data, even that which does not go to China, including the level of sensitivity of that data
- Undergo a security assessment by the Cybersecurity Authority of China (this depends on the scale of the operation)
- Build and obtain approval on many technical and resource items, including:
  - Finding a legal approach to comply with Chinese regulations
  - Communicating with local regulators
  - Procuring software
  - Staffing a local team to ensure local compliance regulations are met
  - Setting up new services and configure the relevant apps
  - Planning, testing, and executing a data and code migration
  - Onboarding users

This process often takes between one and two years. Furthermore, corporations need to choose strategies that are resilient to regulatory change, enable growth in the China market, and allow business alignment between their Chinese Mainland operations and the rest of the world. There are steps and strategies corporations can take now to conduct business in China while protecting customer data and addressing regulatory and legal concerns.

[1] World Economic Outlook database: April 2024
[2] Key Data Privacy and Cybersecurity Laws
[3] Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021

Overview of China's Data Regulations

There are multiple overlapping laws and regulations related to the care and processing of customer data in the Chinese mainland, including the Cybersecurity Law (CSL) in 2017, the Data Security Law (DSL) in 2021, the Personal Information Protection Law (PIPL) in 2021, and the Cryptography Law in 2020.[4] Similar laws and regulations are also present in Hong Kong and Macau.



Personal Information Protection Law (PIPL)

13th Oct, 2020

- The first draft of PIPL was submitted to the National People's Congress of the People's Republic of China for review

21st Oct, 2020

- The National People's Congress published PIPL (Draft) and invited public comment

19th Nov, 2020

- Closed public comment for PIPL draft

30th Apr, 2021

- The second draft of PIPL was released for public comment

20th Aug, 2021

- Issued by the Standing Committee of the National People's Congress of the PRC

1st Nov., 2021

- Came into effect

The Measure of CBDT Security Assessment

7th Jul., 2022

- '**The measure of CBDT security assessment**' and 'standard ' issued by the CAC

1st Sep. 2022

- 'The measure of cross-border Data Transfer security assessment' came into effect

28th Feb. 2023

Complete the cross-border data transfer material submission work by the end of Feb. 2023

China Cybersecurity Law (CSL)

Mid of 2015

- CSL (draft) published and opened for public comments
- CLS was further modified based on the comments from public

Nov, 2016

- CSL passed by the National People's Congress

Jun, 2017

- CSL enacted by the Standing Committee of the National People's Congress and went into effect

Data Security Law (DSL)

Jul 2nd , 2020

- The Standing Committee of the National People's Congress of China ("NPC") released the draft Data Security Law ("Draft Law") for public comment

Apr 29th , 2021

- Released the updated draft for public comment

Jun 10th , 2021

- Issued by the Standing Committee of the National People's Congress of the PRC

Sep 1st , 2021

- Came into effect

Regulation on CBDT* Standardization and Facilitation

Sep, 2023

- To clarify those business scenarios which do not need CBDT security assessment and government authorization
- The regulation was published for public comments

Regulations on Promoting and Regulating the Cross-border Data Flow

Mar, 2024

- Came into effect

Figure 1: Legal updates between 2020 and 2024. Deloitte Consulting (Shanghai) Company Limited, 2024.

[4] 网络安全和数据安全相关法律法规文件

The laws not only apply to corporations within the Chinese mainland, but also to entities outside the Chinese mainland that are offering goods or services to individuals inside the Chinese mainland or monitoring their behavior (such as marketing and marketing analytics).

There are a variety of measures in place to regulate cross-border data transfers (CBDT)[5] of personal data, the protection of minors online, management of infrastructure security, processing of personal or sensitive data, collection of personal data, collection of data using mobile devices, and more. Depending on the scale and classification of data transfer, the data transfer would need to be pre-approved by regulators.

The interpretation and implementation of all of these regulations are frequently examined and refined.

Deciphering the Regulation Hierarchy

China has an overlapping matrix of data regulations and many companies find it confusing to know which laws apply to them.

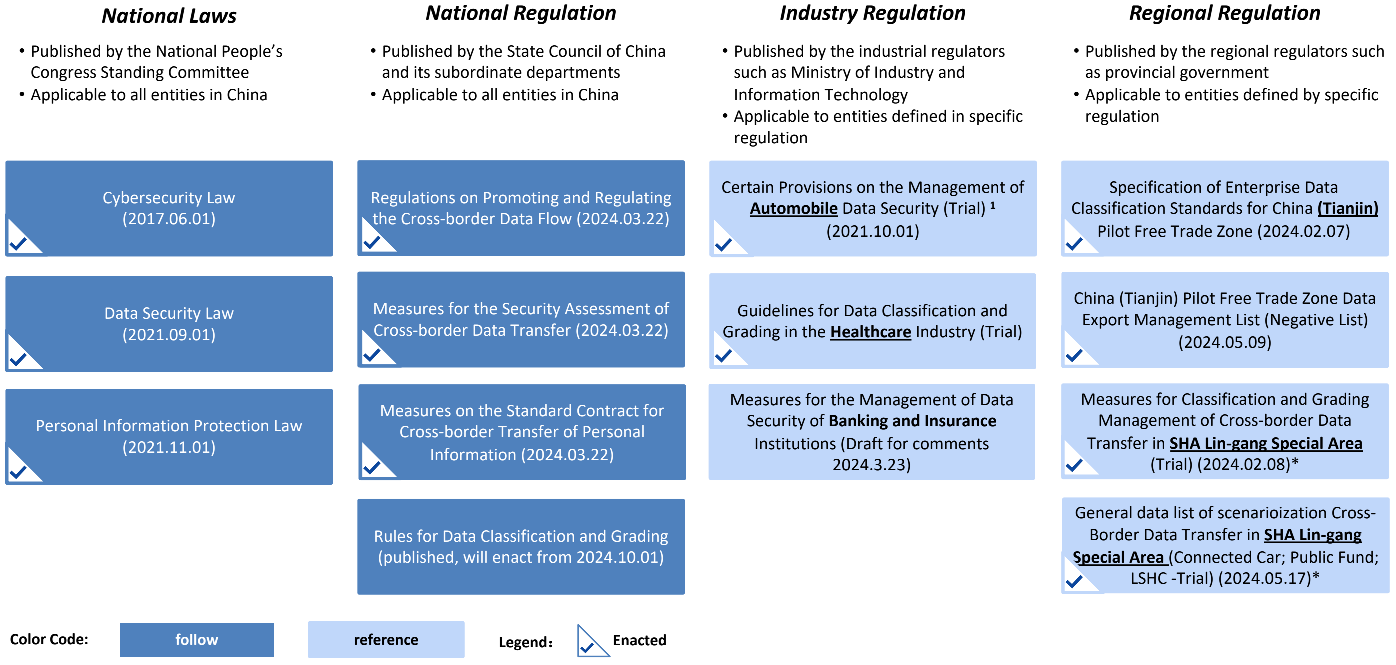
Currently, the the Chinese mainland data and cyber regulations can be broken down into four categories:

- National laws
- National regulations
- Industry regulations
- Regional regulations

The National People's Congress passes laws applicable nationally, and have precedence over other laws and regulations. Next, regulations drafted by state councils and departments will add more detail to the national laws, followed by industry regulations drafted by industrial regulators, followed by regulations from regional regulators.

For example, as an auto manufacturer in Shenzhen, not only is your corporation affected by the Cybersecurity law, but also by the national regulations that further define national laws, and also the regulations specific to your industry, and finally by the regulations in the regions where your corporation does business. All need to be considered in planning your data strategy.

Enacted & drafted the Chinese mainland data and cyber regulation



National Laws

- Published by the National People's Congress Standing Committee
- Applicable to all entities in China

Cybersecurity Law (2017.06.01) ✓

Data Security Law (2021.09.01) ✓

Personal Information Protection Law (2021.11.01) ✓

National Regulation

- Published by the State Council of China and its subordinate departments
- Applicable to all entities in China

Regulations on Promoting and Regulating the Cross-border Data Flow (2024.03.22) ✓

Measures for the Security Assessment of Cross-border Data Transfer (2024.03.22) ✓

Measures on the Standard Contract for Cross-border Transfer of Personal Information (2024.03.22) ✓

Rules for Data Classification and Grading (published, will enact from 2024.10.01)

Industry Regulation

- Published by the industrial regulators such as Ministry of Industry and Information Technology
- Applicable to entities defined in specific regulation

Certain Provisions on the Management of **Automobile** Data Security (Trial) ¹ (2021.10.01) ✓

Guidelines for Data Classification and Grading in the **Healthcare** Industry (Trial) ✓

Measures for the Management of Data Security of **Banking and Insurance** Institutions (Draft for comments 2024.3.23)

Regional Regulation

- Published by the regional regulators such as provincial government
- Applicable to entities defined by specific regulation

Specification of Enterprise Data Classification Standards for China **(Tianjin)** Pilot Free Trade Zone (2024.02.07) ✓

China (Tianjin) Pilot Free Trade Zone Data Export Management List (Negative List) (2024.05.09) ✓

Measures for Classification and Grading Management of Cross-border Data Transfer in **SHA Lin-gang Special Area** (Trial) (2024.02.08)* ✓

General data list of scenarioization Cross-Border Data Transfer in **SHA Lin-gang Special Area** (Connected Car; Public Fund; LSHC -Trial) (2024.05.17)* ✓

Figure 2: Enacted & drafted Chinese Mainland data and cyber regulation. Deloitte Consulting (Shanghai) Company Limited, 2024.

[5] Cross-border Data Policy Index

Planning Recommendations

Teams will need to carefully consider their time, dedication, resources, and budget if they plan to move forward. The consequences for mishandling data can be severe and costly. Laws and regulations surrounding data compliance in China overlap and are subject to revision and multiple interpretations. Keep track of restrictions as they may change while you're planning or executing your strategy.

Depending on internal circumstances and goals, companies should consider these recommended steps:

- **Scope the opportunity and the risk:** Understand strategies for risk and determine which one your business will use.
- **Identify the data and systems that need protection:** Classify data and systems for their level of sensitivity. Plan for data remediation and data transfers as well.
- **Formulate a localization strategy:** Fit the strategy to needs and scale, and align it with compliance trends

Managing Opportunity and Risk

Corporations typically enter markets after qualifying the addressable market size, creating business plans, and doing due diligence. The target audience of this document has already scoped and qualified the opportunities, and many of the costs and risks.

In this section, we will assume that the market opportunity is significant, and share methods to reduce risk. As mentioned previously, the risks include civil penalties such as fines, market exclusion, and criminal penalties.

Strategies for Risk

There are multiple strategies for corporations to address business risk when considering conducting business in China. Three of the key strategies organizations employ when managing restrictions to the Chinese market are avoidance, acceptance and mitigation.

Avoidance is when an enterprise leaves the China marketplace for their competitors. For the vast majority of multinational corporations, the market size and market opportunity of working in China is too large for this strategy to be practical.

Acceptance of residual risk after mitigation is a common strategy, but the full penalties can be harsh. Individuals held responsible can be personally fined significant amounts of money, in addition to fees billed to the organization.

Any income associated with the violations can be confiscated. Individuals held responsible can be sentenced to jail time of up to seven years and can be banned from doing business in China for a period of time. Tort liabilities also exist.

In July 2022, the Cybersecurity Authority of China ("CAC") fined one company $1.2 billion, which was nearly 5% of the company's total revenue. The global CEO was also personally fined, and the company was banned from adding new users while their mobile apps were removed from China mobile app stores for a period of time.

Mitigation primarily involves implementing a long-term strategy that enables compliance to the laws and regulations and is robust enough to handle the ongoing evolution of those regulations. Technology and operational processes play an important role in mitigating risk—including maintaining data residency, controlling access to regulated data, and obtaining consent. Mitigation is often the best strategy.

If your company chooses to mitigate the risk, the next step would be to identify and assess what data is impacted.

Identifying Data Affected by Privacy and Data Security Regulations

Understanding regulated data in China can be confusing because of the varying definitions. In laws like the PIPL, the Cybersecurity Law, the Data Security Law, previous legislation, and affiliated regulations, protected data is defined in several different ways. The PIPL covers "personal" data and "sensitive personal" data. The Cybersecurity Law and the Data Security Law both cover "important" data.

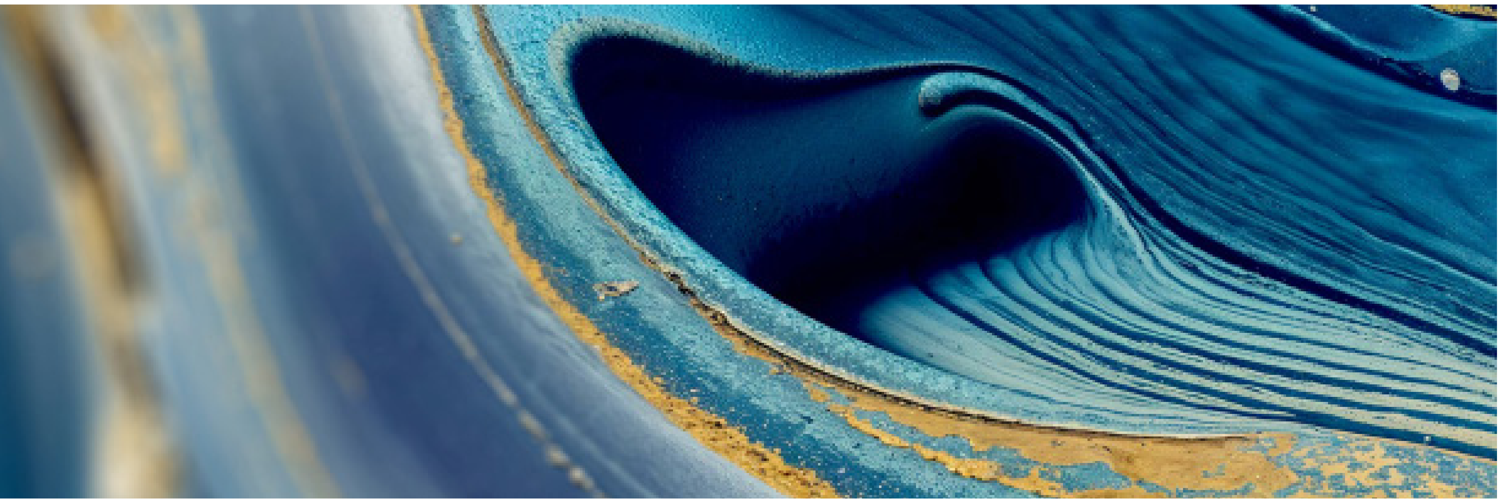
Furthermore, there is a Multi-Level Protection Scheme (MLPS 2.0) which defines five levels of impact—ranging from impact to organizations and individuals, at the least regulated level, up to national security impacts as the most regulated level.

So alternately, in some situations data may be categorized as personal, sensitive, or important; in others, it may be defined by MLPS levels and impact levels. When planning, both categorization schemes can be useful.

Business data can fall into many of these categories. Names, phone numbers, and other personally identifiable fields in one scheme would be considered "personal data", and may also fit into MLPS level 1. Personal Health Information (PHI) would be considered "sensitive" under the PIPL, and would require a higher level of protection. This higher level of protection can be seen in access control, the need for a stronger justification and consent for processing the data, and more restrictions on transferring the data across national boundaries.

Other examples of sensitive information include religious beliefs or affiliation, financial data, and location tracking. This data is often stored in business systems—for example, provider management, HR, account management, scheduling, and retail execution can all include various forms of sensitive information.

The guidance on the data classification can be concluded by different objects with impact levels, as defined by MLPS 2.0. and as well the latest GB/T 43697-2024[6].



[6] GB/T 43697-2024《数据安全技术 数据分类分级规则》发布

The MLPS classification levels are as follows:

- **Core Data:** Directly impacts national security, political security, people's livelihoods, and major public interests.
- **Important Data:** May affect national security, economic operation, social stability, health or safety. Data that affects a single organization or individual typically does not qualify for this category.
- **General Data:** Does not fall into the Core Data or Important Data categories.
- **Personal Data:** Personally identifiable information.
- **Sensitive Personal Data:** Personal information, which if leaked or destroyed, could impact an individual's health, safety, or property.

Core data is more sensitive (has a higher risk) than Important data, which is in turn more sensitive than general data. Data should be graded and evaluated by the potential impact based on the scale of the effect and the scale and precision of the data.

	Impact Level		
Categories	***Especially severe***	***Severe***	***Normal***
National Security	Core data	Core data	Important data
Economy	Core data	Important data	General data
Social Order	Core data	Important data	General data
Public Interest	Core data	Important data	General data
Org/Ind rights	General data	General data	General data

Figure 3: Data classification vs. impact level chart. Deloitte Consulting (Shanghai) Company Limited, 2024

Furthermore, depending on the industry or the region, additional restrictions can come into play. For example, Internet of Things (IoT) data is restricted from cross-border data transfer. In health care, treatment information is restricted. Additional examples include:

- **Automotive Manufacturing:** A luxury car manufacturer develops a personalized driver assistance system that learns from individual driving habits. The system collects and processes data on acceleration patterns, braking behavior, and route preferences. This information, while crucial for optimizing the driving experience, is highly sensitive as it could reveal personal routines and locations if compromised.
- **Life Sciences:** A pharmaceutical company conducts clinical trials for a new cancer treatment. They collect extensive patient data, including genetic markers, treatment responses, and quality of life indicators. This information is not only medically sensitive but also potentially revealing about individuals' long-term health prospects and could affect their insurability or employment if disclosed.
- **Luxury Retail:** A high-end jewelry brand offers a bespoke service where clients can design custom pieces. The company maintains a database of client preferences, purchase history, and personal events (e.g., anniversaries, birthdays). This information, while valuable for personalized marketing, is sensitive as it could reveal a client's financial status, personal relationships, and lifestyle choices if breached.

Corporations may choose to classify data using multiple parameters:

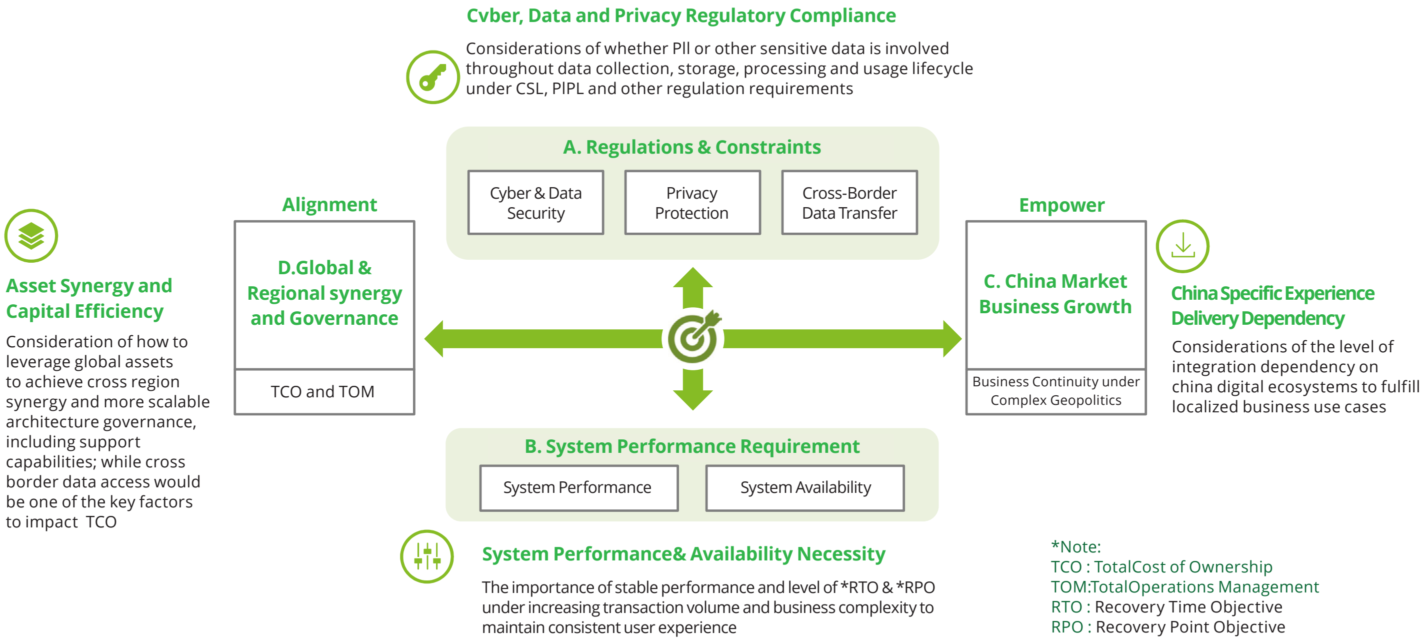
- Classify data by level of sensitivity. This can typically be done based on the data schema.
- Classify cross-border data transfers by level of sensitivity. Cross-border data transfers are treated more strictly than data processing; data may be acceptable to process in China but not to transfer outside of China.

Formulating a Localization Strategy

Once a company has assessed risk and classified data, it is time to build a digital strategy to ensure the handling of that data is compliant.

Corporations should carefully consider global and regional governance, local market business support, regulation constraints, and cost efficiency. Companies will need to consider multiple factors to find success, including:

- Cybersecurity issues such as whether sensitive data is involved
- System performance quality and maintaining a consistent user experience while transaction volume increases
- The level of integration dependency on China's digital ecosystems to fulfill localized use cases
- How to best manage and leverage global assets across borders



Cvber, Data and Privacy Regulatory Compliance

Considerations of whether PII or other sensitive data is involved throughout data collection, storage, processing and usage lifecycle under CSL, PIPL and other regulation requirements

A. Regulations & Constraints

Cyber & Data Security | Privacy Protection | Cross-Border Data Transfer

Alignment

D.Global & Regional synergy and Governance

TCO and TOM

Asset Synergy and Capital Efficiency

Consideration of how to leverage global assets to achieve cross region synergy and more scalable architecture governance, including support capabilities; while cross border data access would be one of the key factors to impact TCO

Empower

C. China Market Business Growth

Business Continuity under Complex Geopolitics

China Specific Experience Delivery Dependency

Considerations of the level of integration dependency on china digital ecosystems to fulfill localized business use cases

B. System Performance Requirement

System Performance | System Availability

System Performance& Availability Necessity

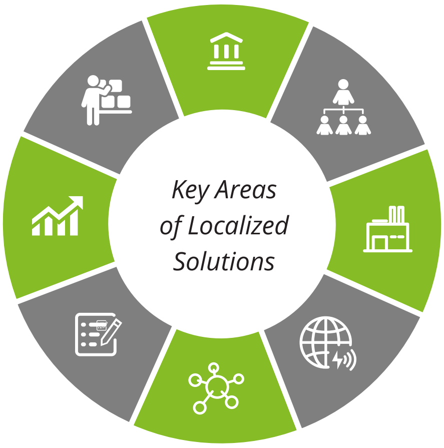
The importance of stable performance and level of *RTO & *RPO under increasing transaction volume and business complexity to maintain consistent user experience

*Note:
TCO : TotalCost of Ownership
TOM:TotalOperations Management
RTO : Recovery Time Objective
RPO : Recovery Point Objective

Figure 4: Localization considerations. Deloitte Consulting (Shanghai) Company Limited, 2024.

Given the potential breadth of a corporation's customer relationship management (CRM) system, the data within it should be stored locally to meet localization requirements, have proper security measures in place to control access and compliance with local laws and regulations, all while being useable to meet the business needs. The affected data and technical domains can be wide-ranging, including employee data, customer data, business partner data and identity, and more.

A corporation's CRM is often connected to their marketing systems, social media, enterprise resource planning (ERP) software, analytics platform, data platform, and more systems, further affecting which data needs to be protected and compliant. Since sensitive data is stored and shared from these systems, all of them are affected to some degree, and their integrations also need to be secure and compliant.



ERP

- China ERP with own instance
- Locally sourced ERP

Workspace & Collaboration

- O365 (including E-mail)
- Collaboration Tools
- ITIL tools

Sales & Marketing

- WeChat touchpoints
- E-Commerce / ordering portal
- Sales Enablement
- CRM (i.e. Salesforce)

Data Platform

- Consumer Data Platform
- Other Data Platform including important data

HR

- Global/local split of the HR systems in view of the regulatory requirements and local ecosystem

Sales & Marketing

- Standard Global solution hosted in China
- China localized solution with customization
- Tailor-made solution with cloud providers in China

Data Platform

- Dedicated Domain for CN services (Certificate/ICP)
- Local authorized DNS
- Independent VPCs/subnets for Chinas
- Local access for user profile e.g., VPN, Identity

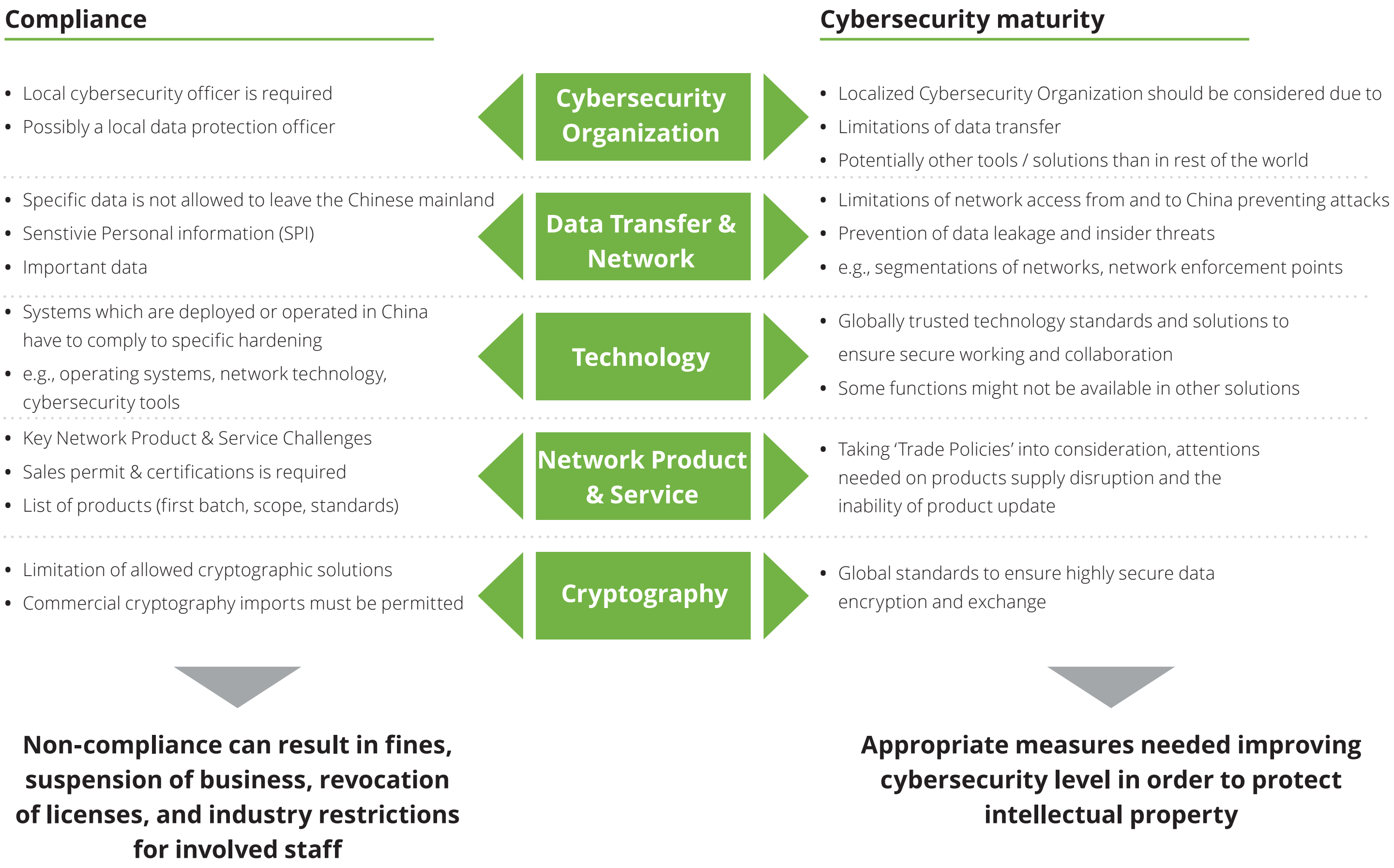
Security

- IAM/ AD Separation / MFA
- Zero Trust
- Vulnerability scan and Pentest
- Cyber Security

Figure 5: Key areas of localized solutions. Deloitte Consulting (Shanghai) Company Limited, 2024.

Cybersecurity Considerations

Achieving compliance while enhancing the cybersecurity level in China and the rest of the world is a challenge. For example, specific data is not allowed to leave the Chinese mainland, like Sensitive Personal Information. Non-compliance can result in fines, but improving cybersecurity is key to protecting intellectual property. Companies will need to find a balance between the two to satisfy all parties and keep information secure.



Compliance		Cybersecurity maturity
• Local cybersecurity officer is required • Possibly a local data protection officer	**Cybersecurity Organization**	• Localized Cybersecurity Organization should be considered due to • Limitations of data transfer • Potentially other tools / solutions than in rest of the world
• Specific data is not allowed to leave the Chinese mainland • Senstivie Personal information (SPI) • Important data	**Data Transfer & Network**	• Limitations of network access from and to China preventing attacks • Prevention of data leakage and insider threats • e.g., segmentations of networks, network enforcement points
• Systems which are deployed or operated in China have to comply to specific hardening • e.g., operating systems, network technology, cybersecurity tools	**Technology**	• Globally trusted technology standards and solutions to ensure secure working and collaboration • Some functions might not be available in other solutions
• Key Network Product & Service Challenges • Sales permit & certifications is required • List of products (first batch, scope, standards)	**Network Product & Service**	• Taking 'Trade Policies' into consideration, attentions needed on products supply disruption and the inability of product update
• Limitation of allowed cryptographic solutions • Commercial cryptography imports must be permitted	**Cryptography**	• Global standards to ensure highly secure data encryption and exchange

Non-compliance can result in fines, suspension of business, revocation of licenses, and industry restrictions for involved staff

Appropriate measures needed improving cybersecurity level in order to protect intellectual property

Figure 6: Cybersecurity consideration categories. Deloitte Consulting (Shanghai) Company Limited, 2024.

Data Residency, Data Access, and Cross-border Data Transfers

Hosting business applications and their data in China supports compliance with the Cybersecurity Law (CSL), Data Security Law (DSL), and Personal Information Protection Law (PIPL) regulations, as well as meeting China market dynamics and speed, and ensuring both global and local cybersecurity.

China's current cyberspace governance strategy is to focus on cybersecurity and protect personal data and important data cross-border transmission. For multinational corporations (MNCs) in China, proper isolation and cross-border data transfer control is becoming an urgent requirement.

Balancing timeliness with need can cause complications across industries. Three compliance aspects commonly arise at this point:

- **Data Residency:** To comply with the laws and regulations discussed in this document, data that is gathered in China needs to be processed and stored in China unless there is an exception granted.

- **Data Access:** Processors need a legal reason to process data, and actors need a legal reason to access the data. Access control is necessary to ensure that the individuals accessing the data are entitled to that privilege.

- **Cross-border Data** Transfers: The default for regulated data is that it needs justification and approval to transmit across borders. Application Programming Interface (APIs) are one mechanism, but remote access of any kind is a data transfer.

A key starting point for corporations therefore, is to consider proper isolation through data residency in China.

Common Scenarios for Data Residency

Applications contain massive amounts of non-HR (non-employee) personal Info, core data, and important data

Over 1 million records with client information are subject to localization requirements and any cross-border data transfer activities must be approved in advance. Core data and important data may impact national security, social stability and public interest, facing more restricted regulation than sensitive personal info. Certain data is not allowed to leave the Chinese mainland at all.

Local administration for business applications, IT infrastructure, and Security Operations Center
Since remote access is considered to be a cross-border data transfer, local administration is necessary for business applications containing massive non-HR (non-employee) personal info, core data, and important data. Administration of IT infrastructure and Security Operations Center means indirect access to business data and creates system vulnerability, not only bringing risk to data, but also to critical system functionality.

Restrict access to global critical business applications and IT infrastructure
Global critical business applications contain core intellectual property and other sensitive business information. Accessing global IT infrastructure from China may impact overall IT confidentiality, integrity, and availability.

Common Practices for Data Security and Access Control

There are two driving factors stemming from regional laws and regulations—Data Security and Privacy. Storing data in China addresses some needs, but controlling who has access to what data is another key approach.

For example, a user managing Hong Kong customers should not have access to Shanghai customer data. A finance user should not have access to personal health information fields. Various teams require access to customer or personal data to perform their roles and responsibilities.

Some common practices and considerations for secure and compliant data access from these teams are:

- **Purpose limitation:** Regulatory restrictions mandate that data be collected and processed only for specified and legitimate purposes. The users and systems with access need to be playing a legitimate role in performing those purposes. The principle of least privilege should be followed.
- **Managed permissions:** Leverage granular permissions to limit user access and privileges to only what is appropriate for their role and the processes that they should be engaged in. To the extent systems support these permissions, control access to categories (tables or objects), individual records, field-level access, and APIs and capabilities.
- **Data Minimization:** To support privacy regulations, gather only the data that is needed to complete the purposes for which it is gathered. Purge unnecessary data from the system.
- **Consent:** Processing and non-consensual actions should be blocked where consent has not been granted.
- **Privileged Access Management (PAM):** Consider implementing PAM solutions to monitor access to critical systems and sensitive data.
- **Multi-Factor Authentication (MFA):** Implement MFA across your IT systems to defend against social engineering, password sharing, and other forms of inappropriate or unauthorized access.
- **Secure API Access:** Use API keys, OAuth tokens, or other secure methods for programmatic access to data.
- **Logging and Auditing:** Monitor and audit detailed systems logs and built-in audit trail functionality to understand who accesses and or modifies what data on which occasions. Respond when these trends change.
- **Incident Response Planning:** Develop and regularly test incident response plans for data breaches or unauthorized access, communicate these widely among the necessary teams.

Common Practices for Cross-Border Data Transfers

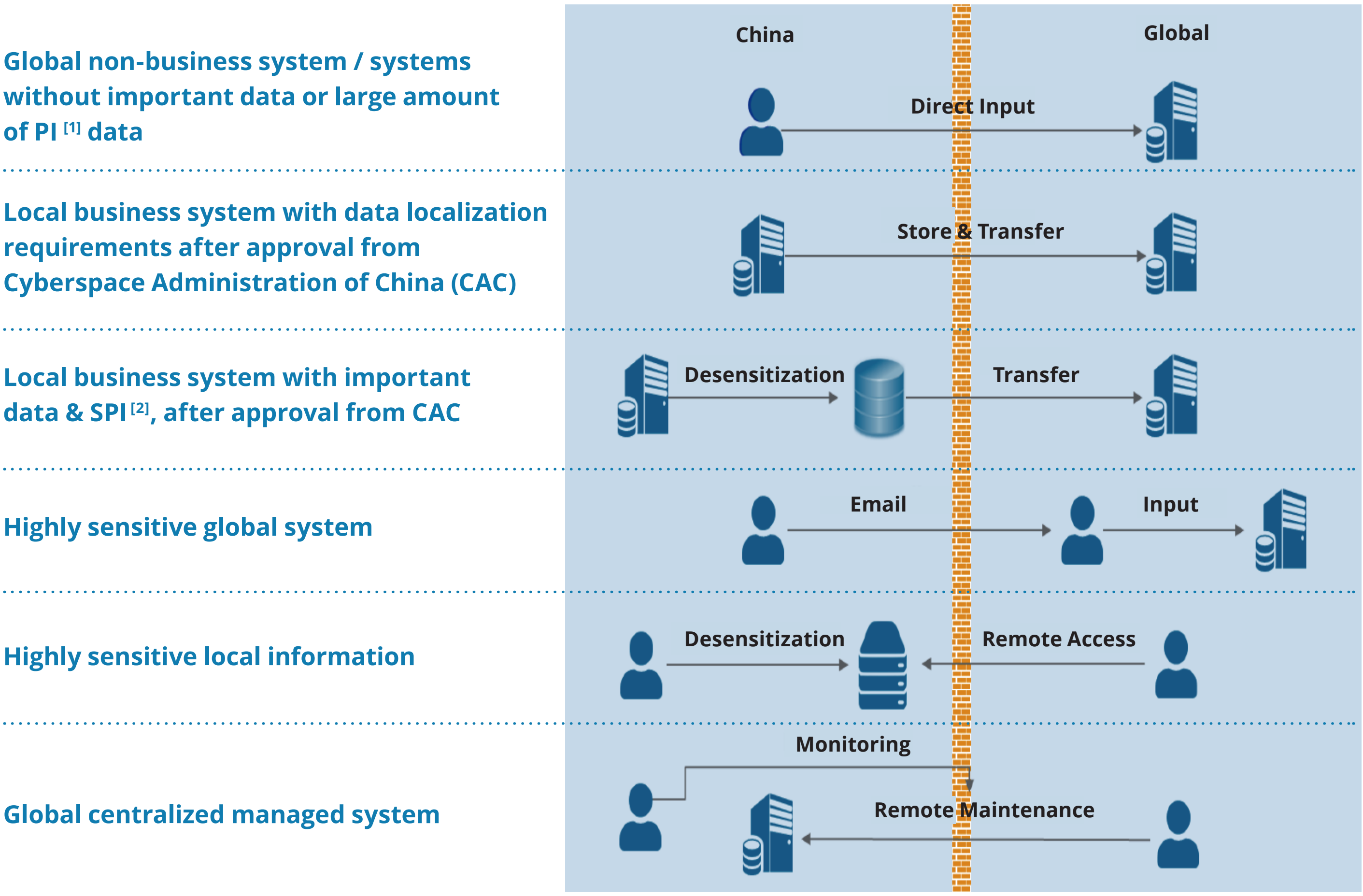
Controlling cross-border data transfer is a key aspect of complying with Chinese privacy and security laws. Data transfer controls are in addition to data storage and data security controls. The Cybersecurity Law and related regulations subjects many international data transfers to a security assessment by a relevant industry regulator. Furthermore, the PIPL restricts the transfer of sensitive personal information, and can require a regulatory review and approval process to transfer or transmit the data internationally.

Some recent exceptions and allowances have been made:

- Data necessary to enable cross-border sales, manufacturing, transportation, or academic collaboration. Sensitive personal and important data is not included in this exemption.

- Personal information necessary to protect a person's life, health, or property in the event of an emergency.
- The transfer of non-sensitive personal information for less than 100,000 persons in a calendar year, for entities that are not critical information infrastructure operators.
- Data necessary to perform contracts in which the individual is a party—signatures, booking flights and hotels, cross border payments or remittances, visa processing, and examinations services—have an exemption.
- Employee data necessary to perform HR functions is exempted, but it must follow the minimum and necessary principles of the PIPL.

However, unless a data transfer is known to be permitted, the safer operating principle is to assume that its not permitted until permission is granted.


China
Global
Global non-business system / systems without important data or large amount of PI [1] data
Direct Input
Local business system with data localization requirements after approval from Cyberspace Administration of China (CAC)
Store & Transfer
Local business system with important data & SPI [2], after approval from CAC
Desensitization
Transfer
Highly sensitive global system
Email
Input
Highly sensitive local information
Desensitization
Remote Access
Global centralized managed system
Monitoring
Remote Maintenance

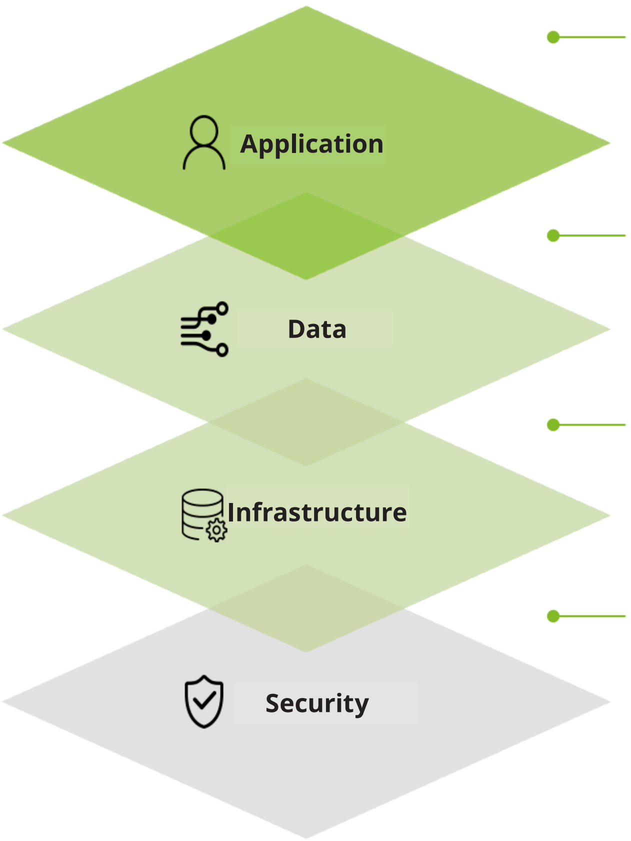
Note: [1] PI: Personal Information. [2] SPI: Sensitive Personal Information
Figure 7: Cross-border data transfer processes. Deloitte Consulting (Shanghai) Company Limited, 2024.

Technical Considerations

After reviewing the opportunities and risks, classifying and reviewing data and security, an architectural strategy can be created by designing a localization strategy. The China localization strategy will encompass assessment and changes to your IT platform and application architecture, or existing services that implicitly provide the required capabilities or can be configured to do so. From a technical perspective, businesses should consider these elements:

- **Application:** Customer information platforms
- **Data:** Data-related capabilities enabling customer information platforms
- **Infrastructure:** China-based hosting cloud
- **Security:** Basic local capabilities aligned to global standards

IT Platform & Application Architecture



Moves of China for China Strategy

The experience layer with customer / consumer facing applications is usually among the first wave of pilots, incl.

- WeChat touchpoints
- E-Commerce / ordering portal
- Digital services
- Marketing automation
- SCRM
- Sales enablement
- Distributor ERP and CRM
- ……

All data related capabilities enabling customer / consumer facing applications should be built first

- Consumer Data Platform
- Data storage
- Data analytics
- Data visualization

China-based hosting cloud, including private and public cloud solutions, is primarily considered:

- Private hosting (on-premise, Private cloud, etc.)
- Public cloud (Ali Cloud, AWS, Azure, Tencent Cloud, etc.)
- APIs

Build the basic local capabilities with global standards aligned:

- Compliance: CSL, DSL, PIPL
- Assessment: CPCS, CBDT, PIA
- Network and boundary security
- IAM, Zero Trust
- Vulnerability scan and Pentest
- SIEM, SOC, SOAR
- Incident Response

Figure 8: Layers of technical considerations. Deloitte Consulting (Shanghai) Company Limited, 2024.

Localization Assessment

Usually a system localization assessment will be done at the very first step as a study phase. The following decision tree is proposed to guide organizations in determining the right localization strategy for core systems and surrounding systems, based on Chinese laws and regulation compliance requirements. The system localization assessment will provide crucial insights when designing a China localization strategy.

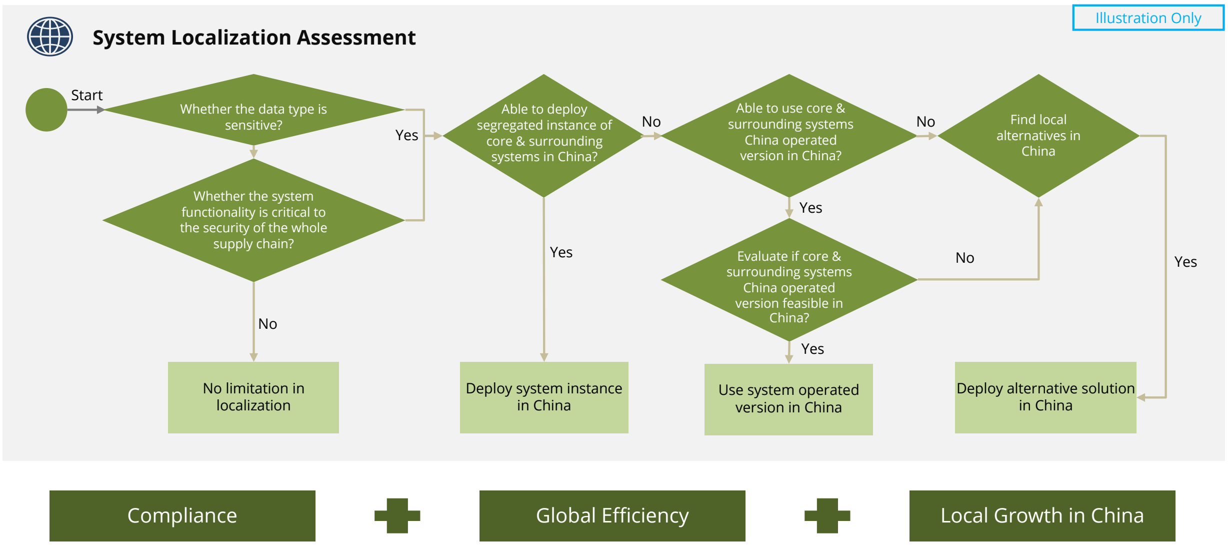


Illustration Only
System Localization Assessment
Start
Whether the data type is sensitive?
Yes
Whether the system functionality is critical to the security of the whole supply chain?
No
No limitation in localization
Able to deploy segregated instance of core & surrounding systems in China?
Yes
Deploy system instance in China
No
Able to use core & surrounding systems China operated version in China?
Yes
Evaluate if core & surrounding systems China operated version feasible in China?
Yes
Use system operated version in China
No
No
Find local alternatives in China
Yes
Deploy alternative solution in China
Compliance
Global Efficiency
Local Growth in China

Figure 9: System Localization Assessment flow chart. Deloitte Consulting (Shanghai) Company Limited, 2024.

Key Takeaways

Planning and focus

China's laws and regulations essentially add up to data residency requirements for personal and sensitive personal data, in addition to controls on important and core data. These laws overlap, change, and interpretations may vary by industry and region. Business processes move slowly and it's important to plan for the most restrictive interpretations of these laws.

Companies doing business in China typically benefit from using local systems and hosting the systems of record for business in China. With proper preparation and approval, those systems can integrate with systems outside of China. Planning ahead regarding data compliance and creating a localization strategy is key to their success. The focus should be on the protection of important data and regionalized operations.

Data strategy

Assume the global source of truth for data about Chinese data subjects or operations needs to be in China as its primary home. Sometimes, data can be mirrored outside of China after an export review approval and explicit consent. Data approved for export from China requires local storage.

Remember that some data may not be approved for export or may require anonymization or classification as part of the export process. Keep it simple, if you don't need to export the data, then don't export it.

Not all data is personal or sensitive. Some data may be exportable from China, after a risk review and an approval process. A risk assessment should be performed before transmitting any data across national borders, and depending on scale, approvals may be required. Cross-border data transfer does not change requirements to store data locally.

Want to find out more?

To continue your discovery on how Deloitte can support on this topic, please visit our dedicated webpage. Please contact us to learn more.

Barry O'Neill
Partner
barroneill@deloitte.dk

Barry is part of the leadership here at Deloitte Digital in the Nordics. With over 20 years experience on front-office transformations across CRM, e-commerce and marketing, Barry has a wealth of experience across technologies including Salesforce, Microsoft, and CommerceTools.

Malene Fagerberg
Partner
mfagerberg@deloitte.dk

Malene is a Partner in Deloitte Technology & Transformation with more than 15 years of experience with cyber risk. Malene combines expertise across technical and legal fields to ensure a complete view on risk across various cyber domains such as data privacy, cyber security, cloud transformation, artificial intelligence, critical infrastructure, intelluectual property rights, data transfer and data compliance.

Appendix I

Acronyms

CAC: Cybersecurity Authority of China
CBDT: Cross Border Data Transfer
CIIO: Critical Information Infrastructure Operator
CSL: Cybersecurity Law
DSL: Data security Law
IP: Intellectual Property
MLPS: Multi-Level Protection Scheme
MNC: Multinational Corporation
PI: Personal Information
RPO: Recovery Point Objective
RRR: Reserve Requirement Ratio
RTO: Recovery Time Objective
SIEM: Security Information and Event Management
SOAR: Security Orchestration, Automation and Response
SOC: Security Operations Center
SPI: Sensitive Personal Information

Appendix II

Regulation Trend: National Standards

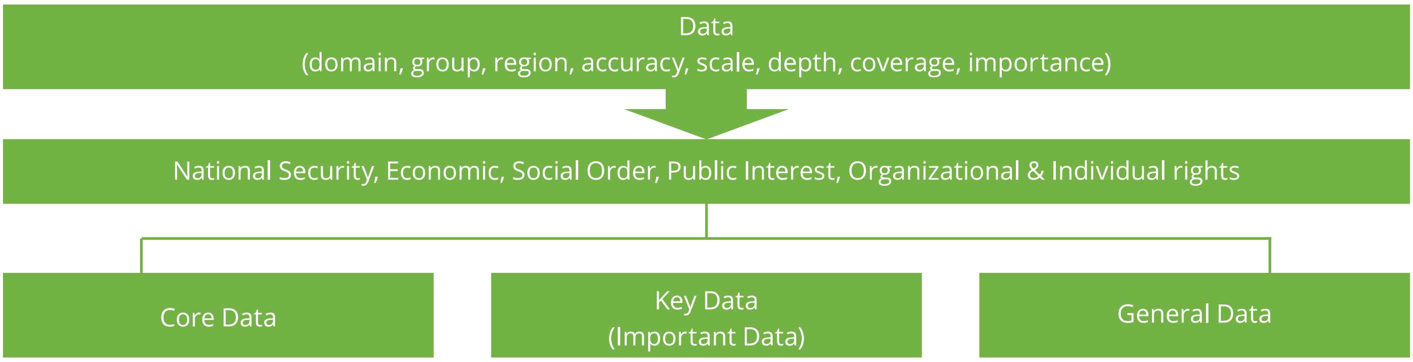

Data
(domain, group, region, accuracy, scale, depth, coverage, importance)
National Security, Economic, Social Order, Public Interest, Organizational & Individual rights
Core Data
Key Data
(Important Data)
General Data

Figure 10: Sensitivity of data hierarchy. Deloitte Consulting (Shanghai) Company Limited, 2024.

Examples of sensitive data include, but are not limited to:

- Critical Information Infrastructure Operator (CIIO) core business data[7]
- Historical and cultural heritage data
- Location, construction data, security info of important sites
- Export control data
- Security protection, core SW/HW and supply chain info of CIIO
- Ethnic characteristics, genetic information, and major outbreaks of infectious diseases
- Unpublished statistic data and critical trade secrets

Note: GB/T 43697: The latest rules for data classification and grading were announced and will be effective on 1 October 2024.[8]

Regulation Trend: Industry and Regional Regulations

Industrial requirements are considered before regional requirements. Some industries already have management standards and cases as reference for practice, and some economic zones, such as free trade zones, have taken the lead in exploring the establishment of legal, safe and convenient cross-border data transfer mechanisms to encourage enterprises to carry out more convenient, secure and efficient cross-border data transfer.

Industry-specific Standards and Guidelines[9]

Automobile, Healthcare, and Financial Services

- Certain Provisions on the Management of Automobile Data Security (for Trial Implementation), effective as of 1 October 2021
  - Geographic information, personnel flow, vehicle flow and other data in important and sensitive areas such as military management zones, national defense science and industry offices, and party and government institutions at or above the county level
  - Vehicle traffic, logistics and other data reflecting economic performance
- Guidelines for Data Classification and Grading in the Healthcare Industry (Trial)
  - Over 1 million instances of personal information (PI) or 100,000 sensitive personal information (SPI)
  - National wide business data, health population data of 100,000 people, biological characteristics or medical

[7] After 5 Years, China’ s Cybersecurity Rules for Critical Infrastructure Come Into Focus
[8] GB/T 43697-2024 Data security technology — Rules for data classification and grading (English Version)
[9] 网络安全和数据安全相关法律法规文件

resource of 10,000 ethnic groups, diagnosis and treatment data, medical rescue guarantee data, and specific drug experimental data of 100,000 people

- Measures for the Management of Data Security of Banking and Insurance Institutions
  - – General data further segmented into sensitive data and other general data
  - – Dynamic data grading

Retail, Manufacturing, and Energy

- No clear standards or guidelines on classification and management of important data in the industry yet
- Enforcement cases exist in some industries, and certain data is explicitly restricted from being transferred across borders
  - – IoT data in manufacturing is restricted
  - – Reserve requirement ratio (RRR) for foreign currency deposits is restricted
  - – Information related to basic communication network and cultural security such as ideology and public opinion, which is held by basic telecommunications enterprises, is restricted

Specification in Pilot Free Trade Zones

Except for the Pilot Free Trade Zone, no other administrative or economic regions have issued formal and clear standards for important data identification.

China (Tianjin) Pilot Free Trade Zone (Negative list as of 9 May 2024)

- Internal name, geographical info, construction plan, security planning, security protection layout, production and operation situation, and product transaction situation of military research and production units
- Over 1 million records with client information, or account information, loan data, transaction data, insurance or claim data, financial lease data of important enterprises and institutions
- Behavioral analysis data of sensitive groups such as government officials and veterans, including service record data of military industry, party and government agencies, and critical information infrastructure customers

China (Shanghai) Pilot Free Trade Zone & Lin-gang Special Area

- Information that is not suitable for public disclosure during the provision of services to government agencies, military enterprises
- Provides sensitive information and personal information related to party, government, military, and confidential units overseas
- Large or mega institutions in the financial industry, as well as important core node institutions in the financial transaction process
- National economic operation data, important industry business data, statistical data, etc. that need to be protected or controlled for dissemination

Regulation Trend: Regional Regulations – General Data List

According to the Measures for Classification and Grading Management of Cross-border Data Transfer in SHA Lin-gang Special Area, “The data processor can apply for registration and filing with the Lin-gang New Area Management Committee for the data listed in the general data list, and freely flow under relevant management requirements.”[10] General Data should not include key data or core data and more than 100,000 PI (not including SPI), general data list does not apply to the CIIO.

[10] 关于印发《中国（上海）自由贸易试验区临港新片区智能网联汽车领域数据跨境场景化一般数据清单（试行）》的通知

Resources

General Data should not contain face or license plate info, VIN can’ t be link to PI on receiver side, can’ t directly cross-border through vehicle.

- Cross border production and manufacturing (Not reflect national economic, de-identified PI, not related to major incident, VIN not link to PI)
  - Production management,
  - procurement of parts and materials,
  - inventory management,
  - quality management,
  - remanufacturing of problematic parts
- Global R&D (Not involving major national research and development projects)
  - Product design
  - product testing
  - R&D management
- Global Post Sales Service
  - Basic vehicle information
  - Post-sales process records
  - fault analysis
  - Post-sales service reports
- Global trade for used cars
  - Basic vehicle information
  - Maintenance info
  - insurance info

Public Fund

- Market Research (Not involving securities value analysis and market trend data)
  - Industry research report
  - Macroeconomic analysis report
- Internal Management
  - Settlement data management
  - Supplier Data Management
  - Investor Data Management
  - Marketing Service Management Data
  - Product Management Data
  - Risk management data
  - Compliance audit management data
  - Financial management data
  - Project Management Data

LSHC

- Clinical trials and research and development
  - De-identified basic info of subjects
  - Physiological health info
  - Basic info of researchers
  - Education info of researchers
- Drug Alert and Medical Device Adverse Event Monitoring (Can only be used for security assessment)
  - De-identified basic info of patients & reporters
  - Basic physiological condition
- Medication records
  - Adverse reaction information
  - Summary reports
  - Medical Inquiry
  - De-identified basic info of inquiries.
  - Inquiry info
- Product Complaints
  - De-identified basic info of complainants & patients
  - Complaint info
- Business Partner Management
  - Background info
  - Filling info
  - Contract management info
  - Basic contact PI
  - Bank account info
  - Qualification info

Figure 11: Examples of general data. Deloitte Consulting (Shanghai) Company Limited, 2024.

Office locations

Copenhagen
Weidekampsgade 6
2300 København S, Danmark
+45 36 10 20 30

Oslo
Dronning Eufemias gate 14
0191 Oslo
+47 23 27 90 00

Helsinki
Itämerenkatu 25
00180 Helsinki
+358 (0)20 755 500

Stockholm
Rehnsgatan 11
Stockholm
+46 75 246 20 00

MAKING AN
IMPACT THAT
MATTERS
since 1845

About Deloitte
Deloitte China provides integrated professional services, with our long-term commitment to be a leading contributor to China's reform, opening-up and economic development. We are a globally connected firm with deep roots locally, owned by our partners in China. With over 20,000 professionals across 31 Chinese cities, we provide our clients with a one-stop shop offering world-leading audit, tax and consulting services.

We serve with integrity, uphold quality and strive to innovate. With our professional excellence, insight across industries, and intelligent technology solutions, we help clients and partners from many sectors seize opportunities, tackle challenges and attain world-class, high-quality development goals.

The Deloitte brand originated in 1845, and its name in Chinese (德勤) denotes integrity, diligence and excellence. Deloitte's global professional network of member firms now spans more than 150 countries and territories. Through our mission to make an impact that matters, we help reinforce public trust in capital markets, enable clients to transform and thrive, empower talents to be future-ready, and lead the way toward a stronger economy, a more equitable society and a sustainable world.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of DTTL, its global network of member firms or their related entities is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.

© 2024. For information, please contact Deloitte China.

CQ_025EN_24

This is printed on environmentally friendly paper