KPMG

Navigating China's cybersecurity landscape

Cybersecurity regulatory considerations in China

Background

China's reopening is expected to provide global markets access to one of the world's largest growth opportunities. As organizations seek to capitalize on the opportunity, foreign players must be prepared and equipped to comply with China's cybersecurity requirements. For years, China has taken steps to increase its national and personal security by implementing additional laws and standards. Companies that have operations or are looking to expand operations into China must be made aware of these recent changes, as their noncompliance could lead to significant business disruptions, penalties, and legal ramifications.

Laws and standards

China's cybersecurity regulatory landscape continues to evolve rapidly, implementing additional security regulations to protect national and personal security. The foundation of China's cybersecurity compliance requirements is Cybersecurity Law, Data Security Law, and Personal Information Protection Law. Companies must understand those cybersecurity laws and associated regulations to prepare for the formal certification process effectively.

Multilevel protection scheme certification process

1 System identification and grading

- List systems and create an inventory based on their operations and plans.
- Follow MLPS requirements like setting system boundaries, assigning personnel for security, and grading internal systems based on various factors.

2 Self-assessment and remediation

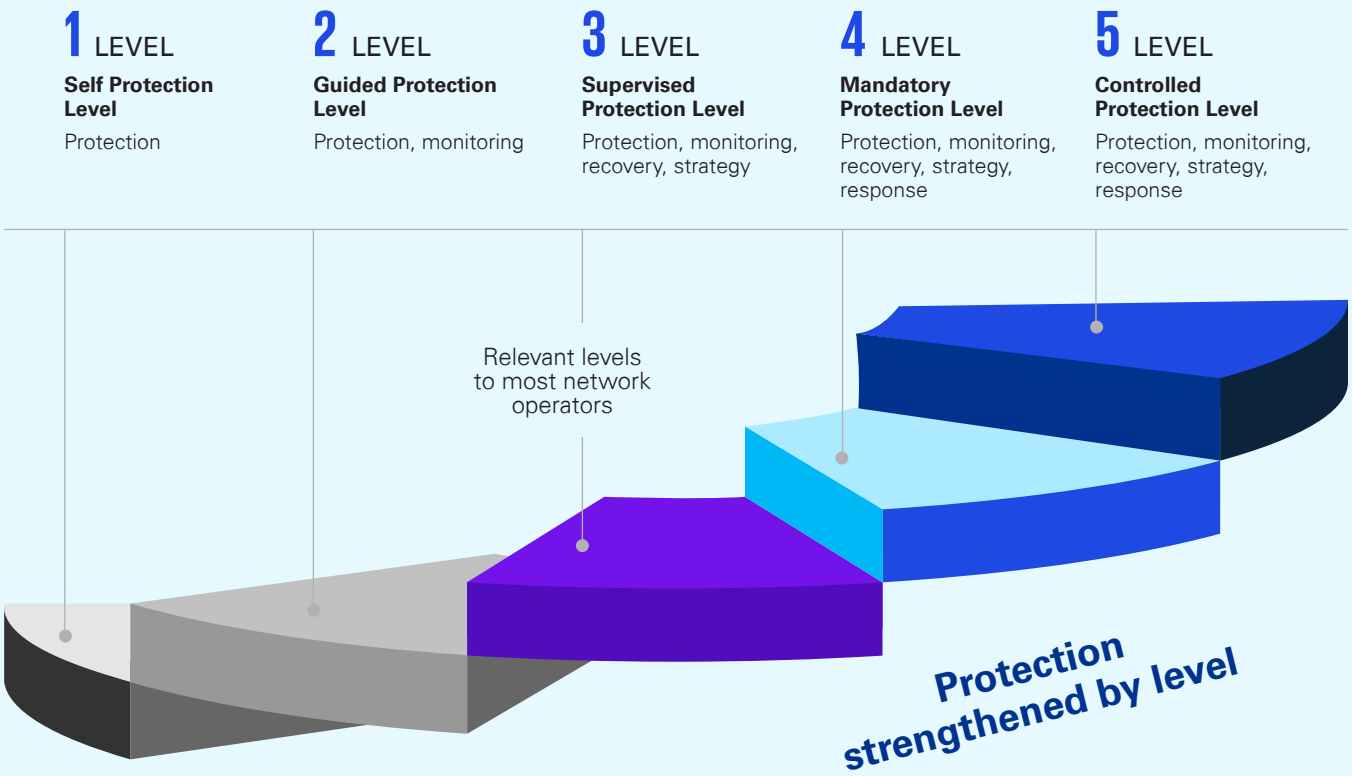
- Conduct MLPS gap analysis and produce self-assessment reports based on the graded objects.
- Implement technical measures, improve management policies, and create a remediation plan to address unfulfilled items.
- Conduct compliance assessment, risk assessment, and technical testing as required by the CSL to complement MLPS compliance.

3 Third-party assessment and filing

- Compile grading documents, arrange expert reviews, receive necessary approvals, and submit filings (level 2 and above).
- Approved agencies conduct tests, implement recommended security measures, and obtain level 3 or higher filing certification.
- Systems of level 3 or above must be tested once a year, and level 2 systems are recommended to be tested once every 2 years.

4 Continuous improvement

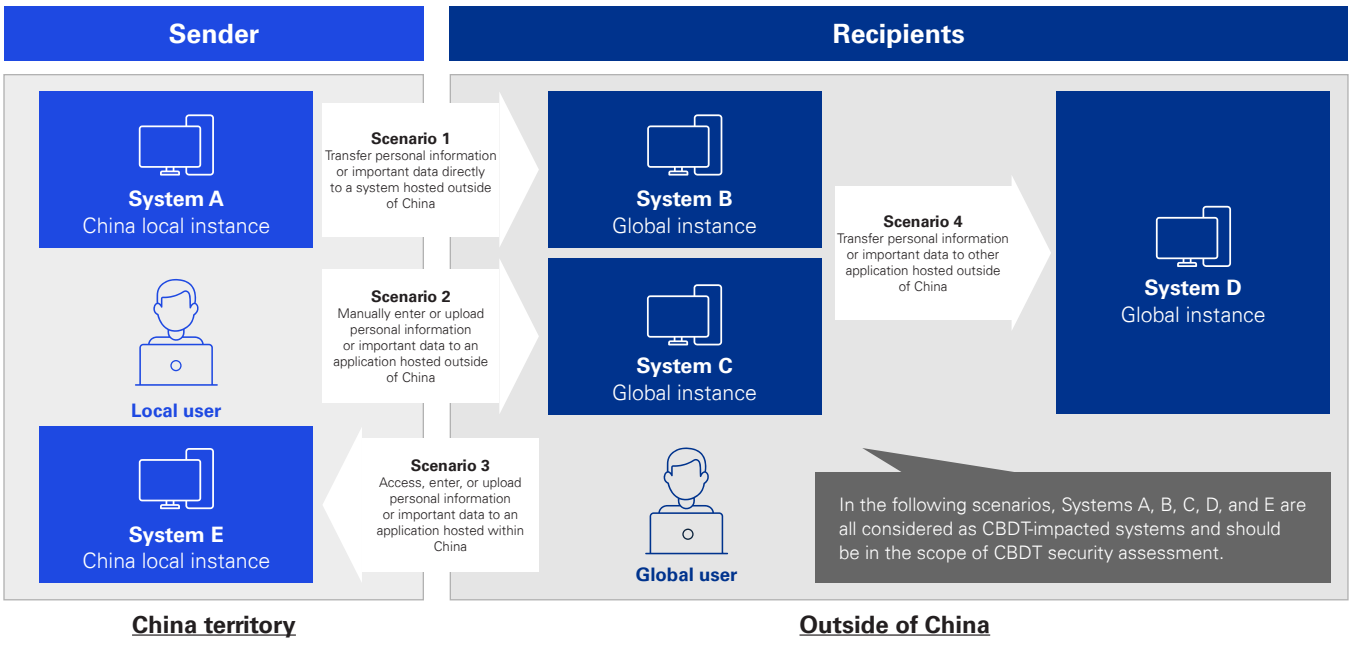
- Develop security plans and prioritize cybersecurity tasks based on MLPS assessment findings and governance goals.
- Improve cybersecurity technical protection systems (e.g., identification, protection, detection, etc.) and regularly perform assessments in line with MLPS 2.0.
- Stay current on cybersecurity laws, policies, and standards and promptly address new regulations.



The Multilevel Protection Scheme (MLPS) is a regulation under China's Cybersecurity Law that grades companies from levels 1 to 5, each with different cybersecurity requirements, depending on risk level. Compliance is mandatory and aims to create a cybersecurity standard across all organizations in China. To comply, organizations should assess their security level, develop a security plan and implement necessary measures, and conduct regular security assessments while submitting compliance documentation. Following these steps will help alignment with compliance requirements and protect against cyber threats.

Cross-boarder data transfer certification process

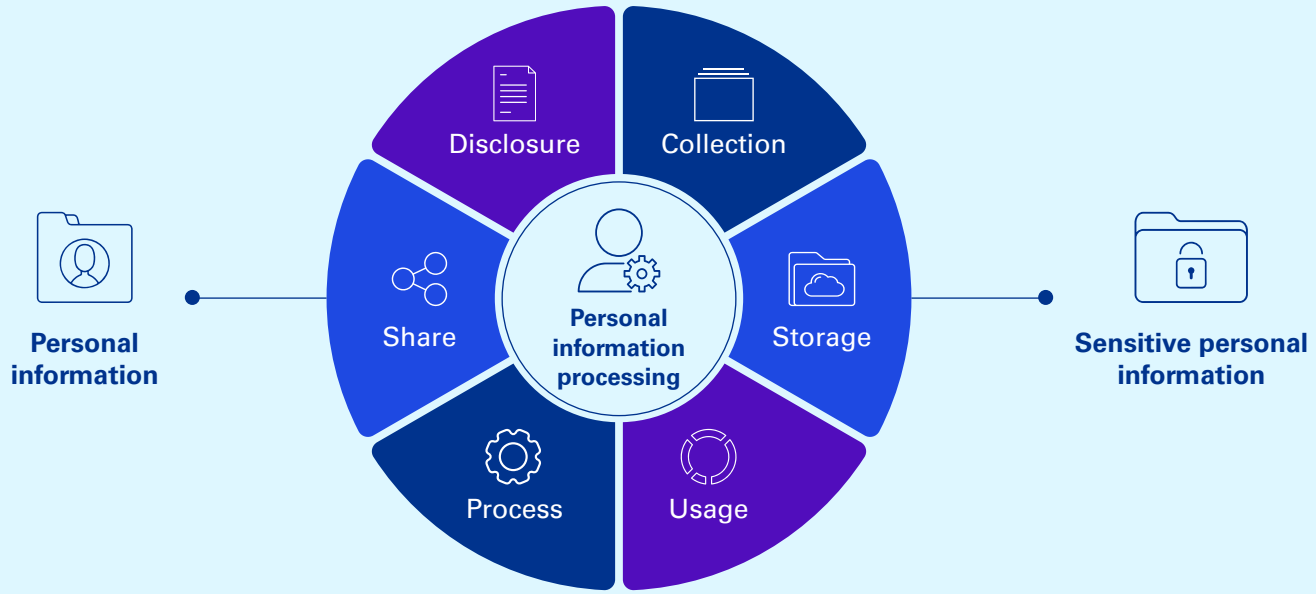
Impacted scenarios:



Cross-border data transfer (CBDT) has strict requirements for companies transferring data outside its border. Companies must pass a security assessment before transferring data overseas. The security assessment will evaluate whether the data transfer meets the criteria set out in the law and whether it poses any potential risks to national security and public interests.

Companies that fail to comply with the CBDT requirements may face penalties such as fines, suspensions, and license revocation. Therefore, it is important for companies operating in China to review their data protection obligations, including those related to cross-border data transfer, to ensure compliance.

Privacy considerations



Personal Information Protection Law (PIPL) significantly impacts businesses operating in China, requiring stricter and more detailed data protection and privacy requirements. It applies to organizations that process personal information within the territory of China or about China's citizens. They must only collect necessary information and receive informed consent from individuals before collecting, processing, and storing personal information. In addition, the PIPL requires organizations to establish and implement effective data protection systems and conduct security risk assessments periodically.

How can we help?

We understand that navigating China's cyber regulations can be daunting for companies. To ease the process, the KPMG US team provides pro bono strategy discussions and knowledge-sharing sessions to better understand your needs and for KPMG to provide you with our insights given we have served many of our clients on the entire cycle of the compliance journey (i.e. readiness assessment, scoping, strategy, remediation, certification, and maintenance). We are committed to helping companies successfully navigate China's regulations and achieve business success. Please get in touch with us for more details on how we can assist you.

Contact us

Danny Le
Cyber Principal
dqle@kpmg.com

Paul Torres
China Compliance Lead
ptorres@kpmg.com

Lauren DeFrancesco
China Compliance Co-Lead
ldefrancesco@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia