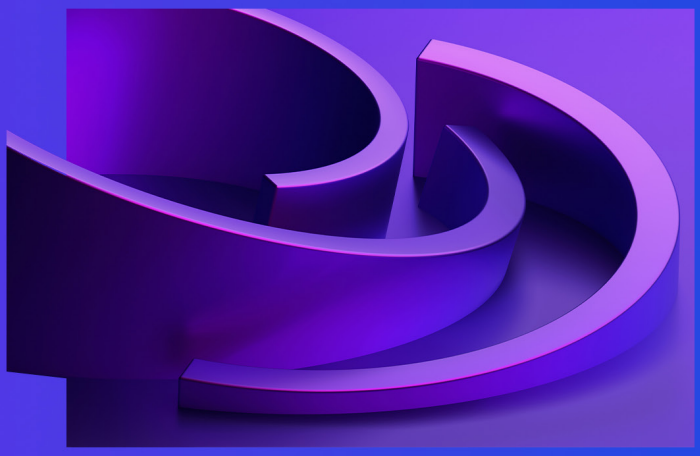
Cyber Considerations for Banking Expansion into China



By: Brittany Weinstein and Ashley Ryan

China accelerated opening its financial sector in the past few years to allow foreign organizations to operate wholly-owned ventures, permitting unprecedented access into the world's second-largest capital market. In response, international financial institutions seek to capitalize on the lucrative opportunity and expand their business in mainland China. While the profit opportunity is substantial, the cybersecurity considerations are significant as multinational financial entities navigate a complex, ever-evolving cyberspace with China's vast and stringent cybersecurity national standards.

History of foreign banking in China[1]

Developments to open China's financial sector began to materialize nearly two decades after joining the World Trade Organization (WTO) in 2001. In 2018, the Chinese government instituted a new, centralized financial regulatory framework to increase efficiency and manage systematic risk to safeguard its economic welfare, positioning China for the expansion of foreign investors in the country's market. China made aggressive strides to commit to its pledge of opening its financial sector following the reformation, including a phased approach to lifting foreign ownership caps. In Fall of 2018, the China Security Regulatory Committee (CSRC) released a new measure permitting foreign securities majority ownership for joint ventures, raising the maximum approval stake from 49% to 51%.[2] In April 2020, the Chinese government eliminated the ownership ceiling, allowing wholly owned units on Chinese terrain. Since the ownership lift, various multinational banking conglomerates have received approval to take control of their onshore joint ventures, trailblazing the pathway for full-ownership expansion in China.

Enforcement of new cybersecurity regulations

In parallel to transforming its financial regulatory structure and abolishing foreign ownership restrictions for its financial services sector, China bolstered its cybersecurity and data governance regime by publishing three critical and robust regulations. The Cybersecurity Law (CSL) formed the foundation of the triad and is supported by the Data Security Law (DSL) and the Personal Information Protection Law (PIPL). Collectively, the CSL, DSL, and PIPL, amongst other cybersecurity laws, make China a high standard when it comes to data regulatory and cyber compliance for foreign firms due to their extensive scope.

[1] China lifts foreign ownership limits on securities, fund management firms, April 2, 2020, The State Council Information Office, The People's Republic of China

[2] Trade deal touts financial sector wins; China to scrap securities business cap faster, January 15, 2020, Thomson Reuters

Key considerations

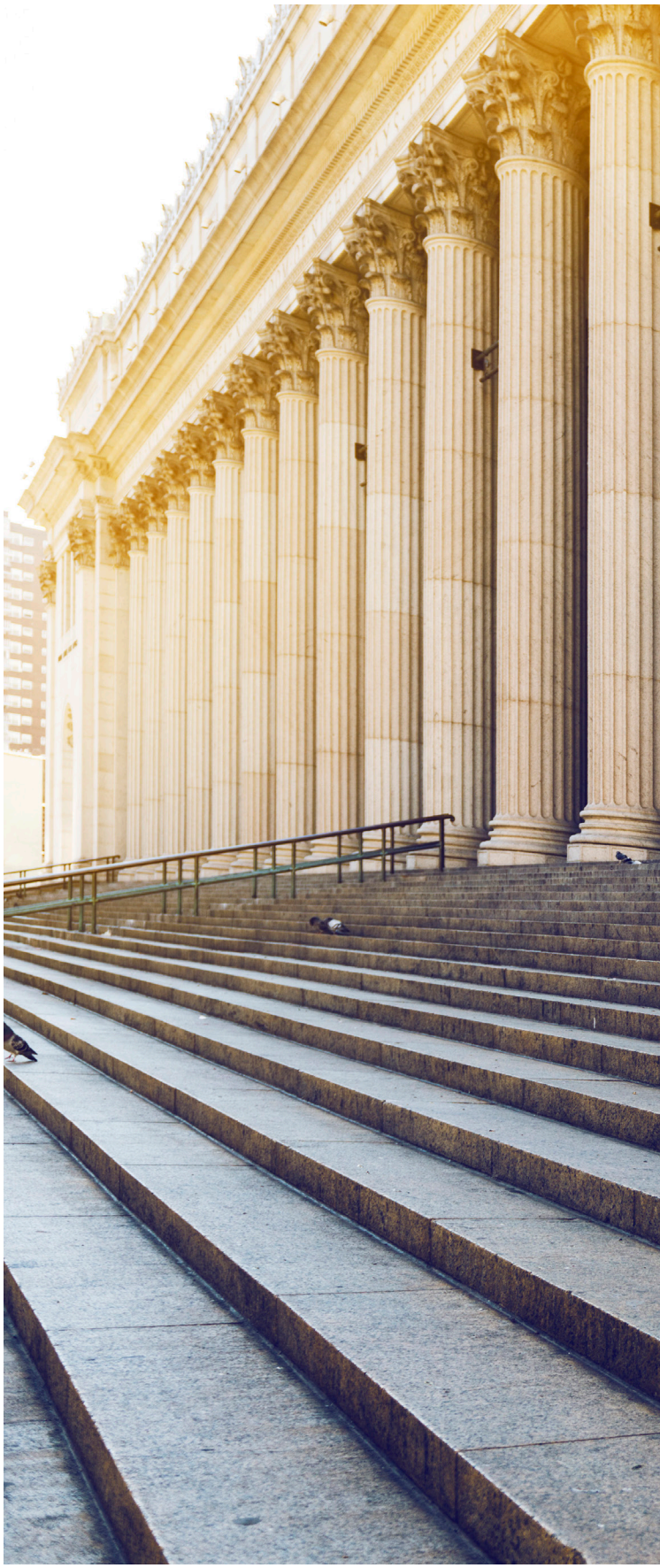
While China welcomes financial entities to increase their presence in the nation's market, foreign players must be prepared and equipped to comply with the country's cybersecurity standards, performing the necessary due diligence to increase visibility and awareness to make informed, proactive decisions. Multinational banks may consider the following key themes that transpire through the interplay between the CSL, DSL, and PIPL, amid other cyber laws, as they maximize their stakes in the Chinese marketplace and develop their expansion strategy:

Developing requirements[3]

Laws are crafted with language for interpretation across definitions, requirements, and roles and responsibilities of regulators, so organizations may experience varying degrees of regulatory enforcement. Organizations with limited prior interaction with Chinese law and regulators may find this challenging as pioneers of banking expansion in China. Standards may be deemed recommended, but, in practice, most are mandatory for critical infrastructure sectors, including finance, to conduct business operations. Therefore, multinational banks must actively communicate and collaborate with regulators to gauge expectations and define requirements, receiving greater color and clarity regarding Chinese cyber regulations in order to demonstrate compliance and maintain business continuity.

Extensive reviews and assessments[4]

China's Cybersecurity Review Measures grant regulators the ability to administer comprehensive assessments for two broad use cases: (1) Critical Information Infrastructure Operators (CIIO) and network operators that impact or may impact national security and (2) Network platform operators processing more than one million users' personal information intending to list shares abroad. The circumstances defined by the measures provide the regulators flexibility to conduct extensive investigations, which may reveal source code, corporate information/ intellectual property, and encryption methods when evaluating equipment to prove adequate security. Inspections may require enterprises to redesign products or configure specific technologies and platforms to comply with laws.



[3] China's Cyber Security Law: The Impossibility of Compliance?, May 29, 2017, Forbes

[4] Translation: Cybersecurity Review Measures (Revised) - Effective Feb. 15, 2022, January 10, 2022, Stanford University

Data classification[5]

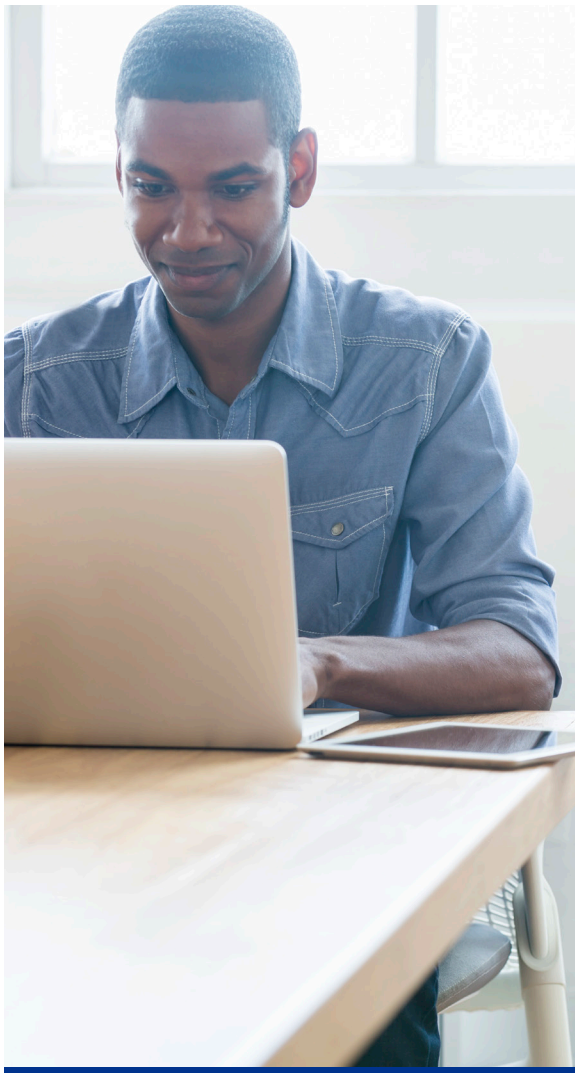
Financial industrial standards (e.g., JR/T 0197-2020 Financial data security—Guidelines for data security classification) provide detailed guidance on how local financial organizations could classify their data properly. Entities must consider the potential impacts on national security, public interests, and business operations, amongst other areas, to determine appropriate data classification. In addition to embracing the government-defined schema, Chinese law stipulates businesses are to adopt an agile data inventory with the ability to perform data classification updates. Instances in which data classification updates are necessary may include but are not limited to data fusion, data content modification, and data anonymization.

Data localization[6]

The finance sector is considered a key industry for data localization, especially those with significant domestic market presence, along with other industries like public communication and information services, energy, transportation, etc. Local financial organizations should understand the key regulators for data localization (e.g., CBIRC, CSRC, PBOC, CAC, etc.) and clearly understand the specific industrial requirement for data localization and cross-border data transfer management. In addition, to adhere to China's data localization standards, multinational banks should invest in onshore data servers or incur additional expenses by hiring an onshore local server provider licensed and authorized by the Chinese regulators. Financial organizations may only be approved for cross-border data transfer if there's a business need upon a series of actions: passing the Cyberspace Administration of China (CAC) security assessment, obtaining data subject consent, and conducting an internal risk assessment. Data classification may impact a foreign bank's ability to receive approval for cross-border transfers.

Incident response[7]

Data controllers must establish an effective and enforceable incident response plan, empowering the business to respond swiftly and uniformly to contain and remediate threats. In the event of a breach, entities must comply with the requirements defined by the Chinese government for notifying regulators and impacted parties, including controllers notifying affected parties of a breach within 72 hours. However, if an incident exposes personal or important data of more than 100,000 individuals, the accountability becomes higher where the window substantially decreases, and the controller is obligated to inform the CAC within eight hours of the breach's occurrence. Upon resolution of an incident, a subsequent report is required to be submitted to the CAC within five business days.



Summary

As organizations seek guidance to navigate the Chinese landscape, extensive cyber security considerations exist to drive expansion successfully. While regulations may be challenging, we suggest focusing on critical areas from the start to help reduce business and regulatory risks and non-compliance.

[5] China's Personal Financial Information Protection, February 22, 2021, Information Systems Audit and Control Association

[6] What to know about China's new cross-border data transfer security assessment guidelines, September 27, 2022, International Association of Privacy Professionals

[7] Translation: Online Data Security Management Regulations (Draft for Comment) - Nov. 2021

Contact us

Matt Miller
Principal, Cyber Security Services
E: matthewpmiller@kpmg.com

Brittany Weinstein
Manager, Cyber Security Services
E: brittanyweinstein@kpmg.com

Ashley Ryan
Associate, Cyber Security Services
E: ashleyryan@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