Cloud Compliance Center - China

Regulatory notifications

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# 5. Does the outsourcing need to be notified to the regulator?

**1. General outsourcing notification requirements**

According to the Circular of Risk Management Guidelines for Outsourcing by Banking Financial Institutions issued by the China Banking Regulatory Commission (now known as the China Banking and Insurance Regulatory Commission or "**CBIRC**") (Yin Jian Fa [2010] No. 44), a bank must periodically conduct a comprehensive audit and appraisal of its outsourcing activities and periodically submit appraisal reports on its outsourcing activities to the local counterpart of the CBIRC. In addition, the bank must promptly report to the local counterpart of the CBIRC any incident that has a significant impacts, customer information security or reputation.

**2. Notification requirements applicable to IT outsourcing**

The notification requirements under the Circular of the General Office of the CBIRC on Issuing the Measures for the Supervision and Administration of IT Outsourcing Risks of Banking and Insurance Institutions (Yin Bao Jian Ban Fa [2021] No. 141) apply to: (i) the entire outsourcing of data centers (server rooms), (ii) off-site IT outsourcing (such as using cloud services not hosted at a regulated institution's own premises), affiliated IT outsourcing and cross-border IT outsourcing (such as engaging a service provider located outside China) that meet the conditions for important outsourcing (such as outsourcing involving centralized storage or processing of a regulated institution's important data and customers' sensitive personal information), and (iii) other IT outsourcing deemed important by the CBIRC. These must be reported to the CBIRC or its local counterpart at least 20 working days before an outsourcing contract is executed.

**3. Governmental clearance for procuring network products and services that may pose threat to national security**

According to the draft Regulations on Network Data Security Management published by the Cyberspace Administration of China ("**CAC**") on 14 November 2021, if a financial institution in China is a critical information infrastructure ("**CII**") operator, its procurement of cloud computing services would be subject to a security assessment as organized by the CAC.
On 28 December 2021, the CAC major data enforcement and rulemaking government agency in China, together with different central industrial regulators, published the Measures for Network Security Review ("**Security Review Measures**"). According to the Security Review Measures, with effect from 15 February 2022, a CII operator, among others, must obtain governmental clearance in respect of any procurement of network products and services that endanger national security.

CII is broadly defined under the PRC Cybersecurity Law and the Regulations on the Security Protection for Critical Information Infrastructure ("**CII Regulations**") as "important network facilities and information systems in important industries and fields" (**including finance**) and "important network facilities and information systems that, in the event of damage, loss of function, or data leakage, might seriously endanger national security, national welfare or the livelihood of the people, or public interest." According to the CII Regulations, in the financial services industry, the regulators, including the People's Bank of China ("**PBOC**") and the CBIRC, will formulate more specific CII identification rules and be responsible for CII identification work. In addition, local counterparts of the PBOC and the CBIRC may reach out to financial institutions in their jurisdictions to assess and identify whether they are operating any CII based on their internal rules/guidelines that are not published. If a financial institution operates a network facility or information system that supports its core business and is critical for its financial services, such a facility or system may be identified as a CII and the financial institution may be considered a CII operator accordingly.

Cloud services are a type of "network products and services" expressly listed in the Security Review Measures. Hence, if a financial institution is a CII operator, its use of cloud services is likely to be subject to a network security review, depending on the impact of such cloud services on national security. In practice, the Chinese government has wide discretion to determine on a case-by-case basis whether a network product or service may cause any national security concerns.

Accordingly, if the procurement of cloud services from a cloud service provider might pose an actual or potential threat to national security, the financial institution will have to perform a self-assessment and prepare an analysis report for the CAC's and the PBOC's review, and then obtain clearance therefrom before starting to use the cloud services.

On a related note, the Security Review Measures also grant the CAC and the PBOC the ex post authority to compel a financial institution to submit relevant documentation of its (proposed) procurement of network products and services for their review if (i) the financial institution does not first file its application voluntarily, and (ii) the CAC and the PBOC reasonably believe that national security is at stake.

©Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership**: This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion**: All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising**: This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction**: Reproduction or copying of the Content on this Site without express written authorization is strictly prohibited.