Cloud Compliance Center - China

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

China

*This content was last reviewed around March 2023.*

**Cloud challenging**

**1. Are financial institutions legally permitted to use cloud services?**

Yes, provided that the financial institution meets all the applicable legal requirements to use cloud services.

**2. Are there any rules that apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?**

Yes. As the use of cloud may constitute outsourcing (and more specifically, IT outsourcing), the following rules will be applicable:

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)

Guidelines for the Information Technology Risk Management of Commercial Banks issued by the CBIRC (Yin Jian Fa [2009] No. 19)

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)

**3. Are there any specific contractual requirements for cloud outsourcing?**

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 sign a written contract with its outsourcing service provider. The contract should contain certain terms and conditions required by the CBIRC, and in particular requires the following from the outsourcing service provider:

Periodically reporting on the outsourcing services to the bank

Promptly reporting of any emergency to the bank

Cooperating with the bank in any CBIRC investigation

Keeping the services and customer information safe and confidential

Not carrying out any activity in the name of the bank, etc.

The outsourcing contract must also prohibit subcontracting of major aspects of the outsourcing activities to a subcontractor outside the service provider's group, and make the service provider responsible for its permitted subcontractor's performance.

Further requirements apply to IT outsourcing by banks. Under the Guidelines for the Information Technology Risk Management of Commercial Banks (Yin Jian Fa [2009] No. 19) and 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), a contract between an institution and its outsourcing service provider must be tailored to the particular services, risk assessment and due diligence investigation results, and must have certain minimum content, including the following:

Details of and arrangements for the services

Compliance with internal controls and laws and regulations

Service continuity

Risk assessments, monitoring, inspections, audits and cooperation (by and with both the institution and the CBIRC)

Provisions dealing with amendment, termination and transmission

Intellectual property arrangements

Provisions on resource guarantees

Service requirements on security, confidentiality and protection of consumers' rights and interests

Dispute resolution mechanisms and breach/indemnity clauses

Reporting mechanisms

Additionally, subcontracting of IT outsourcing services by a service provider to a third party is generally prohibited, unless the service provider undertakes the following in the service contract:

It will not subcontract or subcontract in disguise the main outsourced services to any third party.

In the case of permitted subcontracting, it will do the following:

Be responsible for the services rendered by the subcontractor and ensure that the subcontractor will strictly comply with the requirements in the contract entered between the bank and the vendor.

Monitor the subcontractor and report to and obtain approval from the bank in respect of any engagement or change of subcontractor.

Finally, in the case of cloud outsourcing, a financial institution is considered to have entrusted a cloud service provider to host data as an entrusted data processor. According to Article 21 of the PRC Personal Information Protection Law, the financial institution must agree with the cloud service provider on the purposes, duration, means of personal information processing, the categories of personal information involved, the data protection measures, and other relevant rights and obligations of the parties, to enable the financial institution to monitor the cloud service provider's personal information processing activities. In terms of data other than personal information, the draft Regulations on Network Data Security Management publicized by the Cyberspace Administration of China on 14 November 2021 have proposed similar requirements on the financial institution as a "data processor" in China.

In the case of disputes over the outsourcing contract, under 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), jurisdiction generally lies with the Chinese courts or arbitration institutions. PRC law (as the governing law) will apply.

**4. When does cloud outsourcing fall within the scope of the rules?**

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, "**Circular 44**") applies to outsourcing. According to Circular 44, if a banking financial institution established in China engages a service provider to continuously conduct certain business activities that fall within the scope of the bank's own responsibilities, such engagement is considered "outsourcing." Therefore, engaging a cloud service vendor for data storage and processing could be viewed as "outsourcing" under Circular 44.

The Circular 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) applies to "IT outsourcing" as a special category of "outsourcing." This is defined to broadly cover, among other things, hosting or operation and maintenance of data centers (server rooms) and other physical environments, data processing and data utilization activities, other business outsourcing activities, and IT activities in collaboration with third parties that involve processing important data or customers' personal information with banking and insurance institutions. Engaging a cloud service vendor for data storage and processing and hosting of server rooms is a common form of IT outsourcing in China. While the circular only directly applies to commercial banks and other banking financial institutions, insurance group (holding) companies, insurance companies, insurance asset management companies and financial asset management companies incorporated in China, the rules and requirements thereunder apply similarly to other financial institutions regulated by the CBIRC and its local counterparts.

**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.

**6. What are the potential consequences for breaching financial services rules on cloud outsourcing?**

Criminal liabilities are only imposed in extreme circumstances (e.g., where national security, public interest or financial market stability is threatened or where there are other serious consequences).

However, a breach of the outsourcing requirements described above can result in administrative sanctions, including but not limited to (i) a warning, (ii) a compulsory order from the China Banking and Insurance Regulatory Commission ("**CBIRC**") or its local counterparts to rectify and adopt remedial measures, (iii) fines, and (iv) in serious cases, revocation of a financial operating permit.

Additionally, if a financial institution infringes individuals' rights and interests as a result of noncompliance with the relevant outsourcing requirements, it will incur civil liability toward those individuals.

In addition, if the CBIRC or its local counterpart considers that the risk associated with a regulated outsourcing arrangement is substantial, it may take certain regulatory actions. These may include a suspension order.

**7. Are there any data privacy and/or data security laws that would apply?**

Yes. Currently, the main laws, regulations, rules and standards that include relevant data privacy and security requirements for financial institutions in China are as follows:

The PRC Cybersecurity Law

The PRC Data Security Law

The PRC Personal Information Protection Law

The Personal Financial Information Protection Technical Specification

The Financial Data Security — Guidelines for Data Security Classification

The Measures for the Security Assessment of Outbound Data Provision

The Announcement on the Implementation of Personal Information Protection Certification

The Measures for Standard Contracts for Outbound Personal Information Provision

The Implementing Measures of the People's Bank of China for Protection of Rights and Interests of Financial Consumers

The Measures for the Administration of Protection of Rights and Interests of Consumers of Banking and Insurance Institutions

**8. Are there any restrictions under local data protection laws that would impact the overseas hosting of data?**

Yes. Financial institutions in China may be subject to the following data residency requirements under current PRC laws:

**1. Local operation of core systems of commercial banks**

Under the Guidelines for the Information Technology Risk Management of Commercial Banks (Yin Jian Fa [2009] No. 19), a bank must independently operate its core systems (involving customer information, financial information and product information, etc.) in China. It must maintain the highest administrative permissions, enable the China Banking and Insurance Regulatory Commission ("**CBIRC**") to supervise and conduct an on-site inspection, and prevent cross-border risks. If core systems are still operated by a bank in China, but a copy of the data from these core systems is transmitted abroad (e.g., for central storage and processing by the overseas headquarters), arguably this data transmission and overseas storage will not constitute a violation of these requirements.

Therefore, for cloud services associated with the storage and processing of any personal financial information obtained in China, a financial institution should generally only engage a cloud service provider operating in China with servers located in China. The exception is in the case of a Chinese branch of a foreign bank where the relevant conditions imposed by the People's Bank of China ("**PBOC**") Shanghai Notice are met.

**2. Local residency requirement and restrictions on data export transfer applicable to personal information and important data of an operator of critical information infrastructure ("CII")**

The PRC Cybersecurity Law ("**CSL**") also requires that any **personal information** or **important data** collected and/or generated by a CII operator through its China operations must be **stored on servers within China**. As stated in Q&A 5 on "Does the outsourcing need to be notified to the regulator?", a financial institution may be regulated as a CII operator and, therefore, be subject to the data localization requirement under the CSL. In this context, "personal information" and "important data" are defined as follows:

"Personal information" includes all kinds of information recorded electronically or otherwise that relates to an identified or identifiable natural person, excluding anonymized information under the PRC Personal Information Protection Law (the "**PIPL**"). The mainstream view is that the personal information subject to the data residency requirement is that directly related to the operation of the relevant CII.

"Important data," which is not defined in the CSL, means "any data, the manipulation, damage, leakage, or illegal acquisition or use of which, once it takes place, may endanger national security, economy operation, social stability, public health and security etc." under the Measures for the Security Assessment of Outbound Data Provision issued by the Cyberspace Administration of China ("**CAC**") on 7 July 2022 ("**CBDT Assessment Measures**").

Local governments and industrial regulators will formulate specific catalogues of important data and organize data processors within their jurisdiction to identify their important data. For example, according to the Financial Data Security — Guidelines for Data Security Classification (JR/T 0197-2020), a set of **recommended industrial standards** issued by the PBOC on 23 September 2020 (with no mandatory force), the PBOC takes the position that (a) important data is data (including raw data and derivative data) that is closely related to national security, economic development and public interests, (b) important data **may include macro feature data, derivative feature data derived from massive information aggregation, data in the decision-making and law enforcement process of industry regulators, and information on network security defects in CII, etc.**, and (c) **an enterprise's production, operation and internal management information, and personal information is generally not considered important data**.

The CSL also provides that a CII operator must only provide personal information or important data overseas for "truly necessary" (this is not defined in the CSL) business reasons, and it must undergo a security assessment and obtain governmental clearance in accordance with the CBDT Assessment Measures ("**CAC Security Assessment**").

**3. Local residency requirement and restrictions on onward transfer applicable to personal information of a personal information operator that processes a large volume of personal information**

The PIPL, effective from 1 November 2021, further requires that any personal information processor ("**PIP**", akin to a controller in EU terminology) located in China that processes an over-the-threshold volume of personal information should also store the personal information it collects and/or generates through its China operations on servers within China. "Truly necessary" outbound provision of such personal information is generally subject to the CAC Security Assessment and other requirements under the PIPL and the CBDT Assessment Measures (including obtaining individuals' standalone consent).

Where the CAC Security Assessment is not triggered and applicable under the CSL, the PIPL and the CBDT Assessment Measures, a PIP in China (such as a financial institution in China) should either (i) pass a voluntary personal information protection certification by a qualified institution in China in accordance with the Announcement on the Implementation of Personal Information Protection Certification and its related rules, or (ii) conclude a data transfer contract based on the Standard Contract for Outbound Personal Information Provision ("**Standard Contract**") with the overseas recipient of personal information provided abroad ("**Overseas Recipient**") in accordance with the Measures for Standard Contracts for Outbound Personal Information Provision. These measures will take effect from 1 June 2023, and grant a six-month grace period until 30 November 2023 for rectification. The Standard Contract is prescribed by the CAC and provides for extensive personal information protection rights and imposes obligations on the parties to the Standard Contract. The PIP in China and the Overseas Recipient are only allowed to enter into supplemental agreements that are compatible with the Standard Contract. The executed Standard Contract, together with a personal information protection impact assessment report concerning the export of personal information, should be filed with the provincial office of the CAC for recordal within 10 working days after the Standard Contract takes effect.

**9. Does a cloud service provider need a financial services authorization or license to provide cloud services?**

Yes.

The provision of public cloud services and hybrid cloud services within the territory of China is strictly regulated. While there are no unified definitions of "public cloud," "private cloud" and "hybrid cloud" under current Chinese laws and regulations, and there are no clear rules to distinguish between IaaS, PaaS and SaaS, the mainstream view in China is that providing public cloud, hybrid cloud, private cloud (to multiple customers), IaaS or PaaS would generally be considered a form of regulated value-added telecommunications services ("**VATS**"), and some forms of SaaS may also fall within the scope of regulated VATS. Therefore, if cloud services to be procured and used by an entity operating in China are provided in China, the entity would generally request or expect that, to the extent applicable, the cloud service provider holds the relevant VATS operating license and complies with the industry standards for providing the relevant VATS issued by the regulator of telecommunications services.

In addition, cloud service providers that offer cloud computing platforms (including private clouds and group/public clouds) to financial institutions in China would also be expected by their financial institution customers to obtain a fintech product certification pursuant to the Rules on Certification of Fintech Products and other relevant rules. So far it appears that such product certification is not a market-entry-type license, but merely a nice-to-have certification that can bring more business opportunities to the cloud service providers.

The People's Bank of China (which is the central bank of China, "**PBOC**") issued the draft Measures for the Administration of Recordal of Financial Clouds (for Trial Implementation) to certain market players (rather than the general public) in June 2021. Reportedly, the PBOC proposed the following under those draft measures: (a) any public cloud or financial community cloud services (which refers to a cloud service used by several financial institutions at the same time) provided to financial institutions in China would be subject to a compulsory recordal with the National Internet Finance Association of China as designated by the PBOC; (b) financial institutions in China will not be allowed to use those cloud services without the recordal; and (c) the recordal for private cloud services provided to financial institutions would be voluntary.

**10. Is express consent from customers or other data subjects required before moving data to the cloud?**

Yes.

According to the Guidelines for the Information Technology Risk Management of Commercial Banks (Yin Jian Fa [2009] No. 19), when a bank's IT outsourcing involves its customers' materials, the bank must notify the relevant customers (whether institutional or individual customers). In terms of those institutional customers, whether the customers' authorization or consent is required depends on the bank's relevant policies and on confidentiality or other agreements with the clients.

From a general personal information protection law perspective, the PRC Personal Information Protection Law ("**PIPL**") does not require a personal information processor ("**PIP**", akin to a controller in EU terminology) (e.g., a financial institution) in China to obtain standalone consent from relevant individuals if the PIP merely **entrusts** a person (e.g., a cloud service provider) with processing relevant personal information pursuant to the agreed processing purpose, duration, method and other terms, provided that the entrusted processing falls within the scope of the original consent that the PIP obtained from relevant individuals. Moreover, the PIP will remain responsible for the processing activities. Use of cloud services may involve such entrusted processing of personal information because cloud service providers generally do not have discretion to decide the processing purposes and methods for personal information stored on their servers.

However, in relation to cross-border/outbound provision or transfer of personal information to an overseas recipient (whether it is a PIP or an entrusted processor), the PIPL requires the PIP in China to obtain the relevant data subjects' separate and informed consent. The data subjects must be informed of the overseas recipient's name, contact details, personal information processing purposes and methods, categories of personal information provided abroad, and the methods and procedures for the data subjects to exercise their rights under the PIPL, etc.

The consent should be revocable. After consent is revoked by a data subject, the financial institution would have to cease processing the data subject's personal information, unless such processing is based on a stipulated legal ground other than the data subject's consent such that it is necessary to conclude or perform a contract to which the individual is a party.

**11. Are there any local laws that require a cloud service provider to be able to access the data it hosts?**

No.

**12. Are there any local laws that would require a cloud service provider to disclose the data it hosts to any third parties in any circumstances (including regulatory or law enforcement authorities)?**

Yes.

**Procedural laws and regulations**, such as the PRC Civil Procedure Law, the PRC Criminal Procedures Law, the PRC Administrative Litigation Law and the Rules Concerning Several Issues Relating to Evidence in Administrative Procedure may give the people's courts, the people's procuratorate (public prosecutor), the national security bureaus and the public security bureaus statutory the power to request that a cloud service provider that is domiciled in China produce certain data (including financial institution data, if requested) as evidence in civil, criminal and administrative litigation and other legal proceedings. The cloud service provider will generally be obliged to accommodate such requests, unless it has reasonable grounds to assert that the authorities are abusing their powers or otherwise unlawfully demanding disclosure of the data.

**The PRC Administrative Penalties Law, the PRC Anti-Terrorism Law and the Cybersecurity Law** give PRC administrative authorities the ability to request disclosure of data (including financial institutions' data stored on the cloud service provider's servers) on legitimate grounds. A cloud service provider that is domiciled in China is obliged to cooperate with such request.

Conversely, according to the PRC Data Security Law, any organization or individual (such as a cloud service provider) in China is prohibited from providing any data it hosts within China to any foreign judiciary or law enforcement authority before it has obtained approval from the competent authority. The detailed procedure for obtaining such approval from the Chinese authority has not been announced.

# Permissibility of cloud

## 1. Are financial institutions legally permitted to use cloud services?

Yes, provided that the financial institution meets all the applicable legal requirements to use cloud services.

# Rules for cloud outsourcing

## 2. Are there any rules that apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?

Yes. As the use of cloud may constitute outsourcing (and more specifically, IT outsourcing), the following rules will be applicable:

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)

Guidelines for the Information Technology Risk Management of Commercial Banks issued by the CBIRC (Yin Jian Fa [2009] No. 19)

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)

# Contract requirements

## 3. Are there any specific contractual requirements for cloud outsourcing?

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 sign a written contract with its outsourcing service provider. The contract should contain certain terms and conditions required by the CBIRC, and in particular requires the following from the outsourcing service provider:

Periodically reporting on the outsourcing services to the bank

Promptly reporting of any emergency to the bank

Cooperating with the bank in any CBIRC investigation

Keeping the services and customer information safe and confidential

Not carrying out any activity in the name of the bank, etc.

The outsourcing contract must also prohibit subcontracting of major aspects of the outsourcing activities to a subcontractor outside the service provider's group, and make the service provider responsible for its permitted subcontractor's performance.

Further requirements apply to IT outsourcing by banks. Under the Guidelines for the Information Technology Risk Management of Commercial Banks (Yin Jian Fa [2009] No. 19) and 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), a contract between an institution and its outsourcing service provider must be tailored to the particular services, risk assessment and due diligence investigation results, and must have certain minimum content, including the following:

Details of and arrangements for the services

Compliance with internal controls and laws and regulations

Service continuity

Risk assessments, monitoring, inspections, audits and cooperation (by and with both the institution and the CBIRC)

Provisions dealing with amendment, termination and transmission

Intellectual property arrangements

Provisions on resource guarantees

Service requirements on security, confidentiality and protection of consumers' rights and interests

Dispute resolution mechanisms and breach/indemnity clauses

Reporting mechanisms

Additionally, subcontracting of IT outsourcing services by a service provider to a third party is generally prohibited, unless the service provider undertakes the following in the service contract:

It will not subcontract or subcontract in disguise the main outsourced services to any third party.

In the case of permitted subcontracting, it will do the following:

Be responsible for the services rendered by the subcontractor and ensure that the subcontractor will strictly comply with the requirements in the contract entered between the bank and the vendor.

Monitor the subcontractor and report to and obtain approval from the bank in respect of any engagement or change of subcontractor.

Finally, in the case of cloud outsourcing, a financial institution is considered to have entrusted a cloud service provider to host data as an entrusted data processor. According to Article 21 of the PRC Personal Information Protection Law, the financial institution must agree with the cloud service provider on the purposes, duration, means of personal information processing, the categories of personal information involved, the data protection measures, and other relevant rights and obligations of the parties, to enable the financial institution to monitor the cloud service provider's personal information processing activities. In terms of data other than personal information, the draft Regulations on Network Data Security Management publicized by the Cyberspace Administration of China on 14 November 2021 have proposed similar requirements on the financial institution as a "data processor" in China.

In the case of disputes over the outsourcing contract, under 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), jurisdiction generally lies with the Chinese courts or arbitration institutions. PRC law (as the governing law) will apply.

# Regulated cloud outsourcing

## 4. When does cloud outsourcing fall within the scope of the rules?

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, "**Circular 44**") applies to outsourcing. According to Circular 44, if a banking financial institution established in China engages a service provider to continuously conduct certain business activities that fall within the scope of the bank's own responsibilities, such engagement is considered "outsourcing." Therefore, engaging a cloud service vendor for data storage and processing could be viewed as "outsourcing" under Circular 44.

The Circular 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) applies to "IT outsourcing" as a special category of "outsourcing." This is defined to broadly cover, among other things, hosting or operation and maintenance of data centers (server rooms) and other physical environments, data processing and data utilization activities, other business outsourcing activities, and IT activities in collaboration with third parties that involve processing important data or customers' personal information with banking and insurance institutions. Engaging a cloud service vendor for data storage and processing and hosting of server rooms is a common form of IT outsourcing in China. While the circular only directly applies to commercial banks and other banking financial institutions, insurance group (holding) companies, insurance companies, insurance asset management companies and financial asset management companies incorporated in China, the rules and requirements thereunder apply similarly to other financial institutions regulated by the CBIRC and its local counterparts.

# Regulatory notifications

## 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.

# Consequences of regulatory breach

## 6. What are the potential consequences for breaching financial services rules on cloud outsourcing?

Criminal liabilities are only imposed in extreme circumstances (e.g., where national security, public interest or financial market stability is threatened or where there are other serious consequences).

However, a breach of the outsourcing requirements described above can result in administrative sanctions, including but not limited to (i) a warning, (ii) a compulsory order from the China Banking and Insurance Regulatory Commission ("**CBIRC**") or its local counterparts to rectify and adopt remedial measures, (iii) fines, and (iv) in serious cases, revocation of a financial operating permit.

Additionally, if a financial institution infringes individuals' rights and interests as a result of noncompliance with the relevant outsourcing requirements, it will incur civil liability toward those individuals.

In addition, if the CBIRC or its local counterpart considers that the risk associated with a regulated outsourcing arrangement is substantial, it may take certain regulatory actions. These may include a suspension order.

# Data privacy and security

## 7. Are there any data privacy and/or data security laws that would apply?

Yes. Currently, the main laws, regulations, rules and standards that include relevant data privacy and security requirements for financial institutions in China are as follows:

The PRC Cybersecurity Law

The PRC Data Security Law

The PRC Personal Information Protection Law

The Personal Financial Information Protection Technical Specification

The Financial Data Security — Guidelines for Data Security Classification

The Measures for the Security Assessment of Outbound Data Provision

The Announcement on the Implementation of Personal Information Protection Certification

The Measures for Standard Contracts for Outbound Personal Information Provision

The Implementing Measures of the People's Bank of China for Protection of Rights and Interests of Financial Consumers

The Measures for the Administration of Protection of Rights and Interests of Consumers of Banking and Insurance Institutions

# Overseas hosting

## 8. Are there any restrictions under local data protection laws that would impact the overseas hosting of data?

Yes. Financial institutions in China may be subject to the following data residency requirements under current PRC laws:

**1. Local operation of core systems of commercial banks**

Under the Guidelines for the Information Technology Risk Management of Commercial Banks (Yin Jian Fa [2009] No. 19), a bank must independently operate its core systems (involving customer information, financial information and product information, etc.) in China. It must maintain the highest administrative permissions, enable the China Banking and Insurance Regulatory Commission ("**CBIRC**") to supervise and conduct an on-site inspection, and prevent cross-border risks. If core systems are still operated by a bank in China, but a copy of the data from these core systems is transmitted abroad (e.g., for central storage and processing by the overseas headquarters), arguably this data transmission and overseas storage will not constitute a violation of these requirements.

Therefore, for cloud services associated with the storage and processing of any personal financial information obtained in China, a financial institution should generally only engage a cloud service provider operating in China with servers located in China. The exception is in the case of a Chinese branch of a foreign bank where the relevant conditions imposed by the People's Bank of China ("**PBOC**") Shanghai Notice are met.

**2. Local residency requirement and restrictions on data export transfer applicable to personal information and important data of an operator of critical information infrastructure ("CII")**

The PRC Cybersecurity Law ("**CSL**") also requires that any **personal information** or **important data** collected and/or generated by a CII operator through its China operations must be **stored on servers within China**. As stated in Q&A 5 on "Does the outsourcing need to be notified to the regulator?", a financial institution may be regulated as a CII operator and, therefore, be subject to the data localization requirement under the CSL. In this context, "personal information" and "important data" are defined as follows:

"Personal information" includes all kinds of information recorded electronically or otherwise that relates to an identified or identifiable natural person, excluding anonymized information under the PRC Personal Information Protection Law (the "**PIPL**"). The mainstream view is that the personal information subject to the data residency requirement is that directly related to the operation of the relevant CII.

"Important data," which is not defined in the CSL, means "any data, the manipulation, damage, leakage, or illegal acquisition or use of which, once it takes place, may endanger national security, economy operation, social stability, public health and security etc." under the Measures for the Security Assessment of Outbound Data Provision issued by the Cyberspace Administration of China ("**CAC**") on 7 July 2022 ("**CBDT Assessment Measures**").

Local governments and industrial regulators will formulate specific catalogues of important data and organize data processors within their jurisdiction to identify their important data. For example, according to the Financial Data Security — Guidelines for Data Security Classification (JR/T 0197-2020), a set of **recommended industrial standards** issued by the PBOC on 23 September 2020 (with no mandatory force), the PBOC takes the position that (a) important data is data (including raw data and derivative data) that is closely related to national security, economic development and public interests, (b) important data **may include macro feature data, derivative feature data derived from massive information aggregation, data in the decision-making and law enforcement process of industry regulators, and information on network security defects in CII, etc.**, and (c) **an enterprise's production, operation and internal management information, and personal information is generally not considered important data**.

The CSL also provides that a CII operator must only provide personal information or important data overseas for "truly necessary" (this is not defined in the CSL) business reasons, and it must undergo a security assessment and obtain governmental clearance in accordance with the CBDT Assessment Measures ("**CAC Security Assessment**").

**3. Local residency requirement and restrictions on onward transfer applicable to personal information of a personal information operator that processes a large volume of personal information**

The PIPL, effective from 1 November 2021, further requires that any personal information processor ("**PIP**", akin to a controller in EU terminology) located in China that processes an over-the-threshold volume of personal information should also store the personal information it collects and/or generates through its China operations on servers within China. "Truly necessary" outbound provision of such personal information is generally subject to the CAC Security Assessment and other requirements under the PIPL and the CBDT Assessment Measures (including obtaining individuals' standalone consent).

Where the CAC Security Assessment is not triggered and applicable under the CSL, the PIPL and the CBDT Assessment Measures, a PIP in China (such as a financial institution in China) should either (i) pass a voluntary personal information protection certification by a qualified institution in China in accordance with the Announcement on the Implementation of Personal Information Protection Certification and its related rules, or (ii) conclude a data transfer contract based on the Standard Contract for Outbound Personal Information Provision ("**Standard Contract**") with the overseas recipient of personal information provided abroad ("**Overseas Recipient**") in accordance with the Measures for Standard Contracts for Outbound Personal Information Provision. These measures will take effect from 1 June 2023, and grant a six-month grace period until 30 November 2023 for rectification. The Standard Contract is prescribed by the CAC and provides for extensive personal information protection rights and imposes obligations on the parties to the Standard Contract. The PIP in China and the Overseas Recipient are only allowed to enter into supplemental agreements that are compatible with the Standard Contract. The executed Standard Contract, together with a personal information protection impact assessment report concerning the export of personal information, should be filed with the provincial office of the CAC for recordal within 10 working days after the Standard Contract takes effect.

# Financial services authorizations licenses

## 9. Does a cloud service provider need a financial services authorization or license to provide cloud services?

Yes.

The provision of public cloud services and hybrid cloud services within the territory of China is strictly regulated. While there are no unified definitions of "public cloud," "private cloud" and "hybrid cloud" under current Chinese laws and regulations, and there are no clear rules to distinguish between IaaS, PaaS and SaaS, the mainstream view in China is that providing public cloud, hybrid cloud, private cloud (to multiple customers), IaaS or PaaS would generally be considered a form of regulated value-added telecommunications services ("**VATS**"), and some forms of SaaS may also fall within the scope of regulated VATS. Therefore, if cloud services to be procured and used by an entity operating in China are provided in China, the entity would generally request or expect that, to the extent applicable, the cloud service provider holds the relevant VATS operating license and complies with the industry standards for providing the relevant VATS issued by the regulator of telecommunications services.

In addition, cloud service providers that offer cloud computing platforms (including private clouds and group/public clouds) to financial institutions in China would also be expected by their financial institution customers to obtain a fintech product certification pursuant to the Rules on Certification of Fintech Products and other relevant rules. So far it appears that such product certification is not a market-entry-type license, but merely a nice-to-have certification that can bring more business opportunities to the cloud service providers.

The People's Bank of China (which is the central bank of China, "**PBOC**") issued the draft Measures for the Administration of Recordal of Financial Clouds (for Trial Implementation) to certain market players (rather than the general public) in June 2021. Reportedly, the PBOC proposed the following under those draft measures: (a) any public cloud or financial community cloud services (which refers to a cloud service used by several financial institutions at the same time) provided to financial institutions in China would be subject to a compulsory recordal with the National Internet Finance Association of China as designated by the PBOC; (b) financial institutions in China will not be allowed to use those cloud services without the recordal; and (c) the recordal for private cloud services provided to financial institutions would be voluntary.

# Customer data subject consent

## 10. Is express consent from customers or other data subjects required before moving data to the cloud?

Yes.

According to the Guidelines for the Information Technology Risk Management of Commercial Banks (Yin Jian Fa [2009] No. 19), when a bank's IT outsourcing involves its customers' materials, the bank must notify the relevant customers (whether institutional or individual customers). In terms of those institutional customers, whether the customers' authorization or consent is required depends on the bank's relevant policies and on confidentiality or other agreements with the clients.

From a general personal information protection law perspective, the PRC Personal Information Protection Law ("**PIPL**") does not require a personal information processor ("**PIP**", akin to a controller in EU terminology) (e.g., a financial institution) in China to obtain standalone consent from relevant individuals if the PIP merely **entrusts** a person (e.g., a cloud service provider) with processing relevant personal information pursuant to the agreed processing purpose, duration, method and other terms, provided that the entrusted processing falls within the scope of the original consent that the PIP obtained from relevant individuals. Moreover, the PIP will remain responsible for the processing activities. Use of cloud services may involve such entrusted processing of personal information because cloud service providers generally do not have discretion to decide the processing purposes and methods for personal information stored on their servers.

However, in relation to cross-border/outbound provision or transfer of personal information to an overseas recipient (whether it is a PIP or an entrusted processor), the PIPL requires the PIP in China to obtain the relevant data subjects' separate and informed consent. The data subjects must be informed of the overseas recipient's name, contact details, personal information processing purposes and methods, categories of personal information provided abroad, and the methods and procedures for the data subjects to exercise their rights under the PIPL, etc.

The consent should be revocable. After consent is revoked by a data subject, the financial institution would have to cease processing the data subject's personal information, unless such processing is based on a stipulated legal ground other than the data subject's consent such that it is necessary to conclude or perform a contract to which the individual is a party.

# Data access requirements

## 11. Are there any local laws that require a cloud service provider to be able to access the data it hosts?

No.

# Data disclosure requirements

## 12. Are there any local laws that would require a cloud service provider to disclose the data it hosts to any third parties in any circumstances (including regulatory or law enforcement authorities)?

Yes.

**Procedural laws and regulations**, such as the PRC Civil Procedure Law, the PRC Criminal Procedures Law, the PRC Administrative Litigation Law and the Rules Concerning Several Issues Relating to Evidence in Administrative Procedure may give the people's courts, the people's procuratorate (public prosecutor), the national security bureaus and the public security bureaus statutory the power to request that a cloud service provider that is domiciled in China produce certain data (including financial institution data, if requested) as evidence in civil, criminal and administrative litigation and other legal proceedings. The cloud service provider will generally be obliged to accommodate such requests, unless it has reasonable grounds to assert that the authorities are abusing their powers or otherwise unlawfully demanding disclosure of the data.

**The PRC Administrative Penalties Law, the PRC Anti-Terrorism Law and the Cybersecurity Law** give PRC administrative authorities the ability to request disclosure of data (including financial institutions' data stored on the cloud service provider's servers) on legitimate grounds. A cloud service provider that is domiciled in China is obliged to cooperate with such request.

Conversely, according to the PRC Data Security Law, any organization or individual (such as a cloud service provider) in China is prohibited from providing any data it hosts within China to any foreign judiciary or law enforcement authority before it has obtained approval from the competent authority. The detailed procedure for obtaining such approval from the Chinese authority has not been announced.

©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.