China Banking IT Regulation Tightened Up

By King & Wood Mallesons on March 16, 2015 Posted in Finance

By Banking Team King & Wood Mallesons

Overview

The China Banking Regulatory Commission ("**CBRC**") jointly with three other government departments promulgated the CBRC Guidance Opinions on the Use of Secure and Controllable Technology to Strengthen the Internet Security and Information Construction of Banking Industry (YINJIANFA (2014) No. 39, the "**CBRC Opinion**") on 3 September 2014. The Guidelines on Promoting the Use of Secure and Controllable Technology in Banking Industry (2014-2015) (YINJIANBANFA (2014) No. 317, the "**CBRC Guidelines**") were later issued on 26 December 2014, as the detailed implementing rules of the CBRC Opinion. Targeting to improve the information security in the banking sector and in a larger sense, the financial security of China, the CBRC Opinion and the CBRC Guidelines (collectively, the "**New Rules**") require that banks, within a specific timeframe, achieve a series of fixed targets in relation to applying "secure and controllable" IT products. This may have a significant impact on China's banking industry and thus have already fuelled concerns in the market.

1. Who is subject to the New Rules?

Based on the CBRC Guidelines, the New Rules shall be applicable to all the banking financial institutions set up in the PRC.

There have been different opinions in the market on whether or not foreign-invested banks, especially the PRC branches of foreign banks shall comply with the New Rules. Subject to the further clarifications of CBRC, it seems that a foreign-invested bank (no matter in the form of an independent legal person or a branch) shall fall into the category of the so-called "banking financial institutions set up in the PRC" and therefore shall keep in compliance with the New Rules, although the primary target of the regulator at the current stage to apply these New Rules to seems to be the former.

2. What is a "secure and controllable" IT product?

The New Rules define the "secure and controllable" IT products in a relatively broad way. Nonetheless, the appendix of the CBRC Guidelines (the "**Appendix**") divides IT products into 10 categories and more than 60 sub-categories (including various kinds of equipment, software and technical services), each with its own "secure and controllable" requirements set out in detail. An IT product thus shall only be deemed as "secure and controllable" if it satisfies its corresponding "secure and controllable" requirements specified in the Appendix. Some notable "secure and controllable" requirements include:

- **Local R&D & Service Centers** – The IT vendors are generally required to establish its own R&D & service centers in China.
- **Independent IP Right** – The IP right in relation to certain products shall be independent IP right owned or controlled by PRC citizens or institutions.
- **Source Code Filing** – The source code of certain products are required to be filed with CBRC.
- **Controllable Supply Chain** –The risk of product supply chain shall be controllable, which may equate to greater localization of the vendors.

3. Major requirements

The major requirements of the New Rules on banks are outlined as follows:

- **Proportion of the Use of "Secure and Controllable" IT Products** – The CBRC Opinion sets a goal that the proportion of "secure and controllable" IT products over the total IT products used by each bank should increase at least 15% each year, and reach a minimum of 75% by 2019. The Appendix further provides detailed usage proportion requirements for 2014-2015 on each category of IT products.
- **Plan Making and Submission** – Each bank is required to submit a plan to CBRC or its local branches by 15 March 2015, which includes its lead team and its strategic, overall and annual plans for the use of "secure and controllable" IT products.
- **Research Budget** – Each bank shall assign at least 5% of its budget for research on secure and controllable IT system every year.
- **IT Framework and Disaster Recovery Plan** – Each bank shall change its overarching IT framework into a more open and flexible one and complete a disaster recovery plan based on "secure and controllable" information technology by the end of 2015.
- **Annual Assessment by CBRC** – CBRC will conduct annual assessment on the IT security and controllability of the banks and their vendors.

4. Issues to be noticed / considered by banks

As a result of the New Rules, banking institutions may face a lot of new issues and challenges as we highlight below:

- **Overall Strategy** – Above all, banks may need to formulate an overall and short-term to long-term strategy before considering any contingent tactics to deal with any new issues

and challenges that may be brought about by the New Rules based upon a thorough understanding of what they really mean and an in-depth evaluation of their possible impacts.

- **Due Diligence on the Vendors** – Banks may need to conduct due diligence on their existing and potential vendors, to check whether the IT products provided by such vendors are in compliance with the New Rules. For the purpose of such due diligence, banks may consider designing a survey form and requesting the relevant vendors to fill in such forms.
- **Termination of the Existing Supplier/Service Agreements** – In case an existing vendor is unable to comply with the New Rules or is likely to leave the PRC market because of the New Rules, the banks may need to consider terminating the existing supplier or service agreements with the vendor. Such termination of agreements shall be carefully dealt with, in order to avoid incurring any liability on or any commercial claim against the banks.
- **Ensuring Continuity of Business** – In case a bank decides to replace the existing IT vendor with a new qualified one, it shall also carefully manage the transition and take necessaryn measures to ensure its business continuity is not affected.
- **Incorporating Relevant Clauses in the Supplier/Service Agreements** – Banks shall be more prudent when entering into new IT supplier/service agreements. It is advisable to have the vendors expressly undertake in the relevant agreements that they will comply with the "secure and controllable" requirements of CBRC from time to time, provide the assistance and cooperation which the banks may require for compliance purpose, and notify the banks as soon as it is aware that it may no longer be able to comply with the CBRC requirements.
- **Drafting of Internal Policies** – In addition to the plans submitted to the CBRC, banks shall make sure that the requirements under the New Rules are also taken into consideration in their relevant internal policies, e.g. the business continuity plan and the disaster recovery plan.
- **Compatibility of the Products Provided by Domestic Vendors** – The New Rules demonstrate a preference to the domestic vendors, though not in an express manner. Banks may thus consider turning to the domestic vendors more often, and as a practical issue, a bank (especially a foreign-invested bank) may need to make sure that its PRC-supplied IT system is compatible with its global IT system.
- **Future Change of Relevant Regualtions** – The CBRC Guidelines only set out the requirements for 2014-2015, which means that the relevant "secure and controllable" product requirements may be updated annually. It is therefore advisable for the banks to keep a close eye on the possible changes of the relevant CBRC rules.

CONTACT US

陈运（Yun Chen）
联系邮箱：chenyun@cn.kwm.com

王军（Jack Wang）
联系邮箱：jackwang@cn.kwm.com

陈胜(Sheng Chen)
联系邮箱：armstrong.chen@cn.kwm.com

郑立柱（Richard Zheng）
联系邮箱：zhenglizhu@cn.kwm.com