KPMG

cutting through complexity

Cyber Security and the Impact on Banks in China

Regulatory Policy Development and Updates

March 2015

kpmg.com/cn

KPMG
cutting through complexity

Executive Summary

The China Banking Regulatory Commission (CBRC) issued two circulars (Circulars No. 39 and No. 317) in 2014 regarding the use of 'secure and controllable IT', which require banks to strengthen their stance on cyber security. The issuance of these circulars will likely result in significant changes in the composition of technologies for banks in China. Under the guidance of various policies and supervision, relevant stakeholders, including financial institutions, technology firms, research institutes, industry alliances and technology service firms, will need to amend their business strategy in order to cope with the new requirements.

Regulatory requirement highlights:

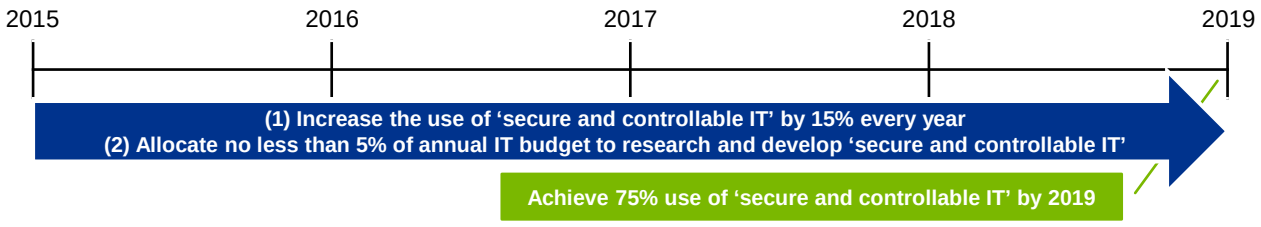
- By 2019, 75 percent of information technology (IT) should be 'secure and controllable'. This directive has now been clearly defined by the CBRC.
- Between 2015 and 2019, relevant guidance and requirements will be further defined, and corresponding evaluation criteria, safeguards, examination and supervision will be clearer to guide banks in complying with the stated circular.
- There are clear indications of a regulatory push for local development and innovations to drive 'secure and controllable IT' initiatives.

Actions for financial institutions:

Financial institutions will need to review and amend IT strategy and planning, management systems, governance structures, people management, innovation mechanisms, performance evaluations, system development, and technology procurement to drive effective compliance with the regulations. Banks in China should pay particular attention to the following areas:

- The governance system: There is an immediate need to set up a steering committee and relevant response team involving key business functions and work streams. This team will lead the work plan for 'secure and controllable IT' as well as implement this across the bank.
- Infrastructure development: The implementation of 'secure and controllable IT' should give priority to peripheral technologies (e.g. network, storage and security devices), followed by core technologies (e.g. mainframe computers). Therefore, the proportion of 'secure and controllable IT' applied in peripheral technologies should increase year-on-year, and investments in research and know-how of 'secure and controllable IT' should also increase.
- Supporting frameworks: Due to the regulations, banks' management frameworks, such as risk management and information security management frameworks, will be impacted directly. This will include the adjustment of the risk tolerance level, risk assessment framework and risk monitoring indicators, and the improvement of information security standards.

Action timeline:



KPMG
cutting through complexity

Cyber Security and the Impact on Banks in China

Regulatory Policy Development and Updates

Content

KPMG
cutting through complexity

Policy Background

1 Current State of China's Cyber Security

Internet finance, big data analytics and cloud computing are all developing across the China market. There is also an increasing awareness that business and personal information is at risk of leakage, theft or eavesdropping. Changes are therefore taking place in terms of how internet usage is evolving and how developments should be controlled.

Cyber security has become an important national concern for China. The Chinese Government has escalated cyber security to national strategic development level, supervised directly under China's leadership.

In recent years, the internet in China has evolved and security policies around IT networks have been driven using a top-down approach. Government and regulatory bodies have issued various policies to govern the security and controllability of IT and the development of the internet, with the aim of mitigating risks as a result of internet growth and IT developments.

China's Strategic Deployment

The Chinese Government has escalated cyber security issues to a national strategy level, as it has been faced with the general public's rapid adoption of internet technologies, and complications arising from high-profile international and local security incidents:

- In July 2012, China's State Council issued *Suggestions of the State Council on Promoting the Development of Informationization and Ensuring Information Security* (《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》) [1] which stipulates the decision by the council to **escalate information security matters to the same level as that of technology development nationally**.
- In November 2013, the National Security Council was officially formed, with China's President Xi Jinping named as president of the council. [2] **Information security was again confirmed as a matter of national strategy,** demonstrating the desire of the country's leadership to safeguard China's information security.
- In February 2014, **the Central Leading Group for Cyberspace Affairs** was established, with China's President Xi Jinping named as group president. [3]

The CBRC has since released two policies governing the security and controllability of cyber development:

– CBRC Circular No. 39, *Guiding Principles on Strengthening the Banking Network Security and Information Technology Infrastructure through Secure and Controllable IT* (《关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见》(银监发〔2014〕39号)

– CBRC Circular No. 317, *Guidelines on Promoting the Application of Secure and Controllable IT (Year 2014-2015)* (《银行业应用安全可控信息技术推进指南(2014—2015年度)》 (银监办发〔2014〕317号))

In this publication, we highlight the key points of these policies and provide suggestions for implementation by banks in China.

[1] Source: 'Suggestions of the State Council on Promoting the Development of Informationization and Ensuring Information Security', 17 July 2012, http://www.gov.cn/zwgk/2012-07/17/content_2184979.htm
[2] Source: 'Bulletin of the Third Plenary Session of the 18th Central Committee of the Communist Party of China', 14 November 2013, http://news.xinhuanet.com/house/tj/2013-11-14/c_118121513.htm
[3] Source: 'Establishment of the Central Leading Group for Cyberspace Affairs', 28 February 2014, http://news.xinhuanet.com/info/2014-02/28/c_133148759.htm

KPMG
cutting through complexity

Abstract of Related Policies for the Banking Industry

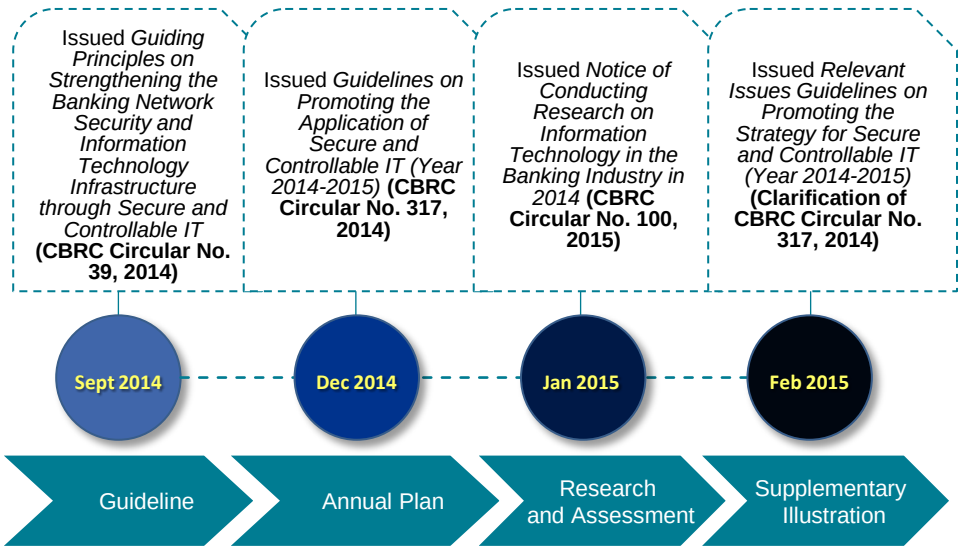
1 Current State of China's Cyber Security

- **The Chinese Government** is focusing on information security strategies. The establishment of the National Security Council and the Central Leading Group for Cyberspace Affairs demonstrates that the Chinese Government has escalated the issue of system and cyber security to the national strategy level.
- **Regulatory bodies** – particularly the banking regulatory body, the CBRC – have responded to the security strategies and have issued related guiding principles and guidelines to support the need to protect 'secure and controllable IT' systems, providing clarity of accountability and required timelines for implementation.
- **Financial institutions**, under the requirements defined by the CBRC, need to develop plans for implementing 'secure and controllable IT' systems, with a particular emphasis on the ability to take control of the know-how and development of various technologies implemented locally in China.
- **IT companies** developing products locally within the China market are maturing, with innovations and products becoming widely adopted locally. This has challenged the dominant role of foreign technology companies. A key focus will be how technology firms provide open-source architecture, and/or ensure that their technologies meet the government's concept of 'secure and controllable IT'.

Objectives of the 'secure and controllable IT' principle:

- IT shall become secure and within the control of management; critical information systems shall have the ability to be independently controlled by the organisation.
- Research and development on locally grown application systems should be enhanced.
- Core and fundamental technologies shall not be externally reliant.
- Information security shall be upheld.
- Cost of ownership shall be lowered.

Policies relating to the application of 'secure and controllable IT' as issued by the CBRC for the banking industry:



- Long-term plan for the adoption of 'secure and controllable IT'
- Secure and controllable technology infrastructure
- Development and collaboration
- Research and development to focus on local innovation of IT

- Objectives, tasks and requirements, and major measures for 'secure and controllable IT'
- IT asset categories and security and controllability indicators
- Evaluation criteria and mechanisms
- Relevant safeguards

- Research on the safety and controllability of technology
- Self-assessment

- Clarification on source code filing
- Clarification on software owning independent intellectual property rights
- Clarification of the national differences

KPMG
cutting through complexity

Abstract of CBRC Circular No. 39, 2014

2 Policy Development and Interpretation


中国银监会
国家发展改革委
科技部
工业和信息化部 文件

银监发〔2014〕39号

关于应用安全可控信息技术加强
银行业网络安全和信息化建设的指导意见

各银监局，各省（自治区、直辖市及计划单列市）发展改革委、科技厅（委、局）、工业和信息化主管部门，各政策性银行、国有商业银行、股份制商业银行、金融资产管理公司，邮政储蓄银行，各省级农村信用联社，银监会直接监管的信托公司、企业集团财务公司、金融租赁公司：

为进一步贯彻落实创新驱动发展战略，提升银行业网络安全保障能力和信息化建设水平，推动银行业深化改革、发展转型，促

— 1 —

Abstract for Circular No. 39

Guiding Principles on Strengthening the Banking Network Security and Information Technology Infrastructure through Secure and Controllable IT (CBRC Circular No. 39, 2014) ("the CBRC Guidelines"):

- The CBRC Guidelines were jointly issued by the CBRC, National Development and Reform Commission (NDRC), Ministry of Science and Technology, and Ministry of Industry and Information Technology.
- The overall objective proposed is a medium- to long-term policy to accelerate the localisation of domestic IT in the banking industry, and a proposal to reach a 75 percent usage of 'secure and controllable IT' within banks in China by 2019.
- The CBRC guidelines also focus on the need for banks to establish an innovation ecosystem. Banks shall not only maintain control of the technology infrastructure installed, but also drive a development and innovation life cycle and work together with the IT sector to establish an alliance.

KPMG
cutting through complexity

Interpretation of CBRC Circular No. 39

2 Policy Development and Interpretation

Overall Objectives

A long-term plan should be in place for the adoption of 'secure and controllable IT' within banks in China. This plan should be supported by policies, standards and full implementation. By 2019, banks in China should have the following in place:

- The knowledge and know-how of core information technologies implemented within the bank
- A reasonable distribution of key network and application infrastructure such that the key infrastructure and services used will not pose a concentration risk for the bank
- A target of 75 percent coverage for the overall utilisation rate of 'secure and controllable IT'
- The continuing evolution and improvement of the development of IT, with the overriding aim of protecting consumer rights, and the stability of society and the economy.

Secure and Controllable IT

The concept of 'secure and controllable IT' means that in addition to satisfying the system and cyber security needs of banks, the following is also satisfied: knowledge, outsourcing and supply chain risks such that financial institutions are in control of the know-how of the deployed technology.

Specific Tasks and Requirements

- There should be a well-defined IT governance structure within a bank.
- The technology infrastructure within a bank should be constantly improved.
- Technology investments should be prioritised, with 'secure and controllable IT' technologies given priority.
- There should be research and development within banks to focus on local innovation for IT.
- Proactive research and development of 'secure and controllable IT' should be performed.
- The establishment of intellectual property rights should be enhanced to protect IT rights.

Two Quantifiable Indicators

- From 2015, each financial institution should increase the use of 'secure and controllable IT' by **no less than 15 percent** every year, until they reach an overall objective of 75 percent implementation in 2019.
- From 2015, financial institutions should allocate no less than **5 percent** of their annual IT budget to forward-looking, innovative and structured research on the use of 'secure and controllable IT'.

KPMG
cutting through complexity

Interpretation of CBRC Circular No. 39

2 Policy Development and Interpretation

The CBRC Guidelines require financial institutions to fulfil the needs of information security while maintaining control over three key risk areas.

Implementing 'secure and controllable IT' means satisfying system and cyber security needs from banks, while also mitigating technology, outsourcing and supply chain risks.

— Guiding Principles on Strengthening the Banking Network Security and Information Technology Infrastructure through Secure and Controllable IT

(CBRC Circular No. 39, 2014)

The CBRC Guidelines identify that banks should have a long-term plan in place for the adoption of 'secure and controllable IT'. This plan should be supported by policies, technology standard settings and full implementation so as to fulfil the information security requirements in financial institutions and effectively control technology risks, outsourcing risks and supply chain risks.

Information Security Requirements

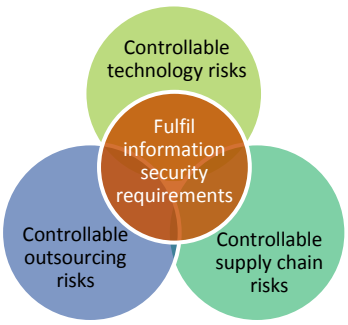
Information security is an element of technology risk management and is part of a wider risk management framework. It is defined in the information security requirements of *Guidelines on the Information Technology Risk Management for Commercial Banks* issued by the CBRC in 2009. This policy defines the information security requirements for banks in nine aspects: staff's security awareness, management functions, security strategy, access control, security domain, system security, encryption, end-point security and information life cycle management.

Technology Risk

Technology risk refers to inherent and operational risks derived from the use of IT. IT assets within a financial institution should largely be categorised into 10 categories and 68 subcategories, including IT hardware, software, service assets and network. Detailed categories are available in the appendix to *Guidelines on Promoting the Application of Secure and Controllable IT (Year 2014-2015)*.

According to the circular, financial institutions should identify, monitor and control technology risks, and develop a road map to adopt 'secure and controllable IT'.

IT companies should therefore support financial institutions to identify technology risks, and provide sufficient knowledge, skills and technical support for banks to identify and take control of technical risks.



Outsourcing Risk

Outsourcing risk refers to the risk of loss of technology know-how, rendering business interruptions or information leakage due to outsourcing. Financial institutions should conduct outsourcing risk management in accordance with relevant requirements in *Supervision Guidance on Information Technology Outsourcing Risks in Financial Institutions* (CBRC Circular No. 5, 2013) and *Notice on Strengthening Management of Off-Site and Centralised Outsourcing Risks in Banking Institutions* (CBRC Circular No. 187, 2014).

Supply Chain Risk

Supply chain risk refers to the inability to obtain the necessary maintenance, support, upgrade or other services due to the disruption of the supply of products/services or limitations of intellectual property. According to the circular, financial institutions should enhance their supply chain management for core technologies by proactively implementing 'secure and controllable IT'.

KPMG
cutting through complexity

Interpretation of CBRC Circular No. 317

2 Policy Development and Interpretation

CBRC Circular No. 317 requires banks to establish formal IT asset inventory records and determine targets for implementing 'secure and controllable IT'.

Summary of Circular No. 317

Guidelines on Promoting the Application of Secure and Controllable IT (Year 2014-2015) (CBRC Circular No. 317, 2014):

- This circular was jointly compiled by the CBRC and Ministry of Industry and Information Technology.
- It includes an annual work plan for adopting 'secure and controllable IT', defining what it is, and refining the work objectives and requirements for 2015.
- The circular emphasises the need for development in applications and research. It not only requires banks to enhance security and controllability of IT, but also puts forward requirements on the research and development of system security and controllable IT.

By 2019, the proportion of 'secure and controllable IT' should reach 75 percent

IT asset categories

The CBRC has published an IT asset catalogue that classifies IT assets into 10 categories and 68 subcategories. Each category of IT assets is identified by a unique category code with names and descriptions. The security and controllability requirement for each category and subcategory of IT assets has been clearly defined.

Indicators of 'secure and controllable IT'

In assessing the security and controllability of IT, banks should consider the purpose of the application and follow evaluation methods as stipulated in the appendix of Circular No. 317. Banks should progressively achieve the aim of 'secure and controllable IT' with the suggested approaches below:

1) **Focus on new developments, then assess the existing situation**
In 2015, banks should focus on implementing 'secure and controllable IT'. At the same time, according to CBRC Circular No. 39 requirements, they should increase the use of 'secure and controllable IT' by at least 15 percent a year, with a target of 75 percent by 2019.

2) **Focus on market mature products, then focus on development**
In 2015, market mature products such as network devices, storage devices, and medium to low-end servers should be prioritised. For other products such as operating systems, mainframes/minicomputers and databases, research and development efforts should be in place so that technology infrastructure can progressively reduce the reliance on high-end complex servers and be replaced by open-source x86 server clusters.

Requirements of 'secure and controllable IT'

With a focus on openness, applicability and transparency of IT, products and services, IT companies should progressively make available their core technology know-how, and share intellectual property rights accordingly. For foreign technology firms, this can be achieved via joint venture or joint research and development with Chinese firms. This is to ensure the continuation of services and that Chinese financial institutions can solve security issues as they arise.

KPMG
cutting through complexity

Interpretation of CBRC Circular No. 317

2 Policy Development and Interpretation

Critical information systems have been defined as:
1) systems that support the critical processes of an organisation and where the security and service reliability have a direct impact on the general rights and interests of Chinese citizens, legal persons and other organisations within China; or 2) systems that are of public interest, or that relate to the order of Chinese society, and to national security concerns.

These systems largely include systems that are customer-facing, and which are involved in business operations, channels, and customer risk management. Associated infrastructure, such as computer rooms, and networks that support the operation of these systems, are also considered critical information systems.

— Notice on issuing the Measures for the Commissioning and Change of Important Information Systems of Banking Institutions (CBRC Circular No. 437, 2009)

The core business processing of banks that relies on closed-source systems will need to be changed. Closed-source systems, such as proprietary mainframe computers, have created a challenge, as obtaining a working knowledge of these systems and access to the source code (including operating systems, middleware and database programs) have been restricted. In certain situations, it has been considered difficult to solve problems arising from these closed-source systems, which can hinder the security and controllability of IT for banks in China.

In order to achieve 'secure and controllable IT', the banking industry will need to explore and address issues resulting from stability, capacity, security and risk management on the technical level by progressing towards an open-source architecture. The CBRC encourages a gradual and steady implementation strategy for 'secure and controllable IT', and this technology architecture transformation will likely impact the Chinese banking industry for a certain period of time.

The CBRC requires banks to establish a self-evaluating mechanism on the level of achievement with respect to 'secure and controllable IT'.

Based on CBRC Circular No. 100, *Notice of Conducting Research on Information Technology in the Banking Industry in 2014*, each financial institution will need to perform a self-assessment on its level of 'secure and controllable IT' using the evaluation criteria as well as the categories defined in the appendix to CBRC Circular No. 317. Such self-assessment should include, among others, the total number of IT devices, the manufacturers of the IT devices and the country of origin of the manufacturers. This information will need to be submitted to the CBRC.

KPMG
cutting through complexity

Interpretation of CBRC Circular No. 317

2 Policy Development and Interpretation


中国银行业监督管理委员会
CHINA BANKING REGULATORY COMMISSION
树立监管权威 提高监管有效性
当前位置：中国银行业监督管理委员会 > 政务信息 > 公告通知

发布时间：2015-02-12 文章来源：信科部 文章类型：原创

关于《银行业应用安全可控信息技术推进指南（2014—2015年度）》
（银监办发〔2014〕317号）
的相关说明

2014年银监会会同工信部发布了《银行业应用安全可控信息技术推进指南（2014—2015年度）》（银监办发〔2014〕317号），现就有关事项进一步说明如下：

一、源代码备案具体工作还在研究中，备案方式和流程将在充分听取各方意见后实施。

二、在银行业范畴以内，关于随机软件拥有自主知识产权，现阶段只要求供应商提供软件的知识产权证明或合法来源证明。

三、相关要求不存在国别差别。

On 12 February 2015, the CBRC issued further clarification on Circular No. 317 to provide clarity on the requirements for source code filing and the management of intellectual property rights.

- With respect to source code filing, including mainframe, operating system, middleware and database, the supplementary guidance indicates that the controllability requirement can be subject to negotiation with the CBRC, and that further market consultation will be performed before actual implementation.

- The requirement to share intellectual property rights has been relaxed. Software firms supplying bundled software will only need to provide intellectual property rights certifications or certificates of origin. This allows foreign developed IT products to continue to be recognised as ‘secure and controllable IT’ for banks.

- It is emphasised that when selecting ‘secure and controllable IT’, banking institutions do not necessarily need to consider product nationality. Foreign technology firms can also be considered as candidates for ‘secure and controllable IT’, in terms of sharing core technology know-how, enhancing cooperation and communication, and participating in joint development and joint innovation of technology.

KPMG
cutting through complexity

Contact Us

All banks in China will need to assess the impact resulting from the implementation of 'secure and controllable IT' by performing an inventory analysis to understand current technology infrastructure and gaps in the stated requirements. Plans and a road map will need to be put in place to define the activities for 2015-2019 and a remodelled governance structure is required to address potential gaps arising from local developments and innovations for banks' IT systems. KPMG China has dedicated teams focusing on security that can help you navigate these complex requirements.

For inquiries related to the CBRC circulars, please contact us:

Beijing

Benson Tran
Partner, Management Consulting

T: +8610 8508 5413
E: benson.tran@kpmg.com

Kevin Liu
Partner, Management Consulting

T: +8610 8508 7094
E: kevin.liu@kpmg.com

Shanghai

Reynold Liu
Partner, Management Consulting

T: +8621 2212 3626
E: reynold.jg.liu@kpmg.com

Richard Zhang
Director, Management Consulting

T: +8621 2212 3637
E: richard.zhang@kpmg.com

Hong Kong

Henry Shek
Partner, Management Consulting

T: +852 2143 8799
E: henry.shek@kpmg.com

Shenzhen

Kelvin Leung
Partner, Management Consulting

T: +86 755 2547 3338
E: kelvin.oc.leung@kpmg.com

KPMG

cutting through complexity