KPMG
cutting through complexity

IT Regulatory Compliance – What's the next 'Big Thing'?

The **evolving** compliance landscape

Based on the recent supervisory activities of the Hong Kong Monetary Authority (HKMA) and the Securities and Futures Commission (SFC), it is evident that the regulators are increasing their focus on regulatory requirements for information technology.

In particular, the HKMA issued a circular on 12 August 2014 extending its guidance on incident responses to system disruptions and system maintenance. Furthermore, the SFC updated its Code of Conduct this year to include more focused regulations for system controls and the security of electronic trading platforms.

With the rapid adoption of technology to support business activities, we expect that regulators will continue to strengthen their regulations through the issuance of new requirements and on-site examinations to ensure the safety and soundness of banks' IT systems.

TOP 5 REGULATORY FOCUSES

1. ***Customer data protection***
2. ***Bring-your-own-device (BYOD)***
3. ***Cloud computing security***
4. ***Electronic banking and cybersecurity***
5. ***Operational and IT controls over rogue trading***

Emerging regulatory focus

Customer Data Protection

In light of the rapid advancement in data loss protection (DLP) technologies, as well as a number of recent high-profile customer data leakage incidents, the HKMA reinforced its requirements regarding the handling of customer data through the issuance of a new *Customer Data Protection* circular in October 2014. The latest circular introduces a number of new customer data protection requirements, including the use of an automatic detection mechanism for the unauthorised data transfer of customer data through emails, identification of customer data in a bank's network, and regular audits by an independent party to ensure the adequacy of data protection controls.

Bring-your-own-device (BYOD)

In the past, bank staff were not allowed to use their own computing equipment (i.e. smartphones and personal computers) for storing or accessing the bank's emails and customer data. Following the issuance of the HKMA's new *Customer Data Protection* circular in October 2014, this requirement has been relaxed. The use of staff-owned computer equipment for work purposes is allowed as long as there are appropriate controls in place which comply with the requirements stipulated by the Hong Kong Association of Banks (HKAB).

3 *Cloud Computing Security*

With the recent change in regulatory stance regarding banks' adoption of cloud computing, a number of banks have been migrating their non-critical IT functions to the cloud. In view of the recent high-profile security breaches of a number of well-known cloud service providers, we expect the regulators to closely monitor the adoption of cloud services by banks and fine-tune the security requirements for the use of cloud technology accordingly.

4 *Electronic Banking and Cybersecurity*

Over the past years, we have observed a rise in cybersecurity threats and new technologies being adopted for electronic banking. The HKMA issued the Supervisory Policy Manual (SPM), *TM-E-1 Supervision of E-banking,* in 2004, which set out the minimum control standards for e-banking platforms over the past 10 years. While a number of circulars have been issued to supplement TM-E-1, the SPM content has remained unchanged.

In view of emerging cyberattack techniques such as distributed denial of service attacks and advanced persistent threats, as well as newly adopted banking channels such as mobile banking, we expect regulators to refresh the e-banking guidelines to keep abreast of these changes in the industry. Banks should consider adopting best practices with regard to e-banking and cybersecurity to protect their infrastructure, and take heed of the upcoming regulatory changes.

5 *Operational and IT Controls over Rogue Trading*

A number of high-profile rogue trading incidents have occurred in recent years, leading to significant losses for a number of banks. Such incidents revealed loopholes in risk management governance and technology infrastructures, as well as deficiencies in trading surveillance. As a result, both the SFC and HKMA have increased efforts to ensure that banks strengthen their controls over electronic trading, with a particular focus on rogue trading. We expect the HKMA and SFC to continue reinforcing the relevant control requirements through their regular supervision activities (e.g. on-site examinations).

How to **prepare** yourself

We expect many of the regulation changes mentioned above to be implemented by mid-2015. Based on your level of maturity, you may need to consider the following:

1. **Do you understand the emerging requirements?**
2. **Are you aware of the gaps in your organisation?**
3. **Do you have a plan to respond?**

For more information regarding the emerging regulatory requirements, please contact one of our Information Protection and Business Resilience team leaders.

Henry Shek
Partner, Advisory
KPMG China
T: +852 2143 8799
E: henry.shek@kpmg.com

Kelvin Leung
Senior Manager, Advisory
KPMG China
T: +852 2847 5052
E: kk.leung@kpmg.com

Alvin Li
Senior Manager, Advisory
KPMG China
T: +852 2978 8233
E: alvin.li@kpmg.com

Sidney Kwong
Manager, Advisory
KPMG China
T: +852 2847 5177
E: sidney.kwong@kpmg.com