KPMG

Managing Your IT Service Providers

The HKMA's requirements on IT supplier risk management

kpmg.com/cn

Over the past few years, the banking industry has experienced unprecedented change brought upon by various external and internal factors. Tightened banking regulations, coupled with mounting pressure to achieve business growth while reducing costs, has prompted many banks to reassess their overall business strategy. For years, banks have outsourced/offshored various back office functions, such as data centres and IT support, to save costs. As the banking business continues to evolve, outsourcing has grown beyond cost savings to address various business and regulatory initiatives such as the "follow the sun" trading model, recovery planning and data centralisation. Since many of these new initiatives involve the use of technology, it has led to more sophisticated technology outsourcing arrangements where systems are being hosted and maintained across different jurisdictions around the world.

In Hong Kong, banks are required to comply with the "Supervisory Policy Manual – Outsourcing (SA-2)" issued by the Hong Kong Monetary Authority (HKMA) with respect to outsourcing activities. The HKMA has also issued Risk Assessment Forms specifically for technology outsourcing (e.g. outsourcing of system maintenance and administration) and the use of public clouds. Banks are required to fulfil the HKMA outsourcing requirements and notify the HKMA prior to commencing the outsourcing arrangements. Do your outsourcing policies and framework adequately meet the HKMA outsourcing requirements?

Quick Compliance Check

- ❑ *Does your outsourcing policy/framework meet all applicable HKMA outsourcing requirements?*
- ❑ *Is your business/IT/compliance department aware of the HKMA's outsourcing requirements?*
- ❑ *Do you know when and how to notify the HKMA regarding new outsourcing initiatives?*
- ❑ *Do you have an outsourcing register to record and manage all outsourcing activities?*
- ❑ *Do you have a framework to assess the ability and performance of your technology service providers?*
- ❑ *Do you perform regular audit for outsourcing management?*

Common Questions about Technology-Related Outsourcing

Based on our experience working with various banking clients, it is common for banks to be uncertain about whether their outsourcing activities should be reported to the HKMA. Hence, we have provided some typical questions and answers below:

What kind of technology-related outsourcing should be reported to the HKMA?

All outsourcing arrangement material related to the bank's operations should be reported to the HKMA via a Notification Letter. The Notification Letter should include, among other items, information regarding the service to be outsourced, the service provider, date of outsourcing, and whether the HKMA's SA-2 requirements have been observed and complied with. In general, a notification letter should be submitted to the HKMA 3 months prior to the commencement of the outsourcing activity.

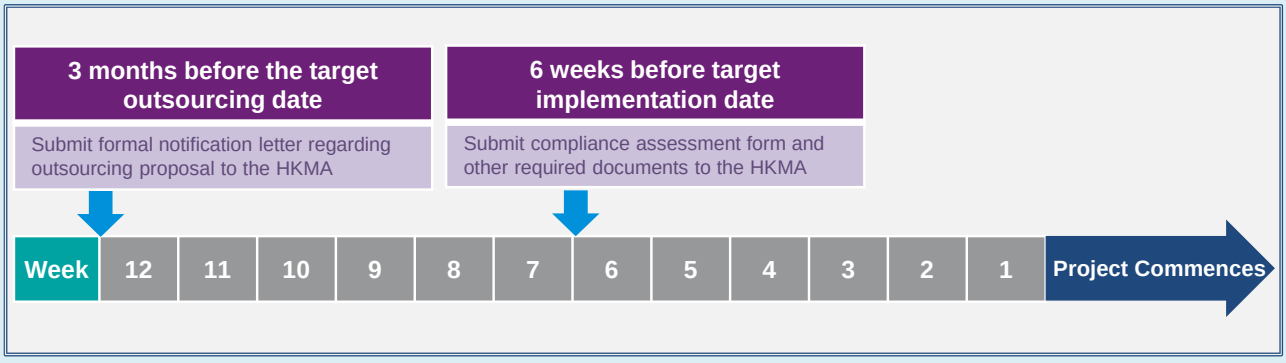
For technology-related outsourcing, the bank should first assess whether the technology/system being outsourced is (1) critical to the bank; or (2) involves sensitive customer data. For outsourcing of technology/systems that are critical to the bank or involve sensitive customer data, the bank should complete the relevant Risk Assessment Forms for technology-related outsourcing and submit them to the HKMA. In general, such Risk Assessment Forms should be submitted to the HKMA 6 weeks prior to the commencement of the outsourcing activity.

Do banks need to perform an independent assessment for technology-related outsourcing?

Yes. For outsourcing of technology/systems that are critical to the bank or involve sensitive customer data, banks should perform an independent assessment of the outsourcing arrangement according to requirements #4 and #5 of the Risk Assessment Forms for technology-related outsourcing. In general, external auditors, risk management or internal audit functions of banks can be admitted as an independent party to perform the assessment.

What is the timeline for HKMA submission and acknowledgement?

A high level timeline regarding the submission of information to the HKMA is depicted below.



Technology-related Outsourcing Best Practices

Regulators in the Asia-Pacific region are stepping up their outsourcing supervision efforts, and KPMG has been assisting a number of banks to comply with the regulatory requirements of different jurisdictions. The following are some best practices to address the concerns of different regulatory requirements.

1 A Clearly Defined Outsourcing Control Framework

Banks should demonstrate that a control framework to monitor and manage outsourcing risk is aligned with the regulatory requirements (e.g. SA-2), and the framework is clearly articulated in the relevant risk management policies and documents. The control framework should be designed with roles and responsibilities that align with the regulatory requirements, and should be transferable to be adopted, tailored and used by entities across other jurisdictions. The following key elements should be included in the control framework:

- Outsourcing Governance
- Risk Assessment
- Outsourcing Due Diligence
- Outsourcing Agreement Management
- Customer Data Management
- Contingency Planning & System Resilience
- Monitoring Outsourced Activity

2 Materiality Assessment

Banks should develop a set of criteria based on their business model and the regulatory requirements for classifying and identifying the critical outsourcing activities. Management can then assess the risk for each outsourcing activity and implement commiserating controls to manage the risks.

3 Comprehensive Outsourcing Register

Banks should maintain a comprehensive "outsourcing register" that includes all the activities outsourced/offshored to other entities. The objective of maintaining such a register is to support management's oversight and tracking of outsourced activities.

4 Service Provider Management

Regulators expect banks' management to be responsible for all outsourcing activities and to proactively manage the risk of such activities. Due to different regulatory requirements in different jurisdictions, the technology or outsourcing controls imposed by the home regulator may not be followed by the service provider offshore. Banks should perform a regular assessment on the critical service providers to confirm whether the regulatory requirements imposed by the home regulators are effectively followed.

How can KPMG help?

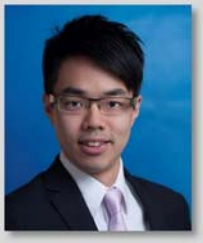
KPMG has assisted numerous banks in Hong Kong with defining and evaluating their outsourcing framework. Our team has in-depth knowledge and experience in regulatory compliance, and can provide banks with a wide range of support regarding technology-related outsourcing:

Outsourcing Controls Framework Advisory	• Review the outsourcing control framework including the relevant policies and procedures • Identify the control gaps and provide recommendations according to the SA-2
Review of Materiality Assessment	• Evaluate the criteria against the relevant materiality principles stated in the SA-2 • Validate the result of the materiality assessment
Review of Outsourcing Register	• Review the completeness and accuracy of the outsourcing register • Assess the controls over the maintenance of the outsourcing register
Regulatory Reporting and Advisory	• Perform independent assessments of outsourcing activities • Support banks in handling queries from the HKMA

Contact us

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

Kelvin Leung
Director
IT Advisory
KPMG China
T: +852 2847 5052
E: kk.leung@kpmg.com



Alvin Li
Associate Director
IT Advisory
KPMG China
T: +852 2978 8233
E: alvin.li@kpmg.com

kpmg.com/cn

Publication date: July 2016