Overview of Singapore MAS Technology Risk Management (TRM) Guidelines and Notices
September 2013

With rapid advancements in technology, financial institutions (“FIs”) rely increasingly on IT to operate their business activities and commercial functions, in order to meet their customers’ needs and requirements.

To better address existing and emerging technology risks faced by FIs, the Monetary Authority of Singapore (“MAS”) conducted a public consultation in June 2012 inviting views on a new set of technology risk management guidelines to update and consolidate the MAS Internet Banking and Technology Risk Management Guidelines (“IBTRM Guidelines”), and a new notice on technology risk management setting out certain mandatory requirements. Following the public consultation, MAS issued the Technology Risk Management Guidelines (“TRM Guidelines”) and Technology Risk Management Notices (“TRM Notices”) on 21 June 2013.

Introduction to TRM Guidelines and TRM Notices
The TRM Guidelines consolidates the IBTRM Guidelines and several circulars, including the 2010 Circular on Information Systems Reliability, Resiliency and Recoverability and the 2009 Circular on Endpoint Security and Data Protection. These consolidated circulars have been cancelled upon the issuance of the TRM Guidelines on 21 June 2013.

The TRM Guidelines and TRM Notices do not supersede the 2004 Guidelines on Outsourcing and the 2011 Circular on IT Outsourcing dealing with operational risk, which remain applicable in full force. Unlike the IBTRM which only applies to banks and internet banking, the TRM Guidelines have a wider application as they apply to all FIs which are licensed, approved, or otherwise regulated by MAS.

The TRM Guidelines are statements of industry best practices which FIs are expected to adopt, and although they are not legally binding, the degree of observance with the spirit of the TRM Guidelines by a FI will be taken into account by MAS in its risk assessment of the FI.

The TRM Notices on the other hand have legal force, and sets out the legal requirements relating to technology risk management for FIs, including requirements for a high level of reliability, availability and recoverability of critical IT systems. Contravention of the TRM Notices requirements will attract the penalties under the relevant Act which each TRM Notice is issued. The TRM Notices will take effect as from 1 July 2014.

In addition to the TRM Guidelines and TRM Notices, the MAS also issued the following:
- Compliance Checklist for TRM Guidelines
- Response to Public Feedback for Consultation Paper – TRM Guidelines
- Response to Public Feedback for Consultation Paper – Notice on TRM
- FAQs – Notice on Technology Risk Management
- Incident Report Template
- Instructions on Incident Notification and Reporting to MAS.

To access the above documents, please click here.
Some key areas covered by the TRM Guidelines

- **Greater oversight by the board and senior management (paragraph 3 of the TRM Guidelines)**
  FIs’ board and senior management are expected to be more involved in decisions on key IT procurements and operation of the FIs, and also be responsible for ensuring effective internal controls and risk management practices are put in place to achieve security, reliability, resiliency and recoverability of their systems. The board and senior management are also expected to oversee the establishment of IT policies, standards and procedures to comply with the TRM Guidelines.

- **TRM framework (paragraph 4 of the TRM Guidelines)**
  FIs are expected to establish a TRM framework to manage technology risk in a systematic and consistent manner. The TRM framework should contain the roles and responsibilities in managing technology risks, identify information system assets for protection and associated risks. After identifying and assessing the risks, FIs should develop and implement risk mitigation and control strategies that are consistent with the value of the IT system assets.

- **Management of IT outsourcing risks (paragraph 5 of the TRM Guidelines)**
  FIs are expected to perform due diligence on service providers to determine their viability, capability and reliability in the provision of outsourcing services. FIs should ensure that appropriate contractual terms and conditions are set out fully in the agreements with service providers, such as responsibilities and conditions relating to performance targets, services levels, security, contingency planning and disaster recovery capability.

In particular, FIs should be aware of the unique attributes and risks of cloud computing especially in the area of data integrity, sovereignty, commingling, platform multi-tenancy, recoverability and confidentiality, regulatory compliance, auditing and data offshoring. FIs should also have the contractual power and means to promptly remove or destroy data stored at the cloud service provider’s systems and backups.

- **Systems reliability, availability and recoverability (paragraph 8 of the TRM Guidelines)**
  MAS expects FIs to have in place effective internal controls and risk management practices to ensure their IT systems and infrastructures’ reliability, resiliency and recoverability. In particular, FIs should achieve high availability for critical systems. FIs are also expected to refrain from adopting untested or untried recovery measures because this will be counter-productive to the efforts to have secured and reliable systems. All recovery measures should also be tested and validated at least annually.

- **Operational infrastructure security management (paragraph 9 of the TRM Guidelines)**
  FIs are expected to implement appropriate security solutions at the data, application, database, systems and network layers to address risks of data theft, data loss and data leakage from endpoint systems and devices. In particular, the use of unsecured internet services such as social media sites, cloud-based internet storage sites and web-based emails to communicate or store confidential information should be prohibited.

- **Enhanced data centre protection and controls (paragraph 10 of the TRM Guidelines)**
  The TRM Guidelines recommend the establishment of a Threat and Vulnerability Risk Assessment to identify security threats and operational weaknesses in a data centre in order to determine the level and type of protection to be established. Other recommendations on the physical security of data centres such as access security, fire security and availability of backup power are also included.

- **Mobile online services (paragraph 12 and Appendix F of the TRM Guidelines)**
  Security measures applicable to online financial systems are similarly applicable to mobile online services. FIs are expected to identify fraud scenarios and ensure the integrity and authenticity of payment applications. FIs are also expected to require encryption of sensitive data used in transactions made through their online systems, and to put in place measures to protect customers who use online systems.

- **Payment card security (ATM, credit and debit card) (paragraph 13 of the TRM Guidelines)**
  FIs who provide for such cards, ATMs and payment kiosks should ensure the safety and security of such services. The TRM Guidelines provide separate guidelines for payment cards, ATMs and payment kiosks centering on card skimming attacks and payment card fraud including counterfeit, lost/stolen, card-not-received and card-not-present fraud.

**Obligations under the TRM Notices**

- **Identification of “critical system”**
  FIs are required to put in place a framework and process to identify “critical system”, which is a system, the failure of which will cause significant disruption to the FIs’ operations or materially impact a FIs service to its customers.

- **Maintenance of “high availability” and maximum unscheduled downtime permitted**
  FIs are also required to make all reasonable efforts to maintain high availability for their critical systems. FIs are required to ensure that the maximum unscheduled downtime for each critical system does not exceed a total of four hours within any period of 12 months.

- **Recovery time objective (“RTO”)**
  FIs are also required to establish a RTO of not more than four hours for each critical system, and the time starts to run from the point of disruption (as opposed to “upon discovery”). FIs have to validate and document at least once in every 12 months, how they perform their system recovery testing and when the RTO is validated during the system recovery testing.
• Notification of “relevant incident” within 1 hour “upon discovery”
FIs are required to notify MAS as soon as possible but not later than one hour, upon the discovery of a relevant incident. A “relevant incident” means a system malfunction or IT security incident which has a severe and widespread impact on the FI’s operations or materially impacts the FI’s service to its customers. FIs can contact their respective MAS Supervisory Officer during office hours to report a relevant incident, or the MAS duty officer via a 24 hour MAS hotline after office hours.

• Submission of root cause and impact analysis report (“RCIA Report”)
A FI is required to submit a RCIA Report to MAS within 14 days (or such longer period as MAS may allow) from the discovery of the relevant incident. MAS has provided a template for the RCIA Report, and an instructions sheet on how to complete a RCIA. The RCIA Report should contain:
  - an executive summary of the relevant incident
  - an analysis and explanation on the root cause which triggered the relevant incident
  - a description of its impact on the FI’s compliance with laws and regulations, its operation and service to its customers
  - a description of the remedial measures taken to address the root cause and consequences of the relevant incident.

• Protection of customer information
FIs are also required to implement IT controls to protect customer information from unauthorised access or disclosure. This requirement appears to be a “catch-all” provision to cover all systems (whether or not they are “critical systems”), which contain customer information.

Preparing for compliance
• As the TRM Notices will take effect from 1 July 2014, FIs will have less than 12 months to work towards being compliance ready with the TRM Notices requirements. In terms of next steps, FIs should first review their current processes and practices and perform a gap analysis to determine:
  - whether the FIs’ current internal measures and procedures are sufficient for compliance
  - what systems need to be relooked to ensure compliance
  - whether the terms and conditions of current agreements with service providers facilitate the FI’s compliance with the TRM Guidelines and TRM Notices.

To facilitate compliance, we recommend that FIs consider putting in place following:
• A checklist of:
  - all key IT related matters and decisions which the board and senior management must oversee and be involved in
  - key issues or matters to be considered in the performance of due diligence on IT service providers (not limited to due diligence on IT outsourcing service providers)
  - key contractual terms recommended under the TRM Guidelines for negotiation of future IT contracts.

• Establish a dedicated compliance team to oversee the implementation and continuous observation and compliance of the TRM Guidelines and TRM Notices.

• Establish a dedicated incident preparedness and response team to respond to IT incidents.

FIs should also start reviewing existing agreements with their services providers to determine whether there is a need to renegotiate to include terms recommended by the TRM Guidelines and to match the service levels reflected in the TRM Notices. If renegotiation is not possible, FIs may need to consider alternative service providers and making the necessary transition.

If you have any questions in relation to the above or would like to learn more about what we can offer to you, please do not hesitate to contact:

Bryan Tan  
Partner  
Singapore  
T: +65 63 058 490  
E: bryan.tan@pinsentmasons.com

Rosemary Lee  
Counsel  
Singapore  
T: +65 63 050 912  
E: rosemary.lee@pinsentmasons.com