Wong & Partners.
Member Firm of
Baker & McKenzie International

Financial Services and Regulation
Kuala Lumpur

Client Alert

October 2018

Bank Negara Malaysia issues Exposure Draft of Risk Management in Technology

Bank Negara Malaysia (the Malaysian Central Bank) ("**BNM**") had, on 4 September 2018, issued an exposure draft of the Risk Management in Technology policy document ("**RMiT Exposure Draft**"). BNM is proposing for the policy to come into force on 1 June 2019 and it will apply to licensed banks[1], licensed insurers, licensed takaful operators, prescribed development financial institutions, operators of a designated payment system and eligible issuers of e-money (collectively, "**FIs**").

Given the increasing reliance by FIs on technology and online systems and the increasing threat of cyber attacks, the introduction by BNM of minimum standards on technology risk and cyber security management by FIs in Malaysia is timely. If the RMiT Exposure Draft is finalized, there will begin to be some (but not complete) alignment by BNM and the Monetary Authority of Singapore ("**MAS**") on managing technology risk[2].

The key requirements and standards that BNM is proposing to introduce are set out below.

1. Board and Senior Management Responsibilities

Similar to the MAS Technology Guidelines, the board of directors of FIs ("**Board**") will have overall responsibility and oversight for the implementation of a robust technology risk management framework. The Board is required to among others put in place a technology risk management framework (i.e. a framework for safeguarding the FI's information infrastructure, systems and data) ("**TRMF**") and a cyber resilience framework (i.e. a framework for ensuring the FI's financial resilience) ("**CRF**"). The senior management of FIs are tasked with implementing the TRMF and CRF through specific policies and procedures.

Stricter requirements are imposed on large FIs[3] under the RMiT Exposure Draft.

2. Chief Information Security Officer

The RMiT Exposure Draft mandates FIs to designate a Chief Information Security Officer responsible for among others, ensuring information assets and technologies are adequately protected and enforcing compliance with the TRMF and CRF.

For further information, please contact:

Brian Chia
Partner
+603 2298 7999
Brian.Chia@WongPartners.com

Sue Wan Wong
Partner
+603 2298 7884
SueWan.Wong@WongPartners.com

Serene Kan
Senior Associate
+603 2299 6437
Serene.Kan@WongPartners.com

[1] Including, licensed investment banks and licensed Islamic banks

[2] The MAS issued the Technology Risk Management Guidelines ("**MAS Technology Guidelines**") in June 2013.

[3] Defined as (a) FI with one or more business lines that are significant in terms of market share in the relevant industry; or (b) FI with large network of offices within or outside the country through operations of branches and subsidiaries.

3. Data Centres

Given the importance of data centres to the operations of an FI, the RMiT Exposure Draft will require FIs to ensure that its production data centres[4], among others, meet international standards (such as having multiple paths for power as well as cooling systems in place). Minimum technical requirements must also be put in place where the FIs host its production data centres on third-party facilities.

4. Cloud Storage

There is also greater clarity on the use of cloud services. Save for certain critical technology functions and confidential information which cannot be hosted on a public cloud, the RMiT Exposure Draft does not prohibit the use of cloud.

5. Outsourcing to Third-Parties

Similar to the MAS Technology Guidelines, the RMiT Exposure Draft requires comprehensive due diligence to be conducted on third-party service providers before critical technology functions and systems can be outsourced. The outsourcing arrangements will also need to be recorded in service level agreements and incorporate certain minimum requirements. For licensed banks and insurers, additional obligations are encapsulated in the outsourcing policy document issued by BNM[5].

Conclusion

The issuance of the RMiT Exposure Draft reflects the growing sentiment among financial service regulators in the region that FIs will need to bolster its cyber defences to ensure that its systems and customer data are afforded greater protection. MAS for example, has recently issued a consultation paper on Notice on Cyber Hygiene on 6 September 2018, which seeks to prescribe certain cyber security practices as baseline hygiene standards for cyber security. The RMiT Exposure Draft is a move in a similar direction.

Given the scope and standards of the requirements introduced under the RMiT Exposure Draft, FIs should immediately take the opportunity to review its existing systems, frameworks and processes. This includes revising any existing policies that are similar to the TRMF and CRF to ensure that it meets the stipulated requirements. In addition, FIs should begin identifying appropriately qualified candidates for the various offices and positions; given the competition for talent in this space.

www.wongpartners.com

Wong & Partners
Level 21
The Gardens South Tower
Mid Valley City
Lingkaran Syed Putra
59200 Kuala Lumpur

[4] This includes all facilities hosting active critical production application systems irrespective of location.
[5] Note that BNM had on 20 September 2018 also issued an exposure draft on outsourcing which should be read in conjunction with the RMiT Exposure Draft.