LHAG update

Raphael Tay Choon Tien
Partner
Corporate | FinTech
T: +603 6208 5831
E: rtt@lh-ag.com

Ko Chia Chea
Associate
Corporate | FinTech
T: +603 6208 5879
E: cck@lh-ag.com

30 JUNE 2020

BNM Policy on Risk Management in Technology

On 19 June 2020, Bank Negara Malaysia (**BNM**) issued a Policy Document on Risk Management in Technology (RMiT) pursuant to s 266 of the Financial Services Act 2013, s 277 of the Islamic Financial Services Act 2013 and s 126 of the Development Financial Institutions Act 2002.

Scope of application

The Policy Document is applicable to licensed financial institutions including licensed banks, approved issuers of electronic money, operators of designated payments systems and other licensed financial institutions.[1] It sets out the requirements with regard to the financial institutions' risk management in their use of IT systems, applications, platforms and infrastructure.

In complying with the requirements, a financial institution must have regard to the size and complexity of its operations. Hence, larger and more complex financial institutions are expected to have more robust risk management practices and controls which are commensurate with their increased technology risk exposure.[2]

Board of directors and senior management

The board of directors and the senior management of the financial institutions must be aware that they have designated responsibilities pursuant to the Policy Document which may result in enforcement action if not complied with. For example, the board must periodically review and affirm a sound and robust technology risk management framework (TRMF), and cyber resilience framework (**CRF**) at least once every three years for the financial institution.[3]

---

1 Part A, para 2.1
2 Part A, para 1.3
3 Part B, para 8.3

Chief Information Security Officer

It is mandatory for a financial institution to designate a Chief Information Security Officer (**CISO**), by whatever name called, who will be responsible for the technology risk management function of the financial institution.[4] The CISO must:

1. be independent from day-to-day technology operations;

2. keep apprised of current and emerging technology risks which could potentially affect the financial institution's risk profile; and

3. be appropriately certified.

Risk management areas

1. **Data centre resilience:** A financial institution must ensure that production data centres and recovery data centres are concurrently maintainable.[5]

2. **Data centre operations:** A financial institution must ensure it has adequate system storage, central processing unit (CPU) power, memory and network bandwidth for its capacity needs. The financial institution must also establish real-time monitoring mechanisms to track its capacity utilisation.[6]

3. **Third-Party Service Provider:** Prior to engaging a third-party service provider for critical technology functions and systems, a financial institution must conduct proper due diligence on its competency, system infrastructure and financial viability. The Policy Document also prescribes the minimum criteria for service-level agreements (SLA) which the financial institution must establish when engaging third-party service providers.[7]

4. **Cloud Services**: A financial institution is required to consult BNM prior to the use of public cloud for critical systems.[8] The Policy Document prescribes the mandatory areas for the risk assessment which the financial institution must then perform in respect of the use of public cloud for critical systems.[9]

5. **Cyber Risk Management**: In addition to the CRF which each financial institution must develop, a large financial institution must implement a centralised automated tracking

---

4 Part B, para 9.4
5 Part B, paras 10.22 and 10.23
6 Part B, paras 10.26 and 10.27
7 Part B, paras 10.41 to 10.43
8 "critical system" refers to any application system that supports the provision of critical banking, insurance or payment services, where failure of the system has the potential to significantly impair the financial institution's provision of financial services to customers or counterparties, business operations, financial position, reputation, or compliance with applicable laws and regulatory requirements
9 Part B, para 10.51

system to manage its technology asset inventory and establish a dedicated in-house cyber risk management function to manage cyber risks or emerging cyber threats.[10]

Ko Chia Chea (cck@lh-ag.com)

If you have any queries, please contact the author or her team partner **Raphael Tay Choon Tien** (rtt@lh-ag.com).

Lee Hishammuddin Allen & Gledhill

Level 6, Menara 1 Dutamas
Solaris Dutamas
No. 1, Jalan Dutamas 1
50480 Kuala Lumpur
Malaysia

T +603 6208 5888
F +603 6201 0122/0136
E enquiry@lh-ag.com
W www.lh-ag.com

Published by the Corporate Department

© Lee Hishammuddin Allen & Gledhill. All rights reserved. The views and opinions attributable to the authors or editor of this publication are not to be imputed to the firm, Lee Hishammuddin Allen & Gledhill. The contents of this publication are intended for purposes of general information and academic discussion only. It should not be construed as legal advice or legal opinion on any fact or circumstance.

Feedback Unsubscribe

[10] Part B, para 11.3