LH AG ADVOCATES AND SOLICITORS

LHAG update

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

14 DECEMBER 2018

Technology Risk Management in Financial Institutions

Bank Negara Malaysia's Exposure Draft

| by Lo Yien Peng |

On 4 September 2018, the Central Bank of Malaysia (BNM) issued an exposure draft on Risk Management in Technology.

BNM proposes for this draft policy document to take effect from 1 June 2019, and, once in force, will be applicable to all licensed financial institutions (FIs).[1]

The draft policy document addresses the following areas:

Governance

The Board of the FIs must periodically review and reaffirm its technology risk management framework (TRMF)[2] and cyber resilience framework (CRF)[3] at least biennially and the Board must have at least one member with relevant technology experience and competencies.

Technology Risk Management

Each FI must have a Chief Information Security Officer (CISO) responsible for information assets and technologies as part of his/her technology risk management function.

Data Centre Resiliency

Production data centre of each FI must meet international standards and include a comprehensive and forward-looking capacity management plan commensurate with its potential future business growth plans.[4]

Cloud Services

The usage of public cloud computing services in managing, operating or hosting critical technology functions, systems and confidential information continues to be prohibited. FIs are required to conduct risk assessment prior to adopting any cloud services.

Third Party Service Providers

Due diligence must be conducted on the competency, system infrastructure and financial viability of a third party service provider, and a service-level agreement (SLA) must be entered into.

The issuance of a draft policy document specifically on risk management technology reflects the continuing threat of cyber attacks and the need for FIs to strengthen their cyber defence and offer greater customer data protection.

Click here to view the Exposure Draft on Risk Management Technology.

Lo Yien Peng (loy@lh-ag.com)

If you have any queries regarding the draft policy document, please contact the author or her team partner Ooi Bee Hong (obh@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

[1] Licensed banks; licensed investment banks; licensed Islamic banks; licensed international Islamic banks; licensed Takaful operators; licensed international Takaful operators; prescribed development financial institutions; eligible issuer of e-money; and operator of a designated payment system.

[2] A framework for safeguarding the FIs' information infrastructure, systems and data

[3] A framework for ensuring the FIs' cyber resilience

[4] This would include adequate system storage, central processing unit (CPU) power, memory and network bandwidth