

LHAG Insights

Technology, Media & Telecommunications



ABOUT THE AUTHORS



G. Vijay Kumar
Partner
TMT

(Corporate & Commercial Disputes)

E: vkg@lh-ag.com



Ng Yih Xiang
Associate
TMT

(Corporate & Commercial Disputes)

E: nyx@lh-ag.com



Nicole Shieh E-Lyn
Associate
TMT

(Corporate & Commercial Disputes)

E: sel@lh-ag.com

17 JANUARY 2023

New IT Regulatory Requirements for EMIs

Following-up on their exposure draft issued in June 2021, Bank Negara Malaysia (“**BNM**”) has recently issued a Policy Document on the requirements and guidance applicable to approved issuers of electronic money (“**EMI**”).¹ Serving a twofold purpose, the [Policy Document](#) aims to:

- (a) Ensure the safety and reliability of E-money issued by EMI; and
- (b) Preserve customers’ and merchants’ confidence in using or accepting E-money for the payment of goods and services.

The usage of E-money has grown exponentially in recent times. Based on BNM’s data, the average number of digital payment transactions per capita has more than quadrupled over the last 10 years, increasing from 49 transactions per capita in 2011, to over 221 transactions per capita in 2021. In 2020, the nation saw 3 million new mobile banking service subscriptions, largely due to the COVID-19 pandemic. In light of our increasing reliance on E-money, it is of utmost importance that the integrity of E-money payment systems is duly safeguarded.

¹ This Policy Document was issued by BNM pursuant to s. 11 of the Financial Services Act 2013 or the Islamic Financial Services Act 2013. This Policy Document will supersede the BNM guidelines on E-money issued in 2008.

The Policy Document is divided into 5 parts –

- a) **Part A** – Overview;
- b) **Part B** – Governance;
- c) **Part C** – Operational and Risk Management Requirements;
- d) **Part D** – Information Technology (IT) Requirements; and
- e) **Part E** – Regulatory Process.

This Update will focus on **Part D** of the Policy Document, which sets out the IT requirements imposed by BNM. With over 20 pages dedicated to IT Requirements, the Policy Document imposes extensive risk assessment and management obligations, including:

- a) Establishing a Technology Risk Management Framework (“**TRMF**”) to safeguard the EMI’s information infrastructure, systems and data as an integral part of the EMI’s risk management framework;
- b) Establishing an independent enterprise-wide technology risk management framework for implementing the TRMF as well as a Cyber Resilience Framework (“**CRF**”);
- c) Appointing a Chief Information Security Officer (“**CISO**”) to be responsible for the technology risk management function of the EMI;
- d) Establishing an Enterprise Architecture Framework that provides a holistic view of technology systems and functions of the EMI;
- e) Establishing clear risk management policies and practices for key phases of the system development cycle (“**SDLC**”);
- f) Establishing proper management of data infrastructures, authorisation procedures to ensure confidentiality, integrity and availability of data;
- g) Conducting a comprehensive risk assessment prior to cloud adoption which considers the inherent architecture of cloud services;

- h) Implementing an appropriate and robust access control policy for logical and physical technology access controls;
- i) Implementing additional controls for high-risk transactions or transactions above RM10,000.00; and
- j) Ensuring that technology systems and applications are properly audited.

In devising and implementing risk management measures for all technology functions in an EMI, the Policy Document further provides that the following factors should be considered:

- a) Risk measures adopted should be proportional to the size of the operations of the EMI;
- b) Periodic and rigorous testing of the efficacy of risk measures;
- c) Ensuring that proper authorisation procedures and adequate measures are adopted when sensitive data is involved;
- d) Identifying risks that could lead to a broader impact on the EMI's operational capabilities;
- e) Appointing technically competent external technology service providers to assess and improve on risk management measures; and
- f) Ensuring that the implementation of risk assessment measures is properly recorded, and that it is available upon request by BNM.

With an overarching theme of accountability, it is clear that BNM expects key personnel, comprising of the Board of Directors and Senior Management, to be actively involved in monitoring the efficacy of the IT risk management measures. As set out in the Policy Document, the engagement of technology service providers, including engagements for independent assessment, does not in any way reduce or eliminate the EMI's principal accountabilities and responsibilities over the security and reliability of technology functions and systems. Further, the risk management measures implemented by the EMI must be properly documented and made available upon BNM's request.

Head Office

Level 6, Menara 1 Dutamas
Solaris Dutamas
No. 1, Jalan Dutamas 1
50480 Kuala Lumpur
Malaysia
Tel: +603 6208 5888
Fax: +603 6201 0122

Johor Office

Suite 21.01
21st Floor, Public Bank Tower
No.19, Jalan Wong Ah Fook
80000 Johor Bahru, Johor
Tel: +607 278 3833
Fax: +607 278 2833

Penang Office

51-12-E, Menara BHL Bank,
Jalan Sultan Ahmad Shah,
10050 Penang
Pulau Pinang
Tel: +604 299 9668
Fax: +604 299 9628

Email

enquiry@lh-ag.com

Website

www.lh-ag.com

Thus, key players in the industry must actively assess and improve on their EMI's IT risk management measures and carry out robust due diligence on third party service providers. These steps are crucial in minimizing the risk of technology functions disrupting an EMI's operations. Though extensive and rather onerous, it is imperative that EMIs implement the requirements in the Policy Document in a timely manner. This will serve to enhance the integrity of their payment systems and avoid the risk of enforcement actions by BNM.

See also our previous publications on related matters:

- a) [Navigating the E-money Landscape](#)
- b) [Islamic E-money under the New Bank Negara Regulations](#)

If you have any queries on legal issues relating to Technology, Media and Telecommunications (TMT), please do not hesitate to contact associates, **Ng Yih Xiang** (nyx@lh-ag.com), **Nicole Shieh E-Lyn** (sel@lh-ag.com) or team partner, **G. Vijay Kumar** (vkg@lh-ag.com).