

ITU Digital Financial Services Security Clinic Asia Pacific Region

Digital security measures in Malaysian financial sector

Ng Lee See

Deputy Director (Risk Specialist)

Risk Specialist & Technology Supervision Department

Bank Negara Malaysia

Seoul, Korea

24 April 2024



BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Disclaimer

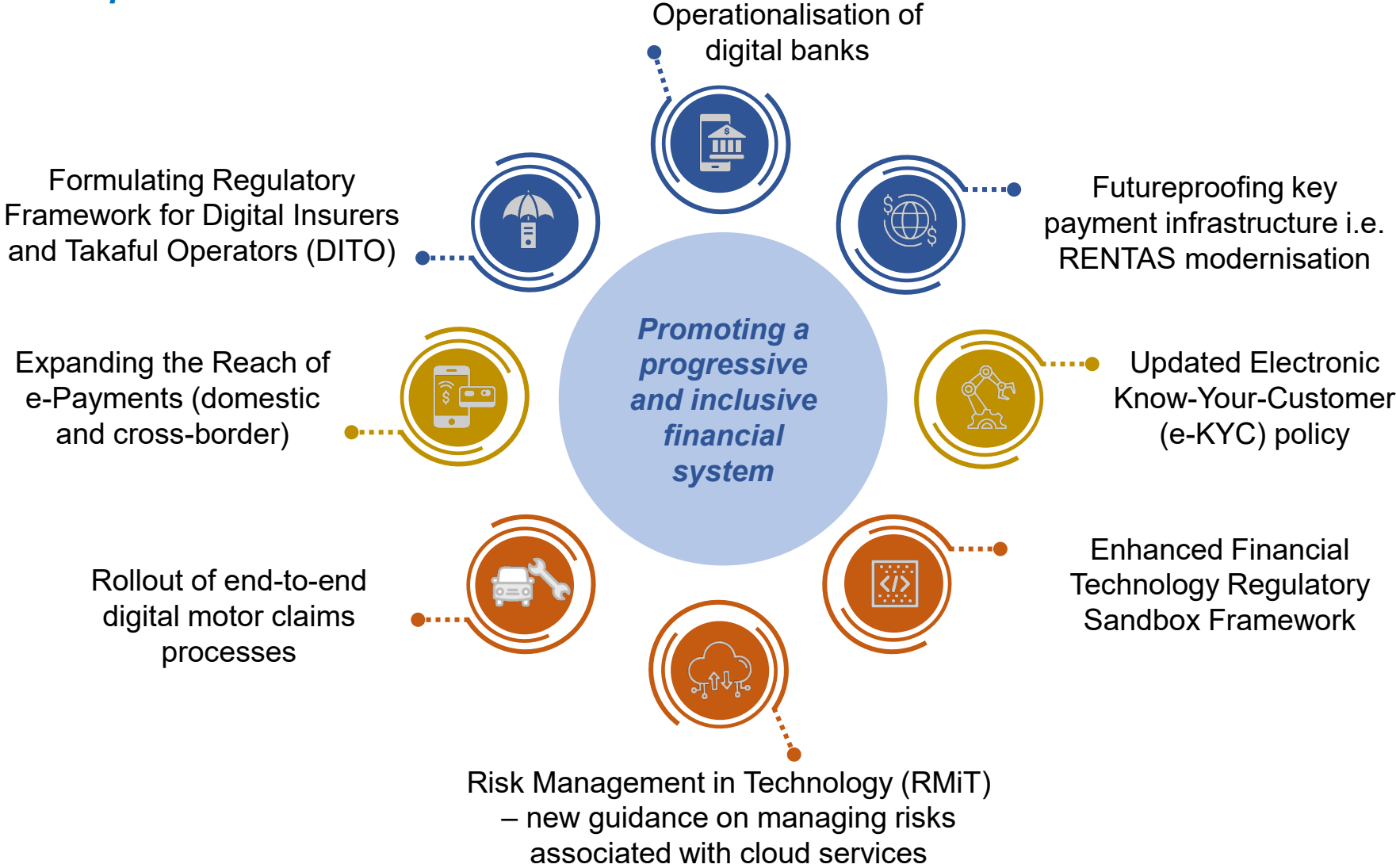
The information was not prepared with the specific consideration of any particular individual or entity.

Any views expressed in this document are those of the author and are not necessarily those of BNM. While every care is taken in the preparation of the information, no responsibility can be accepted by BNM for any errors and any liability for any loss or damage arising from the use of, or reliance on, the information contained in this document.



Fostering inclusive digital financial services in Malaysia

Current priorities



BNM's Risk Management in Technology (RMiT) sets the minimum baseline to raise industry standards

Effective board oversight on IT and cyber risks

- Reviewing and approving IT and cyber security strategic plans and technology risk appetite through a designated board-level committee

Strong second line of defence for technology risk management

- Fortifying the independent enterprise-wide technology risk function to implement technology risk management and cyber resilience frameworks
- Designate a CISO responsible for this function

01



03

Building resilient IT infrastructure to ensure continued service availability

- Embedding security considerations in the application systems and network services
- Time limits on unplanned downtime
- Risk controls for cloud computing

04

Greater cyber resilience to emerging risks associated with new technologies

- Establishment of Security Operations Centre capabilities to monitor, identify and respond to potential breaches
- Periodic security assessments to provide independent view of the state of the financial institution's cyber security

4 key thrusts of the RMiT

Application on a proportionate basis where additional standards are imposed for larger FIs



Strengthened expectations on RMiT to safeguard against risks from cloud adoption in June 2023

Cloud controls in RMiT emphasise on strong governance, clarity of FI's responsibility, and robust information security controls over the solution development lifecycle.

Key risk and control measures for cloud services					
Part A: Cloud Governance	Part B: Cloud Design & Controls				
1	Cloud risk management	1	Cloud architecture	8	Cryptographic key management
2	Cloud usage policy	2	Cloud application delivery models	9	Access Controls
3	Due diligence	3	Virtualisation and containerization management	10	Cybersecurity Operations
4	Access to authoritative third-party certifications	4	Change Management	11	Distributed Denial of Services
5	Contract management	5	Cloud backup and recovery	12	Data Loss Prevention
6	Oversight over cloud service provider	6	Interoperability and Portability	13	Security Operation Centre
7	Skilled personnel with knowledge on cloud services	7	Exit Strategy	14	Cyber response and recovery

The updated PD is available at: <https://www.bnm.gov.my/documents/20124/938039/PD-RMiT-June2023.pdf>



Continuous ‘whole-of-nation’ efforts to combat digital fraud is essential to preserve confidence in online banking and digital payments

Continuous collaboration between BNM, financial institutions and law enforcement agencies has yielded results

Three workstreams to sustain vigilance and promote continuous investment to get ahead of constantly-evolving scams

1

Prevention

- Frequent **supervisory guidance** to FIs on enhancing security of online banking since 2021
- Implementation of **5 key countermeasures** announced in Sep 2022
- Additional guidance for effective protection of high-risk and vulnerable customer segments
- Issuance of **enhanced standards on fraud detection systems and practices**
- Expansion of key countermeasures to **non-bank payment providers**
- On-going review of Risk Management in Technology policy** to ensure FIs maintain highest standards of cybersecurity operation and technology risk management
- Enhancement of e-KYC policy** to strengthen identity proofing

2

Recovery

- Operationalisation of National Scam Response Centre (NSRC)** to block and trace stolen funds
- 997 hotline** facilitated efforts to trace suspected fraudulent activity and flag mule accounts
- Over 40,000 mule accounts disrupted** by financial institutions since October 2022
- Development of National Fraud Portal** (expected to go live in 2024)
- Development of **Joint Responsibility Framework** to foster fairer compensation for fraud victims


3

Education

- On-going awareness initiatives in collaboration with financial industry and government agencies**

5 key countermeasures implementation

- Migration away from SMS OTP
- Tighten fraud detection
- Cooling off period for first-time enrolment
- Limit 1 customer to 1 mobile device
- Dedicated 24/7 hotlines

 On-going initiatives

Support nationwide secure digital initiatives

- MCMC* issued directive to prohibit **SMS with hyperlinks** in July 2023.
- Inter-industry collaboration to take down/block malicious content, websites
- Support enactment of new legislation “**Digital Safety Bill**”

*Malaysian Communications and Multimedia Commission