Take5 for business

Volume 14 Issue 1 - 24 January 2025

Inside the Risk Management in Technology (RMiT) Exposure Draft

Enhancing cybersecurity posture in the financial industry

In November 2024, Bank Negara Malaysia (BNM) issued an exposure draft of the Risk Management in Technology (RMiT) policy document for public feedback.

The exposure draft raises the bar by outlining new requirements on financial institutions' (FIs) management of technology risks. These requirements aim to further upgrade the resilience of financial services and enhance system-wide cyber defense.

This policy revision enhances supervisory review processes for emerging technologies to better facilitate digitalization of the financial system in Malaysia.

The proposed additions may affect FIs that need to adjust to the increased burden of compliance.

2024 RMiT Exposure Draft updates include:

- Expanded scope of the policy
- Introduction of the Cyber Security Act 2024
- Management of the cybersecurity supply chain
- Updated requirements related to digital services and emerging technologies
- Implementation of cybersecurity controls
- Updated assessment requirements

BNM invites written feedback on the proposed requirements in the exposure draft by 31 January 2025

Source: *Risk Management in Technology Exposure Draft*, November 2024, Bank Negara Malaysia

"

In an industry where the threat landscape is constantly expanding, raising the risk of security breaches, regulations and compliance should not merely be a checklist.

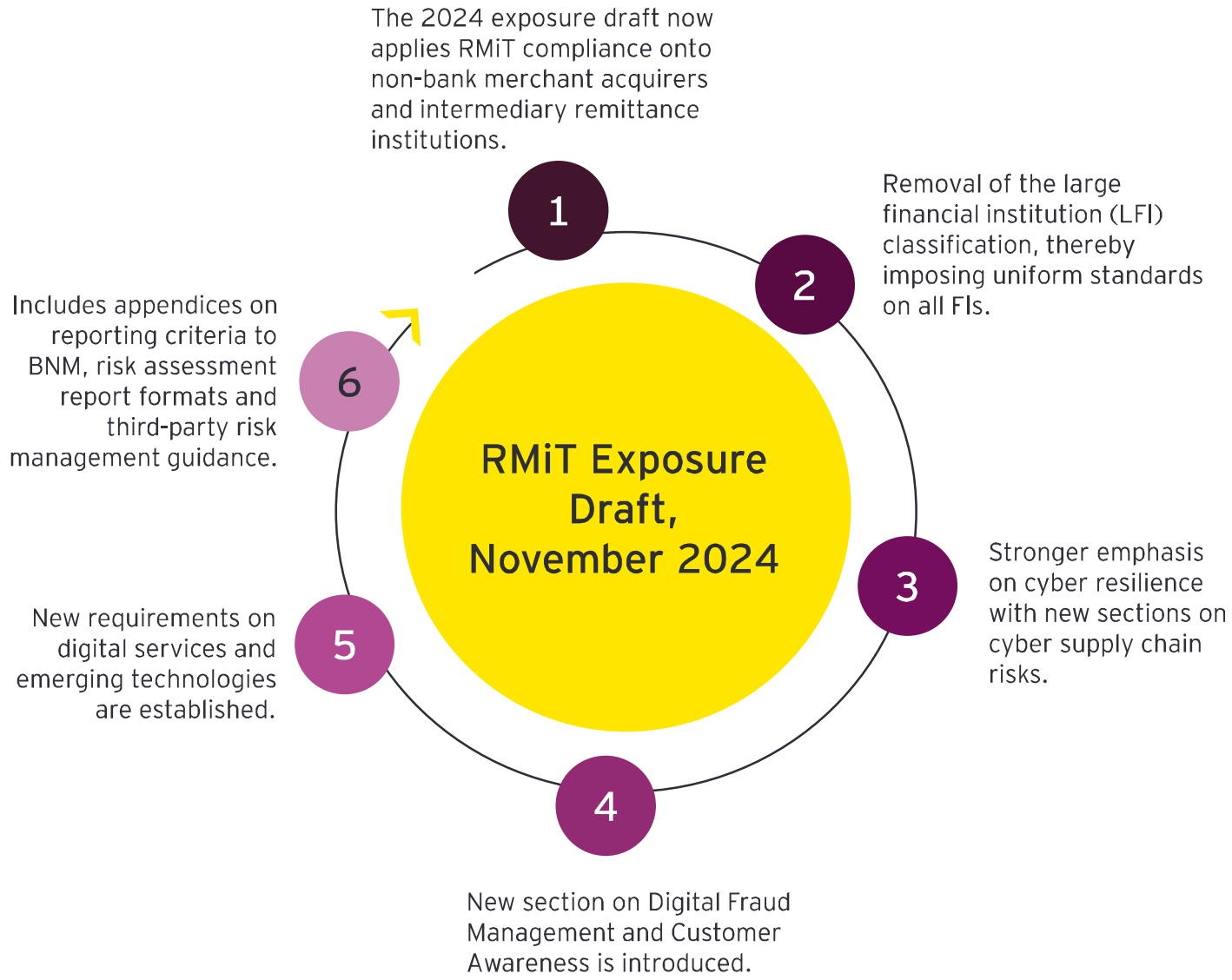
Instead, these requirements should act as a reference guide that helps organizations continuously enhance their security posture and safeguard their operations.

Jason Yuen
Malaysia Cybersecurity Leader; and Partner
Ernst & Young Consulting Sdn. Bhd.

Essential updates for RMiT compliance

In the 2024 exposure draft, BNM has enhanced cybersecurity protocols for FIs. The draft underscores third-party risk management, demands robust recovery plans and enforces transparent incident reporting.

Set out below are six key enhancements:



Source:
- *Risk Management in Technology Exposure Draft*, November 2024, Bank Negara Malaysia
- EY analysis

Widening the applicability of RMiT policy

BNM's RMiT policy document outlines the necessary technology-related requirements for FIs.

The 2024 exposure draft now broadens the applicability of the RMiT to encompass non-bank merchant acquirers and intermediary remittance services.

Financial services that are included in the RMiT exposure draft:

1. Licensed banks
2. Licensed investment banks
3. Licensed Islamic banks
4. Licensed insurers including professional reinsurers
5. Licensed *takaful* operators including professional re*takaful* operators
6. Prescribed development FIs
7. Operator of a designated payment system
8. Approved issuers of electronic money
9. Non-bank merchant acquires
10. Intermediary remittance institutions

Source:
- *Risk Management in Technology Exposure Draft*, November 2024, Bank Negara Malaysia
- EY analysis

Widening the applicability of RMiT policy (cont'd)

The exposure draft also plans to remove the specific requirements for LFIs and impose all requirements outlined across the entire sector.

Below are the extended requirements which were previously required only for LFIs now applicable to all FIs:

Responsibilities of the senior management

Assign specialized staff to supervise technology risk management.

Technology audit

Ensure internal audit includes certified technology audit experts familiar with the institution's technology advancements

Patch and end-of-life system management

Allocate resources for regular updates and management of end-of-life technology systems.

Internal awareness and training

Provide continuous training in technology operations, cybersecurity and risk management.

Security operations center (SOC)

Require SOC to provide monthly threat assessment report.

Access control

- Deploy an identity access management system for user access control and monitoring.
- Utilize automated audit tools for anomaly detection.

Data center infrastructure

- Ensure recovery data centers are maintainable.
- Ensure that data centers feature redundant components and distributions paths for equipment.

Cyber risk management

- Implement a centralized system for technology asset inventory management.
- Establish a dedicated in-house cyber risk management function.

Cybersecurity operations

- Conduct quarterly vulnerability assessment for critical systems network components
- Perform independent compromise assessments on technology infrastructure's critical systems at least once in every three years.

Source:
- *Risk Management in Technology Exposure Draft*, November 2024, Bank Negara Malaysia
- EY analysis

New requirements and expanded scope

FIs that are designated as National Critical Information Infrastructure (NCII) entities are subject to Cyber Security Act 2024 requirements. Guidelines includes:

- Complying with any relevant Codes of Practice issued by the NCII sector lead
- Conducting cybersecurity risk assessments and audits
- Providing information to the relevant NCII sector lead when requested
- Notifying the relevant NCII sector lead and the chief executive when there is a cybersecurity incident

Cybersecurity supply chain risks

FIs are required to assess potential risks and impacts that may arise from cyber supply chain incidents. By understanding and preparing for these risks, FIs can better safeguard their operations against the effects of cyber threats within their supply chains.

- Vetting of personnel to ensure trustworthy staff
- Vetting of third-party or open-source software to prevent vulnerabilities due to systems interdependence
- Third-party risk management for essential subcontractors to mitigate potential risks
- Addressing concentration and geopolitical risks that can affect the supply chain security

Digital services

FIs are also required to ensure security for digital services which includes payment, remittance, banking, Islamic banking, insurance and *takaful* services provided through electronic channels such as the internet, mobile devices, self-service kiosks and point-of-sale terminals.

Emerging technologies

Guidelines related to managing risks associated with emerging technologies are being introduced, which include:

- Enhancing risk management practices
- Adhering to ethical and legal standards
- Establishing clear governance for adoption
- Continuously fortifying cybersecurity
- Thoroughly testing technologies before use
- Preparing crisis suspension protocols
- Consistently monitoring and informing users of risk

Source:
- *Risk Management in Technology Exposure Draft*, November 2024, Bank Negara Malaysia
- EY analysis

Enhancing cybersecurity control measures and assessment requirements

The exposure draft has strengthened the requirement for cybersecurity control measures, introducing new areas such as application programming interface (API) security as well as enhancing the requirements for vulnerability assessment, penetration testing and cryptography.

Key requirements for API security measures

- Centralized management of API inventory
- Scalability and mitigate against service disruptions
- Secure coding and third-party code validation
- Strong encryption and key management
- Implement user authentication and access controls
- Regular security assessments and continuous monitoring
- Quick revocation of compromised API keys

Cryptography

In response to the emerging threats posed by quantum computing and the potential for current cryptographic methods to become unsafe, the RMiT cryptography requirements have been revised.

Increased review frequency

Cryptographic standards and algorithms are now subject to an annual review, enhancing the institution's ability to respond to new threats and technological changes more swiftly than the previous three-year review cycle.

Expansion of IT asset inventory

Newly updated requirement for expanded IT asset inventory that includes all cryptographic tools and algorithms currently in use. This inventory must provide detailed explanation for the choice of each cryptographic method and map these methods clearly to the application system.

Vulnerability assessment and penetration testing

To address evolving cybersecurity challenges, the exposure draft's requirements for vulnerability assessment and penetration testing have been updated with the following:

Pre-deployment penetration testing

FIs are now required to perform intelligence-led penetration tests before introducing new systems, ensuring the IT infrastructure remains secure and not inadvertently exposed by new network configurations.

Extended compromise assessment cycle

The frequence for independent compromise assessments of critical systems' technology infrastructure has been extended from annually to once every three years, with a stipulation for timely reporting of the findings to senior management and the board.

Source:
- *Risk Management in Technology Exposure Draft*, November 2024, Bank Negara Malaysia
- EY analysis

Next steps

As technology continues to advance and the threat landscape broadens, the diligent enforcement of RMiT is important in mitigating potential cybersecurity risks. The following are some key actions that FIs can consider:

1. Conduct a self-assessment and review the enhanced requirements to ensure that your cybersecurity strategy and initiatives are aligned with the new requirements.
2. Evaluate the adequacy of existing cybersecurity controls and assessment approaches to ensure they meet current requirements and effectively protect against emerging threats in the evolving technology landscape, such as artificial intelligence (AI) and quantum computing.
3. Review existing approaches to managing third-party and supply chain risks to better safeguard operations against the effects of cyber threats within the supply chain.

Source: EY analysis

Contacts

Dato' Abdul Rauf Rashid
Malaysia Managing Partner,
Ernst & Young PLT

abdul-rauf.rashid@my.ey.com

Jason Yuen
Malaysia Cybersecurity Leader; and
Partner,
Ernst & Young Consulting Sdn. Bhd.

jason.yuen@my.ey.com

Shankar Kanabiran
Malaysia Deputy Consulting Leader; and
Partner,
Ernst & Young Consulting Sdn. Bhd.

shankar.kanabiran@my.ey.com

Jaco Benadie
EY ASEAN Cybersecurity Energy Leader
and OT Cybersecurity Competency Lead
Ernst & Young Consulting Sdn. Bhd.

jaco.benadie@my.ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

APAC no. 07010941
ED None

ey.com