Updates to the Risk Management in Technology policy document

Strengthening proactive, risk-informed technology and cyber resilience

December 2025

Bank Negara Malaysia's Risk Management in Technology (RMiT) Policy Document (PD) was revised and issued in **November 2025**. It signals a bold shift that goes beyond incremental updates and pushes for deeper accountability, broader coverage, and stronger resilience. With sharper emphasis on board accountability, cyber resilience, and ethical governance of emerging technologies, the PD enables organisations to move from compliance-based oversight to proactive, risk-informed resilience.

Key highlights

Build resilience for continuous service delivery and customer confidence

What's new

- Prescriptive time-bound obligations for capacity planning and degradation detection
- Operational telemetry tying resilience to customer impact
- Stand-in processing for least-substitutable services
- Resilience against cross-service interdependency failures

Action points

- Conduct proactive capacity planning exercises that factor in peak loads, projected growth, and upcoming architecture changes
- Implement early-warning systems to detect service degradation and failed transactions
- Measure customer impact during outages (number of affected customers and transaction volumes)
- Review and mitigate IT interdependencies regularly to prevent cascading failures
- Establish stand-in processing capability by 30 September 2027 for least-substitutable services, with fraud controls

Close the supply chain gap with proactive third-party risk management to prevent breaches

What's new

- Mandatory due diligence on all service providers and subcontractors
- Continuous monitoring of vendor risk and SLA compliance, including cybersecurity posture
- Enforcement of SLAs that require immediate disclosure of incidents and remediation timelines
- Introduction of cyber supply chain risk controls, including adoption of Software Bill of Materials (SBOM) for continuous vulnerability monitoring and secure open-source software practices

Action points

- Review and renegotiate SLAs to include disclosure and resilience clauses by Q2 2026
- Implement continuous vendor risk monitoring tools
- Implement SBOM tools to automate vulnerability detection in third-party components
- Establish open-source security policies covering repository access, secure coding, and malware prevention

Key highlights (cont'd)

Embed 'Secure by Design' principles to prevent vulnerabilities during deployment

What's new

- Enterprise technology architecture must integrate security throughout the system development life cycle (SDLC)
- Mandatory Technology Architecture Framework to support identification of single points of failure and enable business impact analysis

Action points

- Develop a Technology Architecture Framework outlining infrastructure, system interconnectivity, dependencies, and security controls
- Adopt DevSecOps practices

Elevate security of digital channels and customer protection to counter digital fraud and phishing

What's new

- The scope of cybersecurity threats and mitigation strategies has been expanded to encompass customers' mobile devices and access points
- Mandatory fraud detection standards and continuous review of fraud models
- Stronger authentication and monitoring for digital services

Action points

- Deploy real-time fraud detection with behavioural analytics and automated blocking
- Update incident response procedures to include rapid credential revocation and re-issuance for incident involving potential fraud or compromise of customer data
- Maintain and review a fraud management playbook annually to counter evolving fraud tactics
- Empower customers through regular awareness programmes

Eliminate systemic weaknesses through board-level and senior management tech risk oversight

What's new

- Mandatory identification of critical technology functions and their interdependencies
- Board and senior management must actively govern and review technology risks, including emerging threats, as a standing agenda.
- Reinforcement of the independence and authority of the Chief Information Security Officer (CISO)

Action points

- Map critical technology functions and dependencies
- Update governance charter to reflect new responsibilities

Build cyber resiliency to withstand evolving cyber threats

What's new

- The Cyber Resilience Framework (CRF) includes zero-trust architecture and advanced threat intelligence
- Mandatory proactive security testing
- Involvement of board and senior management in cybersecurity preparedness

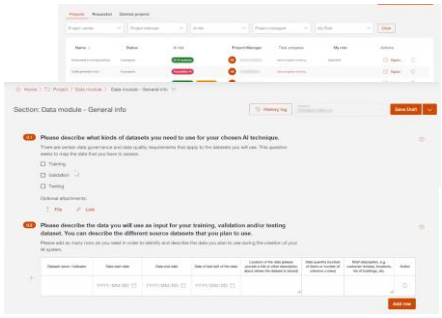
Action points

- Enhance the CRF to include layered defences such as zero-trust architectures and centralised technology asset tracking
- Establish a cyber risk management function to bolster cyber risk oversight
- Conduct quarterly vulnerability assessments, annual penetration tests, and Red Team exercises every three years
- Update Cyber Incident Response Plan to include out-of-band communication and cross-border incident handling
- Conduct annual cyber drills and ensure senior management and board-level engagement in cybersecurity preparedness

Our accelerator tools

AI-enabled technology and cyber compliance toolkit

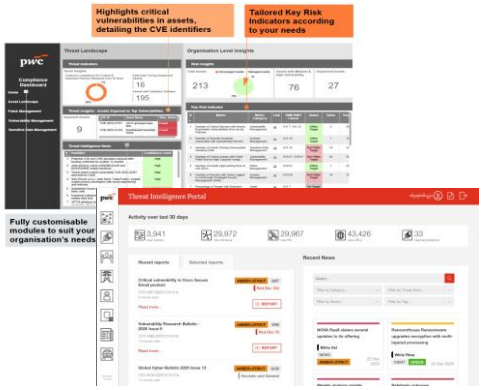
Our AI-powered compliance toolkit delivers faster, more accurate compliance assessments while reducing manual effort. It features a centralised library of technology and cyber-related regulatory guidelines—including RMiT, NACSA's Cyber Security Act (CSA) and its sector-specific guidelines, and the Securities Commission's Guidelines on Technology Risk Management (GTRM)—enabling timely responses to regulatory changes and sustained compliance.



CISO dashboard for real-time cyber risk and threat intelligence

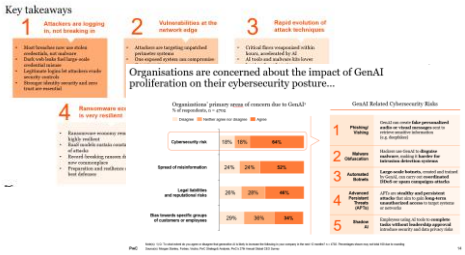
Our customisable CISO dashboard is designed to meet the practical needs of CISOs in Malaysia, providing a unified, real-time view of organisational risk and threat posture. Powered by enriched data connectors to PwC's Global Threat Intelligence Platform (TIP), it is scalable and adaptable to evolving local regulatory, industry, and threat landscape requirements.

By leveraging our solution without the need to build and maintain a dashboard from scratch, CISOs can remain laser-focused on what matters most—timely and effective threat response—while benefiting from consistent board-level reporting, key metrics, indicators, and actionable insights.



Board and senior management training and update pack

Our standardised training and update pack equips boards and senior management with targeted learning materials aligned to the latest requirements, enabling organisations to stay focused on meeting new regulatory expectations effectively.



Reach out to the team

Clarence Chan
Partner
Digital Trust and Cybersecurity Leader
PwC Malaysia
clarence.ck.chan@pwc.com

Kelvin Lee
Partner
Financial Services and Banking Leader
PwC Malaysia
kelvin.t.lee@pwc.com

Cathryne Teh
Director
Cybersecurity Governance, Risk and Compliance Lead
PwC Malaysia
pei.gee.teh@pwc.com

Alex Cheng
Director
Cybersecurity Threat Operations Lead
PwC Malaysia
alex.ct.cheng@pwc.com

Tanvinder Singh
Director
Cybersecurity Technology and Architecture Lead
PwC Malaysia
tan.singh@pwc.com

Choong Feng Lie
Senior Manager
Cybersecurity Governance, Risk and Compliance
PwC Malaysia
feng.lie.choong@pwc.com