SecurityScorecard

WHITE PAPER

Meeting BNM RMiT 2025: A Guide to Third-Party & Supply Chain Cyber Risk Requirements

A comprehensive guide for financial institutions, payment providers, and regulated entities meeting the expanded TPCRM obligations under Bank Negara Malaysia's updated Risk Management in Technology policy.

Executive Summary

Bank Negara Malaysia (BNM) updated its Risk Management in Technology (RMiT) policy on 28 November 2025, marking one of the most significant overhauls to Malaysian financial sector cybersecurity regulation in recent years. The revised framework expands applicability to new market participants, introduces mandatory continuous monitoring of third-party vendors, mandates Software Bill of Materials (SBOM) practices, and enforces stricter service-level agreement (SLA) requirements for incident disclosure and remediation.

For financial institutions, payment service providers, and other regulated entities now within RMiT's expanded scope — including certain non-bank merchant acquirers and intermediary remittance institutions meeting relevant BNM criteria — the updated RMiT is not merely a compliance exercise. It represents a fundamental shift in how cyber risk must be governed, especially across supply chains and vendor ecosystems. The consequences of non-compliance extend from regulatory censure to reputational damage and increased exposure to third party-originated breaches.

Third-party cyber risk just got harder to manage under RMiT 2025. This white paper examines the key changes introduced by the update, with particular focus on expanded Third-Party Cyber Risk Management (TPCRM) obligations and how SecurityScorecard helps institutions meet those obligations at scale with continuous, data-driven third-party risk monitoring.

2025
RMiT Revised
Revised and issued by BNM on 28 November 2025

Rising
Third-Party Risk
Third-party involvement in breaches is increasing sharply across the financial sector

12M+
Entities Rated
SecurityScorecard's global intelligence network

Understanding the Updated 2025 RMiT Framework

The Risk Management in Technology policy serves as the cornerstone of BNM's cybersecurity governance framework for the financial sector. Since its original issuance, RMiT has evolved to reflect the growing sophistication of cyber threats and the increasing reliance of financial institutions on digital infrastructure and third-party service providers.

What Changed in November 2025?

The 2025 revision introduced sweeping changes across several dimensions of technology risk management:

- **Expanded applicability:** The policy's scope has been extended to include certain non-bank merchant acquirers and intermediary remittance institutions meeting relevant BNM criteria, alongside traditional banking institutions. Organisations should verify their specific applicability with reference to the BNM policy document and, where appropriate, seek legal or regulatory guidance.
- **Strengthened cloud security controls:** Enhanced requirements for cloud service governance, including more rigorous due diligence on cloud service providers and clearer accountability structures.
- **Cyber resilience enhancements:** Stricter expectations for operational resilience, business continuity, and recovery time objectives for critical systems.
- **Fraud detection and prevention:** New controls addressing the increasing sophistication of financial fraud, including requirements for real-time monitoring and anomaly detection.
- **Third-party and supply chain risk management:** The most substantive expansion, introducing mandatory continuous monitoring, SBOM requirements, and enhanced vendor oversight obligations.

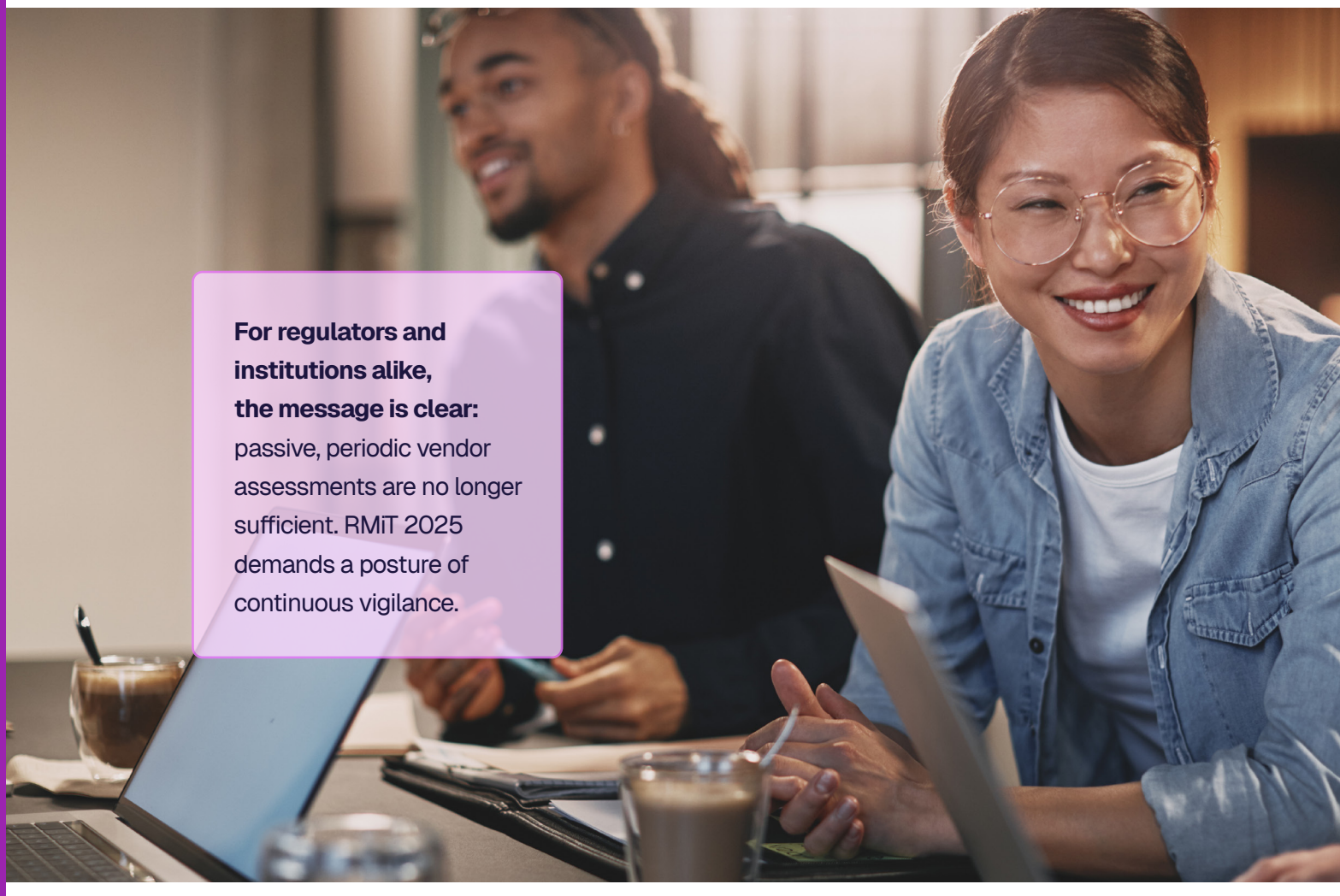
Regulatory Context

BNM's 2025 RMiT update aligns Malaysia's financial sector regulation with global best practices, including DORA (EU), the NIST Cybersecurity Framework, and evolving APAC standards. Entities regulated under RMiT must demonstrate compliance through both internal governance and documented evidence of third-party risk management practices.

Policy Objectives: Why This Matters Now

BNM's decision to revise RMiT in 2025 reflects a clear-eyed assessment of the threat landscape facing Malaysian financial institutions:

- Supply chain attacks have increased dramatically, with adversaries targeting vendors and technology providers as a route into financial institutions rather than attacking them directly.
- Open-source software dependencies have created new vectors for risk, with vulnerabilities in widely used libraries capable of compromising multiple institutions simultaneously.
- Cloud adoption has accelerated, making it critical for institutions to maintain visibility and control over their externally hosted systems and data.
- The proliferation of digital services has expanded the attack surface, requiring more comprehensive and continuous monitoring rather than periodic point-in-time assessments.



For regulators and institutions alike, the message is clear: passive, periodic vendor assessments are no longer sufficient. RMiT 2025 demands a posture of continuous vigilance.

Deep Dive: Expanded TPCRM & Supply Chain Cyber Controls

The most operationally significant changes in the 2025 RMiT revision relate to third-party cyber risk management and supply chain security. These changes demand that regulated institutions move from compliance-driven, checkbox-based vendor assessments to genuinely risk-informed, evidence-based oversight programs.

Mandatory Due Diligence for All Service Providers

RMiT 2025 introduces a tiered but comprehensive due diligence framework that extends obligations beyond primary vendors to include subcontractors and fourth-party relationships. Key requirements include:

- **Pre-engagement assessments:** Institutions must evaluate the cybersecurity posture, financial stability, and regulatory compliance of prospective service providers before entering into contracts.
- **Ongoing due diligence:** Assessments cannot be one-time exercises. Institutions must maintain current, evidence-based views of vendor security posture throughout the contract lifecycle.
- **Subcontractor visibility:** Due diligence obligations extend to material subcontractors used by primary vendors, recognising that fourth-party risk represents a significant and often underappreciated exposure.
- **Documentation requirements:** All due diligence activities must be documented and available for regulatory inspection, creating an audit trail that demonstrates the institution's risk governance in practice.

Continuous Monitoring Mandates

Perhaps the most transformative aspect of RMiT 2025 is the explicit requirement for continuous monitoring of third-party cybersecurity posture. This moves the compliance paradigm decisively away from annual audits and questionnaire-based assessments:

- **Real-time posture visibility:** Institutions must maintain up-to-date awareness of their vendors' security configurations, exposure to vulnerabilities, and incident history — not just a snapshot from the last assessment cycle.
- **SLA compliance monitoring:** Contractual service-level commitments must be actively monitored, with institutions required to demonstrate that they track vendor performance against agreed-upon security standards.
- **Incident notification timelines:** Vendors must notify institutions of material security incidents within defined timeframes, and institutions must have processes to receive, escalate, and respond to such notifications.
- **Remediation tracking:** Identified vulnerabilities and security gaps must be tracked through to remediation, with evidence of follow-up maintained in governance records.

Software Bill of Materials (SBOM) & Open-Source Risk

In a landmark development in Malaysian financial regulation, RMiT 2025 introduces requirements for software supply chain transparency through SBOM practices. This reflects growing global recognition that software component visibility is fundamental to managing cyber risk:

- **Software supply chain controls:** RMiT introduces software supply chain security requirements, including SBOM adoption to support vulnerability monitoring and open-source risk governance. Institutions are expected to maintain awareness of the software components underlying critical systems to enable timely identification and response to disclosed vulnerabilities.
- **Open-source governance:** Use of open-source software must be governed through formal processes that include license compliance, vulnerability tracking, and patch management for open-source dependencies.
- **Vendor software transparency:** Material technology vendors should provide sufficient visibility into the software components used in services delivered to the institution.
- **Vulnerability response:** When vulnerabilities are identified in software components — whether through SBOM analysis, threat intelligence feeds, or public disclosures — institutions must have defined processes to assess impact and drive remediation.

Enhanced SLA Enforcement & Incident Disclosure

RMiT 2025 significantly strengthens expectations around how institutions structure and enforce vendor contracts from a security perspective:

- **Mandatory security provisions:** Contracts with material service providers must include specific cybersecurity obligations, including minimum security standards, right-to-audit clauses, and incident notification requirements.
- **Defined incident disclosure windows:** Vendors must be contractually obligated to disclose material security incidents within defined timeframes, enabling institutions to take protective action and meet their own regulatory notification requirements.
- **Remediation timeframes:** Contracts should specify expected remediation timeframes for identified vulnerabilities, with escalation paths when vendors fail to remediate within agreed periods.
- **Termination rights:** Institutions must retain the right to terminate vendor relationships where security standards cannot be maintained and must have transition plans for such eventualities.

KEY INSIGHT: THE SBOM CHALLENGE

While SBOM requirements represent best-practice cyber governance, implementing them in practice is non-trivial. Organisations typically rely on hundreds of software packages, many of which contain dozens of transitive dependencies. Without automated tooling and threat intelligence integration, meeting SBOM-related obligations at scale is operationally infeasible for most institutions.

Challenges for Malaysian Financial Institutions

The expanded requirements under RMiT 2025 create real operational challenges for regulated entities. Understanding these challenges is the first step toward addressing them effectively.

Scale & Complexity of Vendor Ecosystems

Most financial institutions maintain relationships with hundreds or even thousands of third-party vendors, spanning technology infrastructure, software, professional services, and outsourced functions. Managing continuous monitoring across this ecosystem using manual processes — spreadsheets, questionnaires, periodic reviews — is neither scalable nor reliable. RMiT 2025 essentially requires institutions to instrument their vendor portfolios to provide persistent, evidence-based visibility, a requirement that demands automation.

Questionnaire Fatigue & Assessment Reliability

Traditional vendor risk assessments rely heavily on vendor-completed questionnaires. This approach has well-documented limitations: questionnaires are time-consuming to complete and review, responses may be outdated by the time they are submitted, and self-reported data cannot be independently verified. RMiT's emphasis on continuous monitoring implicitly acknowledges that questionnaire-based assessment alone is insufficient — institutions need objective, externally sourced data to complement self-reported information.

Fourth-Party Visibility Gaps

Identifying and monitoring subcontractors used by primary vendors represents a particularly difficult challenge. Institutions may have limited contractual visibility into their vendors' supplier relationships, and those vendors may in turn rely on additional layers of providers. This creates complex dependency chains that are difficult to map, let alone monitor. RMiT's requirements in this area push institutions toward supply chain mapping capabilities that they currently lack.

Regulatory Reporting & Evidence Production

As regulatory scrutiny of technology risk management intensifies, institutions face increasing demands to demonstrate the effectiveness of their TPCRM programs — not just to assert that they have processes in place, but to produce evidence of ongoing monitoring activities, risk decisions made, and remediation actions taken. Building and maintaining the documentation infrastructure to support this is a significant ongoing operational burden.

EMERGING THREAT CONTEXT

The financial sector in Southeast Asia has experienced a significant increase in supply chain attacks over recent years. Threat actors have demonstrated sophistication in targeting technology service providers to achieve lateral movement across multiple financial institutions simultaneously. BNM's RMiT 2025 update directly addresses this threat vector by mandating continuous, evidence-based monitoring capable of detecting supply chain compromise at scale.

SecurityScorecard's Approach to RMiT-Aligned Risk Management

SecurityScorecard is the global leader in cybersecurity risk ratings, delivering continuous, automated, outside-in security intelligence across vendor ecosystems. With more than 12 million entities rated globally, SecurityScorecard's platform is designed to support organisations in operationalising and evidencing key RMiT 2025-aligned controls — including continuous monitoring, vendor risk visibility, SLA tracking, vulnerability intelligence, and regulatory reporting.

Platform Capabilities Mapped to RMiT Requirements

Capability	How It Supports RMiT Compliance
Continuous Security Ratings	Automated, daily-updated security ratings across 10 risk factor groups — including network security, endpoint security, patching cadence, DNS health, application security, and hacker chatter — provide a continuous, evidence-based view of vendor cyber posture. Directly supports RMiT's continuous monitoring mandate.
Third-Party Risk Management	Purpose-built workflows for vendor onboarding, tiering, assessment, and ongoing monitoring at scale. Automates questionnaire distribution, collects vendor responses, and triangulates self-reported data with independent security ratings for a comprehensive risk picture.
Supply Chain Intelligence	Fourth-party mapping capabilities identify the technology providers and subcontractors behind primary vendors, providing visibility into supply chain dependencies that institutions cannot observe through direct relationships alone.
Automatic Alert & Incident Notifications	Real-time alerts notify institutions of material changes in vendor security posture — such as newly disclosed vulnerabilities, score degradation, or breach intelligence — enabling rapid, SLA-aligned response and regulatory incident-notification compliance.
Software Vulnerability Intelligence	Integration of CVE and vulnerability intelligence with vendor profiles enables institutions to assess exposure when new vulnerabilities are disclosed and track remediation progress, supporting SBOM-adjacent risk governance requirements.
Regulatory Reporting	Configurable reporting and evidence export capabilities enable institutions to generate documented evidence of monitoring activities, risk decisions, and remediation tracking for regulatory inspections and audits.
Automated Questionnaires	Pre-built questionnaire templates aligned to global frameworks (NIST, ISO 27001, and others) accelerate vendor assessment programs. Responses are automatically scored and triangulated with independent data to reduce questionnaire fatigue and improve assessment quality.
Benchmarking & Peer Comparison	Industry and peer benchmarking enable institutions to contextualise their own security posture and that of their vendor portfolios relative to comparable organisations, supporting board-level reporting and regulatory dialogue.

RMiT Requirement-to-Capability Mapping

RMiT Requirement	Key Obligation	SecurityScorecard Capability
Mandatory vendor due diligence (pre-engagement & ongoing)	Evidence-based assessment of cybersecurity posture before and throughout vendor relationships	Continuous security ratings + automated questionnaires provide objective, current due diligence evidence
Continuous third-party monitoring	Persistent visibility into vendor security posture, not periodic point-in-time	Daily updated ratings across 10 factor groups with real-time alert triggers
Subcontractor & fourth-party oversight	Visibility into vendors' own supplier relationships and technology dependencies	Supply chain intelligence maps fourth-party dependencies automatically
SBOM & open-source risk governance	Software component visibility; tracking of open-source vulnerabilities	Vulnerability intelligence and software exposure tracking integrated with vendor profiles
Incident disclosure & SLA enforcement	Rapid notification of material vendor security incidents; contractual SLA compliance	Real-time breach intelligence alerts enable immediate notification and response workflows
Documentation & regulatory evidence	Audit trail of TPCRM activities available for regulatory inspection	Configurable reporting exports provide timestamped evidence of monitoring activities and decisions

Use Cases & Implementation Models

The following use cases illustrate how SecurityScorecard helps Malaysian financial institutions operationalise and evidence key RMiT 2025-aligned controls in practice.

USE CASE 1

Continuous Vendor Portfolio Monitoring at Scale

A mid-sized Malaysian bank maintains relationships with over 400 technology and service vendors. Under RMiT 2025, it must demonstrate continuous monitoring of cybersecurity posture across this portfolio — not just for tier-1 critical vendors, but for all material service providers.

- SecurityScorecard ingests the institution's vendor list and immediately begins monitoring all entities using outside-in telemetry — no vendor action required.
- Daily-updated security ratings flag any vendor whose score falls below the institution's defined risk appetite thresholds, triggering automated alerts to the vendor risk team.
- The institution's risk team can, at any point, evidence the security posture of its entire vendor portfolio — with timestamped historical data demonstrating continuous monitoring.
- Regulatory reporting is generated directly from the platform, reducing the time required to prepare evidence for BNM inspection from weeks to hours.

USE CASE 2

Third-Party Incident Response

A significant vulnerability is disclosed in a widely used database software product. Several of the institution's vendors are likely affected, but the institution does not know which are exposed.

- SecurityScorecard's vulnerability intelligence identifies which vendors in the institution's portfolio have exposure to the affected software, drawing on outside-in telemetry and CVE data.
- The institution is alerted within hours of the vulnerability disclosure, with a prioritised list of affected vendors and recommended response actions.
- Remediation tracking capabilities enable the institution to follow up with affected vendors and document their progress — supporting the evidence of RMiT-aligned, continuous vendor oversight.
- The entire workflow — from vulnerability identification to vendor notification to remediation closure — is documented within the platform, providing a complete audit trail.

USE CASE 3

New Vendor Onboarding & Due Diligence

A payment service provider newly subject to RMiT 2025 must establish a compliant vendor onboarding process that meets the policy's due diligence requirements.

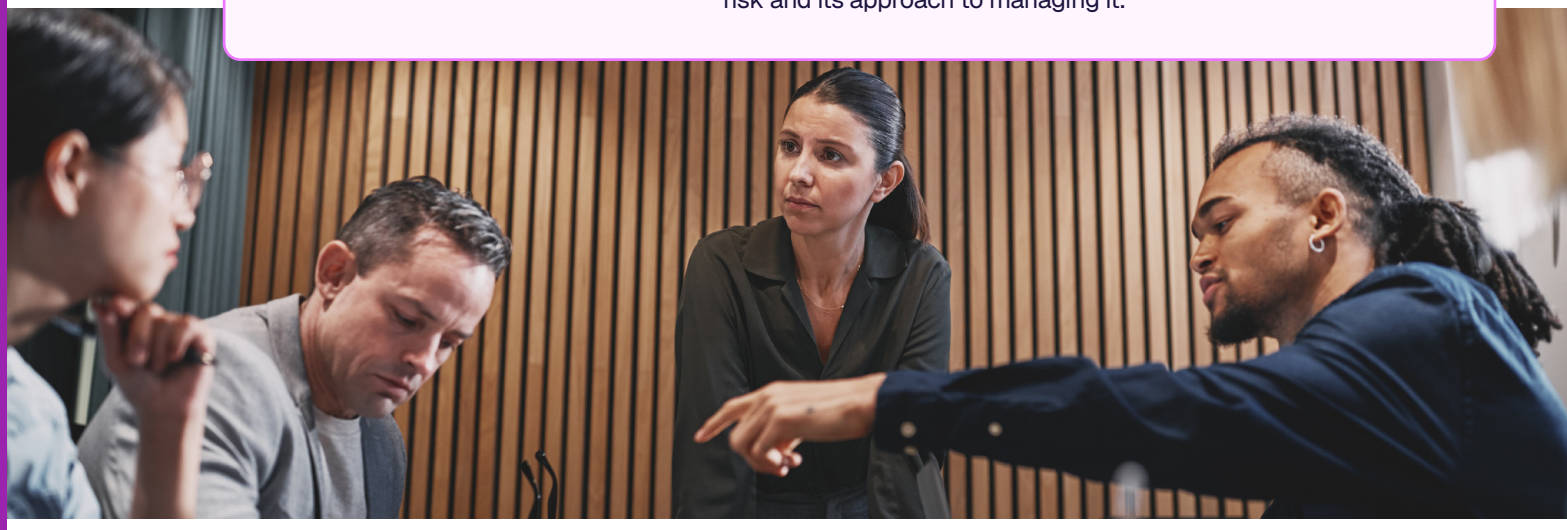
- SecurityScorecard's automated assessment workflows initiate an outside-in security rating for any prospective vendor as part of the onboarding process, providing immediate, objective risk data.
- A standardised questionnaire aligned to RMiT requirements is dispatched to the vendor, with responses scored and triangulated against the independent rating.
- Risk tiering is applied based on a combination of security posture, data access scope, and operational criticality, ensuring that oversight intensity is proportionate to risk.
- The completed assessment — including rating evidence, questionnaire responses, and risk tier decision — is stored within the platform and available for regulatory inspection.

USE CASE 4

Supply Chain Mapping for Fourth-Party Risk

A financial institution needs to understand its exposure to a cloud infrastructure provider that is used by multiple primary vendors — creating a concentration risk that is invisible through direct vendor monitoring alone.

- SecurityScorecard's supply chain intelligence capability maps the technology dependencies of primary vendors, identifying shared infrastructure providers and subcontractors.
- The institution identifies that seven of its top 20 vendors share a common cloud infrastructure provider, creating a previously unrecognised concentration risk.
- The cloud infrastructure provider is added to the monitoring program, and a contingency planning exercise is initiated to assess the institution's exposure in the event of a material incident affecting that provider.
- The supply chain map is documented and available for regulatory review, demonstrating the institution's awareness of fourth-party risk and its approach to managing it.



Conclusion & Call to Action

The 2025 update to BNM's Risk Management in Technology policy represents a decisive shift in how Malaysian financial institutions must approach third-party and supply-chain cyber risks. The era of periodic questionnaire-based vendor assessments — already recognised as inadequate in an environment of increasingly sophisticated supply chain attacks — is now explicitly superseded by a regulatory expectation of continuous, evidence-based monitoring.

For institutions subject to RMiT, the compliance journey involves three parallel workstreams:

- **Policy and governance:** Updating vendor risk management policies, contractual frameworks, and internal processes to reflect RMiT 2025 requirements.
- **Technology capability:** Deploying automated tooling capable of providing continuous, scalable monitoring across large and complex vendor portfolios.
- **Evidence and reporting:** Building the documentation infrastructure and reporting capability to demonstrate compliance with BNM and other stakeholders.

SecurityScorecard supports the technology capability workstream by providing the automated, data-driven monitoring infrastructure that helps organisations operationalise and evidence key RMiT-aligned controls. Beyond the compliance dimension, SecurityScorecard helps reduce genuine exposure to third-party-originated breaches — the underlying risk that RMiT 2025 was designed to address.

TAKE THE NEXT STEP

Ready to assess your current third-party risk management program against RMiT 2025 requirements? SecurityScorecard offers a complimentary risk posture assessment for Malaysian financial institutions navigating the updated policy. Visit securityscorecard.com or contact your regional SecurityScorecard representative to schedule a consultation.

About SecurityScorecard

SecurityScorecard is transforming how organizations defend against the fastest growing threat vector – supply chain attacks. Our industry-leading security ratings serve as the foundation and core strength, while our AI-powered (or threat-informed) TPRM solutions continuously monitor third-party risks using our factor-based ratings, automated assessments and proprietary threat intelligence, to resolve threats before they become breaches. MAX enables response and remediation capability, working through our service partners to protect the entire supply chain ecosystem while strengthening operational resilience, enhancing third-party risk management, and mitigating concentrated risk.

Trusted by over 3,000 organizations—including two-thirds of the Fortune 100—and recognized as a trusted resource by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Backed by Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, NGP, Intel Capital, and Riverwood Capital, SecurityScorecard delivers end-to-end supply chain cybersecurity to safeguard business continuity. For more information, visit securityscorecard.com or connect with us on LinkedIn.

securityscorecard.com | marketing-apac@securityscorecard.com

SecurityScorecard