Compliance with Malaysia Risk Management in Technology (RMiT) Using RidgeBot

RIDGE SECURITY

Protect Financial Institutions and Transactions from Technology Risks

Abstract

This white paper discusses how RidgeBot capabilities—including asset discovery, attack surface identification, iterative security validation, automated and on-demand penetration testing, and vulnerability exploitation and remediation—can help Malaysian financial institutions comply with the legal requirements regarding the strength of technology and digital security in their operations.

Introduction

The Malaysian government regulates and monitors the technology risk management of financial institutions operating in Malaysia through its Central Bank (Bank Negara Malaysia). Technology risk emanates from the use of improperly secured IT systems, applications, platforms, networks or infrastructure, as well as services accessed via the Internet or cloud platforms. Security failures or breaches can result in financial loss, disruptions in financial services or operations, customer vulnerability, or reputational harm to a financial institution.

The use of technology in providing financial services is increasingly prevalent, compelling financial institutions to bolster their technology resilience against, and awareness of, operational disruptions. The growing sophistication of cyber threats requires increased vigilance and strengthened capability to respond to emerging threats in a fast-changing landscape. Digital security measures must ensure continuous availability of financial services to customers and adequate protection of customer data.

The Malaysia Risk Management in Technology (RMiT) policy document went into effect on 1 January 2020, and sets out the Central Bank's requirements of financial institutions' technology risk management. Incorporating RidgeBot's cost-effective capabilities in your institution's ongoing security procedures and operations significantly amplifies your ability to meet and exceed RMiT requirements.

RMiT Legal Compliance

The RMiT policy document consists of 8 Sections and 9 Appendices that detail the regulations that must be complied with. The sections comprise the legal requirements organizations must follow to demonstrate compliance, while the appendices provide additional supportive information directly referenced from the applicable sections.

Several sections comprise requirements of the human behavior and management procedures (covering boards, committees, management staff and employees) of a financial institution, while others explicitly address technology resilience where RidgeBot can be of help in complying.

RMiT Content Outline

To provide perspective on where RidgeBot can help with compliance, the structural outline of the RMiT policy document is given below, highlighting the specific sections that concern the protection of technology resources. The full text of the specification can be viewed here.

PART B: Policy Requirements

- **Section 8: Governance**
- **Section 9: Technology Risk Management**
- **Section 10: Technology Operations Management**
- **Section 11: Cybersecurity Management**
- **Section 12: Technology Audit**
- Section 13: Internal Awareness and Training

PART C: Regulatory Process

- Section 14: Notification for Technology-Related Applications
- Section 15: Assessment and Gap Analysis

Appendices

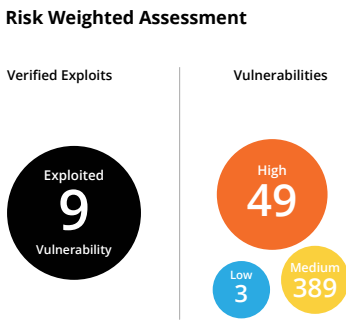
- **Appendix 1: Storage and Transportation of Sensitive Data in Removable Media**
- **Appendix 2: Control Measures on Self-service Terminals (SST)**
- **Appendix 3: Control Measures on Internet Banking**
- **Appendix 4: Control Measures on Mobile Application and Devices**
- **Appendix 5: Control Measures on Cybersecurity**
- Appendix 6: Positive List for Enhancements to Electronic Banking, Internet Insurance and Internet Takaful Services
- Appendix 7: Risk Assessment Report
- Appendix 8: Format of Confirmation
- Appendix 9: Supervisory Expectations on External Party Assurance

Overview of How RidgeBot can Help

RidgeBot helps you find security deficits in your assets, and provides guidance and priority ranking on how to immediately remediate any exposures. Moreover, RidgeBot helps you maintain, on a continuing and cost-effective basis, a security posture that is always in compliance with the latest attack methods and threat intelligence.

Some of RidgeBot's key benefits to your organization's security posture include:

- **Improve and Simplify Security Activities and Process**
  - Discover, inventory and document system components, assets and attack surfaces. Because RidgeBot is fully automated, you can do this continuously, or at much more frequent intervals, than previous periodic manual processes.
  - Reports help document vulnerabilities found, exploited, remediated and validated.
  - Reports provide clear risk ranking to focus manual remediation activity on the highest risk vulnerabilities.
  - RidgeBot's flexibility allows you to run attack testing from inside and outside your environment.
  - RidgeSecurity's Threat Intelligence Platform knowledge base ensures that you are always up to date with industry-leading security vulnerability information.
  - Run RidgeBot attacks and scans as a standard part of your ongoing security policy.



- **Continuous Security Validation**
  - RidgeBot provides no-cost iterative, continuous hardening and asset inventory. You can run different scans periodically or continuously—because it is fully automated, no manual intervention is required until a vulnerability is reported.
  - Continuous monitoring and asset discovery protect against hacker intrusion caused by an employee (or any other person) accidentally or maliciously connecting untrusted or unplanned IoT, wireless or other unauthorized devices to the environment.
  - Scan reports provide a short list of must-fix exploitable vulnerabilities to document and resolve. Report output ensures all software patches and updates needed to resolve dangerous vulnerabilities are installed on all affected assets.
- **DevOps/SecOps Software Development and Patch/Release Testing**
  - Use RidgeBot during the software development process to help ensure that dangerous coding practices that introduce vulnerabilities never ship in new releases of software.
  - Use RidgeBot to harden software patches, software upgrades, new devices, and any configuration changes before pushing them into the production environment.

- **Security Posture Validation**
  - Continuously, iteratively attack the production environment to maintain security posture and discover misconfigurations in wireless or defensive security appliances or services such as firewall rules or UTM appliances.
  - Continuously monitor and harden login credentials on sensitive assets.
- **Compliance Audit**
  - Continuous asset discovery scanning, and attack and exploitation attempts (and the reports issued) mean your environment is always audit-ready.
  - Use RidgeBot reports to submit evidence of vulnerabilities probed, remediated and resolved.
- **Security Incident Response**
  - Scan reports, containing recommended solutions for each vulnerability found, provide critical information to your security incident response/escalation team.
  - Risk ranking of vulnerabilities feed into the priorities and procedures for incident response.
  - RidgeBot AI/ML exploitation attacks provide forensic capabilities to investigate the origin and path taken by a breach, as well as step-by-step guidance on how to resolve the entry point vulnerability.

RidgeBot includes several template scans that you can easily use, as well as the flexibility to completely customize your own scans. The system templates include:

- **Full scan:** This test launches numerous attack techniques used by real-world hackers. Based on threat intelligence and an exploit knowledge base, RidgeBot profiles assets, mines vulnerabilities and launches attacks against target assets, which may be internal or external to your environment, in a private or public environment.
- **Ransomware scan:** This test is specifically focused on combating ransomware attacks. It launches scans for 27 high-profile ransomware entry point vulnerabilities, includes the ability to attack and exploit these vulnerabilities, and reports in detail exactly how successful exploitations were achieved. Definitions of more ransomware attacks will be added over time, and you can add these to your security arsenal by downloading periodic RidgeBot updates.
- **Weak password scan:** This test launches direct or iterative attacks based on sensitive information collected via weak credential or unauthorized access vulnerabilities. Attack targets include redis, elasticsearch, ActiveMQ, database, web login and other applications.
- **Struts 2 scan:** This test launches direct or iterative attacks based on known 1-day or n-day vulnerabilities detected on targets using the Struts 2 framework.
- **Weblogic scan:** This test launches direct or iterative attacks based on known 1-day or n-day vulnerabilities detected on targets using Weblogic middleware.
- **Web scan:** This test launches cyberattacks against target websites, web applications and all related attack surfaces to gain control of the target website for both self-developed and contact management system-based websites.
- **Host scan:** This test launches direct or iterative attacks from inside a corporate network to validate the security system's response to an internal threat. Target systems include all network-accessible internal hosts and servers.

RMiT Technical Requirements

Salient extracts of the RMiT requirements that pertain to technical data-and-network security posture are enumerated below. The full text of the Bank Negara Malaysia's Risk Management in Technology (RMiT) specification can be viewed here.

- An "S" accompanying a requirement denotes a **standard**, an obligation, a requirement, specification, or provision that must be complied with.
- A "G" accompanying a requirement denotes **guidance** to promote common understanding, advice or recommendations that are encouraged to be adopted.

Specific RidgeBot capabilities that can help you comply with the RMiT regulations are summarized in the next section entitled "RidgeBot Capabilities Summary". The entries in the right-most column in the tables below provide a cross-reference to each specific RidgeBot capability that can help you comply with each RMiT regulation.

Part B, Section 8: Governance

Requirement	Description Extract	RidgeBot Reference
8.3 "S"	"…the effective implementation of a sound and **robust technology risk management framework (TRMF) and cyber resilience framework (CRF)**, as required to be developed under paragraphs 9.1 and 11.2… safeguard the financial institution's information infrastructure, systems and data… ensuring the financial institution's cyber resilience… also **periodically review and affirm** the TRMF and CRF, at least once every three years…"	All RidgeBot capabilities
8.4 "S"	"…the committee shall… ensure that **risk assessments** undertaken in relation to material technology applications… **are robust and comprehensive**."	R1, R2
8.7 "S"	"…audit committee… is responsible for ensuring the effectiveness of the **internal technology audit function**…"	A2, A3, D2, S1, S4, W1

Part B, Section 9: Technology Risk Management

Requirement	Description Extract	RidgeBot Reference
9.2 "S"	"…The TRMF must include… (e) **risk measurement and assessment** approaches and methodologies; (f) risk controls and **mitigations**; and (g) **continuous monitoring** to timely detect and address any material risks."	A2, A3, D2, R1, R2, S3, V1, V2, W1

Part B, Section 10: Technology Operations Management

Requirement	Description Extract	RidgeBot Reference
10.1 "S"	"…This shall include project oversight… and **risk assessments** throughout the project life cycle."	S3, V1, V2, V4
10.2 "S"	"…The **risk assessments** shall identify and address the key risks arising from the implementation of technology projects… (e) the robustness of system and user **testing strategies to reduce risks** of undiscovered system faults and functionality errors…"	D1, R1, V1, V2, V4
10.5 "S"	"…must establish clear risk management policies and practices for the key phases of the system development life cycle (SDLC) encompassing system design, development, **testing, deployment, change management**, maintenance and decommissioning…"	A2, D1, R1, V1-5, W1
10.6 "G"	"…encouraged to deploy **automated tools** for software development, **testing, software deployment, change management**…"	A1, A3, S3, S4
10.8 "S"	"…establish a sound methodology for **rigorous system testing** prior to deployment…"	A3, S3, V1, V2, V4
10.9 "G"	"…[In addition to 10.8] should include… **application security testing**, stress and **regression testing**…"	S3
10.10 "S"	"…ensure… changes to the source code… [are] **secure… prior to introducing any system changes.**"	V1, V2, V4
10.24 "S"	"…shall host critical systems in a dedicated space… [that] must be physically **secured from unauthorised access**…"	S2, V3, W1-2
	"…required to appoint [an] external service provider to carry out a production **data centre resilience and risk assessment** (DCRA)… [T]he assessment [must be] conducted at least **once every three years or whenever there is a material change** in the data centre infrastructure…"	A3, D2, R1, R2, S1, S3, S4, V5, W1-2
10.33 "S"	"…must design a reliable, scalable and **secure enterprise network**…"	A1-2, D2, R1, S1, S3, V1, V5, W1
10.36 "S"	"…ensure network services supporting critical systems are designed and implemented to ensure the **confidentiality**, integrity and availability…"	W1-2
10.37 "S"	"…establish and maintain a **network design blueprint** identifying all of its internal and external network interfaces and connectivity…"	A1-3
10.38 "S"	"…ensure sufficient and relevant network **device logs** are retained for investigations and forensic purposes…"	S2, V3, W2
10.40 "S"	"…required to appoint [an] external service provider to carry out regular **network resilience and risk assessments** (NRA)…"	S4
10.42 "S"	"…conduct proper due diligence on the third-party service provider's competency, **system infrastructure**… prior to engaging its services… an **assessment** shall be made of the third-party service provider's capabilities in managing… specific risks… (e) **cyber threats**…"	S1
10.47 "S"	"…ensure the storage of its data… There shall be proper controls over and periodic review of the **access provided to authorised users**."	W1-2
10.49 "S"	"…must fully understand the inherent risk of adopting cloud services… to conduct a comprehensive **risk assessment prior to cloud adoption**… (g) **exposure to cyber-attacks** via cloud service providers…"	S1
10.61 "S"	"…must ensure… (a) access controls to enterprise-wide systems are **effectively managed and monitored**; and (b) user activities in critical systems are **logged for audit** and investigations…"	S2, V3, W2
10.62 "S"	"…institutions are required to… (b) deploy **automated audit tools** to flag any anomalies."	A1, A3, S3, S4, V4

Requirement	Description Extract	RidgeBot Reference
10.63 "S"	"…must ensure that critical systems are not running on outdated systems with **known security vulnerabilities**…"	V2, V4, V5
10.65 "S"	"…must establish a… management framework which addresses… (a) identification and risk assessment of all technology assets for **potential vulnerabilities** arising from undeployed patches… (b) conduct of compatibility **testing for critical patches**…"	V2, V4, V5
10.76 "S"	"…must ensure… [that] **digital service logs** are retained for investigations and forensic purposes for at least three years."	S2, V3, W2
10.81 "S"	"…must perform continuous surveillance to **assess the vulnerability** of the **operating system** and… technology **platform** used for its digital delivery channels to security breaches… In view of the evolving threat landscape, these safeguards must be **continuously reviewed and updated**…"	A3, D2, R1, V5

Part B, Section 11: Cybersecurity Management

Requirement	Description Extract	RidgeBot Reference
11.1 "S"	"…must ensure that there is an **enterprise-wide focus** on effective cyber risk management…"	A1-2, D2, R1, S1, S3, V1, V5, W1
11.2 "S"	"…must be able to support the effective **identification, protection, detection,** response, and recovery (IPDRR) of systems and data…"	D2, D3, D4, R1-2, S3
11.3 "S"	"…must consist of… (b) **identification**, classification… of critical systems, information, **assets and interconnectivity**… to obtain a **complete and accurate view** of the… information assets, critical systems, interdependencies and cyber risk profile… (c) **identification of cybersecurity threats** and countermeasures…"	A1-3, D2, R1
11.4 "S"	"…is required to (a) implement a centralised **automated tracking system** to manage its technology **asset inventory**… (b)(i) perform detailed analysis on cyber threats, **provide risk assessments** on potential cyber-attacks… (b)(ii) proactively **identify potential vulnerabilities** including those arising from [third-party] infrastructure…"	A1-3, D2, R1, S3, V1, V5
11.5 "S"	"…must establish clear responsibilities for cybersecurity operations… include implementing appropriate **mitigating measures**… that correspond to the… phases of the cyber-attack lifecycle: (a) **reconnaissance**…"	D2, R1, S1, S3, V5
11.7 "S"	"…must deploy effective tools to support the **continuous and proactive** monitoring and timely **detection** of anomalous activities in its technology infrastructure…"	A2, A3, D2, R1, R2, S3, V1, V2, W1
11.8 "S"	"…must ensure that its cybersecurity operations **continuously prevent and detect** any potential **compromise of its security controls** or weakening of its security posture…"	A3, S2, V3, W2
11.9 "S"	"…must conduct annual intelligence-led **penetration tests** on its internal and external network infrastructure as well as critical systems including web, mobile and all external-facing applications… must engage suitably accredited penetration testers and service providers to perform this function."	S4, V1-5, W1
11.10 "S"	"…must undertake independent **compromise assessments** on the technology infrastructure of its critical systems…"	S4
11.11 "S"	"…must establish standard operating procedures (SOP) for **vulnerability assessment and penetration testing** (VAPT) activities…"	R1-2, S1, S3, V5
11.12 "S"	"…must ensure the outcome of the **penetration testing exercise is properly documented**…"	D1-2

Requirement	Description Extract	RidgeBot Reference
11.13 "S"	"…must ensure its technology systems and infrastructure, including critical systems outsourced to or hosted by third party service providers, are adequately **protected against all types of DDoS attacks**…"	A1-3, D1, D3, R1, S1, V5
11.18 "S"	"…must be able to perform… (c) **vulnerability management**; (d) **threat hunting**…"	D2, D3, A1-2, R1
11.19 "S"	"…must ensure that the SOC [Security Operations Centre] provides a regular threat assessment report… (b) **intelligence on emerging and potential threats** including tactics, techniques and procedures (TTP)…"	V5
11.20 "S"	"…must **subscribe to reputable threat intelligence services** to identify emerging cyber threats…"	V5

Part B, Section 12: Technology Audit

Requirement	Description Extract	RidgeBot Reference
12.2 "S"	"The internal audit function must be adequately **resourced with relevant technology** audit competencies…"	S3
12.4 "S"	"In addition to… 12.2… must establish a dedicated internal technology audit function that has **specialised technology audit competencie**s to undertake technology audits."	All RidgeBot capabilities
12.5 "S"	"…must establish a technology audit plan that provides **appropriate coverage of critical technology services**…"	A1, D1, R1

Appendices

Appendix / Control	Description Extract	RidgeBot Reference
Appendix 1: Storage and Transportation of Sensitive Data in Removable Media		
Control 2	"Implementing authorised access control to sensitive data (e.g. **password protection**, user access matrix)."	W1-2
Appendix 2: Control Measures on Self-service Terminals (SSTs)		
Cash SST Control 3	"Ensuring Cash SST operating system is running on a **secure version operating system** with continued developer or vendor support for **security patches** to fix any operating system security and vulnerabilities."	S3, V1, V5
Cash SST Control 9	"Enforcing firewall and Intrusion Prevention System (IPS) at the financial institution's network **to filter communication** between the host server and the Cash SST."	A1, S1
Cash SST Control 13	"Enforcing secure system parameter setting… (a) **changing defaults password**…"	W1-2
Cash SST Control 17	"Installing **closed-circuit cameras** and transaction triggered cameras…"	A3, S2, V3, W2
Non-cash SST Control 2	"Deploying **closed-circuit television** to monitor…"	A3, S2, V3, W2
Non-cash SST Control 3	"Ensuring adequate control over **network security** of the self-service terminals to ensure that the **kiosks are secured** and segregated from the internal network…"	A2, S1

Appendix / Control	Description Extract	RidgeBot Reference
Appendix 3: Control Measures on Internet Banking		
Control 1(a)	"…should ensure the adequacy of security controls implemented for Internet banking… (a) Ensure Internet banking only **runs on secured versions of web browsers** that have continued developer support for security patches to fix any vulnerabilities…"	A1, D1, R1, S1, S3, V1-5, W1
Appendix 4: Control Measures on Mobile Application and Devices		
Control 1(c)	"…undertake proper due diligence processes to ensure the **application distribution platforms** used to distribute the mobile application are reputable."	A2, S1, W1
Appendix 5: Control Measures on Cybersecurity		
Control 1	"Conduct periodic review on the configuration and rules settings for all security devices. Use **automated tools** to review and monitor changes to configuration and rules settings."	A1-3, D2, S3, S4, V4, W2
Control 4	"Ensure technology **networks are segregated** into multiple zones… each zone shall be adequately protected by… firewall and Intrusion Prevention System (IPS)… must include mobile and wireless networks…"	A1-3
Control 6(d)	"Ensure security controls for remote access to server… **close relevant ports** immediately upon expiry of remote access."	D2, R1
Control 8	"…protect the Network Time Protocol (NTP) **server against tampering**."	A1, R1, S1

RMiT Technical Requirements

RidgeBot Reference	Capability Description
Automated Asset Discovery and Inventory	
A1	Automated asset discovery can help you compile and maintain an **inventory** of all data processing assets and attack surfaces.
A2	An asset discovery scan iteratively **discovers and documents changes** in the presence of assets that should be included in a risk assessment or asset inventory.
A3	An automated asset discovery scan verifies on an ongoing basis that **no new, unplanned devices are connected to the infrastructure that can introduce vulnerabilities**. For example, an attacker might set up a rogue wireless access point, or install an IoT device that allows remote access to the internal network.
Documentation, Reporting and Forensics	
D1	Regular automated asset discovery scans on an ongoing basis can help **ensure all assets and attack surfaces are identified and documented**.
D2	Scan-and-exploitation reports can assist you in **compiling consistent and comparable documentation of vulnerabilities** found, vulnerability ranking, successful exploits, and the mitigation and remedial steps taken. This information can be used to take mitigation actions and/or to prepare management reports.
D3	Scan-and-exploitation reports—which include recommended solutions for each vulnerability—provide critical information for your **security incident response/escalation or forensics** team to ensure timely and effective handling of all situations.
D4	A forensic scan—after a security incident has occurred—can help **determine where and how the breach was perpetrated**. From there it can be extrapolated as to which systems and what data might have been exposed.
Risk Assessment and Mitigation	
R1	A pen-test-and-exploit scan identifies, analyzes and evaluates all risks found. The scan reports provide **a ranked list of vulnerabilities found** based on each vulnerability's likelihood to be exploited, including those that were successfully exploited during the test. The reports also provide an evaluation with granular steps to remediate each vulnerability.
R2	The recommended **remedial steps in RidgeBot reports** provide evidence that risks are being adequately found, measured, reviewed and treated.
Scanning and Penetration Testing	
S1	A pen-test-and-exploit scan helps **verify the security posture of all internal systems**, as well as any **provider- or cloud-hosted** assets and services.
S2	A pen-test-and-exploit scan can **reveal weak points in physical security processes and systems** (cameras, surveillance systems, logging systems, digitally-controlled door locks) that could grant an attacker physical or electronic access to secure systems or areas, or allow tampering with surveillance cameras or stored logs or footage.
S3	Automated pen-test-and-exploit capabilities can be run cost-effectively as frequently as necessary, rather than doing occasional one-time tests. This ensures peace of mind that your **assets are continually locked-down and that new vulnerabilities are detected immediately** after—or often before—they're introduced into your production environment.
S4	Automated pen-test-and-exploit capabilities can be run iteratively and cost-effectively to **prepare for an audit or a third-party verification** of your security posture.

RidgeBot Reference	Capability Description
Vulnerability Exploitation and Intelligence	
V1	A full scan, with exploitation turned on, **discovers, exploits and documents all vulnerabilities** found. Run this scan as a regular part of your policy/process for hardening software patches, software upgrades, new devices, and any configuration changes before pushing them live into the production environment.
V2	A full scan, with exploitation turned on, discovers, exploits and documents all vulnerabilities found. Run this scan as a **regular part of your software development and software validation processes**.
V3	A pen-test-and-exploit scan can ensure that **all systems or devices used to document events and activities are secure from software/malware vulnerabilities** where a hacker can get access to erase or alter logs, video surveillance footage, or forensic audit trail information.
V4	A pen-test-and-exploit scan can be run as a regular part of your policy/process to **harden software patches, software upgrades, new devices, and any configuration changes** before pushing them live into the production environment.
V5	RidgeBot's built-in AI/ML exploitation engine uses RidgeSecurity's **industry leading knowledge base of attack techniques and intelligence**, and ensures that your assets are always hardened with the most up to date vulnerability information. It is the best way to **stay abreast of emerging technical vulnerabilities** in a structured and systematic way.
Weak Password and Credentials	
W1	A weak password scan run against all assets **documents and resolves login credential vulnerabilities**.
W2	A pen-test-and-exploit scan can ensure that **all systems or devices used to document events and activities are secure from weak credential** vulnerabilities where a hacker can get access to erase or alter logs, video surveillance footage, or forensic audit trail information.

Ridge Security Technology Inc.

www.ridgesecurity.ai