New Policy from Bank Negara Malaysia - Risk Management in Technology (RMiT)

RMiT comes into effect 2020 and applies to Financial Institutions

Bank Negara Malaysia issued the Risk Management in Technology policy document (RMiT) on July 18, 2019, which sets out Bank Negara's requirements regarding financial institutions' management of technology risk.

The new policy will come into effect on January 1, 2020 and covers the implementation of a comprehensive technology risk management framework. The policy applies regardless if the financial institution operates the data center themselves or if they are working with an outsourcing partner.

Further, the policy states "A financial institution must perform a gap analysis of existing practices in managing technology risk against the requirements in this policy document and highlight key implementation gaps. The financial institution must develop an action plan with a clear timeline and key milestones to address the gaps identified particularly for gaps that extend beyond the effective date of this policy document. The gap analysis and action plan must be submitted to the Bank no later than 18 October 2019."

This is how we help organizations to comply with RMiT security obligations

The RMiT policy contains requirements as well as guidelines. In this document we have considered the standards, requirements or specifications that must be complied with and where failure to comply may result in one or more enforcement actions according to Bank Negra.

Holm Security VMP Vulnerability Management platform (VMP) enables financial institutions to effectively and systematically comply with key requirements as described by policy.
In the table below "S" denotes a standard, requirement or specification that must be complied with.

RMiT will apply to:

- ✓ Licensed banks
- ✓ Licensed investment banks
- ✓ Licensed Islamic banks
- ✓ Licensed insurers including professional reinsurers
- ✓ Licensed takaful operators including professional retakaful operators
- ✓ Prescribed development financial institutions
- ✓ Approved issuer of electronic money
- ✓ Operator of a designated payment system

"S" denotes a standard, requirement or specification that must be complied with. Failure to comply may result in one or more enforcement actions;

Reference:
Risk Management in Technology (RMiT), BNM/RH/PD 028-98
Issued on: 18 July

HOLM SECURITY

Policy Requirement			Holm Security VMP Solution
Compliance level	Patch and End-of-Life System Management		
	Chapter		
S	10.63	A financial institution must ensure that critical systems are not running on outdated systems with known security vulnerabilities or end-of-life (EOL) technology systems. In this regard, a financial institution must clearly assign responsibilities to identified functions: (a) to continuously monitor and implement latest patch releases in a timely manner; and (b) identify critical technology systems that are approaching EOL for further remedial action	b) Holm Security VMP can provide crucial information regarding patch information, EOL, and security vulnerabilities in network systems and web applications. Holm Security VMP also provides remediation possibilities within the platform.
S	10.65	A financial institution must establish a patch and EOL management framework which addresses among others the following requirements: (a) identification and risk assessment of all technology assets for potential vulnerabilities arising from undeployed patches or EOL systems;	(a) Holm Security VMP network scanning engine allows scheduled and on-demand assessment possibilities. Fulfilling the needs set in 10.65.
S	10.81	A financial institution must perform continuous surveillance to assess the vulnerability of the operating system and the relevant technology platform used for its digital delivery channels to security breaches and implement appropriate corresponding safeguards. At a minimum, a financial institution must implement sufficient logical and physical safeguards for the following channels: (a) self-service terminal (SST); (b) non-cash SST; (c) Internet banking; and (d) mobile application and devices. In view of the evolving threat landscape, these safeguards must be continuously reviewed and updated to protect against fraud and to secure the confidentiality and integrity of customer and counterparty information and transactions.	10.81 Holm Security VMP allows for scanning of SST terminals connected with an IP address (c) Internet banking can be scanned both on a domain level as well as on network level. Holm Security VMP can ensure that correct security structures are in place to safeguard customer data.

Policy Requirement			Holm Security VMP Solution
Compliance level	Cyber Risk Management		
	Chapter		
S	11.3	The CRF must consist of, at a minimum, the following elements: (a) development of an institutional understanding of the overall cyber risk context in relation to the financial institution's business and operations, its exposure to cyber risks and current cybersecurity posture; (b) identification, classification and prioritisation of critical systems, information, assets and interconnectivity (with internal and external parties) to obtain a complete and accurate view of the financial institution's information assets, critical systems, interdependencies and cyber risk profile; (e) timely detection of cybersecurity incidents through continuous surveillance and monitoring;	(a) Holm Security VMP can assist in understanding of the overall cyber security risk by continuous scans of the environment as well as current and future risks. (b) Holm Security VMP provides detailed information on critical systems and assets (Internal and external) as well as provides possibilities to classify and prioritize on asset level, system level and risk level. (e) Holm Security VMP is a pro-active detection scanner highlighting current vulnerabilities and risks allowing institutions to take a pro-active risk approach to cyber security.
S	11.4	In addition to the requirements in paragraph 11.3 above, a large financial institution is required to— (a) implement a centralized automated tracking system to manage its technology asset inventory; and (b) establish a dedicated in-house cyber risk management function to manage cyber risks or emerging cyber threats. The cyber risk management function shall be responsible for the following: (c) (i) perform detailed analysis on cyber threats, provide risk assessments on potential cyber-attacks and ensure timely review and escalation of all high-risk cyber threats to senior management and the board; and (ii) proactively identify potential vulnerabilities including those arising from infrastructure hosted with third party service providers through the simulation of sophisticated "Red Team" attacks on its current security controls.	(a) Holm Security VMP allows tracking of assets and provides inventory capabilities. (b) Holm Security VMP can assist management with prioritizing cyber security risk by doing regular assessment of It infrastructure. (c) Holm Security VMP allows detailed assessments on cyber security risks. Details which can be tailored for both C-level management and board as well as technical personnel and security consultants.

Policy Requirement			Holm Security VMP Solution
Compliance level	Cybersecurity Operations		
	Chapter		
S	11.5	A financial institution must establish clear responsibilities for cybersecurity operations which shall include implementing appropriate mitigating measures in the financial institution's conduct of business that correspond to the following phases of the cyber-attack lifecycle: (a) reconnaissance; (b) weaponisation; (c) delivery; (d) exploitation; (e) installation; (f) command and control;	11.5 Holm Security VMP fulfills the following in the cyber-attack lifecycle: (a) Reconnaissance – Identify vulnerable systems, hosts and applications (c) Testing of users within the environment may prevent this phase from being exploited (d) Identify vulnerable systems and highlight which vulnerabilities can be exploited. This procedure minimizes risk of exposure. (e) Identifying and solving vulnerabilities is key to prevent this step from being archived. (f) Public vulnerability scanning allows for easier identification of outbound assets.
S	11.8	A financial institution must ensure that its cybersecurity operations continuously prevent and detect any potential compromise of its security controls or weakening of its security posture. For large financial institutions, this must include performing a quarterly vulnerability assessment of external and internal network components that support all critical systems	11.8 Holm Security VMP is a continuous scanning engine used on daily, weekly, monthly and quarterly basis.
S	11.9	A financial institution 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. The penetration testing shall reflect extreme but plausible cyber-attack scenarios based on emerging and evolving threat scenarios. A financial institution must engage suitably accredited penetration testers and service providers to perform this function.	11.9 Holm Security VMP used by external pentester and internal network administrators to facilitate these needs.

Compliance level	Policy Requirement		Holm Security VMP Solution
	Cybersecurity Operations		
	Chapter		
S	11.11	A financial institution must establish standard operating procedures (SOP) for vulnerability assessment and penetration testing (VAPT) activities. The SOP must outline the relevant control measures including ensuring the external penetration testers are accompanied on-premises at all times, validating the event logs and ensuring data purging.	11.11 Holm Security VMP allows atomization of all procedures outlined in VAPT. Giving organizations the ability to efficiently work with continuous security improvements.
S	11.12	A financial institution must ensure the outcome of the penetration testing exercise is properly documented and escalated in a timely manner to senior management to identify and monitor the implementation of relevant remedial actions	11.12 Holm Security VMP provides several different reports based on customers' needs and can be tailored for all levels.
	Security Operations Centre (SOC)		
S	11.18	The SOC must be able to perform the following functions: (c) vulnerability management;	(c) Holm Security VMP is a vulnerability management tool built to integrate with SOC's as well as other protection systems.

Policy Requirement			Holm Security VMP Solution
Compliance level	Cyber Response and Recovery		
	Chapter		
S	11.23	A financial institution must establish and implement a comprehensive Cyber Incident Response Plan (CIRP). The CIRP must address the following: (a) Preparedness Establish a clear governance process, reporting structure and roles and responsibilities of the Cyber Emergency Response Team (CERT) as well as invocation and escalation procedures in the event of an incident; (b) Detection and analysis Ensure effective and expedient processes for identifying points of compromise, assessing the extent of damage and preserving sufficient evidence for forensics purposes; (c) Containment, eradication and recovery Identify and implement remedial actions to prevent or minimise damage to the financial institution, remove the known threats and resume business activities;	11.23 (a) Holm Security VMP allows automated procedures of the following requirements in order to easy the process of governance of critical infrastructure, clear reporting of known threats as well as fixed cyber security risks. Escalation procedures can be automated and integrated (b) Detection of unknown threats are automatically detected by scheduled scans of critical infra structure. Reporting and presentation of known threats provides information to easier assess extent of damage proactively. (c) Holm Security VMP facilitates the process of remedial actions by allowing organizations to verify risks solved and threats administered.
	Internal Awareness and Training		
S	13.1	A financial institution must provide adequate and regular technology and cybersecurity awareness education for all staff in undertaking their respective roles, and measure the effectiveness of its education and awareness programmes. This cybersecurity awareness education must be conducted at least annually by the financial institution and must reflect the current cyber threat landscape.	Holm Security VMP gives organizations the ability to continuously train and educate staff on pro-active cyber security measures as well as providing awareness tools based on user behavior.
S	13.2	A financial institution must provide adequate and continuous training for staff involved in technology operations, cybersecurity and risk management in order to ensure that the staff are competent to effectively perform their roles and responsibilities.	Holm Security VMP can tailor continuous training for staff by actively train and educate staff by tailored phishing activities as well as in-house training and education based on these assessments.

Appendix 3- Control Measures on Internet Banking

Chapter		
	1. A financial institution should ensure the adequacy of security controls implemented for Internet banking, which include: (a) Ensure Internet banking only runs on secured versions of web browsers that have continued developer support for security patches to fix any vulnerabilities;	a) Holm Security VMP allows for scanning of http/https domains as well as network equipment.

Appendix 5 Control Measures on Cybersecurity

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.	Holm Security VMP allows for automated security testing to be conducted scheduled and on-demand. Automated monitoring tools allows for identification of configuration changes and rule changes.