BeyondTrust

Mapping BeyondTrust Solutions to Malaysian Risk Management in Technology (RMiT) Frameworks

Introduction

Cybercriminals have long sought to exploit technological vulnerabilities to gain access to sensitive electronic data and financial transactions. With this access, they can cause significant financial losses for any entity or consumer whose private information may be revealed or stolen for illicit purposes. The financial services industry is a significant target for cyber threats due to immediate monetary gain.

Given the severity of the issue and the risk to all regulated entities, certain minimum standards are warranted. Created by the Bank Negara of Malaysia, the Malaysian Risk Management in Technology (RMiT) is a framework constructed to combat the ever-growing threat posed to information and financial systems by nation-states, criminal organisations, and independent criminal actors. This regulation is designed to:

- Promote the protection of customer information
- Promote the protection of information technology systems of regulated entities
- Require organisations to assess its specific risk profile
- Require organisations to design a program that addresses its risks in a robust fashion
- Require organisations to certify compliance with these regulations

According to the Risk Management in Technology document, these requirements are applicable to finance organisations operating within Malaysia, specifically naming licensed banks, investment banks, insurers, licensed Islamic banks and takaful operators, certain financial development institutions, issuers of electronic currency, and operators of payment systems. Because all these listed organisations may be perceived as high-value financial targets by threat actors, the prime objective of RMiT guidance is to minimize or eliminate the damages that potential cyber breaches may have.

Utilising RMiT Guidance for Bank Technology Security

In keeping with Bank Negara of Malaysia's recommendations, BeyondTrust encourages all financial entities to act promptly to adopt a cybersecurity program that meets these objectives. As a leading provider of identity and access security solutions, BeyondTrust can help organisations meet many of the requirements set forth in RMiT BNM/RH/ED 028-11.

This following sections have been assembled to articulate the areas in which BeyondTrust solutions can satisfy core framework requirements, just as they help organisations comply with similar cybersecurity frameworks around the world. In the following table, you will find a detailed mapping of BeyondTrust solutions as they align with individual RMiT requirements.

Mapping Beyondtrust Solutions *to* RMiT Requirements

Section	Description of Guidance	BeyondTrust Solution That Meets Guidance
Access Control		
10.52	A financial institution must implement an appropriate access controls policy for the identification, authentication, and authorisation of users (internal and external users such as third-party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems.	BeyondTrust Privileged Remote Access delivers remote access and protocol-based jump host technology to broker connectivity to sensitive systems and enforce effective access control policies for internal and external users.
10.53	A financial institution must reflect the following principles in its access control policy: a. Adopt a "deny all" access control policy for users by default unless explicitly authorised; b. Enforce "least privilege" access rights or on a 'need-to- have' basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles; c. Employ time-bound access rights which restrict access to a specific period including access rights granted to service providers; d. Employ segregation of incompatible functions where no single person is responsible for an entire operation that may provide the ability to independently modify, circumvent, and disable system security features such as— i. System development and technology operations; ii. Security administration and system administration; and iii. Network operation and network security. e. Enforce dual control functions which requires two or more persons to execute an activity; f. Adopt stronger authentication for critical activities including for remote access; g. Prohibit use of same user ID for multiple concurrent sessions; h. Prohibit sharing of user ID and passwords across multiple users;	a. Multiple BeyondTrust solutions, including Privielged Remote Access and Privilege Management deny access to sensitive systems by default unless explicitly allowed. b. BeyondTrust Endpoint Privilege Management solutions enforce least privilege on Windows, macOS, and Linux devices. c. BeyondTrust policies across solutions are context-aware and support geolocation, IP ranges, and time-based access rights. d. BeyondTrust solutions support advanced workflows and approval processes for access and commands to ensure no single person has authoritative access to systems and circumvent proper roles and responsibilities. e. BeyondTrust solutions support multiple approver and workflow use cases. f. BeyondTrust Privileged Remote Access supports multi-factor and two- factor solutions. g. BeyondTrust Privileged Remote Access limits and manages credentials used for concurrent sessions. h. BeyondTrust solutions can instantiate single usage for all credentials to prevent sharing.

10.54	A financial institution must employ robust authentication processes to ensure the authenticity of identities in use. Authentication mechanisms shall be commensurate with the criticality of the functions and adopt at least one or more of these three basic authentication factors, namely, something the user knows (e.g. password, PIN), something the user possesses (e.g. smart card, security device) and something the user is (e.g. biometric characteristics, such as a fingerprint or retinal pattern).	BeyondTrust solutions integrate with industry leading authentication processes via open standards. Endpoint Privilege Management can apply multi-factor authentication on specific tasks or applications that run within Windows (workstation and server), macOS, and Linux (workstation and server).
10.55	A financial institution shall periodically review and adapt its password practices to enhance resilience against evolving attacks. This includes the effective and secure generation of passwords. There must be appropriate controls in place to check the strength of the passwords created.	BeyondTrust Password Safe is capable of automatically rotating and storing passwords based on a password complexity policy implemented by an administrator. This ensures best practices are always enforced and minimum strength is always adhered to.
10.56	Authentication methods that depend on more than one factor typically are more difficult to compromise than a single factor system. In view of this, financial institutions are encouraged to properly design and implement (especially in high-risk or 'single sign-on' systems) multi-factor authentication (MFA) that are more reliable and provide stronger fraud deterrents.	While BeyondTrust solutions do not provide multi-factor authentication (MFA) itself, they can integrate with industry leading authentication processes via open standards. Your organisation's preferred MFA can be used to authenticate before a login into the solution or during the session on certain tasks or applications.
10.58	A financial institution must establish a user access matrix to outline access rights, user roles or profiles, and the authorising and approving authorities. The access matrix must be periodically reviewed and updated.	BeyondTrust solutions are built ground up based on Role Based Access Control (RBAC). RBAC can be integrated with sources such as Microsoft Active Directory (AD) and tied with authorisatons within the BeyondTrust PAM platform. Example roles include Requesters, Approvers and Auditors. Certain user groups may be given access to specific groups of systems or accounts on those systems. This access can be reviewed by reports available within the solution. In addition, this RBAC can be integrated with leading Identity Governance and Administration platforms such as SailPoint via SCIM.
10.59	A financial institution 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. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.	BeyondTrust solutions include the following technologies that address these requirements: a. Secure remote access and privileged access technology to ensure sessions are monitored, managed, and that default remote access is never granted. b. Complete session monitoring and command indexing to document all user activity and facilities to document that sessions are periodically reviewed.

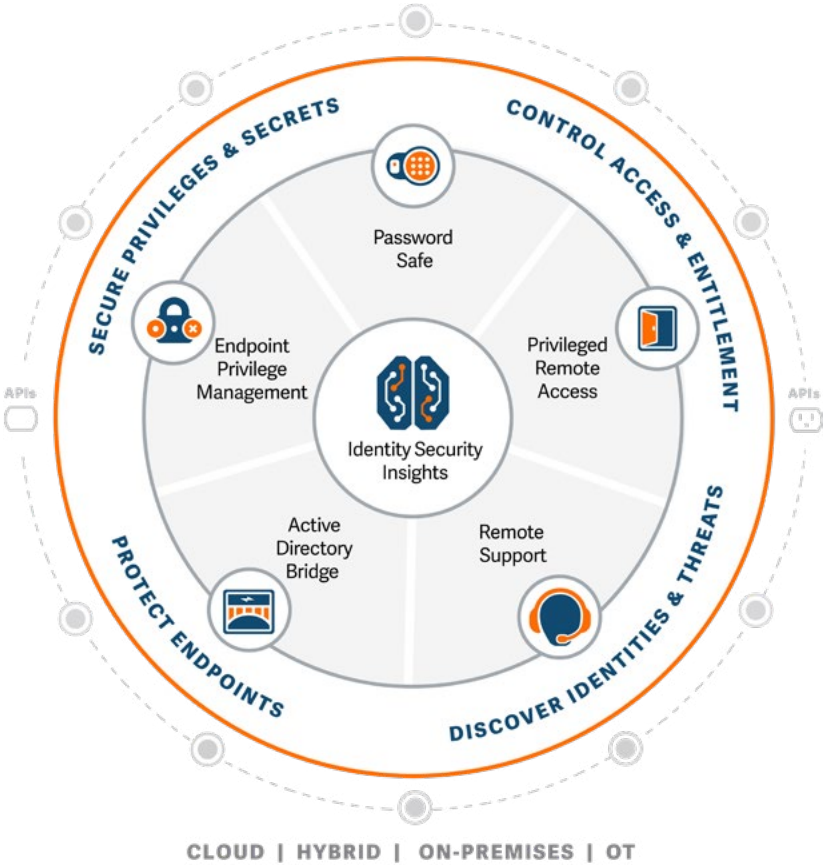
Cybersecurity Operations		
11.5	A financial institution must establish clear responsibilities for cybersecurity operations which shall include implementing appropriate mitigating measures in the financial institution's conduct of business that correspond to the following phases of the cyber-attack lifecycle: a. reconnaissance; b. weaponisation; c. delivery; d. exploitation; e. installation; f. command and control; and g. exfiltration.	**c. Delivery:** BeyondTrust Endpoint Privilege Management offers Trusted Application Protection, a feature that enhances security against malware, ransomware, and phishing attacks, stopping attack chain tools that may exploit commonly used and legitimate applications. This also gives organizations protection against fileless malware and living off the land (LotL) attacks. **d. Installation:** BeyondTrust Endpoint Privilege Management facilitates the removal of local administrator accounts and control of root access by performing privilege escalation and delegation management (PEDM). This can be applied equally to workforce and developer environments. Removing admin rights and enforcing least privilege are best practices that apply across all IT environments, whether Windows, macOS, or Linux Endpoint Privilege Management also allows the creation of allow-listing of approved apps for total control over what users can install or run. **e. Command and Control:** Endpoint Privilege Management protects against lateral movement by protecting privileged accounts via password and session management including the obfuscation of credentials to prevent misuse. In addition, the solution can block unknown tools and scripts from being executed within the environment.
11.7	A financial institution must enable continuous and proactive monitoring and deploy advanced tools to timely detect anomalous activities in its technology infrastructure. The scope of monitoring must be extensive to cover all critical technology applications and systems including its supporting infrastructure.	BeyondTrust solutions include advanced technology for continuous proactive monitoring and anomaly detection of privileged access, remote access, password management, and least privilege via analytics, reports, and third-party event integration.
Appendix 2 – Control Measures on Self-Service Terminals (SSTs)		
5.	Implementing a centralised management system to monitor and alert any unauthorised activities on Cash SST such as unauthorised shutting-down of OS or deactivation of the white-listing programme.	**Endpoint Privilege Management** allows integration with the operating system to provide centralised audit tracing on all applications, tasks, or processes on Windows, macOS, Unix, and Linux operating systems. In addition, it can provide application and task allow-listing and deny-listing operations, such as deactivation of services or running tasks such as system shutdown.
12.	b. Disabling Microsoft default program system (such as Notepad, Internet browser, Windows shortcut, file download, file sharing and command prompt)	**Endpoint Privilege Management** solutions provides an effective way to block applications and tasks from being run on Windows, macOS, Unix, and Linux operating systems.

Appendix 5 – Minimum Control Measures on Cybersecurity		
6.	Ensure security controls for remote access to server include the following: a. Restrict access to only hardened and locked down endpoint devices; b. Use secure tunnels such as TLS and VPN IPSec; c. Deploy 'gateway' server with adequate perimeter defenses and protection such as firewall, IPS and antivirus; and d. Close relevant ports immediately upon expiry of e. remote access.	**Privileged Remote Access enables the following capabilities:** a. Assesses and restricts access to properly hardened hosts. b. Supports strong encryption and secure protocols for access. c. Utilises gateways or jump servers for remote access, including full session monitoring. d. Secures access using a dedicated client so no open ports are exposed
Appendix 10, Part B: Cloud Design and Control		
9.	a. The management plane is a key security difference between traditional infrastructure and cloud computing where remote access is supported by default. This access layer could be prone to cyber-attacks thereby compromising the integrity of the entire cloud deployment. In view of this, financial Institutions should ensure the use of strong controls for accessing the management plane which may include the following: i. allocate dedicated and effectively hardened endpoints and up to date patching of software to access the management plane; ii. implement "least privilege" and strong multi-factor authentication (MFA) e.g., strong password, soft token, privileged access management tool and maker-checker functions; iii. employ granular entitlement allocation for privileged users; iv. conduct continuous monitoring of the activities performed by privileged users; and v. ensure secure communication protocols are in place for accessing the management plane. e.g., secure end-to-end communication channels, whitelisting of IP addresses, etc.	ii. ii) BeyondTrust solutions provide the ability to implement "least privilege" by layering privileges between access to the OS and within the OS itself. This includes password management and password obfuscation when used for hypervisor logins. Combined, these features provide an effective countermeasure against lateral movement. For third party users, BeyondTrust Privileged Remote Access can provide secure, role based access into specific hypervisors or downstream workloads while enforcing access policies such as approval processes and MFA. Endpoint Privilege Management can additionally provide least privilege by removing the need for local administrators on systems and instead replacing them with privilege escalation and delegation. iii. Granular entitlement controls are enabled by all solutions within the BeyondTrust PAM portfolio, including Privileged Remote Access, Password Safe, and Endpoint Privilege Management. iv. BeyondTrust Password Safe and Privileged Remote Access each provide session monitoring, keystroke logging, and command indexing capabilities to document all user activity and ensure holistic review. In addition, BeyondTrust Endpoint Privilege Management allows integrations with the operating system to provide centralised audit tracing on all applications, tasks, or processes on Windows, macOS, Unix, and Linux systems. Finally, note that all audited actions can be streamed into SIEM platforms for analysis and alerting. v. All communications within BeyondTrust solutions are encrypted using https/SSL.

Use BeyondTrust Solutions to Meet RMiT Requirements

The number of successful cyberattacks has been steadily increasing, and the devastating impacts of these attacks of financial services institutions presents irrefutable risk to Malaysian national security. Accordingly, adoption of this cybersecurity program and standardisation of its policies and procedures has been deemed a primary device for enhancing the security of financial systems and organisations operating within the country.

BeyondTrust PAM solutions satisfy numerous requirements set forth in the RMiT, offering a highly efficient and ROI-friendly option for increasing the overall privilege, access, and credential security of any organization.



BeyondTrust Solutions

Endpoint Privilege Management: Enforce least privilege dynamically to prevent attacks, achieve compliance across Windows, macOS, and Linux endpoints, and enable your zero trust strategy — without compromising on productivity.

Privileged Remote Access: Create identity-secure, just-in-time access to all your enterprise environments: cloud, on-premises, and OT.

Password Safe: Manage privileged passwords, accounts, credentials, secrets, and sessions for people and machines, ensuring complete control and security.

Identity Security Insights: Gain a centralized view of identities, accounts, and privileged access across your IT estate, and leverage threat intelligence recommendations to improve your identity security posture.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in intelligent identity and access security, enabling organizations to protect identities, stop threats, and deliver dynamic access. We are leading the charge in innovating identity-first security and are trusted by 20,000 customers, including 75 of the Fortune 100, plus a global ecosystem of partners. Learn more at **beyondtrust.com**