WHITEPAPER

Nagara Bank Malaisya RMiT and Products

segura® | Futureproof Identity Security | segura.security

Introduction

The increasing sophistication of cyber threats and the accelerated adoption of technologies such as cloud computing require financial institutions to effectively manage technological risks. To ensure that financial institutions operate securely and resiliently, Bank Negara Malaysia (BNM) has established the Risk Management in Technology (RMiT), a set of strict guidelines aimed at protecting digital assets, mitigating threats, and ensuring regulatory compliance.

RMiT sets essential cybersecurity requirements, including access control, identity management, continuous monitoring, encryption, and auditing. Organizations that fail to comply with these guidelines may face severe penalties and increased operational risks.

Segura® is a Privileged Access Management (PAM) solution that not only meets the RMiT requirements but exceeds them by offering advanced functionalities for critical access control, continuous monitoring, and protection against internal and external threats.

RMiT Revisions and Updates

The rapid evolution of cyber threats and the rise of technologies like cloud computing require continuous updates to RMiT to ensure its relevance. In response, on June 1, 2023, BNM issued a revised version of RMiT, introducing additional guidelines to strengthen financial institutions' cloud risk management capabilities, along with the following enhancements:

Mandatory implementation of security controls, such as Multi-Factor Authentication (MFA), to enhance the security of online financial transactions and reduce fraud and data breach incidents.

Strengthening access and identity management, reinforcing the application of the Principle of Least Privilege and periodic review of access matrices.

Requirement for continuous monitoring tools to detect anomalous activities in technological infrastructure.

Stricter encryption requirements and protection of the cryptographic key lifecycle.

Enhanced recommendations for incident response and auditing, ensuring greater transparency and governance of technological risks.

RMiT Requirements and Their Applicability

The Risk Management in Technology (RMiT) document issued by Bank Negara Malaysia (BNM) categorizes requirements into two types:

"S" (Standard): Mandatory requirements that financial institutions must comply with to be in alignment with RMiT. These guidelines cover areas such as access controls, authentication processes, encryption, and continuous auditing.

"G" (Guidance): Suggested recommendations from the regulator to strengthen cybersecurity and operational resilience. While not mandatory, adopting these guidelines is considered a best practice for mitigating technological risks.

We present how senhasegura enables Malaysian financial institutions to meet these requirements, ensuring regulatory compliance and enhancing privileged access security, specifically addressing mandates S–10.52 to S–10.60, which cover access control management.

Below, we detail each RMiT requirement and how senhasegura positions itself as a robust solution for access control and risk mitigation.

How Segura® Meets RMiT Requirements

1. Access and Identity Control

Segura® implements an access control model based on the principles of Least Privilege and Default Denial, ensuring that users only have the access strictly necessary to perform their functions.

RMiT Requirement	Compliance with Segura®
Implementation of a robust access control policy, ensuring identification, authentication, and authorization of internal and external users.	Segura® allows granular permission management and applies the Least Privilege principle, ensuring that each user has only the necessary access.
Periodic review of the user access matrix.	Segura® offers automated auditing and alerts to review and adjust permissions as needed. **Review and Certification:** This feature allows the configuration of notifications and frequent access review.
Application of multi-factor authentication (MFA) for critical activities.	Segura® enforces mandatory MFA, strengthening security against unauthorized access. **Access to Segura®:** Allows organizations to require all platform users to configure and use MFA for authentication, ensuring an additional layer of security. **Sessions on Privileged Devices:** In addition to managing the lifecycle of privileged credentials, MFA can be configured for credential authentication, ensuring secure user access. **Personal Passwords:** The MySafe feature enables users to securely manage their personal passwords and MFA, enhancing individual security practices.

2. Digital Services Security

Segura® ensures the confidentiality, integrity, and availability of sensitive information through a secure architecture and advanced controls.

RMiT Requirement	Compliance with Segura®
Robust encryption for protecting data at rest and in transit.	Segura® uses AES-256 for stored data and SHA-256 for password hashing, ensuring protection against attacks.
Secure management of the cryptographic key lifecycle	Segura® integrates with HSM (Hardware Security Module) for advanced key management.
Maintenance of complete audit trails and continuous monitoring.	Segura® logs all privileged activities, enabling detailed audits and regulatory compliance. **Monitored and Recorded Sessions:** Ensures traceability and segregation of duties, distinguishing between requesters, approvers, and executors of critical activities. **Customizable Dashboard:** Provides a high-level security dashboard that can be tailored to offer full visibility into platform activities, allowing executives and security teams to monitor privileged access in real-time.

3. Monitoring and Incident Response

RMiT Requirement	Compliance with Segura®
Implementation of tools for continuous monitoring of suspicious activities.	Segura® provides behavioral analysis and real-time alerts, detecting anomalous activities to enhance security and compliance. **Credential and System Discovery:** Automated identification of critical assets and associated credentials, ensuring full visibility of privileged access usage. Enforces that asset passwords are exclusively managed by Segura®. If discrepancies are detected, the system automatically triggers a password reset to maintain security. **Review and Certification:** Enables automated notifications and periodic access reviews, ensuring continuous monitoring and compliance with security policies.

Monitored and recorded sessions for audit and investigation.	All privileged sessions are recorded and stored with replay capability, ensuring precise auditing and compliance. **Session Recording:** Real-time recording of activities in privileged sessions for detailed auditing and forensic analysis. **User Behavior Analysis:** Detection of suspicious activities with automated alerts for anomalous behavior. **Automated Reports & Alerts:** Instant notifications of unusual activities within the infrastructure to enhance security response. **SIEM Integration:** All user activity logs are sent to the SIEM for real-time monitoring. Clients can terminate sessions or deactivate users via API in response to suspicious activity, ensuring proactive threat mitigation.
Integration with SIEM solutions for rapid incident response.	Segura® integrates with leading SIEM solutions, enabling the automatic termination of suspicious sessions via API. **SIEM Integration:** Sends all user activity logs to the SIEM. The customer has the option to terminate sessions or even deactivate users via API in case of suspicious activity.

4. Compliance and Auditing

RMiT Requirement	Compliance with Segura®
Conducting regular audits to assess the effectiveness of IT controls.	Segura® generates automated reports with detailed logs on access and permissions. With the Review and Certification feature, users can configure notifications and schedule regular access reviews, ensuring continuous security and compliance.
Maintaining records of critical activities for at least three years.	The solution retains complete logs indefinitely, meeting and exceeding regulatory requirements.
Continuous review and adaptation of security policies.	Continuous review and adaptation of security policies. Segura® allows dynamic adjustments to access and security policies, ensuring continuous compliance. **Review and Certification:** This feature enables the configuration of notifications and frequent access reviews.

Updated Table with RMiT Requirements and Correspondence with Segura®

RMiT	Description	How Segura Meets It
S 10.52	Identity and access management ensures that access rights granted to users are in line with and used as defined in the institution's organisational and operational requirements. Identity and access management shall meet the requirements set out in AT 4.3.1 number 2, AT 7.2 number 2 as well as BTO number 9 of MaRisk	Segura® solutions enable organizations to create robust access policies, enforce multi-factor authentication (MFA), and maintain comprehensive audit and compliance controls in cloud environments, ensuring security even before deployment. By using these solutions, institutions can significantly reduce the risks of unauthorized access. **Multilevel Granular Workflow:** senhasegura provides flexible and advanced access segregation mechanisms, including profiles, roles, role groups, and access groups. This versatility allows organizations to easily define and enforce multiple access levels, ensuring strict adherence to corporate policies and minimizing privilege abuse. **Credential Management:** senhasegura uses industry-recognized open connectors to enable native adaptation and control of privileged credentials across a wide range of vendors. This capability simplifies the integration of new devices and credentials without requiring advanced vendor support, streamlining access management and reducing administrative overhead. **Review and Certification:** This feature enables the configuration of notifications and frequent access reviews.

G 10.53(a)	"Deny by default" access policy.	Segura® PAM Core implements access control based on the principle of least privilege, ensuring that only authorized users have access to privileged data. This approach minimizes security risks by restricting access to what is necessary for users' tasks. **Multilevel Granular Workflow:** Segura® provides advanced access segregation mechanisms, including profiles, roles, role groups, and access groups. These flexible configurations allow organizations to define and enforce multiple access levels, ensuring strict adherence to corporate policies. **Credential Management:** By using industry-recognized open connectors, Segura® enables native adaptation and control of privileged credentials across a wide range of vendors. This flexibility allows administrators to easily integrate new devices and credentials without requiring advanced vendor support, streamlining credential management.
G 10.53(b)	Minimum privilege granted to users.	Segura® ensures granular permission control, granting users only the necessary access. **Granular Application Control (GAC):** Execution of privileges based on approved action lists: authorized users can invoke admin privileges to run specific applications, ensuring that only critical applications requiring elevated privileges are executed securely. **Review and Certification:** This feature enables the configuration of notifications and frequent access reviews.
G 10.53(c)	Time-bound access rights.	Segura® allows temporary access configurations, ensuring compliance with audits. **Temporary Access Configuration:** Enables the configuration of temporary access rights, including secure access for third parties and service providers. Ensures that privileged access is granted only for the necessary period, increasing system security and ensuring compliance with audit requirements. **Multilevel Granular Workflow:** Offers advanced access segregation mechanisms, such as profiles, roles, role groups, and access groups. This flexible approach allows organizations to easily manage different access levels, ensuring better compliance with corporate access policies and minimizing the risk of unauthorized access.

G 10.53(f)	Strong authentication for critical activities.	Segura® adopts stronger authentication methods for critical activities, including remote access. **Seamless Remote Access:** Segura® enables simplified remote access to devices without requiring users to log in directly to the device interface. This feature provides quick, secure, and convenient access to managed assets while maintaining high security standards. **Multi-factor authentication (MFA):** senhasegura supports Multi-Factor Authentication (MFA) for critical actions, including remote access. By implementing MFA, Segura® enhances identity verification and strengthens security for sensitive operations, fully aligning with RMiT requirements.
G 10.53(h)	Control over credential sharing.	Segura® password vault prevents credential sharing among users. **MySafe:** Segura® MySafe follows the highest security standards, preventing credential sharing among users. This ensures that each user's identity remains unique and protected, reducing the risk of unauthorized access and enhancing compliance with RMiT requirements. **MySafe Password Manager:** Segura® MySafe solution allows users to create strong password requirements, securely store credentials, and share them with authorized users while adhering to strict security standards. This controlled sharing mechanism ensures that access is granted only to verified users, supporting strict compliance with access management policies. MySafe sharing allows users to determine whether an item can be accessed multiple times and/or whether the password will be visible.
S 10.54	Implementation of robust authentication (password, token, or biometrics).	Segura® supports multi-factor authentication, biometrics, and security tokens.

S 10.55	Periodic review of password practices.	Configurable password policies to enhance security and prevent attacks. **Credential Rotation:** Segura® Credential Rotation functionality provides integrated plugins and ready-to-use templates for automatic credential rotation across devices, services, configuration files, and applications. This is achieved through configurable criteria, ensuring continuous compliance with evolving password policies and minimizing security risks. **Credential Management:** Segura® uses industry-recognized open connectors to enable the native adaptation and control of privileged credentials across a wide range of vendors. This flexibility allows administrators to seamlessly integrate new devices and credentials without requiring advanced vendor support, simplifying credential management while maintaining high security standards. **Review and Certification:** This feature enables the configuration of notifications and frequent access reviews.
S 10.59	Access monitoring and log auditing.	Segura® provides native auditing capabilities, allowing organizations to verify authorized scripts against actual actions performed on target devices. This capability ensures complete governance and user behavior analysis, helping organizations maintain compliance. **Session Recording:** Segura® enables high-compression video session recording without requiring local agents. It also logs key aspects such as typed commands and metadata, ensuring that all actions on critical systems are captured for review. This enhances auditing capabilities and reduces troubleshooting time by providing a detailed record of user activities. **SIEM Integration:** Sends all user activity logs to the SIEM. Customers can terminate sessions or even deactivate users via API in case of suspicious activity.
S 10.60	Deployment of identity management systems and automated auditing.	Segura® IAM features enable centralized identity management and audit automation. **User Provisioning & Deprovisioning:** Segura® allows the automatic creation and removal of users based on the employee lifecycle, reducing the risk of unauthorized access. **Session Recording:** Ensures that all activities are recorded for audit and compliance.

S 11.11	Vulnerability Assessment and Penetration Testing (VAPT)	Procedures Automated reports on vulnerabilities and security compliance management. The Segura® PAM detects exposed or misconfigured credentials and generates automatic alerts. With the Vulnerability Scanner, the solution identifies flaws in privileged credentials and suggests corrections before they can be exploited. **Credential and System Discovery:** senhasegura automatically identifies critical assets and their associated credentials, ensuring complete visibility into where privileged accesses are being used. It also ensures that the asset's password is managed exclusively by Segura®. If it differs, the system forces an automatic password change to ensure security.
S 11.21	Security and Continuous Operation of the SOC	Segura® enables integration with Security Operations Centers (SOCs), as well as integrations with SIEM tools for 24/7 protection. Customizable Dashboard: The platform allows the creation and customization of a high-level security dashboard, providing the board with visibility into everything happening on the platform and its products.
S 12.1	Technological audits proportional to the complexity of the environment.	Automated auditing module and detailed compliance reports. **Recorded and Monitored Sessions:** All activities performed in privileged accounts are recorded with video and detailed logs, allowing precise and continuous audits. **Automated Reports:** Generates audit reports with clear compliance evidence for control evaluation. **Audit Trails:** Provides a complete record of actions performed by privileged users, with date, time, and context. **Review and Certification:** This feature enables the configuration of notifications and frequent access reviews. **SIEM Integration:** Sends all user activity logs to the SIEM. Customers can terminate sessions or even deactivate users via API in case of suspicious activity.

WHITEPAPER

Nagara Bank Malaisya RMiT and Products

segura® | Futureproof Identity Security | segura.security