Complying with the RMiT mandate S–10.52: to S–10.60: Access Control with ARCON | Privileged Access Management (PAM) solution

Table of Content

Cybersecurity Ecosystem in Malaysia

Malaysia has made significant strides in developing a very robust digital economy. This paper discusses how ARCON PAM helps security, risk management and compliance leaders to comply with the Central Bank of Malaysia's mandates in information security.

Malaysia, an economically booming Southeast nation has demonstrated commitment through new strategies for both the civil sector and national defense. The National Cyber Security Policy (NCSP) outlines critical national information infrastructure and emphasizes cyber-security capabilities. The country has strong digital-economic potential, positioning itself as a leading digital hub in ASEAN.

Recently, in 2024, Malaysia introduced the Cyber Security Bill, reinforcing its commitment to secure digital infrastructure and boost confidence among international partners and investors. Earlier in March 2021, Cybersecurity Malaysia launched the SiberKASA initiative, focusing on cyber resilience through a holistic ecosystem approach.

Like many growing markets worldwide, Malaysia faces an increasing number of cyber threats. Organizations in Malaysia experience an average of 1,277 attacks per week, higher than the global average. Hence, government initiative aims to create a safer and more prosperous cyber ecosystem by prioritizing digital security of the citizens. Its strong policy framework positions it well for future growth in the cyber domain.

What is Bank Negara, Malaysia Policy Document RMiT?

The Bank Negara Policy Document RMiT refers to the Risk Management in Technology (RMiT) policy document issued by Bank Negara Malaysia, that is the central bank of Malaysia. This policy document outlines the requirements for financial institutions regarding the management of technology risk. It covers various aspects such as governance, technology risk management, technology operations management, cybersecurity management, technology audit, internal awareness, and training. It also includes regulatory processes like notification for technology-related applications, consultation and notification related to cloud services, assessment, and loophole analysis.

This compliance document emphasizes the implementation of robust risk management controls that exceed the minimum regulatory standards to ensure the secure delivery of financial services and to prevent the exploitation of vulnerabilities in interconnected networks and systems. It aims to maintain public confidence in the financial system by providing robust cyber fortification.

The latest updates to the RMiT policy document, issued on 1 June 2023, include additional guidance to strengthen financial institutions' cloud risk management capabilities and a shift to a risk-based approach in cloud consultation and notification processes. The document is particularly significant as it sets the standards for technology risk management in the Malaysian financial sector.

Bank Negara Policy Document RMiT Compliance is meant for whom?

The Risk Management in Technology (RMiT) Compliance issued by Bank Negara Malaysia applies to all financial institutions operating within Malaysia. This includes banks, insurance companies, investment firms, and other entities in the financial sector. The policy aims to enhance technology risk management practices, strengthen cybersecurity, and maintain public trust in the financial system.

What are the core objectives of Bank Negara Policy Document RMiT compliance?

The Risk Management in Technology (RMiT) Policy Document issued by Bank Negara Malaysia outlines key objectives for financial institutions regarding technology risk management. Here are the core objectives:

Robust Risk Management Controls: All financial institutions must implement robust risk management controls that exceed minimum regulatory standards. These controls ensure efficient financial services delivery while securing systems and preventing the exploitation of weak links in interconnected networks. The goal is to preserve public confidence in the financial system.

Strengthening Cloud Risk Management: The policy provides additional guidance to enhance financial institutions' cloud risk management capabilities. It emphasizes a risk-based approach in cloud consultation and notification processes, promoting resilience against cyber threats.

Meet Compliance Standards: The policy document came into effect on June 1, 2023, with specific provisions applicable to distinct types of financial institutions and meet compliance requirements. Licensed digital banks and licensed Islamic digital banks are all subject to the policy from the effective date. The RMiT policy aims to ensure robust risk management, strengthen cloud security, and maintain public trust in Malaysia's financial industry.

Role of Privileged Access Management (PAM) in complying with Bank Negara Policy Document RMiT

A growing number of enterprise use cases have extended the boundaries of digital identities. Today's financial institutions no longer manage data and workloads in on-premises data centers. Multiple public cloud platforms and managed service providers are being increasingly adopted for better IT operational efficiency.

In this evolving scenario, enterprise IT risk management teams must now manage digital identities and access across all user populations (internal and external), OSes, applications, and hosting models. This has necessitated an effective identity and access management strategy. To prevent authorized access to information systems, password abuse/misuse, account takeover, insider and third-party threats, a strong identity and access management system, including privileged access management (PAM), is required. It is highly imperative for CIOs, CISOs, and IT heads to treat IAM as an integral component of the overall robust enterprise risk management framework.

A robust identity and access management strategy ensures the following:

- Continuous monitoring of digital identities
- Frequent changes and randomization of passwords
- Real-time threat detection and alerts emanating from suspicious digital identities
- Applying multi-factor authentication to access critical IT resources
- Audit trails and reporting of each access to information systems, including privileged accounts.

Bank Negara Policy Document RMiT Checklist

In this paper, we have discussed Bank Negara Policy Document RMiT mandate S–10.52: to S–10.60: Access Control in the below table and how ARCON | Privileged Access Management (PAM) solution helps financial sector of Malaysia to comply with the mandates.

S–10.52: to S–10:60 Access Control Policy Description	Compliance with the Mandate?	Which ARCON PAM feature addresses it?
A financial institution must implement an appropriate access controls policy for the identification, authentication, and authorization of users (internal and external users such as third-party service providers). This must address both logical and physical technological access controls which are commensurate with the level of risk of unauthorized access to its technological systems.	✔	ARCON PAM enables precise access policies for privileged users, which reduces the risks of unauthorized access and misuse of critical systems and enterprise data. With this - ▪ Organizations can limit users' access to only those systems, applications, and data that they need to perform their jobs. ▪ Organizations can maintain control over authorized access and ensure that access is granted only on a "need to know" and "need-to-do" basis. ▪ Granular level access control enables organizations to manage privileged access more effectively and reduce the risk of unauthorized access, insider threats, and cyberattacks.
G 10.53: a) adopt a "deny all" access control policy for users by default unless explicitly authorized	✔	The Zero Trust security approach is based on the principle of "Deny Access" unless the trust is verified at every step. ARCON | PAM helps organizations to follow the principles of Zero Trust security with the help of advanced features. Just-In-Time (JIT) approach, Multi-factor Authentication (MFA), Adaptive Authentication, Identity Governance and Administration (IGA) are some of robust features that build the foundation of a zero-trust security posture.
G 10.53: b) employ "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	✔	The principle of "least privileges" can be implemented with ARCON's Just-In-Time (JIT) privilege capabilities. ▪ It ensures that the right person has access to the right systems at the right time. 24*7 or "always on" privileges are too risky.

		▪ JIT allows users to get temporary access to perform tasks that require elevated privileges without granting them permanent access, lowering the risk of cyber-attacks due to privileged credential misuse. ▪ Every given permission is automatically revoked once the task or operation is completed. Moreover, with fine grained access control mechanism, ARCON | PAM enables organizations to - ▪ Limit users' privileges only on 'need-to-have' basis while monitoring and auditing elevated access requests. ▪ It enables organizations to define and enforce precise access policies for privileged users, reducing the risk of unauthorized access and misuse of sensitive systems and data. ▪ With fine-grained access control, organizations can limit privileged users' access to only those systems, applications, and data that they need to perform their jobs.
G 10.53: c) employ time-bound access rights which restrict access to a specific period including access rights granted to service providers		As mentioned above, ARCON's Just-In-Time (JIT) privilege approach not just grants access based on role-based requirements, but also on time-based requirements. Predefined timeline once incorporated while allowing access rights, helps to automatically revoke rights once the time is over. As a result, there are no standing privileges or 'always-on' privileges, which bears immense IT risks. Moreover, JIT privileged interactive access, known as ephemeral access, automatically generates rule and role-based temporary access rights to prevent unauthorized access. Apart from time-based access, ARCON | PAM offers token-based access (also known as token authentication) where the token acts like a digital key allowing users to access any application/ system without entering the credentials during every access.

G 10.53: f) adopt stronger authentication for critical activities including for remote access		Global Remote Access (GRA) solution of ARCON offers Role-based Access Control where IT administrators manage remote users and their access to critical systems based on their roles and responsibilities. The remote privileged sessions are always supported by Multi-factor Authentication (MFA) mechanism ensuring robust security.
G 10.53: h) limit and control the sharing of user ID and passwords across multiple users		Irrespective of the vastness of IT infrastructure, ARCON PAM ensures that every access to critical systems is made through one admin console. A well-defined access control framework is implemented around people and policies so that every access is granted only on “need-to-know" and “need-to-do" basis. ARCON PAM verifies the passwords of privileged accounts from the target systems regularly and compares them to those stored in the PAM solution. This procedure assists in reducing the risk of unauthorized access or other security breaches caused by outdated or incorrect passwords. Moreover, ARCON PAM offers a password vault or credential vault that ensures every password is stored and managed in a highly secure environment by providing a secure and single point of control. It enables organizations to generate complex, randomized passwords for privileged accounts in an encrypted format to prevent misuse.
S 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).		ARCON PAM offers Multi-Factor Authentication (MFA) that – ▪ Acts as a strategic, relevant, and essential engine to provide multiple forms of identity verification steps before the privileged users are allowed access to the desired network, system, or application. ▪ Along with the traditional verification methods such as SMS and Email OTP mechanisms and hardware tokens, ARCON’s MFA provides integration with various third-party authentication apps, including disparate biometric (fingerprint) and facial recognition technologies.

S 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.		ARCON PAM's automated password management tool enhances resilience against evolving attacks and builds appropriate controls to strengthen password management practices. ▪ ARCON's password vault or credential vault engine ensures that privileged account passwords are stored and managed in a highly secure environment by providing a secure and single point of control. ▪ It enables organizations to generate complex, randomized passwords for privileged accounts and enforce password policies such as password expiration and extent of complexity and rules to ensure that passwords are updated regularly and meet the organization's security standards. ▪ It eliminates the need for privileged users to remember and share passwords, thus lowering the risk of password theft/ misuse.
G 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.		▪ ARCON PAM supports several MFA options, including ARCON Authenticator App, Email OTP, SMS OTP, hardware tokens, TOTPs like Google and Microsoft Authenticator, biometric authentication, Facial Recognition, and many more. ▪ Organizations can select the MFA feature that best meets their security needs while also seamlessly integrating with their existing IT infrastructure. ARCON's Single Sign-On (SSO) allows organizations to overcome the challenge of multiple user-ids, multiple passwords, and multiple approval processes.
S 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.		a) ARCON | PAM helps organizations to restrict random allocation and usage of privileges and eliminates misuse of elevated access rights and enforces fine-grained controls that includes Role-based-Access Control (RBAC) and Policy-Based Access Control (PBAC). Depending on the organization's policies and enterprise-wide IT infrastructure, end-user access is controlled and managed as per RBAC/ PBAC policy. b) ARCON | PAM offers Audit Trails and Reporting for comprehensive security to all databases and

		applications as every command/ query executed by end-users is captured through video/ text logs for a security assessment. And the reports generated provides a 360-degree view of security posture.
S 10.60: In fulfilling the requirement under paragraph 10.59, large financial institutions are required to— a) deploy an identity access management system to effectively manage and monitor user access to enterprise-wide systems; and (b) deploy automated audit tools to flag any anomalies.		a) Identity Access Management (IAM) solution holds the key to manage, control and monitor digital identities and enable robust authentication mechanisms before allowing access to an organization's digital assets. IT security teams use ARCON's IAM solutions to securely control users' access to IT resources across enterprise-wide systems on both on-premises and cloud infrastructure. b) Audit Tools – Same as mentioned above – S 10.59: (b)

Conclusion

ARCON's Privileged Access Management (PAM) and other IAM solutions help organizations (majorly financial industry-based) of Malaysia to –

- Comply with Bank Negara Policy Document RMiT
- Ensure robust privileged identity management environment enterprise-wide
- Mitigate the chances of data breach incidents

about ARCON

ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and Continuous Risk Assessment solutions.

ARCON Privileged Access Management (PAM) is a leading global product and a robust solution that mitigates risks arising out of privilege identity and access management.

Connect with us