Ensuring compliance with Bank Negara, Malaysia Policy Document RMiT

Overview

Cybersecurity and IT governance have become increasingly important for regulatory compliance. Global Central Banks are demanding explicit IT risk management policies, processes, and procedures to safeguard information assets against rising technology risks emanating from corporate insiders, third-parties, and advanced cyber threats. In this context, Identity and Access Management (IAM) will be critical for regulatory compliance. In this paper, ARCON discusses how its robust stack of IAM solutions can enable enterprise information risk management teams to comply with the mandates given by Bank Negara, Malaysia.

Bank Negara Malaysia Policy Document on Risk Management in Information Technology (RMiT)

Bank Negara Malaysia (The Central Bank of Malaysia) is the regulatory authority for the financial service providers in Malaysia. The Central Bank's policy document-Risk Management in Information Technology (RMiT) sets out requirements with regard to financial service providers' management of technology risks.

The policy document is very comprehensive. It lists down an explicit list of requirements ranging from the appointments of key IT personnel for managing IT risks to the responsibility of the board of directors and senior management, including due diligence of third-party environment while hosting data on-cloud and in managed service requirements (MSPs). However, the RMiT policy document has very broad and encompassing requirements for Technology Risk Management.

With the more widespread use of technology in every facet of business, financial service providers have become more and more vulnerable to IT threats. Bank Negara's RMiT policy document requires financial institutions to strengthen their IT resilience against operational disruptions, thereby maintaining confidence in the financial system.

In complying with these requirements:

- A financial institution shall have regard to the size and complexity of its operations.
- Larger and more complex financial institutions are expected to demonstrate risk management practices and controls that are commensurate with the increased technology risk exposure of the institution.
- All financial institutions shall observe minimum prescribed standards stated in the policy document to prevent the exploitation of weak links in interconnected networks and systems that may cause detriment to other financial institutions and the wider financial system. (Source: RMiT…1.3)

Additionally, financial institutions must ensure that Technology Risk Management is an integral part of the enterprise risk management framework. This framework should enable:

a) clear definition of technology risk;

b) clear responsibilities assigned for the management of technology risk at different levels and across functions, with appropriate governance and reporting arrangements;

c) the identification of technology risks to which the financial institution is exposed, including risks from the adoption of new or emerging technology;

d) risk classification of all information assets/systems based on its criticality;

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. (Source: RMit…Technology Risk Management S 9.1 and 9.2)

The Role of Identity and Access Management in reinforcing the enterprise risk management framework:

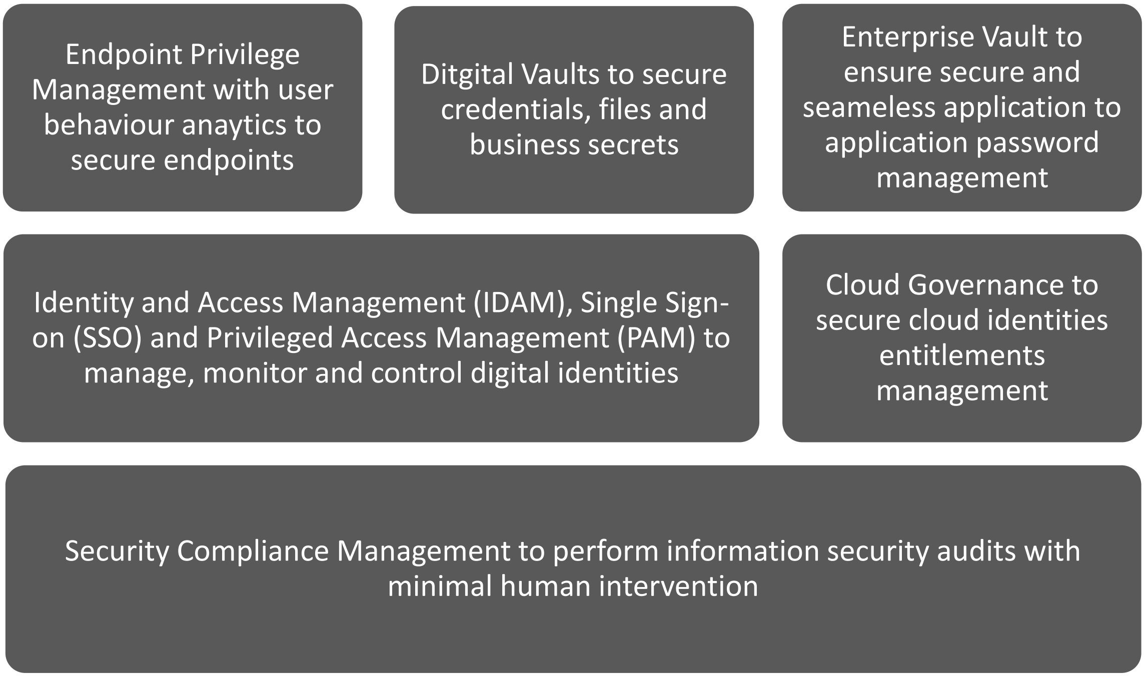
A growing number of enterprise use cases have extended the boundaries of digital identities. Today's financial institutions no longer manage data and workloads in on-premises data centres. Multiple public cloud platforms and managed service providers are being increasingly adopted for better IT operational 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 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 and every access to information systems, including privileged accounts

Building a robust enterprise risk management framework with robust IAM solutions from ARCON



Endpoint Privilege Management with user behaviour anaytics to secure endpoints

Ditgital Vaults to secure credentials, files and business secrets

Enterprise Vault to ensure secure and seameless application to application password management

Identity and Access Management (IDAM), Single Sign-on (SSO) and Privileged Access Management (PAM) to manage, monitor and control digital identities

Cloud Governance to secure cloud identities entitlements management

Security Compliance Management to perform information security audits with minimal human intervention

ARCON enables enterprise risk management teams to secure data and identities at every layer of IT Infrastructure

ARCON is a leading information risk-management solutions provider specializing in Privileged Access Management and Continuous Risk Predictive solutions that leverage Artificial Intelligence and Machine Learning. Built on three founding pillars: Predict, Protect, and Prevent, the company's robust stack of solutions allows modern-enterprises to mitigate looming insider and third-party threats in real-time.

The company creates solutions that enable IT security professionals to create impenetrable perimeter security around datacentres while also developing a comprehensive Governance, Risks, and Compliance (GRC) framework.

Our mission is to provide global organizations with a secure centralized platform for managing, monitoring, and controlling the increasing number of digital identities. Therefore, we always continue to innovate and build best-in-class and highly scalable solutions to support enterprise access control use-cases, whether on-premises, on-cloud or in hybrid infrastructures.

Complying with RMiT Guidelines as mandated by Bank Negara

Access Control

RMiT Guidelines	ARCON Offers
S 10.54 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)	ARCON offers centralized engines IDAM and PAM to govern all users (privileged and non-privileged users) based on pre-defined access control policies. The solutions ensure authorization, authentication and audit of each and every identity (internal and external) accessing information systems.
G 10.55 (a) adopt a "deny all" access control policy for users by default unless explicitly authorised	IDAM and PAM ensures rule and role-based access to target systems. Only those identities that are provisioned to access information systems can access data. The solutions ensure access based on "Need-to-know" and "Need-to-do" basis.
G 10.55 (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	ARCON PAM provides access based on Just-in-Time approach. This method nearly eliminates always-on standing privileges.
G 10.55 C : employ time-bound access rights which restrict access to a specific period including access rights granted to service providers;	ARCON IDAM and PAM offers deepest level of granular controls that includes time-bound access to target systems.
G 10.55 (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.	ARCON PAM offers Virtual Grouping which ensures that users, services, user groups are segregated based on rule and responsibilities. This feature ensures that there are no users with over privileges.
G 10.55 (e) employ dual control functions which require two or more persons to execute an activity	Centralized platforms (IDAM and PAM) enforce a maker checker concept as every user is authorized by admins as per the workflow matrix to execute an activity.

RMiT Guidelines	ARCON Offers
G 10.55 (f) adopt stronger authentication for critical activities including for remote access	Our solutions offer multi-factor authentication mechanism. Our built-in dual factor authentication seamlessly supports integration with third-party authentication tools which includes biometrics.
G 10.55 (g) limit and control the use of the same user ID for multiple concurrent sessions;	Granular controls, session management and session monitoring enable to limit and control the use of the same user ID for multiple concurrent sessions
G 10.55 (h) limit and control the sharing of user ID and passwords across multiple users	User groups with shared IDs and passwords are governed and controlled by PAM
G 10.55 (i) control the use of generic user ID naming conventions in favour of more personally identifiable IDs	Admins can change the user ID as per the policies mandated by IT security staff
S 10.56 A financial institution must employ robust authentication processes to ensure the authenticity of identities in use.	ARCON PAM and IDAM offers robust multi-factor authentication mechanism
S 10.57 A financial institution shall periodically review and adapt its password practices to enhance resilience against evolving attacks.	ARCON Password Vault stores and randomize passwords as per the prescribed mandates and keeps them secure in encrypted form.
S 10.58 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 Single Sign-on authenticates the end-user's identity with several standard identity-based authentication protocols such as 0Auth2.0, OpenID Connect (OIDC) and Security Assertion Markup Language (SAML)
S 10.59 A financial institution is encouraged to adopt dedicated user domains for selected	PAM allows admins to create dedicated user domains for selected and critical IT functions.

RMiT Guidelines	ARCON Offers
critical functions, separate from the broader enterprise-wide user authentication system	
S 10.60 A financial institution must establish a user access matrix to outline access rights, user roles or profiles, and the authorizing and approving authorities.	ARCON IDAM and PAM provides intuitive workflow matrix to ensure seamless user experience, admin efficiency and robust security.
S 10.61 (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.	ARCON IDAM and PAM support typical enterprise access control use cases. The solutions work seamlessly with disparate OSes, applications, hosting models and offer effective management and monitoring of digital identities. Both solutions provide session logs both video and text format for audit purposes.
S 10.62 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.	ARCON IDAM and PAM are highly-scalable and enterprise-grade solutions. The micro service-based architecture ensures seamless integration, keeping TCO low. Besides, the UBA component, which leverages AI and ML detects anomalies on real-time basis. It easily integrates with IAM solutions such as PAM and IDAM.

Cloud Services

RMiT Guidelines	ARCON Offers
S 10.49 (J) ability to meet regulatory requirements and international standards on cloud computing on a continuing basis	ARCON Cloud Governance solution offers complete control over the IT workloads in cloud infrastructure by enforcing robust access control policies across the cloud infrastructure. The solution seamlessly manages cloud identities and entitlements across all public cloud platforms thereby helping to comply with regulatory requirements and international standards related to access management. Cloud Governance offers:

	1. Centralized dashboard 2. Single policy enforcement 3. Seamless monitoring, 4. Dynamic access control policy 5. Automated anomaly detection 6. User entitlements 7. Control over user entitlements 8. Restricted access management

Third Party Service Provider Management

RMiT Guidelines	ARCON Offers
S 10.42 an assessment shall be made of the third-party service providers' capabilities in managing following risks: a) data leakage, f) over reliance on key personnel, g) mishandling of confidential information	ARCON PAM platform offers an easy to configure unified access control framework which allows tenants to make access and service requests in the same manner as if PAM were running on-premises or controlled from the cloud by on site admins. The solution provides workflows to be configured for each customer, according to individual security/business policies and processes. Besides, it offers: 1. Privileged Elevation and Delegation Management 2. JIT Privileges 3. Single Sign-on 4. User Behaviour Analytics 5. Password Vaulting and MFA 6. Granular controls 7. Session logs 8. Comprehensive reports of privileged activities

Conclusion

ARCON's robust stack of identity access control solutions enables:

- Financial institutions to build a resilient enterprise risk management framework
- To mitigate unauthorized access threats to information systems
- Compliance with regulatory and international standards on access control

about ARCON

ARCON is a leading enterprise information risk control solution provider, specializing in Privileged Access Management (PAM) and continuous risk assessment solutions. Our mission is to help enterprises identify emerging technology risks and mitigate them through robust solutions that predict, protect, and prevent IT threats.

Connect with us

arcon