Reinforcing IT Risk Management and Governance with ARCON | Privileged Access Management (PAM)

Learn how ARCON Privileged Access Management helps financial institutions in Malaysia to comply with the Bank Negara's policy document on Technology Risk Management

Overview

Technology risk management and governance are one of the most recurrent topics in the boardroom discussion today. Protecting corporate information assets has become the cornerstone of overall corporate strategy as the cost of cyber-attack is rising whilst the regulatory landscape supporting Information Security gets more stringent. It has become imperative for global organizations to have a well-defined cybersecurity policy framework in place.

However, every year global organizations are witnessing cyber-attacks disrupting normal IT operations. Costs from cyber incidents are escalating. To a large extent, the changing IT risk landscape is the result of the increasing digitalization of business operations.

The number of digital identities, endpoints, business-critical applications, devices and overall IT infrastructure has grown exponentially as global organizations especially financial institutions are developing the digital ecosystem. This ecosystem includes multiple data centers- in premises, on-cloud, or in managed third-party service environments.

Therefore the IT risks and vulnerabilities have also increased. Compromise of identity or unauthorized access to business critical information is the looming threats for today's financial institutions. Therefore, it is of paramount importance for financial institutions to build resilient digital ecosystems and develop digital trust.

Bank Negara, Malaysia in its IT Risk Management policy document very succinctly puts that with the more prevalent use of technology in the provision of financial services, there is a need for financial institutions to strengthen their technology resilience against operational disruptions to maintain confidence in the financial system. The growing sophistication of cyber threats also calls for the increased vigilance and capability of financial institutions to respond to emerging threats.

In this paper, ARCON explains how its robust risk control solution ARCON| Privileged Access Management helps financial institutions in addressing some of the toughest challenges emanating from Information Technology.

Understanding the cyber threats from financial institutions' perspective

- With hundreds of billions of dollars under the responsibility of the management, financial institutions store, process, and manage large amounts of data stored in various systems and applications
- Moreover, for core banking solution providers, technology infrastructure expands along with the increase of multiple data centers, a growing number of endpoints and the transition of IT operations to the IaaS platforms, managed services or hybrid environments
- A huge number of financial records, confidential data, sensitive data, account details, and credit card details can easily fall prey to cyber-attacks stored in systems
- If there are no provisions to encrypt and secure data, no unified governing tool, absence of end-user monitoring, inadequate authentication process, no IT audits and controls, lack of passwords randomization, the risk surface automatically expands. In other words, there is an urgent need to reinforce access control, data center and network resilience

The significance of Privileged Access Management

Financial institutions' business data needs robust security from internal and external threats. Scaling-up of IT infrastructure amid increasing digitization of business operations has put financial institutions' critical business information, intellectual property, customer data among several other types of classified information vulnerable to theft or abuse from organized cybercriminals attacks, malicious third-party users and compromised corporate insiders.

The challenge is compounded by the fact that today's IT environment is very complex. More and more devices are connected. Data is not just stored in on-premises data centers, but moved to Cloud Service Providers (CSP) and Managed Service Providers (MSP). Against this backdrop of distributed and shared IT environments, protecting data demands a secure and efficient IT administrative interface, which is provided by practicing Privileged Access Management.

Indeed, Privileged Access Management has become a central component of a modern-day organization's information security framework. As organizations scale-up their IT operations, the number of privileged users/ identities are also rising to administer day-to-day's privileged tasks. Application accounts, service accounts, network accounts, database accounts, Operating systems accounts and other forms of administrative accounts are rising as organizations structure their IT infrastructure in multiple layers of devices and applications spread both on-premises and third-party environments.

It is this growing number of administrative entitlements that necessitates continuous monitoring and controlling of privileged accounts. A majority of data breach incidents that typically involve malicious corporate insiders or compromised third party users stem from misuse/abuse of privileged accounts. Inadequately protected privileged accounts incentivize cybercriminals and compromised insiders to target critical systems and data. Therefore protecting privileged accounts from unauthorized access forms the foundation of the overall information security framework.

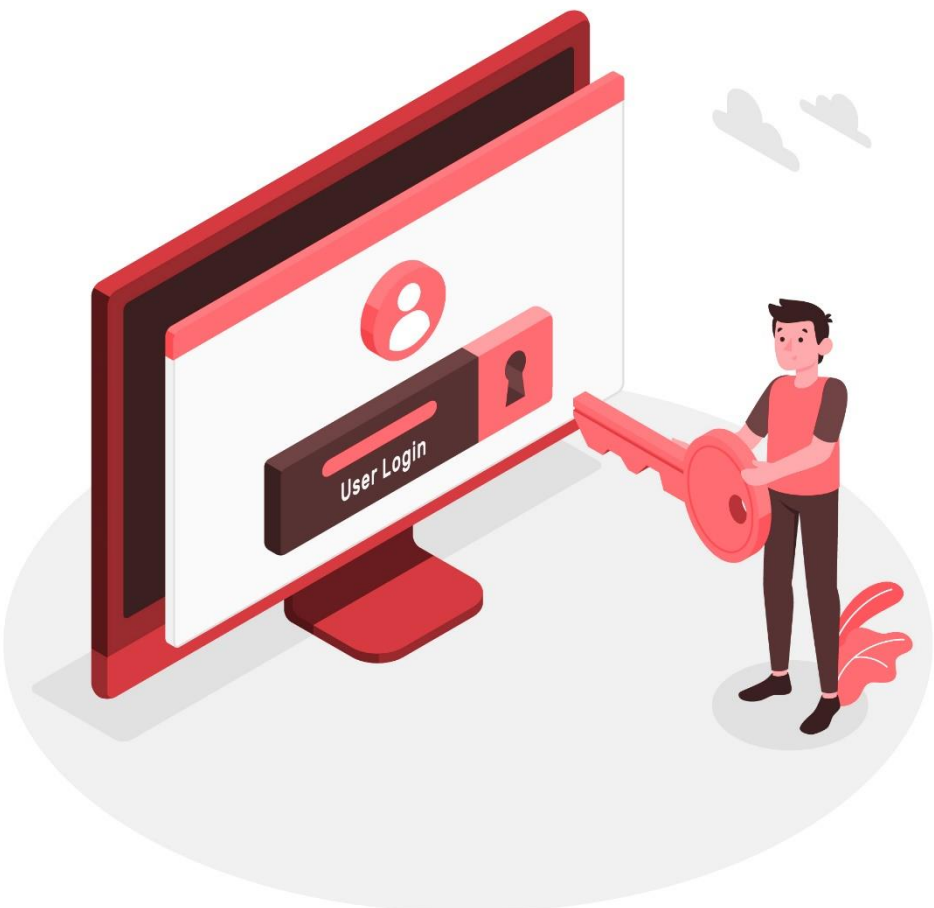
Against this backdrop of expanding risk surfaces, organizations are fast adopting privileged access management. This practice enables the security and risk management team to reinforce the inner realm of IT infrastructure. It allows implementing a rule and role based access to target systems.

Bank Negara Malaysia policy paper S 10.61 explicitly states that:
(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 on time

ARCON Privileged Access Management offers IT risk management and governance teams with the following safeguards

- A unified policy framework to restrict and control privileged user access to target systems
- Granular level control to ensure rule and role-based access to critical information
- Real-time monitoring of privileged users including third party activities on databases, network devices, could applications, servers and other business critical applications
- Robust password vaulting and randomization to secure privileged credentials
- Multi-factor authentication to ensure authorized access to target systems
- Detailed Audit trails of all privileged tasks happening in the IT ecosystem

Financial institutions of all shapes and sizes find ARCON| PAM is a useful tool to gain operational efficiency and mitigate data breach threats. Moreover, the solution helps to comply with regulatory Information Security standards such as the **PCI-DSS, SWIFT CSCF, SOX,** and the **EU GDPR** among others.



ARCON PAM compliance mapping

For RMiT policy, there is a set of standard requirement and specification termed as "S" and a standard guidance consisting of advice and recommendation known as "G". Let us see how ARCON | PAM complies with all the standard policy requirements and why it is the best-in-class solution to ensure a robust security framework for financial institutions. Although the policy document is broader in its scope, ARCON | PAM covers all the elements that are required to keep data confidentiality, data integrity and data sanctity.

Sl No.	Policy No.	Policy Requirements	ARCON | PAM in Action
1	S 10.27 Data Center Resilience	A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators.	▪ Real-time Session Monitoring of privileged activities helps the IT security team to detect any suspicious activity and notify the admin immediately ▪ With the Live Dashboard, the administrators can scrutinize all critical activities performed across the IT infrastructure on real-time basis
2	S 10.28 Data Center Resilience	A financial institution must segregate incompatible activities in the data centre operations environment to prevent any unauthorised activity. In the case where vendors' or programmers' access to the production environment is necessary, these activities must be properly authorised and monitored.	▪ The tool offers a unified governing engine ▪ Access to data center devices is strictly based on rule and role-based policy ▪ Multi-Factor authentication ensures only authorized people have access to the target device ▪ Virtual Grouping enables the IT infrastructure team to segregate privileged users and their access to authorized database and applications ▪ based on assigned roles and duties
3	S 10.36 Network Resilience	A financial institution must ensure network smervices supporting critical systems are designed and implemented to ensure the confidentiality, integrity and availability of data.	▪ The solution mitigates data breach threats and ensures the confidentiality of data by offering Granular control. It restricts and elevates privileges to access network devices ▪ Access to network systems is controlled and restricted through rule and role-based workflows
4	S 10.38 Network Resilience	A financial institution must ensure sufficient and relevant network device logs are retained for investigations and forensic purposes for at least three years.	▪ The solution offers advanced capabilities such as customized reporting, real-time alerts and analytics ▪ Each and every activity performed by end user is captured in a text and video format

Sl No.	Policy No.	Policy Requirements	ARCON | PAM in Action
5	**S 10.45** **Third-Party Service Provider**	A financial institution must ensure its third party service providers comply with all relevant regulatory requirements prescribed in this policy document	With ARCON | PAM third-party service providers can ensure all data security standards including those of RMiT such as ▪ Principle of least privilege ▪ Password rotations ▪ Access strictly based on 'need-to-know and 'need-to-do' basis ▪ Single Sign-On (SSO) ▪ PEDM (Commands/ Process Restrictions) ▪ Granular level access control ▪ Session Monitoring and Recording ▪ SMART Audit Trails ▪ MFA (Multi-factor Authentication) ▪ Account Discovery
6	**S 10.53** **Cloud Services**	A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorized disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.	▪ ARCON|PAM offers centralized policy engine through which all access to management consoles, Hosted applications, virtualization machines are managed, monitored and controlled ▪ ARCON|PAM helps in integrating all the elements under a single command and control console ▪ ARCON|PAM offers a dual factor authentication to ensure secure access and accountability as critical systems are integrated ▪ The access to the devices can be controlled on "Need- to- Know" and ▪ "Need- to- Do" basis i.e. there is a comprehensive workflow to grant access to various devices ▪ Session logs of all administrative activities are recorded i.e. video format as well as a command are tracked centrally and these logs are in a legal hold and not available to end-users

Sl No.	Policy No.	Policy Requirements	ARCON | PAM in Action
7	S 10.54 Access Control	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 unauthorized access to its technology systems.	ARCON | PAM offers best-in-class identification authentication and authorization mechanism which includes the following: ▪ Multi-Factor Authentication - Biometric, Hardware Tokens, Software Token, Mobile OTP, SMS OTP, Email OTP ▪ Command Restrictions ▪ User Access Review ▪ Workflow matrix ▪ File & Folder Watching ▪ Privilege Elevation and Delegation Management ▪ Just-in-time privileges to target systems and applications
8	G 10.55 Access Control	In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy: (a) adopt a "deny all" access control policy for users by default unless explicitly authorized; (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; (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. (e) employ dual control functions which require two or more persons to execute an activity; (f) adopt stronger authentication for critical activities including for remote access;	▪ Solution helps to build a resilient Zero Trust security framework around the so-called 'trusted' identities in the network. It continuously verifies trustworthiness with risk-based assessments. ARCON PAM works under 'deny all access until the trust is verified'. Read our Zero Trust Document for deeper understanding. ▪ Granular level control and restrictions over all privileged users ensure time-bound access and implementation of least privilege principle ▪ Just-In-Time privilege of ARCON | PAM solution removes standing privilege by limiting access to systems/ applications by granting access only when requested exclusively. It even limits access at a granular level and denies full-time access to systems/ applications. ▪ The solution implements access to critical systems only on 'need-to-know' and 'need-to-do' principle which strengthens security. ▪ Multi-factor authentication (MFA) of ARCON | PAM acts as a robust validation mechanism of user access to critical systems

Sl No.	Policy No.	Policy Requirements	ARCON | PAM in Action
9	S 10.56 Access Control	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).	▪ The solution's MFA functionality acts as a strategic entry point to identity management systems and helps managing system based users ▪ ARCON offers native software-based One-Time-Password (OTP) validation to begin a privileged session and the tool seamlessly integrates with disparate third-party authentication solutions such as Gemalto, RSA, Vasco, 3M, Precision, SafeNet and Safran
10	S 10.57 Access Control	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.	▪ The solution provides password vaulting features that ensures compliance with strength and frequency of change requirements demanded by regulators in a seamless manner

Conclusion

ARCON PAM is a robust IT risk management tool which helps financial institutions by Building resilient Information Security framework

- Building resilient Information Security framework
- Ensuring authorized and secure access to systems
- Keeping the brand equity intact as it mitigates data breach incidents
- Winning the digital trust of all business stakeholders
- Complying with all major international security standards

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