

Complying with the mandate 3.3.5: Identity and Access Management with ARCON Privileged Access Management

The kingdom of Saudi Arabia (KSA) is in midst of digital revolution. With Vision 2030, KSA is putting a lot of emphasis on diversified sectors such as ICT, manufacturing, renewables etc. for sustainable growth. What that means is banking entities and financial institutions will be pivotal for economic prosperity and sustained growth. In this backdrop, adhering to the SAMA cybersecurity framework will be crucial for banking and financial institutions' cyber hygiene.

Privileged Access Management provides adequate safeguards against identity and access management related threats. Security and Risk Management (SRM) Leadership will find that ARCON | Privileged Access Management solution is comprehensive solution that offers critical capabilities to comply with the SAMA Guidelines on Identity and Access Management.

Overview

What are SAMA Guidelines?

The SAMA cybersecurity framework is a supervisory mandate for banks, payment providers, insurance companies, finance companies and credit bureaus operating out of the KSA. In May 2017, SAMA prepared and issued a cyber security framework, that mandates SAMA regulated financial institutions/ organizations to effectively identify, and address risks related to cyber security. SAMA framework is based on the exact requirements of the finance organizations,

including standards of the Basel Committee (the Basel III compliance) on Banking Supervision.

This compliance's objective is to create a common approach for addressing cyber security and to achieve an appropriate maturity level of cyber security controls. This way the emerging cyber security risks are effectively managed.

Who must Comply with the SAMA Cybersecurity framework?

The SAMA regulation guidelines provide robust security measures to reinforce the overall financial network within KSA. It is extremely crucial to understand the types of organizations who must comply with this framework. It includes:

- All banks that are functioning inside the country of Saudi Arabia
- Insurance and/or reinsurance companies established and operational in Saudi Arabia
- Financial service providers who offer its services in Saudi Arabia
- Credit bureaus active in Saudi Arabia
- Financial market infrastructural entities (e.g., securities registries, stock exchanges, clearing houses)

In this regard, the banking industry is required to adhere to all areas, or domains, of this framework, covering various requirements such as application security, access control, infrastructure security, etc. Other organizations, depending on their function and risk exposure, may be required to comply with the selected domains. The SAMA compliance ensures that these organizations are prepared to address any cyber threats.

The Core objectives of SAMA Compliance

In addition to mandating the compliance guidelines, the SAMA even evaluates the effectiveness of the guidelines to address cyber security threats for target organizations and guides their cyber security requirements. This proactive initiative by SAMA fosters stakeholder confidence and ensures the security of the financial ecosystem in the KSA.

- Confidentiality – Information assets are accessible only to those authorized.
- Integrity – Information assets are accurate, complete, and processed correctly.
- Availability – Information assets are resilient and accessible when required.

The SAMA is aligned with the best practices and requirements of other regulatory mandates such as the NIST, ISO, BASEL III, and PCI-DSS. It outlines cyber security controls pertinent to various information assets of the member organization, including electronic and physical information, software applications, computer systems, and communication networks.

SAMA Compliance and the significance of Privileged Access Management (PAM)

A growing number of banking organizations and financial institutions' access management use cases happen beyond the traditional boundaries of identity. Indeed, today's financial institutions no longer manage data and workloads in on-premises data centers. Many tasks are conducted by third-party consultants from remote environments. In this evolving scenario, enterprise IT risk management teams must now manage the workforce identities, especially the privileged identities, encompassing big user populations (internal and external) spread in a much-dispersed user environment.

This has necessitated to develop an effective privileged access management strategy. To prevent unauthorized access to information systems, password abuse/misuse, account takeover, insider and third-party threats, a robust privileged access management (PAM) practice is required. Therefore, it is imperative for SRM and GRC (Governance, Risk, and Compliance) to treat PAM as an integral component of the overall robust enterprise risk management framework. A robust privileged access management strategy ensures the following:

- Continuous monitoring of privileged identities
- Frequent changes and randomization of privileged credentials
- Real-time threat detection and alerts emanating from suspicious privileged identities
- Applying multi-factor authentication to privileged identities for accessing critical IT resources
- Audit trails and reporting of each privileged access to information systems

SAMA Compliance Checklist

The SAMA Cybersecurity Framework is broad in scope. It encompasses best-security practices that help to enhance the people and processes management including corresponding relationships and offers the building blocks for strategic process alignment towards strong security posture.

In this paper we have specifically covered SAMA compliance requirements 3.3.5 - Identity and Access Management and explained in the table below how ARCON | Privileged Access Management solution helps to comply with the SAMA Cybersecurity mandates on 3.3.5 Identity and Access Management.




SAMA Guidelines: 3.3.5 Identify and Access Management


Principle






The Member Organization should restrict access to its information assets in line with their business requirements based on the need-to-have or need-to-know principles.

Objective

To ensure that the Member Organization only provides authorized and sufficient access privileges to approved users.

Control Considerations	Does ARCON PAM Helps to Comply with	ARCON Solution
The identity and access management policy, including the responsibilities and accountabilities, should be defined, approved and implemented.		One Admin Control: ARCON offers unified admin console to manage entities, ensuring every access is happening to the target system/ application through authorization. It ensures that the access control framework is built around people and policies only on "need-to-know" and "need-to-do" basis. One Admin Control builds the foundation of robust identity and access management.
Compliance with the identity and access policy should be monitored.		Identity Governance: ARCON's Identity Governance (IG) module encompasses the policies, procedures, and technologies that manage digital identities and their access to critical resources. IG ensures that the right people have the right level of access to the right resources at the right time. It includes the entire identity lifecycle, including identity creation/ deletion, and ongoing monitoring, review, and certification of access rights to ensure that they are appropriate and up to date.
The effectiveness of the cyber security controls within the identity and access management policy should be measured and periodically evaluated.		ARCON PAM offers an outcome-based mechanism so that SRM leaders can evaluate the effectiveness of IAM controls. For example: The ITDR tool- Knight Analytics leverages machine learning, detects identities deviating from baselines and raises red flags with risk-based scorecards.

		Audit Trails and Reporting: ARCON PAM offers 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. These measures ensure better PAM decisions.
The identity and access management policy should include a. business requirements for access control (i.e., need-to-have and need-to-know); b. user access management (e.g., joiners, movers, leavers)		One Admin Control and Identity Governance (IG) addresses both requirements as explained above.
User access requests are formally approved in accordance with business and compliance requirements (i.e., need-to-have and need-to-know to avoid unauthorized access and (un)intended data leakage)		Please refer to row no. 1 – One Admin Control
Changes in access rights should be processed in a timely manner		ARCON’s IGA module offers complete Lifecycle Management as explained in row 2. Also, it provides end-users to check which asset has been preserved/ revoked by the reviewer. In case of revoked assets, the users have a chance to justify with compelling reasons and ask the reviewer to change the decision.
Periodically user access rights and profiles should be reviewed		The IGA module ensures that user access rights and profiles are reviewed periodically.
An audit trail of submitted, approved and processed user access requests and revocation requests should be established.		Workflow Management: ARCON PAM offers workflow matrix that enables IT administrators to configure the approval process for privileged users or user groups by controlling access requests or revocation of requests.
User access management should be supported by automation		Starting from user and account discovery to onboarding and mapping of the users and assigning them role-based tasks and governance of the users – everything is automated through ARCON PAM and ARCON’s Converged Identity platform.

<p>Centralization of the identity and access management function</p>		<p>One Admin Control offers unified engine to manage identities</p>
<p>Multi-factor authentication for sensitive and critical systems and profiles</p>		<p>Multi-factor Authentication (MFA): 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 solution that best meets their security needs while also seamlessly integrating with their existing IT infrastructure. ARCON PAM can also integrate with third-party multifactor applications. (e.g. Cisco Duo)</p>
<p>Privileged and remote access management, which should address the allocation and restricted use of privileged and remote access, specifying:</p> <ul style="list-style-type: none"> a. multi-factor authentication should be used for all remote access; b. multi-factor authentication should be used for privilege access on critical systems based on a risk assessment 		<p>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 mechanism ensuring robust security.</p>
<p>The periodic review of users with privileged and remote accounts</p>		<p>Global Remote Access (GRA) of ARCON offers End-To-End Remote Privileged Session where IT administrators can remotely elevate access rights of the end-users based on requirements without sharing the credentials.</p>
<p>The use of non-personal privileged accounts, including:</p> <ul style="list-style-type: none"> a. limitation and monitoring; b. confidentiality of passwords; c. changing passwords frequently and at the end of each session 		<p>ARCON PAM offers a robust access control module that ensures the deepest level of granular access controls by limiting their access through the least-privilege principle. Every privileged activity is monitored seamlessly with the help of robust session monitoring engine.</p> <p>ARCON PAM's Password Vault ensures that all the privileged account passwords are stored and managed in a highly secure environment by providing a secure and single point of control. It employs strong encryption algorithms, including FIPS approved Advanced Encryption Standard (AES) 256-bit encryption. This way confidentiality of passwords is maintained. Moreover, it helps to generate complex, rotated, and randomized passwords for privileged accounts that cannot be easily guessed or cracked. It eliminates the need for privileged users to remember and share passwords, thus eliminates the risk of password misuse.</p>

Conclusion

ARCON | Privileged Access Management enables SRM leaders to –

- Comply with SAMA cybersecurity guidelines
- Ensure robust identity and access management posture
- Mitigate the chances of data breach incidents and password abuse

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    

All rights reserved by ARCON

This document or any part of the document may not be reproduced, distributed or published in any form without the written consent of the copyright owner under any circumstances. Any kind of infringement in the owner's exclusive rights will be considered unlawful and might be subject to penalties.