BeyondTrust

Mapping BeyondTrust Capabilities to the SAMA's Cyber Security Framework

This document is informational and is intended to provide guidance on how organizations may use BeyondTrust products to meet their own obligations under The Saudi Arabian Monetary Authority (SAMA) cyber security framework. BeyondTrust is not representing that we are subject to or compliant with SAMA.

BeyondTrust

TABLE OF CONTENTS

Overview

This guide has been prepared so that IT and security administrators can quickly understand how using BeyondTrust Identity Security and Privileged Access Management (PAM) solutions map to the requirements set forth in the Saudi Arabian Monetary Authority's (SAMA) Cyber Security Framework.

SAMA established a Cyber Security Framework ("the Framework") to enable Financial Institutions regulated by SAMA ("the Member Organizations") to effectively identify and address risks related to cyber security. To maintain the protection of information assets and online services, the Member Organizations must adopt the Framework.

The objective of the Framework is as follows:

- To create a common approach for addressing cyber security within the Member Organizations.
- To achieve an appropriate maturity level of cyber security controls within the Member Organizations.
- To ensure cyber security risks are properly managed throughout the Member Organizations.

The Framework will be used to periodically assess the maturity level and evaluate the effectiveness of the cyber security controls at Member Organizations and to compare these with other Member Organizations.

What is the Policy Objective?

The Framework defines principles and objectives for initiating, implementing, maintaining, monitoring, and improving cyber security controls in Member Organizations.

The Framework provides cyber security controls which are applicable to the information assets of the Member Organization, including:

- Electronic information
- Physical information (hard copy)
- Applications, software, electronic services, and databases
- Computers and electronic machines (e.g., ATM)
- Information storage devices (e.g., hard disks, USB sticks)
- Premises, equipment, and communication networks (technical infrastructure)

The Framework provides direction for cyber security requirements for Member Organizations and its subsidiaries, staff, third parties, and customers.

For business continuity related requirements, please refer to the SAMA Business Continuity Minimum Requirements.

The Framework has an interrelationship with other corporate policies for related areas, such as physical security and fraud management. This framework does not address the non-cyber security requirements for those areas.

Who needs to implement the Saudi Arabian Monetary Authority's Policy?

The Framework is applicable to all Member Organizations regulated by SAMA, which include the following:

- All Banks operating in Saudi Arabia
- All Insurance and/or Reinsurance Companies operating in Saudi Arabia
- All Financing Companies operating in Saudi Arabia
- All Credit Bureaus operating in Saudi Arabia
- The Financial Market Infrastructure

All domains are applicable for the banking sector. However, for other financial institutions the following exceptions apply:

- Sub-domain (3.1.2) - The alignment with cyber security strategy of banking sector is mandatory when applicable.
- Exclude sub-domain (3.2.3) - However, if the organization stores, processes or transmits cardholder data or deals with SWIFT services, then PCI standard and/or SWIFT Customer Security Controls Framework should be implemented.
- Exclude sub-domain (3.3.12).
- Exclude sub-domain (3.3.13) - However, if the organization provides online services for customers, a multi-factor authentication (MFA) capability should be implemented.

Framework and Structure

The Framework is structured around four main domains, namely:

- Cyber Security Leadership and Governance
- Cyber Security Risk Management and Compliance
- Cyber Security Operations and Technology
- Third-Party Cyber Security

For each domain, several subdomains are defined. A subdomain focuses on a specific cyber security topic.

Per subdomain, the Framework states a principle, objective, and control considerations.

A **principle** summarizes the main set of required cyber security controls related to the subdomain. The **objective** describes the purpose of the principle and what the set of required cyber security controls are expected to achieve. The **control considerations** reflect the mandated cyber security controls that should be considered.

How BeyondTrust Solutions Can Help

BeyondTrust's capabilities can help address seven individual controls across four of the main domains within the **SAMA Cyber Security Framework.**

This whitepaper explains how organizations can use BeyondTrust solutions to map to the **SAMA Cyber Security Framework** in order to maintain security and more easily demonstrate and maintain compliance. BeyondTrust is the global identity security leader protecting Paths to Privilege™, and our identity-centric approach goes beyond securing privileges and access, empowering organizations to manage their entire identity attack surface and neutralize threats, whether from external attacks or insiders.

Each **SAMA Cyber Security** policy requirement is outlined in the following sections and are mapped to these BeyondTrust solutions:

- Identity Security Insights® – Gives organizations unified visibility into identity risk by continuously analyzing human and non-human identities, privileges, and access paths, revealing hidden escalation risks and enabling proactive threat detection.
- Entitle - Cuts off privilege attack paths by eliminating always-on access, replacing it with just-in-time (JIT) automation that reduces risk without slowing down organizations.
- Password Safe® - Enables automated discovery, onboarding, management, and auditing of all privileged accounts, privileged credentials (passwords, secrets, keys, etc.).
- Privileged Remote Access - Delivers secure, just-in-time remote access to cloud, on-premises, and OT environments—using identity-based controls, credential injection, and session auditing—without relying on traditional VPNs.
- Endpoint Privilege Management - Enforces least privilege and application control across Windows, macOS, Unix, and Linux systems by removing standing administrative rights and granting elevated access only to approved applications and tasks.
- Remote Support – Enables service desk technicians to support any user or device, anywhere, all while ensuring enhanced security. Applies least privilege and robust audit controls to all remote access required by employees, vendors, and service desks.
- Active Directory Bridge - Extends Microsoft Active Directory authentication, single sign-on (SSO), and policy controls to Unix and Linux systems, enabling centralized identity governance, consistent access enforcement, detailed auditing, and compliance across mixed operating system environments.

The controls matrix on the following pages highlights the primary applicable SAMA Cyber Security requirements that your organization can address by leveraging the capabilities within BeyondTrust solutions. This is not meant to be an exhaustive list, but rather to highlight the most relevant features for supporting alignment to the SAMA Cyber Security Framework.

Subdomain number & objective	Control Number	Control	Identity Security Insights	Entitle	Password Safe	Privileged Remote Access	Remote Support	Endpoint Privilege Manage-ment	Active Directory Bridge
3.2.3 To comply with mandatory (inter)n ational industry standards.	1	The Member Organization should comply with:							
		a. Payment Card Industry Data Security Standard (PCI-DSS);	✓	✓	✓	✓	✓	✓	✓
		b. EMV (Europay, MasterCard and Visa) technical standard;	✓	✓	✓	✓	✓	✓	✓
		c. SWIFT Customer Security Controls Framework – March 2017.	✓	✓	✓	✓	✓	✓	✓
3.3.5 To ensure that the Member Organization only provides authorized and sufficient access privileges to approved users.	2	The compliance with the identity and access policy should be monitored.			✓	✓			
	3	The effectiveness of the cyber security controls within the identity and access management policy should be measured and periodically evaluated.	✓	✓	✓	✓	✓	✓	✓
	4	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): 1. all identified user types should be covered (i.e., internal staff, third parties); 2. changes of job status or job positions for internal staff (e.g. joiner, mover and leav er) should be instigated by the human resources department; 3. changes for external staff or third parties should be instigated by the appointed accountable party; 4. 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)); 5. changes in access rights should be processed in a timely manner; 6. periodically user access rights and profiles should be reviewed; 7. an audit trail of submitted, approved and processed user access requests and revocation requests should be established;	✓	✓	✓	✓	✓		
		c. user access management should be supported by automation;	✓	✓	✓	✓		✓	✓
		d. centralization of the identity and access management function;	✓	✓	✓	✓	✓	✓	

Subdomain number & objective	Control Number	Control	Identity Security Insights	Entitle	Password Safe	Privileged Remote Access	Remote Support	Endpoint Privilege Manage-ment	Active Directory Bridge
		e. multi-factor authentication for sensitive and critical systems and profiles;		✓	✓	✓	✓	✓	✓
(Cont.) 3.3.5	4	f. privileged and remote access management, which should address: 1. the allocation and restricted use of privileged and remote access, specifying: 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; 2. the periodic review of users with privileged and remote accounts; 3. individual accountability; 4. the use of non-personal privileged accounts, including: a. limitation and monitoring; b. confidentiality of passwords; c. changing passwords frequently and at the end of each session.	✓	✓	✓	✓	✓	✓	✓
3.3.7 To ensure that all change in the information assets within the Member Organization follow a strict change control process.	4	The change management process should include:							
		a. cyber security requirements for controlling changes to information assets, such as assessing the impact of requested changes, classification of changes and the review of changes;	✓	✓	✓	✓			✓
		c. approval of changes by the business owners;	✓	✓	✓	✓			
		h. the procedure for emergency changes and fixes.	✓	✓	✓	✓			
3.3.8 To support that all cyber security controls within the infrastructure are formally documented and the compliance is monitored and its effectiveness is evaluated periodically within the Member Organization.	6	The infrastructure security standard should include:							
		a. the cyber security controls implemented (e.g.,configuration parameters, events to monitor and retain [including system access and data], data-leakage prevention [DLP], identity and access management, remote maintenance);	✓	✓	✓	✓	✓	✓	✓
		b. the segregation of duties within the infrastructure component (supported with a documented authorization matrix);	✓	✓	✓	✓			✓
		c. the protection of data aligned with the (agreed) classification scheme (including privacy of customer data and, avoiding unauthorized access and (un)intended data leakage);		✓	✓	✓	✓		✓

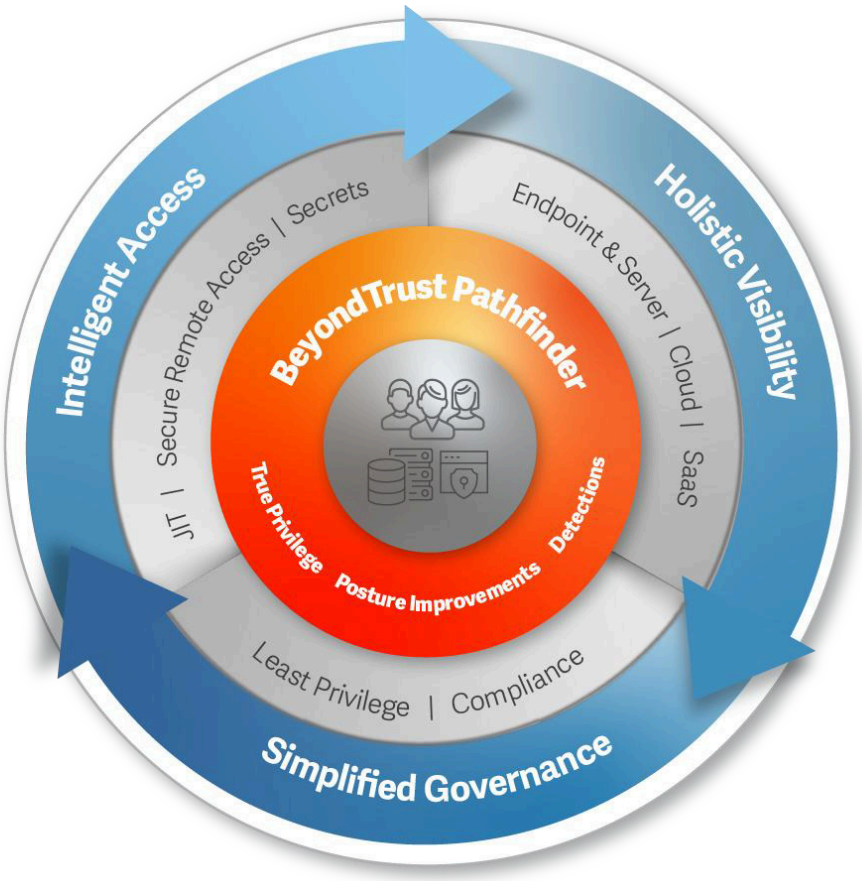
Subdomain number & objective	Control Number	Control	Identity Security Insights	Entitle	Password Safe	Privileged Remote Access	Remote Support	Endpoint Privilege Manage-ment	Active Directory Bridge
(Cont.) 3.3.8	6	d. the use of approved software and secure protocols;		✓		✓	✓		✓
		f. malicious code/software and virus protection (and applying application whitelisting and APT protection);							✓
		j. periodic cyber security compliance review.	✓	✓	✓	✓		✓	✓
3.3.9 To ensure that access to and integrity of sensitive information is protected and the originator of communication or transactions can be confirmed.	4	The cryptographic security standard should include:							
		c. the management of encryption keys, including lifecycle management, archiving and recovery.			✓	✓			
3.3.13 To ensure the Member Organization safeguards the confidentiality and integrity of the customer information and transactions.	4	The infrastructure security standard should include:							
		c. ATMs and POSs: 1. prevention and detection of exploiting the ATM/POS application and infrastructure vulnerabilities (e.g., cables, (USB)-ports, rebooting); 2. cyber security measures, such as hardening of operating systems, malware protection, privacy screens, masking of passwords or account numbers (e.g., screen and receipt), geo-blocking (e.g., disable cards per default for outside GCC countries, disable magnetic strip transactions), video monitoring (CCTV), revoking cards after 3 successive invalid PINs, anti-skimming solutions (hardware/ software), and PIN-pad protection; 3. remote stopping of ATMs in case of malicious activities.			✓	✓	✓		✓
3.3.14 To ensure timely identification and response to anomalies or suspicious events within regard to information assets.	3	To support this process a security event monitoring standard should be defined, approved and implemented:							
		a. the standard should address for all information assets the mandatory events which should be monitored, based on the classification or risk profile of the information asset.		✓	✓	✓	✓	✓	✓
	4	The security event management process should include requirements for:							
		f. detection and handling of security or suspicious events and anomalies;	✓	✓	✓	✓	✓	✓	✓
		i. periodic compliance monitoring of applications and infrastructure cyber security standards;	✓	✓	✓	✓	✓		✓
		j. automated and centralized analysis of security loggings and correlation of event or patterns.	✓	✓	✓	✓	✓		

The BeyondTrust Pathfinder Platform

The BeyondTrust Pathfinder Platform unifies identity visibility, intelligence, and control in a single AI-driven control plane. It maps and manages privilege relationships across human, machine, AI agent, and workload identities—revealing hidden Paths to Privilege™ and enabling proactive risk reduction across the entire identity attack surface.

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions. BeyondTrust was named a Leader in both the The Forrester Wave™: Privileged Identity Management Solutions, Q3 2025 report and the Gartner® Magic Quadrant™ for Privileged Access Management. We believe these accolades reflect strong execution and a comprehensive vision for identity security.

As a centrally managed, extensible platform, Pathfinder allows organizations to deploy a full set of PAM and identity security capabilities at once—or adopt them incrementally over time—while maintaining unified visibility, consistent policy enforcement, and operational efficiency from a single unified console.



About BeyondTrust

BeyondTrust is the global identity security leader protecting Paths to Privilege™. Our identity-centric approach goes beyond securing privileges and access, empowering organizations with the most effective solution to manage the entire identity attack surface and neutralize threats, whether from external attacks or insiders.

BeyondTrust is leading the charge in transforming identity security to prevent breaches and limit the blast radius of attacks, while creating a superior customer experience and operational efficiencies. We are trusted by 20,000 customers, including 75 of the Fortune 100, and our global ecosystem of partners.

Learn more at **www.beyondtrust.com.**