WHITEPAPER

Strengthening Cybersecurity with the SAMA Framework

segura® | Futureproof Identity Security | segura.security

Introduction

With rising cyber threats and increasing regulatory demands, SAMA compliance has become a business-critical priority for financial institutions in the Kingdom.

Banks, insurers, finance companies, and credit agencies operating in Saudi Arabia must follow the cybersecurity standards set by the Saudi Central Bank (SAMA).

The SAMA Cybersecurity Framework was designed to help these organizations strengthen their ability to prevent, detect, and respond to cyber risks—creating a more secure and resilient financial sector across the region.

Its main objectives are to:

- Establish a unified cybersecurity approach across regulated entities
- Set a clear baseline of maturity and control
- Support continuous risk oversight aligned with global best practices

This whitepaper explores how the Segura® 360° Privilege Platform helps financial institutions align with SAMA's core controls. Our integrated platform includes:

- **PAM Core**
- **Endpoint Privilege Manager**
- **DevOps Secrets Manager**
- **Domum Remote Access**

These tools help simplify identity and access management while supporting continuous control, automation, and audit readiness.

Whether you're preparing for a compliance audit or strengthening day-to-day operations, this whitepaper gives you a practical view of how to align SAMA controls with real tools—so you can act faster, reduce risk, and stay in control.

Overview of the SAMA Cybersecurity Framework

The **SAMA Cybersecurity Framework** provides a clear and structured approach for managing cybersecurity across regulated financial institutions.

It's designed to support each stage of your cybersecurity lifecycle—from strategy and setup to improvement and enforcement.

The framework applies to a wide range of assets, including:

- Digital and physical information
- Software, applications, databases, and online services
- IT equipment like ATMs and computers
- Data storage devices (e.g., hard drives, USBs)
- Communication networks and infrastructure

Importantly, SAMA's guidance extends to **subsidiaries, third parties, employees, and customers**—making it essential to build access control into every layer of your organization. It also connects cybersecurity to related governance areas such as fraud prevention and physical security.

Conditional Application

While all domains are mandatory for banks, certain subdomains may be excluded or conditionally applied to other financial entities. For example:

Subdomain 3.1.2: Alignment with a cybersecurity strategy is only required if a documented strategy exists

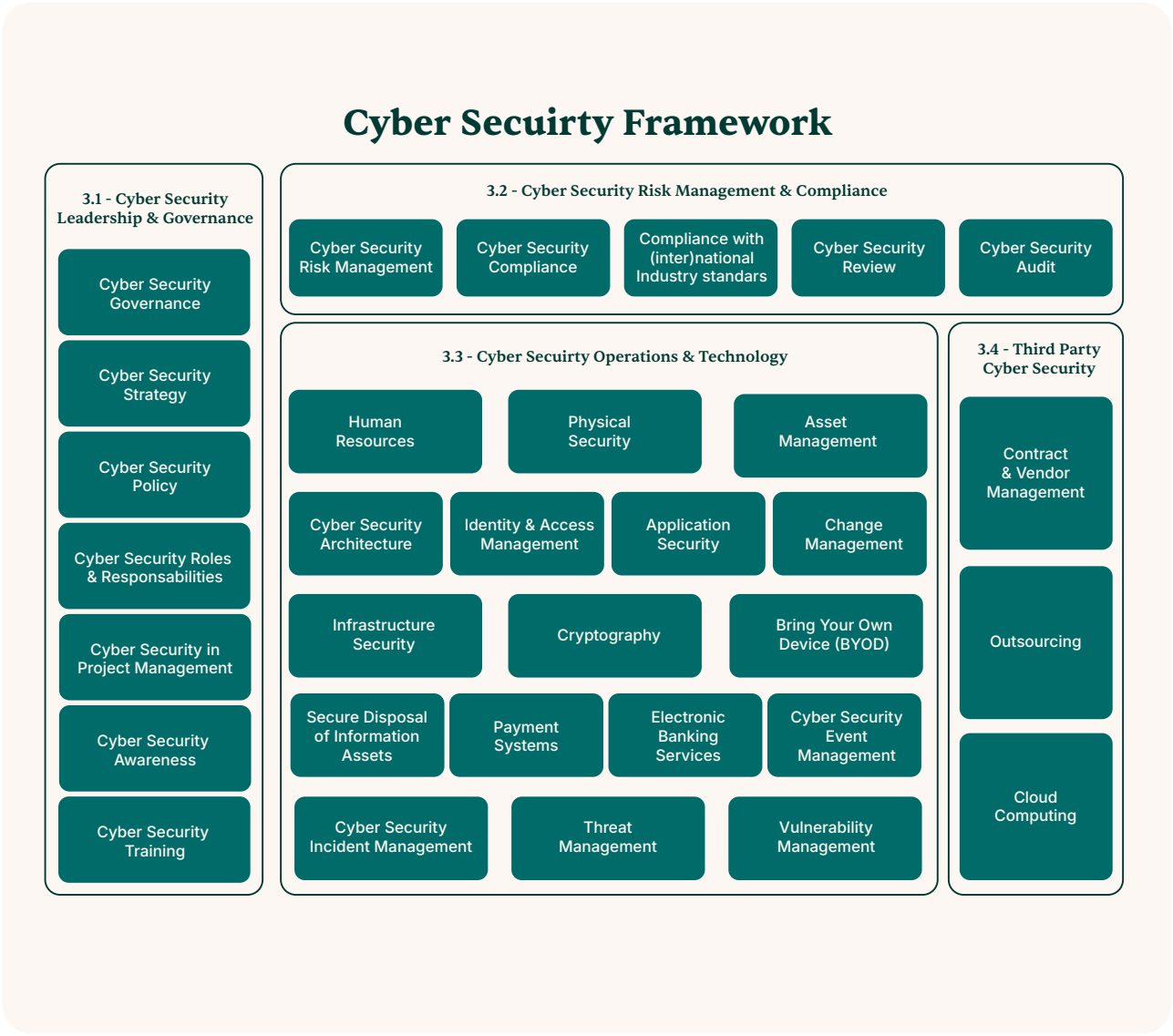
Subdomain 3.2.3: PCI-DSS and SWIFT CSC controls apply only if cardholder data is processed or SWIFT services are used

Subdomain 3.3.12 and 3.3.13: May be excluded unless online services are provided to customers

The Framework is structured into **four core domains**, each composed of subdomains that define principles, objectives, and mandatory controls:

- Cybersecurity Leadership and Governance
- Cybersecurity Risk Management and Compliance
- Cybersecurity Operations and Technology
- Third-Party Cybersecurity

Together, these domains give institutions a complete lens for evaluating controls, building maturity, and demonstrating compliance to SAMA.



Segura® Solutions That Support SAMA Compliance

The Segura® 360° Privilege Platform brings together all the tools IT and security teams need to align with the SAMA Framework, without adding complexity.

Each solution is built to support key SAMA controls with identity governance, secure access, audit tracking, endpoint protection, and automation.

PAM Core

Centralizes and automates credential management to prevent misuse and enforce security policy.

Key capabilities:

- Protects against internal threats and data theft
- Monitors and records privileged sessions
- Automates password rotation
- Securely stores credentials and keys
- Enforces least privilege principles

Domum Remote Access

Delivers secure, VPN-free access for employees, vendors, and third parties, fully aligned with Zero Trust.

Key capabilities:

- Granular access segmentation without requiring PAM logins
- Full session monitoring and recording
- No need for VPN or extra configuration
- Supports compliance with access-related regulatory requirements
- Enhanced control over third-party activities

Endpoint Privilege Manager

Extends access control to endpoint devices through granular privilege management and application control.

Key capabilities:

- Role-based access elevation for Windows and Linux
- Application allow/deny listing per user or group
- Logs and audits all local activity
- Enforces least privilege policies automatically
- Supports multiple compliance mandates for SAMA, along with other regulations like PCI, ISO 27001, SOX, and GDPR

DevOps Secrets Manager

Secures secrets and credentials used in DevOps workflows, cloud environments, and CI/CD pipelines.

Key capabilities:

- Protects machine identities, APIs, and application secrets
- Automates rotation and credential access across environments
- Enhances DevSecOps maturity through secure automation
- Secures CI/CD workflows without slowing down teams
- Supports key identity, encryption, and automation controls under ECC

Mapping Segura® Solutions to SAMA Controls

The chart below shows how each **Segura® 360° Privilege Platform** component supports required subdomains within the **SAMA Cybersecurity Framework.**

Solutions map to core controls such as access governance, session auditing, credential protection, and automation.

Each product supports multiple compliance areas—helping teams track maturity, prepare for audits, and build stronger internal controls.

3.2.3 Compliance with (inter)national industry standards.

To comply with mandatory (inter)national industry standards.

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
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 Identity and Access Management.

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

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
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 leaver) 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 toavoid unauthorized access and (un)intended data leakage));	✓	✓	✓	

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
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;	✓	✓	✓	✓
e. multi-factor authentication for sensitive and critical systems and profiles.	✓	✓		
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;	✓	✓	✓	

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
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 Change Management

To ensure that all change in the information assets within the Member Organization follow a strict change control process.

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
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 owner;	✓	✓	✓	
h. the procedure for emergency changes and fixes.	✓			

3.3.8 Infrastructure Security

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.

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
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 nfrastructure 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);	✓	✓	✓	
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 Cryptography

To ensure that access to and integrity of sensitive information is protected and the originator of communication or transactions can be confirmed.

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
4. The cryptographic security standard should include: c. the management of encryption keys, including lifecycle management, archiving and recovery.	✓			✓

3.3.13 Electronic Banking Services

To ensure the Member Organization safeguards the confidentiality and integrity of the customer information and transactions.

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
4. Electronic banking services security standard should cover: 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;		✓	✓	

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
3. remote stopping of ATMs in case of malicious activities.		✓	✓	

3.3.14 Cyber Security Event Management

To ensure timely identification and response to anomalies or suspicious events within regard to information assets.

Control	Segura® solution			
	PAM Core	Domum	Endpoint Privilege Manager	DevOps Secret Manager
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.	✓	✓	✓	
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 (i.e., Security Information and Event Management (SIEM));	✓	✓	✓	

Conclusion

The SAMA Cybersecurity Framework provides a structured path for building stronger identity and access controls across Saudi Arabia's financial sector.

The Segura® 360° Privilege Platform helps your team align with SAMA faster—reducing time to compliance and helping you move toward a more measurable level of cybersecurity maturity.

With Segura®, your team can:

- Reduce risk from privileged and third-party access
- Support regulatory compliance across SAMA, PCI, ISO 27001, and more
- Streamline internal reviews and audit preparation
- Gain full traceability across sensitive access workflows

Whether you're securing hybrid infrastructure, managing remote users, or protecting DevOps environments, Segura® gives you a platform that's practical, efficient, and built to scale securely.

About Segura®

Segura® (formerly senhasegura) is a cybersecurity company focused on Privileged Access Management (PAM). Its platform helps organizations secure and manage privileged identities, credentials, and secrets across hybrid and cloud environments.

Segura supports use cases such as credential vaulting, session monitoring, privilege elevation, and secrets management for DevOps. Designed to simplify complex identity security challenges, Segura provides IT teams with visibility, control, and tools to reduce risk and support compliance.

The company operates globally through a network of partners and serves customers across key sectors including finance, healthcare, government, telecom, and critical infrastructure.

WHITEPAPER

Strengthening Cybersecurity with the SAMA Framework

Powered by MT4 Group | April 2025

segura® | Futureproof Identity Security | segura.security