

SAMA Cybersecurity Framework v1.0

SAMA Cybersecurity Framework establishes cybersecurity governance and controls for the Saudi financial sector to protect critical systems and customer data.



What it is

The Saudi Arabia SAMA Cybersecurity Framework v1.0 is a regulatory framework that helps financial institutions in Saudi Arabia establish, implement, and maintain effective cybersecurity controls to protect their information assets and ensure regulatory compliance. The framework aims to enhance the overall cyber resilience of the financial sector and reduce risks associated with cyber threats.

Published by the Saudi Arabian Monetary Authority (SAMA), the framework is mandatory for banks, insurance companies, and other financial institutions regulated by SAMA. It covers critical focus areas such as cybersecurity governance, risk management, operational resilience, incident management, and compliance oversight, aligning national requirements with global security best practices.

At a glance

PUBLISHER Saudi Arabian Monetary Authority (SAMA)	TYPE Control Framework	VERSION v1.0
EFFECTIVE May 2017	DOMAIN Cybersecurity	FAMILY Other
REGION Saudi Arabia	INDUSTRY Financial Services	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: <https://rulebook.sama.gov.sa/en/cyber-security-framework-2>

Why it matters

- **Strengthen cybersecurity governance** Promote clear leadership accountability and structured management of cybersecurity risks throughout the entire organization.
- **Enhance regulatory alignment** Support institutions in meeting SAMA and national requirements, minimizing compliance gaps and legal exposure.
- **Promote operational resilience** Help organizations withstand and recover from cyber incidents, ensuring continuity of financial services and operations.
- **Improve risk-based decision making** Enable proactive identification, assessment, and mitigation of threats by integrating risk management into business processes.

How SmartSuite supports SAMA CSF v1.0

Financial Control Framework Library

Structure SAMA control domains with ownership, scope, and implementation status across systems.

Risk Assessment and Regulatory Mapping

Link cybersecurity risks to SAMA controls and financial regulatory requirements.

Policy and Governance Management

Centralize security policies, standards, and approvals aligned to SAMA expectations.

Authentication, Access, and Operations Management

Manage authentication, privileged access, monitoring, and operational controls across environments.

Incident Response and Threat Management

Track incidents, investigations, and response workflows aligned to financial sector requirements.

SAMA Audit Readiness Reporting

Provide dashboards showing control coverage, risk posture, and readiness for SAMA audits.

Common framework mappings

CIS Controls v8.1

COBIT 2019

ISO 27001:2022

ISO 27002:2022

NIST CSF 2.0

NIST 800-53 Rev.5

PCI DSS 4.0.1

SOC 2

Official resources

SAMA Cybersecurity Framework v1.0

Provides detailed requirements and guidelines for cybersecurity in the financial sector in Saudi Arabia.

sama.gov.sa/ar-sa/Laws/Documents/SAMA_Cyber_Security_Framework_v1.0.pdf

SAMA Cybersecurity Implementation Guide

Outlines the implementation process for organizations adhering to the SAMA Cybersecurity Framework.

sama.gov.sa/ar-sa/Pages/FrameworkImplementationGuide.asp

SAMA Cybersecurity Control Catalogue

Defines specific technical controls required for compliance with the SAMA Cybersecurity Framework.

sama.gov.sa/ar-sa/Laws/Documents/SAMA_Cyber_Security_Control_Catalogue.pdf

Frequently asked questions

What is the SAMA Cybersecurity Framework v1.0 used for?

The SAMA Cybersecurity Framework v1.0 is designed to help financial institutions in Saudi Arabia establish and maintain effective cybersecurity controls. It aims to protect critical banking and financial sector assets from cyber threats and ensure regulatory compliance with the Saudi Arabian Monetary Authority’s requirements.

Is compliance with the SAMA Cybersecurity Framework mandatory?

Yes, compliance is mandatory for all SAMA-regulated entities, including banks, insurance companies, and finance companies operating in Saudi Arabia. Organizations are required to implement the framework’s controls and report on their compliance status to SAMA periodically.

Who does the SAMA Cybersecurity Framework apply to?

The framework applies to all banking, insurance, and finance entities regulated by SAMA, regardless of size or ownership structure. Vendors and third parties providing services to these entities may also be subject to relevant controls as part of the broader security program.

What are the key requirements of the SAMA Cybersecurity Framework?

Key requirements include establishing a cybersecurity governance structure, performing regular risk assessments, implementing technical and organizational cybersecurity controls, reporting incidents, and developing a continuous monitoring and improvement program. Documentation such as policies, procedures, and control evidences are required as part of compliance.

How should organizations approach implementing the SAMA Cybersecurity Framework?

Implementation should begin with a gap assessment against the framework's controls, followed by prioritizing remediation based on identified risks. Organizations should tailor control implementation to their risk profile but must address all mandatory requirements, ensuring that responsibilities are clearly assigned and tracked.

How does the SAMA Cybersecurity Framework relate to other standards like ISO 27001 or NCA ECC?

While the SAMA Cybersecurity Framework shares similarities with international standards such as ISO 27001 and the National Cybersecurity Authority Essential Cybersecurity Controls (NCA ECC), it is specifically tailored to the Saudi financial sector. Organizations may leverage previous work on these standards but must address all unique SAMA requirements.

What are the ongoing compliance obligations under the SAMA Cybersecurity Framework?

Entities are expected to maintain compliance through annual self-assessments, formal attestation by executive management, and prompt reporting of any significant cybersecurity incidents. Continuous monitoring, regular updates to controls, and ongoing awareness training are required to maintain the security and compliance posture.

How would SmartSuite support Saudi Arabia SAMA Cybersecurity Framework v1.0?

SmartSuite can help organizations manage SAMA Cybersecurity Framework compliance by enabling centralized risk tracking, facilitating control documentation and assignment, and streamlining evidence collection. The platform supports audit readiness through automated workflows, status dashboards, and comprehensive reporting, making it easier to demonstrate compliance to regulators.

License included / downloadable: Yes Saudi Arabian Monetary Authority (SAMA) publishes the SAMA Cybersecurity Framework v1.0 and it's publicly available for download from SAMA's official website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/saudi-arabia-sama-cybersecurity-framework-v1-0