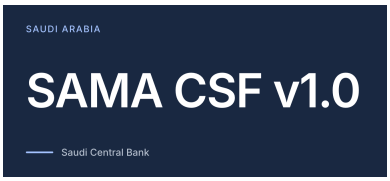
SmartSuite

Framework / Cybersecurity / Other

SAMA Cyber Security Framework (Circular No. 381000091275, May 2017)

The SAMA Cyber Security Framework (May 2017) is the mandatory cybersecurity framework for banks, insurers, financing companies and credit bureaus regulated by the Saudi Central Bank.



What it is

The SAMA Cyber Security Framework is the mandatory cybersecurity framework for financial institutions regulated by the Saudi Central Bank (SAMA, formerly the Saudi Arabian Monetary Authority): all banks, insurance and reinsurance companies, financing companies and credit bureaus operating in Saudi Arabia, and the financial market infrastructure (section 1.4). SAMA issued it under Circular No. 381000091275 dated 28/8/1438H, corresponding to May 24, 2017; the SAMA Rulebook lists it as in force, with a scope of application covering the banking sector, finance sector, payment systems and payment services providers, credit bureaus and the regulatory sandbox. Section 1.5 states that the framework is mandated by SAMA and that member organizations are responsible for adopting and implementing it.

At a glance

PUBLISHER
Saudi Central Bank (SAMA), formerly the Saudi Arabian Monetary Authority

TYPE
Control Framework

VERSION
Version 1.0 (May 2017)

EFFECTIVE
May 24, 2017

DOMAIN
Cybersecurity

FAMILY
Other

REGION
Saudi Arabia

INDUSTRY
Financial Services

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

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

Why it matters

- **A common approach across the sector** Section 1.1 states the framework's three objectives: a common approach to cyber security within member organizations, an appropriate maturity level of controls, and cyber security risks that are properly managed throughout each organization.
- **Maturity that can be measured** The six-level model in section 2.4 defines each level with criteria, from level 0 (non-existent) to level 5 (adaptive); levels 3, 4 and 5 require all criteria of the preceding levels, and SAMA expects level 3 or higher.
- **Board-level governance** A board-mandated cyber security committee headed by an independent senior manager from a control function, a charter with at least quarterly meetings and sufficient budget are control considerations under subdomain 3.1.1.
- **Regulator expectations written into the controls** The controls state when SAMA must be informed or asked: medium or high classified incidents immediately (3.3.15), approval before launching a new electronic banking service (3.3.13), material outsourcing (3.4.2), and cloud services and data outside Saudi Arabia (3.4.3).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports SAMA CSF v1.0

Subdomain and Control Consideration Library

Load the 32 subdomains with their principle, objective and numbered control considerations (section 2.1), each with an owner, the applicable exceptions from section 1.4 and current status.

Maturity Self-Assessment

Score each subdomain on the 0 to 5 model, record the evidence for the level claimed and the gap to level 3 (section 2.4), and keep the questionnaire responses SAMA reviews and audits (section 2.3).

Cyber Security Risk Register

Hold identified risks in a central register (3.2.1.1), their likelihood and impact analysis (3.2.1.2), the treatment chosen and the risk owner's sign-off (3.2.1.3), and the treatment plan progress (3.2.1.4).

Waiver and Update Requests

Record each waiver request with the reason the control cannot be met, the compensating controls, CISO and committee approvals and SAMA's response (Appendix D and E), noting that the framework still applies while a request is pending.

Incident Register and SAMA Reporting

Classify incidents, log the immediate notice to SAMA IT Risk Supervision for medium or high incidents, and assemble the formal post-incident report fields a to k that subdomain 3.3.15 lists.

Third-Party, Outsourcing and Cloud Records

Track contract cyber security requirements and review rights (3.4.1), SAMA approvals for material outsourcing (3.4.2), and cloud approvals, data location and exit terms (3.4.3) per provider.

Common framework mappings

CIS Controls v8.1 · COBIT 2019 · CSA CCM v4 · 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

The SAMA Cybersecurity Framework on the SAMA Rulebook.

rulebook.sama.gov.sa/en/cyber-security-framework-2

SAMA Cybersecurity Implementation Guide

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

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

Frequently asked questions

Who must comply with the SAMA Cyber Security Framework?

Section 1.4 applies it to all banks, insurance and reinsurance companies, financing companies and credit bureaus operating in Saudi Arabia and to the financial market infrastructure; the Rulebook entry lists the banking sector, finance sector, payment systems and payment services providers, credit bureaus and the regulatory sandbox as its scope of application. Section 1.5 states that SAMA mandates the framework and that member organizations are responsible for adopting and implementing it. Non-bank institutions are exempt from subdomains 3.2.3, 3.3.12 and 3.3.13, with multi-factor authentication still required for online customer services.

How is the SAMA Cyber Security Framework structured?

Section 2.1 organizes it into four domains: 3.1 Cyber Security Leadership and Governance, 3.2 Cyber Security Risk Management and Compliance, 3.3 Cyber Security Operations and Technology and 3.4 Third Party Cyber Security. These contain 32 numbered subdomains, each with a principle, an objective and uniquely numbered control considerations that can nest up to four levels. The framework is principle-based (section 2.2), so the principles and objectives are what must be achieved and the control considerations give direction.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What maturity level does SAMA expect?

Section 2.4 defines six maturity levels: 0 non-existent, 1 ad-hoc, 2 repeatable but informal, 3 structured and formalized, 4 managed and measurable and 5 adaptive. Member organizations should operate at level 3 or higher, which means controls are defined, approved and implemented, documented in board-endorsed policies, standards and procedures, monitored for compliance and measured with key performance indicators (section 2.4.1). Level 4 adds key risk indicators and level 5 continuous improvement and peer comparison (sections 2.4.2 and 2.4.3).

What must a member organization report to SAMA after a cyber security incident?

Subdomain 3.3.15 requires the member organization to inform SAMA IT Risk Supervision immediately when a medium or high classified incident has occurred, to obtain SAMA's no objection before any media interaction about it, and to submit a formal incident report after resuming operations. The report covers the title and classification, the dates and times the incident occurred and was detected, the information assets involved, technical details, root-cause analysis, corrective activities performed and planned, a description of the impact, the estimated total cost and the estimated cost of corrective actions.

Can a member organization deviate from a control consideration?

Yes, through the route section 2.2 describes. When a control consideration cannot be tailored or implemented, the member organization should consider compensating controls, pursue an internal risk acceptance and request a formal waiver from SAMA. Appendix D sets the process: a detailed description of why the control cannot be met and of the compensating controls, approval by the CISO and the cyber security committee, a request signed by the CISO and the business owner and sent through the CEO to the deputy governor of Supervision. The framework continues to apply until the waiver is granted.

License included / downloadable: Yes SAMA publishes the Cyber Security Framework on the SAMA Rulebook, where the full text and the original PDF are available to the public.

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