

GOVERNANCE DOCS

SAMA Cyber Security Framework

Gap Assessment Report

Saudi Central Bank (SAMA) Cyber Security Framework

Al Noor Finance Company (sample)

Cyber security for the finance company's core systems, digital channels and head office in Riyadh.

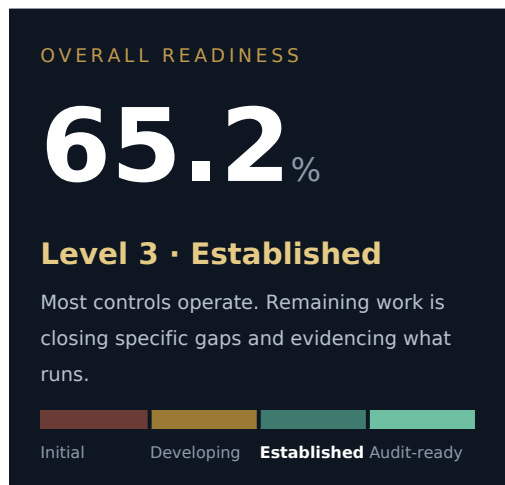
ASSESSED	25 September 2026
EDITION	Version 1.0, May 2017, as amended
IN SCOPE	41 requirements, 41 applicable
PROFILE	Banking and financial services · 50 to 249 people · Saudi Central Bank (SAMA)
PREPARED BY	Governance Docs

CONTENTS

- 1 Executive summary
- 2 Readiness by area and where the next points come from
- 3 Remediation plan
- A About this report

Confidential. Prepared for Al Noor Finance Company (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Al Noor Finance Company (sample) stands against SAMA CSF



APPLICABLE	EVIDENCED	OPEN GAPS	HIGH PRIORITY
41	14	27	9

STATUS OF EVERY REQUIREMENT



GAPS WITH AN OWNER	WITH A TARGET DATE	NOT ANSWERED
11 of 27	4 of 27	0

WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 65.2% against SAMA CSF across 41 applicable controls. 14 of them are implemented and evidenced.
- Most open gaps: 3.3 - Operations and Technology, with 13 at 63%. Strongest area: 3.4 - Third Party Cyber Security at 100%.
- 8 controls are operating but not evidenced. Collecting their records alone lifts the score to 70.1% (+4.9 points), the cheapest gain available.
- 9 gaps are high priority (not started or only planned); 3 of them are in 3.3 - Operations and Technology.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	Put an owner and date against the 3 high-priority gaps in 3.3 - Operations and Technology	Operations Manager	
2	LOW	Evidence the 8 controls that already operate (+4.9 points)	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

The organization achieved an established score of 65.2%, and you must now formalize unstarted high-priority governance and reporting controls.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

The organization achieved an established score of 65.2% against the SAMA Cyber Security Framework, but 27 open gaps remain unresolved. Our primary exposure stems from 9 high-priority gaps across operations and reporting, while only 11 gaps have an assigned owner. To meet Saudi Central Bank expectations, management requires board support to mandate control ownership, set delivery deadlines, and allocate resources to execute the cybersecurity improvement plan.

WHERE YOU STAND

You achieved an overall score of 65.2% on your self-assessment against the SAMA Cyber Security Framework, placing you at readiness level 3 of 4, named Established. Out of 41 applicable requirements, 14 are implemented and evidenced. However, 27 open gaps remain across the organization. These include 2 not started items, 7 planned items, 10 partially implemented items, and 8 items that are implemented but lack evidence. The lowest-scoring areas are Assessment and reporting at 37.5% and Scope and maturity at 45%.

WHAT IT MEANS FOR THE ORGANIZATION

Operating at an established level shows that core safeguards exist, but operational exposure persists. Specifically, 13 open gaps sit in Operations and Technology, while 9 high-priority gaps remain unresolved. These gaps matter to the general expectations of the Saudi Central Bank (SAMA). Furthermore, only 11 gaps have an assigned owner and only 4 have target completion dates. Without formal ownership and documented evidence, the organization cannot demonstrate control operating effectiveness or ensure operational resilience.

WHERE TO FOCUS FIRST

Immediate effort should focus on the 2 unstarted high-priority requirements and the 8 unevidenced controls. Evidencing what already runs raises your score to 70.1% without changing existing practices. Next, assign owners and target dates across all unassigned gaps. Technical teams must prioritize Cyber security architecture, Electronic banking services, and Cyber security event management. Addressing these planned engineering and monitoring requirements establishes a solid baseline and supports your broader improvement plan.

1 · EXECUTIVE SUMMARY

PRIORITIES

PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1 Establish improvement planning and member organization status SC.1 Member organization status · RP.4 Improvement plan	Leaving these high-priority governance requirements unstarted delays structured remediation and conflicts with general Saudi Central Bank expectations.	Assign an executive owner to initiate the formal improvement plan.	Comprehensive SAMA Compliance Toolkit - 38 Documentation Templates	30 DAYS
2 Complete self-assessment reporting and compile operational evidence RP.1 Self-assessment completed · RP.2 Evidence for claimed levels	Unsubstantiated control claims leave operational verification incomplete and expose the organization during regulatory reviews.	Gather operational evidence for the 8 implemented but unevidenced controls.	Comprehensive SAMA Compliance Toolkit - 38 Documentation Templates	30 DAYS
3 Implement critical technical operations and event management controls 3.3.4 Cyber security architecture · 3.3.13 Electronic banking services · 3.3.14 Cyber security event management	Gaps in electronic banking and event management leave banking services vulnerable to undetected security incidents.	Draft technical baseline specifications for electronic banking services and event monitoring.	Comprehensive SAMA Compliance Toolkit - 38 Documentation Templates	60 DAYS
4 Define entity scope and formalize regulatory compliance tracking SC.5 Scope of systems and entities · 3.2.2 Regulatory compliance	Uncertainty around system boundaries and regulatory compliance tracking limits visibility over key technical assets.	Document system boundaries and map applicable regulatory requirements.	Comprehensive SAMA Compliance Toolkit - 38 Documentation Templates	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS • Draft the formal improvement plan and define member organization status. • Gather verification evidence for the 8 implemented but unevidenced controls. • Assign accountable owners and target dates across all 27 open gaps.	DAYS 31 TO 60 • Define security architecture baselines for electronic banking services. • Deploy operational procedures for cyber security event management. • Complete implementation of the 10 partially implemented controls.	DAYS 61 TO 90 • Document the complete scope of systems and entities across operations. • Establish an ongoing tracking register for regulatory compliance requirements. • Review assessment evidence files to confirm closure of prioritized gaps.
--	---	---

Maturity across the standard

Each bar shows how the requirements in one area break down by status, weakest on the left. The score is the average across applicable requirements; the chips count open gaps by priority.

AREAS	STATUS MIX	SCORE	GAPS H · M · L
Scope and maturity	1 1 2 1	45%	2 2 0
3.1 - Leadership and Governance	1 2 4	86%	0 1 2
3.2 - Risk Management and Compliance	1 1 2 1	65%	1 1 2
3.3 - Operations and Technology	3 6 4 4	63%	3 6 4
3.4 - Third Party Cyber Security	3	100%	0 0 0
Assessment and reporting	1 2 1	38%	3 0 0

Not started
Planned
Partially implemented
Implemented, not evidenced
Implemented and evidenced

WHERE THE NEXT POINTS COME FROM

The score after each kind of work, cheapest first. Gold is what that step adds.

Today

65.2%

Evidence what already runs 8 requirements

70.1%
+4.9

Finish what is partly in place 10 requirements

82.3%
+12.2

Implement what is planned 7 requirements

95.1%
+12.8

Start what has not begun 2 requirements

100.0%
+4.9

DOCUMENTS THAT CLOSE THE MOST GAPS

Each bar counts the open gaps that name the document as the way to close them.

All of these are in the SAMA Compliance Toolkit (38 documents).

Every open gap, grouped by what has to happen next

Work from the top. Requirements not yet started or only planned are the ones a certification auditor reaches first; the last group already operates and needs only its records.

HIGH Not started · 2

Start from a documented baseline: adopt and tailor the document named below, then put it into operation.

Ref	Requirement	Area	Owner · target	Closes it
SC.1	Member organization status	Scope and maturity	HR Manager	
RP.4	Improvement plan	Assessment and reporting	Compliance Lead	

HIGH Planned · 7

Move from plan to implementation. Assign an owner and a date, then put the control into operation.

Ref	Requirement	Area	Owner · target	Closes it
SC.5	Scope of systems and entities	Scope and maturity	HR Manager 12 Nov 2026	
3.2.2	Regulatory compliance	3.2	To assign	
3.3.4	Cyber security architecture	3.3	To assign	
3.3.13	Electronic banking services	3.3	IT Manager	
3.3.14	Cyber security event management	3.3	Operations Manager	
RP.1	Self-assessment completed	Assessment and reporting	To assign	
RP.2	Evidence for claimed levels	Assessment and reporting	To assign	

MEDIUM Partially implemented · 10

Extend the existing approach to the whole scope and apply it consistently, then evidence it.

Ref	Requirement	Area	Owner · target	Closes it
SC.2	Conditionally applicable sub-domains	Scope and maturity	To assign	
SC.4	Understanding the maturity scale	Scope and maturity	IT Manager	
3.1.6	Cyber security awareness	3.1	To assign	
3.2.3	Compliance with industry standards	3.2	To assign	
3.3.1	Human resources	3.3	HR Manager	
3.3.3	Asset management	3.3	HR Manager 12 Nov 2026	
3.3.8	Infrastructure security	3.3	Risk Manager	

3.3.9	Cryptography	3.3	Operations Manager 12 Nov 2026
3.3.10	Bring your own device	3.3	To assign
3.3.17	Vulnerability management	3.3	Operations Manager 24 Dec 2026

LOW Implemented, not evidenced · 8

Collect and file evidence an auditor can sample. The control is operating; what is missing is the record of it.

Ref	Requirement	Area	Owner · target	Closes it
3.1.2	Cyber security strategy	3.1	To assign	
3.1.5	Cyber security in project management	3.1	To assign	
3.2.1	Cyber security risk management	3.2	To assign	
3.2.5	Cyber security audits	3.2	To assign	
3.3.2	Physical security	3.3	To assign	
3.3.5	Identity and access management	3.3	To assign	
3.3.12	Payment systems	3.3	To assign	
3.3.16	Threat management	3.3	To assign	

How it was scored

STATUS WEIGHTS

Status	Weight	Meaning
■ Not started	0.00	No policy, process or activity exists for this requirement.
■ Planned	0.25	Approach agreed and scheduled, but nothing is in place yet.
■ Partially implemented	0.50	In place for part of the scope, or inconsistently applied.
■ Implemented, not evidenced	0.75	Operating as intended, but you could not prove it to an auditor today.
■ Implemented and evidenced	1.00	Operating as intended, with records an auditor can sample.
■ Not applicable	—	A justified exclusion. Removed from the score - record why in your notes.

READINESS LEVELS

1 • Initial (0%+)

Most requirements are not yet in place. Build the foundations before thinking about an audit.

2 • Developing (40%+)

The programme is under way, with material gaps an auditor would find.

3 • Established (65%+)

Most controls operate. Remaining work is closing specific gaps and evidencing what runs.

4 • Audit-ready (85%+)

Controls operate and are evidenced. Ready for an internal audit and a certification body.

WHAT THIS REPORT IS

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The scores, readiness levels, gaps, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

A control that is running but cannot be evidenced scores 0.75, not 1.00. Auditors sample records, not intentions. Closing that distance is usually the fastest route to a higher score.

All assessment questions and guidance are original wording by Governance Docs. Clause and control references are used as identifiers; no text from the standard is reproduced. You need your own licensed copy of the standard to implement it.

YOUR WORKBOOK

The Excel workbook that comes with this report follows the same sections and colours. Dashboard: sections 1 and 2, recalculated live. Assessment: every requirement; change a status and every score, chart and level updates. Remediation Plan: section 3, with owners, dates and progress since this report. How it was scored: this page.

Governance Docs · governancedocs.com