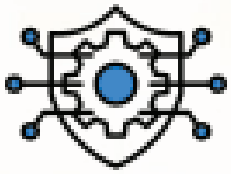
Insights

Third-Party Assurance Is Now Mandatory:

What SAMA's 2026 Cyber Security Framework Means for Saudi Banks



Regulatory & Cyber Risk Advisory

Third-Party Assurance Is Now Mandatory:

What SAMA's 2026 Cyber Security Framework Means for Saudi Banks

Saudi banks and financial institutions are becoming increasingly reliant on cloud providers, payment processors, technology vendors, and outsourced service providers. Reflecting this trend, Saudi Arabia's cybersecurity market is projected to grow from USD 4.55 billion in 2025 to USD 4.98 billion in 2026.

However, this growing dependence also increases exposure to cyber and operational risks. The proportion of global data breaches involving third parties has climbed from 15% to 48% over the past two years, while the average cost of a vendor-related breach has reached USD 4.91 million, with an average containment period of 267 days.

In response, the 2026 SAMA Cyber Security Framework (CSF) requires institutions to strengthen third-party assurance programs and adopt continuous, evidence-based vendor oversight.

At a Glance

Third-party assurance is now a required part of the 2026 SAMA CSF supervisory cycle, not an optional add-on.

SAMA expects institutions to reach at least Maturity Level 3 ("Defined") across all cybersecurity domains, including third-party governance.

Banks must show independent evidence that critical vendors maintain proper cybersecurity controls; self-reported questionnaires cannot carry that burden alone

Board-level reporting on cyber risk, including third-party risk, is moving from an annual to a semi-annual cadence for Tier-1 institutions

Source: SAMA Cyber Security Framework, 2026 audit cycle guidance; SAMA Rulebook.

Why Vendor Questionnaires Are No Longer Enough

Many institutions still manage third-party risk mainly through annual questionnaires, compliance declarations, and standard security clauses in contracts. These tools remain useful, but they only confirm that information was collected. They say little about whether a vendor's controls actually work day to day.

As outsourcing arrangements grow more complex, banks need to know more than whether a vendor has a written security policy. They need to know if that policy is enforced, monitored continuously, and checked by an independent party. In short, the regulatory focus is moving from vendor compliance to vendor assurance.

How the Bar Has Moved

Area	Before 2026	2026 SAMA CSF Expectation
Main Evidence	Vendor questionnaires and self-declarations	Independent assurance reports and external testing
Review Cycle	Annual, often a one-time exercise	Continuous monitoring across the vendor lifecycle
Board Reporting	Annual updates in most cases	Semi-annual reporting expected for Tier-1 institutions
Risk Ownership	Handled mainly by procurement teams	Embedded in Enterprise Risk Management and Board oversight

Table: How SAMA's third-party expectations have shifted heading into the 2026 audit cycle.

Source: SAMA Cyber Security Framework, 2026 audit cycle guidance; SAMA CSF 2026 compliance analysis, InfoSec4TC, June 2026.

Four Priorities for Executives

Boards and senior management can respond to this shift in four practical steps.

01 Identify the Vendors That Matter Most

Not every supplier carries the same level of risk. Institutions should rank vendors by the criticality of the service, the sensitivity of the data they touch, and the impact if that service were to fail.

02 Look Past the Questionnaire

Self-assessments should no longer sit at the center of a bank's assurance program. Institutions should pair questionnaires with independent assurance reports, external testing, certifications, and ongoing monitoring to build a fuller, more objective picture of vendor security

03 Fold Third-Party Risk into Enterprise Risk Management

Vendor risk should not sit apart as a procurement task. It belongs inside Enterprise Risk Management, cybersecurity governance, business continuity planning, and Board reporting, so leadership sees one connected picture of organizational risk.

04 Keep Watching After the Contract Is Signed

Assurance is not a one-time check. Institutions should reassess critical vendors on a regular basis, track changes in their risk profile, review independent reports as they are issued, and confirm that any weaknesses get fixed.

The Insights Perspective

Many risk teams still ask a narrow question:

"Have our vendors completed the security questionnaire?"

A more useful question for the Boardroom is this:

"Can we show, with independent evidence, that our critical vendors are resilient today?"

The difference matters. Compliance shows that information was gathered. Assurance shows that risk is actively understood, tracked, and managed.

The Numbers Behind the Shift

The push toward independent assurance is not happening in isolation. It sits inside a wider trend: outside partners are now the fastest-growing source of cyber risk, and Saudi Arabia is investing accordingly to meet it.

Data Point	Figure	Source
Saudi cybersecurity market value, 2025	**USD 4.55 billion***	MarketsandMarkets, Feb 2026
Saudi cybersecurity market value, 2026	**USD 4.98 billion**	MarketsandMarkets, Feb 2026
Saudi cybersecurity market value, 2027 (forecast)	**USD 5.45 billion***	MarketsandMarkets, Feb 2026

Data Point	Figure	Source
Market CAGR, 2026-2031 (reaching USD 7.81B by 2031)	9.4%	MarketsandMarkets, Feb 2026
Breaches involving a third party, 2024 DBIR	15%	Verizon Data Breach Investigations Report, 2024 edition
Breaches involving a third party, 2025 DBIR	30%	Verizon Data Breach Investigations Report, 2025 edition
Breaches involving a third party, 2026 DBIR (current)	48%	Verizon Data Breach Investigations Report, 2026 edition
Breaches involving a third party, 2026 DBIR (current)	60%	Verizon Data Breach Investigations Report, 2026 edition
Average cost of a supply-chain/third-party breach	USD 4.91 million	IBM Cost of a Data Breach Report, 2025
Average time to identify and contain such a breach	267 days	IBM Cost of a Data Breach Report, 2025

*Table: Verified market and breach figures relevant to third-party cyber risk in Saudi Arabia and globally, 2025-2027. *2025 and 2027 market values are calculated from the source's own stated 9.4% CAGR; all other figures are reported directly.*

Source: MarketsandMarkets (Feb 2026); Verizon Data Breach Investigations Report, 2024-2026 editions; IBM Cost of a Data Breach Report, 2025.

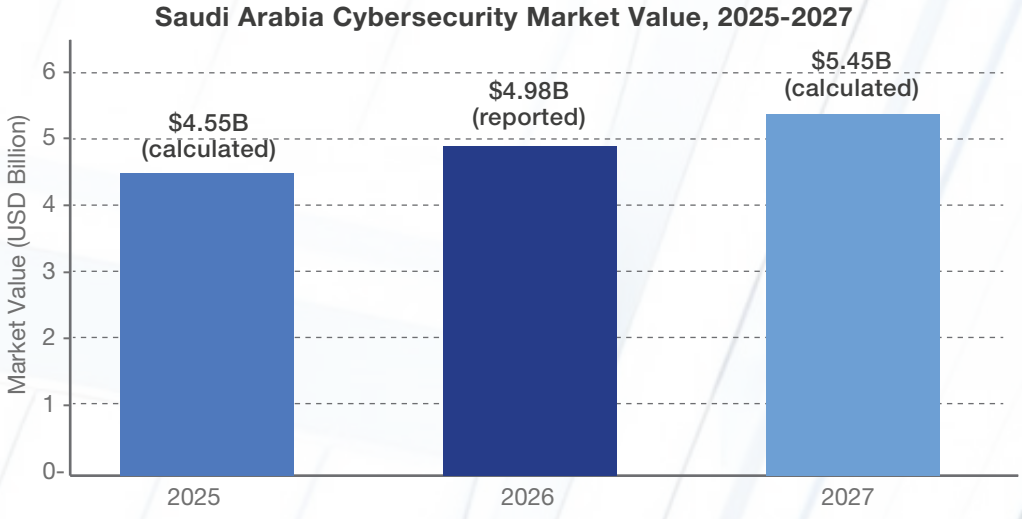


Chart 1: Saudi Arabia's cybersecurity market is set to grow from roughly USD 4.55 billion in 2025 to USD 5.45 billion by 2027, on a reported 2026 base of USD 4.98 billion.

Source: MarketsandMarkets, Kingdom of Saudi Arabia Cybersecurity Market Report, February 2026

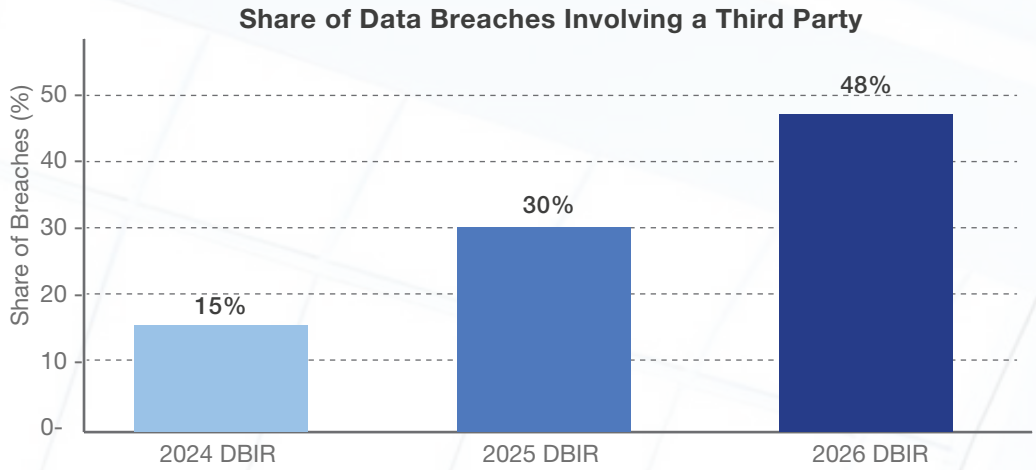


Chart 1: Third-party involvement in global data breaches has grown from 15% to 48% over three consecutive DBIR editions
Source: Verizon Data Breach Investigations Report, 2024, 2025, and 2026 editions

These figures point in one direction. As Saudi institutions spend more on cybersecurity and lean more heavily on outside vendors, the share of incidents that trace back to a third party keeps climbing. A structured, independently verified assurance program is quickly becoming the difference between catching a weak vendor early and learning about it after a breach.

How Insights Helps Organizations

At Insights Financial & Management Consulting, we help institutions strengthen third-party governance through:

- Third-Party Risk Assessments
- Vendor Assurance Reviews
- Third-Party Risk Framework Design
- SAMA CSF Maturity Assessments
- Cybersecurity Governance Reviews
- Operational Resilience Assessments
- Enterprise Risk Management Integration

Our approach helps financial institutions build practical, risk-based assurance programs that align with SAMA's evolving expectations while strengthening resilience across the vendor ecosystem.

Key Takeaway

As Saudi financial institutions lean further on external service providers, third-party risk is becoming one of the biggest drivers of operational resilience. Institutions that build structured assurance capability now will be better placed to meet regulatory expectations, strengthen governance, and keep the confidence of regulators and customers alike.

Vendor relationships can no longer rest on contracts alone. They need independent assurance behind them.

Source: SAMA Cyber Security Framework and 2026 audit cycle guidance, SAMA Rulebook.

SAMA CSF 2026 compliance analysis, InfoSec4TC, June 2026.
Verizon Data Breach Investigations Report, 2024, 2025, and 2026 editions.
IBM Cost of a Data Breach Report, 2025.
MarketsandMarkets, Kingdom of Saudi Arabia Cybersecurity Market Report, February 2026.

insights

2026

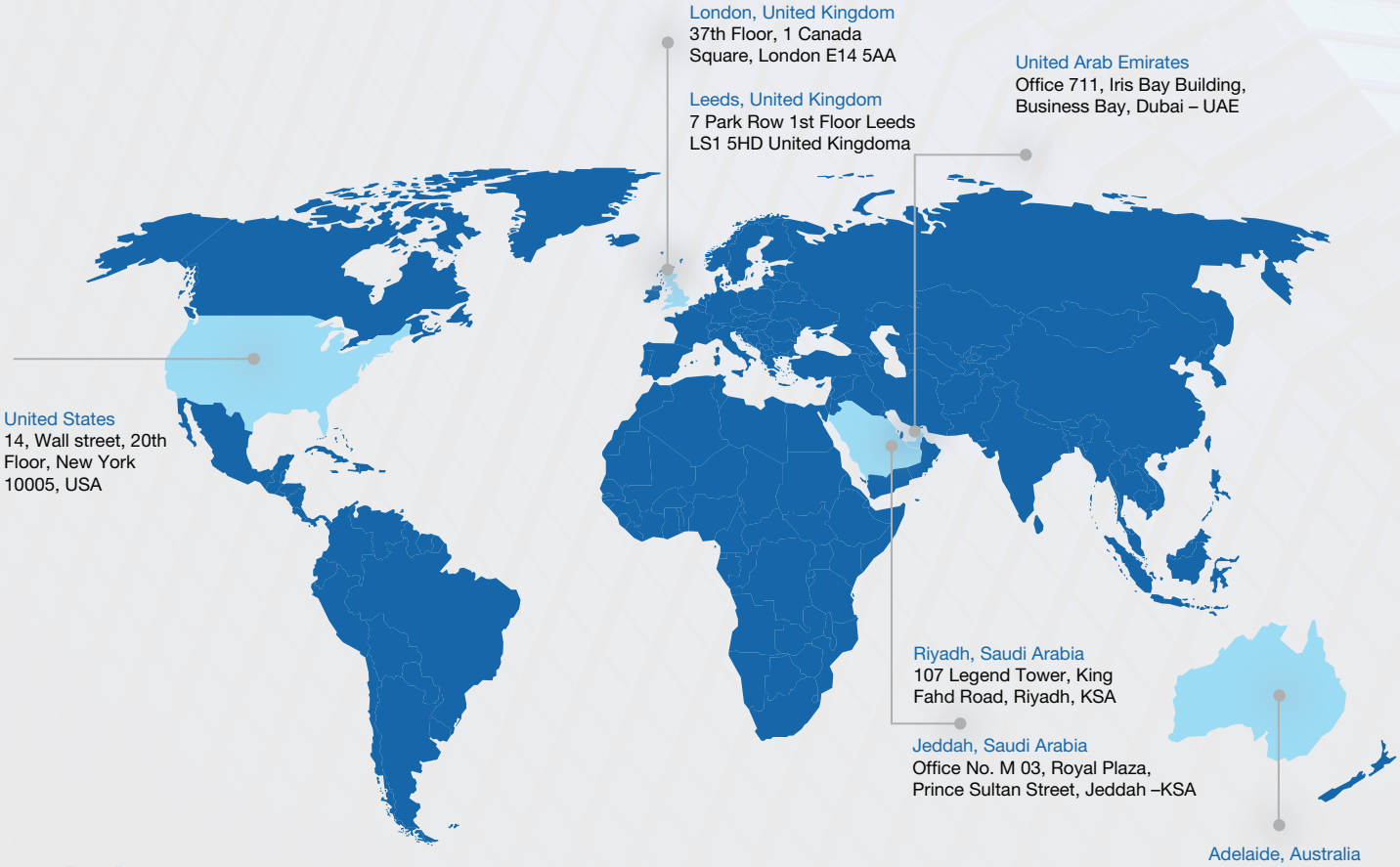
Contact Us

For further information, clarification and discussion concerning the contents, please contact our Real Estate Strategic Consultancy team:

Khawaja Soha Butt
Partner - Financial & Risk Advisory
: sbutt@insightss.co

Nick Whitford
Senior Vice President
: nwhitford@insightss.co

Ameer Abbas
Vice President - Financial & Risk Advisory
: aabbas@insightss.co



Insights

: +966 53 775 0075
: info@insightss.co
: www.insightss.co

Navigating Complexity, Simplifying Success