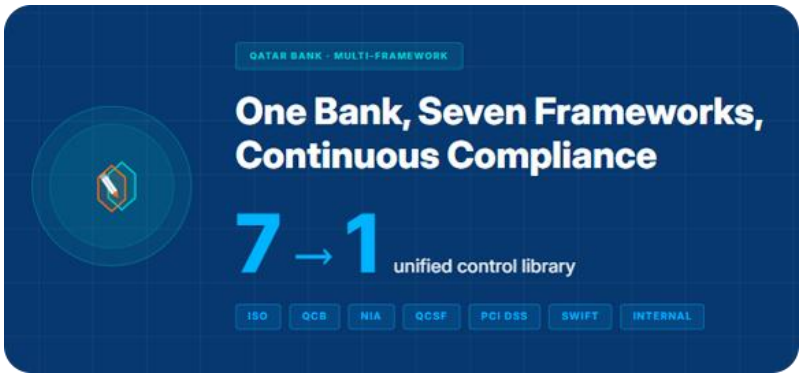
THREATSVIEW
Make it Simple

Qatar Bank Unifies Seven Regulatory Frameworks Into One Continuous Compliance Engine



Client profile

A leading commercial bank headquartered in Doha, Qatar, with retail, corporate, treasury, and digital banking operations, a card-issuing business, branches across the GCC, and correspondent banking relationships globally. Roughly 2,500 employees, 14,000+ IT assets, and a regulatory footprint that touches every major control framework relevant to a Qatar-licensed financial institution.

The challenge

The bank was simultaneously accountable to seven frameworks, each with its own control catalogue, evidence expectations, audit cadence, and regulator:

- ISO/IEC 27001:2022 — Information Security Management System certification with annual surveillance audits.
- QCB Cybersecurity Circulars — Qatar Central Bank requirements covering incident reporting, penetration testing, and third-party risk.
- NIA Policy v2.0 — Qatar National Information Assurance Policy compliance.
- QCSF — Qatar Cyber Security Framework aligned with international standards.
- PCI DSS v4.0 — Compliance for card-issuing and acquiring environments.
- SWIFT CSCF — Customer Security Controls Framework for SWIFT-connected institutions.
- Internal Group Information Security Policy — Board-mandated security controls extending regulatory requirements.

Each framework was tracked in its own Excel workbook by a different control owner. The same underlying control — say, MFA on privileged accounts — was documented separately seven times, evidenced seven times, and audited seven times. Roughly 60–70% of controls overlapped across frameworks, but no one had built a usable mapping. Continuous compliance was effectively impossible; the team operated in audit-panic mode four to five times per year.

Why ThreatsView

ThreatsView's GRC & Resilience module gave the bank the ability to load all seven framework control catalogues, build a unified internal control library, cross-walk every framework to that library, attach evidence once and reuse it across every framework that needed it, and maintain a continuous view of compliance posture across all seven obligations simultaneously.

THREATSVIEW
Make it Simple

Qatar Bank Unifies Seven Regulatory Frameworks Into One Continuous Compliance Engine

Implementation highlights

Unified internal control library

~280 unique internal controls reflecting how the bank actually operates — access control, network security, cryptography, change management, third-party risk, incident response, business continuity, physical security, governance. Each control authored once with an owner, description, implementation procedure, and evidence expectation.

Evidence reuse model

Evidence artefacts — access review reports, MFA configuration screenshots, policy documents, training records, pen test reports, scanner outputs — uploaded against internal controls. Each artefact carries metadata: date, source, owner, validity period. The platform automatically surfaces it under every framework control mapped to that internal control.

Risk register integration

When a control is non-compliant or partially compliant, a risk is automatically created in the risk register with the affected frameworks listed. Risk treatment, target dates, and residual risk flow through the same platform.

Audit-ready posture

Each external auditor — ISO certification body, PCI QSA, QCB inspector, internal audit — receives a scoped read-only view filtered to their framework. The GRC team's role shifts from evidence-gathering to walking the auditor through the platform.

Framework cross-walk engine

All seven framework control catalogues loaded. Each framework control mapped to one or more internal controls. The cross-walk engine handles the inverse: any change to an internal control automatically reflects across every framework it satisfies.

Example: one internal control "Privileged access requires MFA and is reviewed quarterly" simultaneously satisfies ISO 27001 A.5.15/A.5.18/A.8.2/A.8.5, PCI DSS Req 7/8.4/8.5, QCB privileged access requirements, NIA access management controls, QCSF identify/protect functions, SWIFT CSCF principle 5, and the internal group policy access control section. Update evidence once, satisfy seven frameworks.

Continuous compliance dashboards

Per-framework live dashboards show real-time compliance percentage, controls with expired evidence, controls with no assigned owner, controls with open exceptions. A second view rolls all seven frameworks into a single heat-map.

Exception management

Where the bank can't fully meet a control — e.g., a legacy core banking module — formal exceptions are raised, risk-accepted by the appropriate authority, dated for review, and visible to auditors with full context.

Continuous monitoring hooks

Where automation is possible, the platform pulls signals directly. Vulnerability management evidence flows from Tenable.sc. Endpoint protection coverage flows from CrowdStrike. Patch compliance is calculated automatically. Controls previously evidenced once a year are now evidenced continuously.

Qatar Bank Unifies Seven Regulatory Frameworks Into One Continuous Compliance Engine

Results & impact

- Evidence collection effort reduced by approximately 65% through the cross-walk reuse model — one artefact now satisfies multiple framework controls automatically.
- ISO 27001:2022 surveillance audit passed with zero major and zero minor non-conformities in the first cycle after deployment.
- PCI DSS v4.0 attestation completed in roughly half the time of the previous year's effort.
- QCB inspection evidence pack assembled in two days versus the previous norm of three to four weeks.
- Unified control library of 280 internal controls replacing seven parallel spreadsheets — authored once, owned once, evidenced once.
- Continuous compliance posture maintained above 90% across all seven frameworks on the executive dashboard, replacing the previous pattern of dropping to 50–60% between audit cycles and panic-spiking before each audit.
- Cross-framework impact analysis time reduced from days to minutes — when a control fails or changes, the platform instantly shows every framework affected.
- Audit overlap eliminated — internal audit, ISO auditor, PCI QSA, and QCB inspector each work from the same evidence base, scoped to their lens.
- Board reporting transformed — the Group CISO now presents a single-page multi-framework compliance heat-map at every audit committee meeting, generated live from platform data.
- GRC team capacity freed up — approximately 40% of analyst time previously spent on duplicative evidence-collection redirected to actual control improvement work.

> *"We used to live in audit cycles — frantic for two months, recover for one, frantic again. Now compliance is just how we operate. The auditors come, they log in, and the evidence is already there."*
>
> **— Group Chief Information Security Officer**