

Qatar Regulatory Hub

Country-specific obligations, regulatory sources and product workflow mappings.

QAT Regulatory Hub

Region: Middle East

Board-ready governance across Qatar's financial ecosystem

Qatar's regulatory landscape combines Qatar Central Bank supervision, Qatar Financial Centre rules and national privacy requirements. Regulated firms need evidence that risk appetite, control functions, internal audit, resilience plans and breach response operate as one system.

QAT

Middle East governance, risk and compliance intelligence

QCB

Qatar Central Bank

Industries Regulated

Banking and lending, Regulated financial services

QFCRA

Qatar Financial Centre Regulatory Authority

Industries Regulated

Banking, insurance, investment firms and regulated financial services

NCSA

National Cyber Security Agency

Industries Regulated

Capital markets and listed companies, Cross-sector data controllers and processors, Government and critical infrastructure

NDPO

National Data Privacy Office

Industries Regulated

Cross-sector data controllers and processors

Supervisory Priorities

What Regulated Organisations Need to Operationalise.

The applicable perimeter depends on entity type, licence and sector. These priorities provide a practical starting point for programme design and evidence management.

01

Risk Appetite and Material-Risk Monitoring

02

Controlled Functions and Independent Assurance

03

Operational Incidents and Escalation

04

Business Continuity and Third-Party Resilience

05

Cyber-Risk and E-Banking Controls

06

Personal-Data Breach Response

Regulatory Alignment

Qatar Regulation and Product Map.

Each row translates an official regulatory source into an operational GRC focus, then identifies only the platforms with a defensible workflow or evidence role.

Research Review

Official-source and product-fit review completed 1 September 2026.

Primary Fit

The platform directly manages a central process or evidence set described in the requirement.

Supporting Fit

The platform contributes linked evidence, oversight or follow-up but is not the main system for the requirement.

Not Shown

A weak or unsubstantiated product relationship is intentionally omitted.

Qatar Regulation And Product Map

QCB Instructions to Banks 2024 QCB

Applies To: Banks and financial institutions within the QCB's applicable scope

Operational Focus: Banking-risk governance, outsourcing controls, business continuity, incident reporting, technology risk, supervisory reporting and board accountability.

Platform Fit and Workflow Support: Primary fit Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting. Primary fit Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail. Boundary Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.

Source: Source

<https://www.qcb.gov.qa/ar/pages/instructionstobanks2024.aspx>

Governance and Controlled Functions Rules 2020 QFCRA

Applies To: QFC authorised firms

Operational Focus: Corporate governance, risk management, internal controls, internal audit, controlled functions and accountable boards.

Platform Fit and Workflow Support: Primary fit Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and follow-up. Primary fit Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://www.qfcra.com/governance-and-controlled-functions/>

Risk Management Framework and Strategy Requirements QFCRA

Applies To: QFC authorised firms

Operational Focus: Documented risk appetite, material-risk assessment, monitoring, board review and independent periodic review.

Platform Fit and Workflow Support: Primary fit Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. Primary fit Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://www.qfcra.com/en-us/Publications/Documents/Town%20Hall%20meetings/Town%20Hall%20Presentation%2029%20June%202021.pdf?t=1625393100>

Business Resilience and Continuity Requirements QFCRA

Applies To: QFC authorised firms

Operational Focus: Continuity planning, periodic review, testing, accountable governance and evidence of operational readiness.

Platform Fit and Workflow Support: Primary fit Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up. Supporting fit Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership reporting. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://www.qfcra.com/en-us/Publications/Documents/Town%20Hall%20meetings/Town%20Hall%20Presentation%2029%20June%202021.pdf?t=1625393100>

Personal Data Privacy Protection Law No. 13 of 2016 NCSA and NDPO

Applies To: Controllers and processors of electronically processed personal data

Operational Focus: Privacy controls, breach management, incident documentation, regulatory communications and corrective action.

Platform Fit and Workflow Support: Primary fit Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence. Supporting fit Privacy risks, controls, assessments, treatment actions, ownership, approvals and management reporting. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://www.ncsa.gov.qa/en/pages/personal-data-privacy-personal-data-privacy-protection-law>

Data Privacy by Design and by Default Guideline NDPO

Applies To: Regulated controllers and processors

Operational Focus: Privacy risk assessment, embedded controls, accountability records, control testing and evidence across the data lifecycle.

Platform Fit and Workflow Support: Primary fit Privacy risks, controls, assessments, treatment actions, ownership, approvals and management reporting. Primary fit Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

https://ncsa.gov.qa/shared/document_library/94787172324409/33000/8854/1.0~69d3482b-0f68-44c6-a7f1-7aee7475b238?filename=Data+Privacy+by+Design+and+by+Default+-+Guideline+for+Regulated+Entities+%284%29.pdf&mimetype=application%2Fpdf

This mapping is an implementation aid, not legal advice. It describes configurable workflow and evidence support, not automatic compliance. Always validate applicability, current versions, implementation dates and supervisory expectations with qualified advisers and the relevant authority.

Product Mapping Grounded in the 2026 Solution Briefs.

The mapping uses the capabilities documented in the current brochures. It does not extend the platforms beyond their stated functional scope.

Risk and Control Intelligence

Best suited to enterprise risk ownership, risk and control registers, assessments, appetite and tolerances, KRIs, treatments, approvals, dashboards and board reporting.

Central risk and control register

KRI threshold alerts

Treatment action tracking

AI-assisted drafting and classification

Independent Assurance

Best suited to the audit universe, risk-based planning, engagement execution, RCM-linked design and effectiveness testing, evidence, findings, approvals and follow-up.

Risk-based audit planning

ToD and ToE test procedures

Working papers and evidence

GIAS 2024 observation drafting

Incident Response and Closure

Best suited to incident intake, triage, investigation, root-cause analysis, escalation, notifications, corrective and preventive actions, closure and lessons learned.

Central incident register

Investigation and root cause

Escalation and notifications

Corrective-action tracking

Scope boundary

The platforms support governance workflows, accountability, evidence and reporting. They do not calculate regulatory capital or liquidity, replace technical cybersecurity monitoring, provide legal interpretation, issue external-audit opinions or automatically file statutory notifications unless an approved integration and process are configured.

Connected Operating Model

From Obligation to Board-Ready Evidence.

Use one traceable workflow to translate requirements, manage execution and demonstrate oversight.

01

Catalogue Obligations

Structure local requirements by entity, licence, authority and accountable owner.

02

Connect Operational Evidence

Link obligations to risks, controls, incidents, tests, findings and remediation.

03

Monitor and Assure

Track KRIs, control status, audit coverage, incidents and action closure continuously.

Risk intelligence

Independent assurance

Incident response

TransVare Middle East | Qatar

Build a Connected GRC Operating Model for Qatar.

See how TransVare can support local regulatory readiness while preserving regional visibility and board oversight.