

Bahrain Regulatory Hub

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

BHR Regulatory Hub

Region: Middle East

One evidence trail across the CBB Rulebook

The Central Bank of Bahrain is the integrated regulator for banking, insurance, investment business and capital markets. Its Rulebook places strong emphasis on high-level controls, operational-risk management, cyber-risk governance, business continuity and independent audit.

BHR

Middle East governance, risk and compliance intelligence

CBB

Central Bank of Bahrain

Industries Regulated

Banking and lending

PDPA

Personal Data Protection Authority

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

High-Level Controls and Accountability

02

Operational-Risk Governance

03

Cyber Incident Response

04

Independent Control Assurance

Regulatory Alignment

Bahrain 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.

Bahrain Regulation And Product Map

High-Level Controls Module CBB

Applies To: CBB licensees by applicable Rulebook volume

Operational Focus: Board governance, risk and compliance functions, internal audit independence and control accountability.

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

Source: Source

<https://www.cbb.gov.bh/about-cbb/>

Operational Risk Management Module CBB

Applies To: Conventional and Islamic banks and other specified licensees

Operational Focus: Operational-risk identification, loss events, business continuity, monitoring, reporting and control remediation.

Platform Fit and Workflow Support: Primary fit Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership reporting. Primary fit Disruption reporting, escalation, investigation, corrective action, recovery tracking and closure evidence. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://www.cbb.gov.bh/wp-content/uploads/2019/03/Consultation-Operation-Risk-Management-Module.pdf>

Cyber Security Risk Management Requirements CBB

Applies To: Relevant CBB-regulated licensees

Operational Focus: Cyber-risk policy, responsibilities, preventive controls, event handling, resilience and evidence.

Platform Fit and Workflow Support: Primary fit Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership reporting. Primary fit Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail. Boundary GRC workflow and evidence support only. The platforms do not replace technical security monitoring, detection or protection tools.

Source: Source

https://www.cbb.gov.bh/wp-content/uploads/2019/04/Vol-3_RM-Chapter-on-Cyber-Security.pdf

Personal Data Protection Law No. 30 of 2018 PDPA

Applies To: Controllers processing personal data in Bahrain

Operational Focus: Data-security governance, breach response, accountability and documented corrective measures.

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.cbb.gov.bh/wp-content/uploads/2019/01/Vol-1_DA_Digital-Advice-CONSULTATION.pdf

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 | Bahrain

Build a Connected GRC Operating Model for Bahrain

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