POINT OF VIEW - SEPTEMBER 2026

Bahrain: From Regulatory Obligation to Board-Ready Evidence.

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.

REGION
Middle East

REGULATORY HUB
BHR


Bahrain

Country in Brief

2	**4**	**4**	**3**
Regulatory authorities profiled	Official regulatory sources mapped	Supervisory priorities operationalised	Connected TransVare platforms

01 Bahrain Regulatory Landscape

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.

CBB

Central Bank of Bahrain

Industries Regulated

Banking and lending

PDPA

Personal Data Protection Authority

Industries Regulated

Cross-sector data controllers and processors

02 Supervisory Priorities

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

03 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.

04

Report to Leadership

Turn current operational evidence into traceable executive and board oversight.

04 Bahrain Regulation and Product Map

Each official requirement below is translated into an operational GRC focus. Only platforms with a defensible workflow or evidence role are shown as a primary or supporting fit.

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.
ERMVare® **Primary Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
AuditVare® **Primary Fit**	Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and follow-up.
Scope Boundary	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
Official Source	**Open Official Source**

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.
ERMVare® **Primary Fit**	Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership reporting.
InciVare® **Primary Fit**	Disruption reporting, escalation, investigation, corrective action, recovery tracking and closure evidence.
Scope Boundary	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
Official Source	**Open Official Source**

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.
ERMVare® **Primary Fit**	Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership reporting.
InciVare® **Primary Fit**	Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail.
Scope Boundary	GRC workflow and evidence support only. The platforms do not replace technical security monitoring, detection or protection tools.
Official Source	**Open Official Source**

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.
InciVare® **Primary Fit**	Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence.
ERMVare® **Supporting Fit**	Privacy risks, controls, assessments, treatment actions, ownership, approvals and management reporting.
Scope Boundary	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
Official Source	**Open Official Source**

Research Review	Primary Fit	Supporting Fit	Not Shown
Official-source and product-fit review completed 1 September 2026.	Directly manages a central process or evidence set.	Contributes linked evidence, oversight or follow-up.	Weak or unsubstantiated relationships are omitted.

05 Brochure-Validated Product Capability

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

ERMVare®

Risk and Control Intelligence

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

AuditVare®

Independent Assurance

Audit universe, risk-based planning, engagement execution, RCM-linked control testing, evidence, findings, approvals and follow-up.

Risk-based audit planning | ToD and ToE procedures | Working papers and evidence | GIAS 2024 observation drafting

InciVare®

Incident Response and Closure

Incident intake, triage, investigation, root-cause analysis, escalation, notifications, corrective action, 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.

06 Sources, Scope and Next Step

Official sources used in this report are linked directly from each regulation summary. The mapping is an implementation aid and not legal advice.

01	**High-Level Controls Module** CBB	**Official Source**
02	**Operational Risk Management Module** CBB	**Official Source**
03	**Cyber Security Risk Management Requirements** CBB	**Official Source**
04	**Personal Data Protection Law No. 30 of 2018** PDPA	**Official Source**

THE NEXT STEP

Build a Connected GRC Operating Model for Bahrain.

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

TransVare Arabia
Building #7386, Abi Jafar Al Qurtabi Street (Exit 5)
Al-Maseef, Riyadh 12467, Saudi Arabia

For Local Alliance Partner and Sales Contact:
Connect@TransVare.com
TransVare.com