

Oman Regulatory Hub

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

OMN Regulatory Hub

Region: Middle East

Integrated governance for Oman's evolving regulatory landscape

Oman's framework combines Central Bank prudential oversight, Financial Services Authority governance expectations and national personal-data requirements. A connected GRC model helps maintain traceability from risk identification through audit assurance and incident notification.

OMN

Middle East governance, risk and compliance intelligence

CBO

Central Bank of Oman

Industries Regulated

Banking and lending, Regulated financial services

FSA

Financial Services Authority

Industries Regulated

Capital markets and listed companies, Regulated financial services

MTCIT

Ministry of Transport, Communications and Information Technology

Industries Regulated

Telecommunications and digital services

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

Prudential Risk Governance

02

Business-Continuity Readiness

03

Audit and Risk-Committee Oversight

04

72-Hour Data-Breach Workflows

Regulatory Alignment

Oman 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.

Oman Regulation And Product Map

CBO Regulatory Framework CBO

Applies To: Banks and financial institutions within the applicable CBO regime

Operational Focus: Risk management, compliance, corporate governance, prudential monitoring and supervisory reporting.

Platform Fit and Workflow Support: Primary fit Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. Supporting fit Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up. Boundary Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.

Source: Source

<https://cbo.gov.om/Pages/RegulatoryFramework.aspx>

BM 1225 Business Continuity Management Framework CBO

Applies To: Institutions within the circular's scope

Operational Focus: Continuity governance, impact assessment, plans, testing, incident response and evidence of resilience.

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://cbo.gov.om/pages/Circulars.aspx>

Code of Corporate Governance FSA

Applies To: Public listed companies and investment funds within scope

Operational Focus: Audit and risk-management committee oversight, internal controls, internal audit and governance disclosure.

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 Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.

Source: Source

<https://fsa.gov.om/documents/En/Charter2014.pdf>

Personal Data Protection Law and Executive Regulation MTCIT

Applies To: Controllers and processors within scope

Operational Focus: Breach records, risk assessment, corrective measures and notification to the Ministry and affected individuals within 72 hours where required.

Platform Fit and Workflow Support: Primary fit Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence. Primary fit Privacy risks, controls, assessments, treatment actions, ownership, approvals and management reporting. Boundary Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.

Source: Source

<https://mtcit.gov.om/sectors/governance/personal>

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 | Oman

Build a Connected GRC Operating Model for Oman

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