

Kuwait Regulatory Hub

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

KWT Regulatory Hub

Region: Middle East

Risk and resilience evidence for the Kuwaiti market

Kuwait's banking and capital-markets environment is shaped by Central Bank governance, risk and cybersecurity expectations together with Capital Markets Authority requirements. Institutions benefit from a single operating record for risk decisions, control testing, incidents and remediation.

KWT

Middle East governance, risk and compliance intelligence

CBK

Central Bank of Kuwait

Industries Regulated

Banking and lending, Payments and fintech, Regulated financial services

CMA

Capital Markets Authority

Industries Regulated

Capital markets and listed companies

CITRA

Communication and Information Technology Regulatory Authority

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

Bank Governance and Risk Frameworks

02

Cyber and Operational Resilience

03

Internal-Control Evidence

04

Incident and Remediation Tracking

Regulatory Alignment

Kuwait 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.

Kuwait Regulation And Product Map

Corporate Governance Rules for Kuwaiti Banks CBK

Applies To: Banks operating in Kuwait

Operational Focus: Board oversight, risk governance, internal controls, control functions and transparent accountability.

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 Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

https://www.cbk.gov.kw/en/images/digital-bank-establishment-app-form-169768_v20_tcm10-169768.pdf

Strategic Cybersecurity Framework for the Banking Sector CBK

Applies To: Kuwaiti banking sector

Operational Focus: Cyber governance, risk assessment, resilience, monitoring, response and sector-level assurance.

Platform Fit and Workflow Support: Primary fit Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership reporting. Supporting 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.cbk.gov.kw/en/cbk-news/announcements-and-press-releases/press-releases/get-list?seYear=&showAll=1>

Risk Management Framework for Digital Banks CBK

Applies To: Digital-bank applicants and licensed digital banks

Operational Focus: Key-risk identification, segregation of duties, continuous mitigation, business continuity and crisis management.

Platform Fit and Workflow Support: Primary fit Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership reporting. Supporting 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.cbk.gov.kw/en/images/digital-bank-establishment-app-form-169768_v20_tcm10-169768.pdf

Cyber and Operational Resilience Framework 2025 CBK

Applies To: Local banks and financial institutions within the framework's issued scope

Operational Focus: Cyber governance, technology and operational resilience, third-party dependencies, disruption response, recovery, control assurance and supervisory evidence.

Platform Fit and Workflow Support: Primary fit Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting. Supporting fit Risk-based assurance, control testing, evidence, findings, approvals and remediation follow-up. Boundary GRC workflow and evidence support only. The platforms do not replace technical security monitoring, detection or protection tools.

Source: Source

<https://www.cbk.gov.kw/en/cbk-news/announcements-and-press-releases/press-releases/get-list?seYear=2025&showAll=1>

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 | Kuwait

Build a Connected GRC Operating Model for Kuwait.

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