POINT OF VIEW - SEPTEMBER 2026

Kuwait: From Regulatory Obligation to Board-Ready Evidence.

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.

REGION
Middle East

REGULATORY HUB
KWT


Kuwait

Country in Brief

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

01 Kuwait Regulatory Landscape

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.

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

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 Bank governance and risk frameworks	02 Cyber and operational resilience
03 Internal-control evidence	04 Incident and remediation tracking

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 Kuwait 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.

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.
ERMVare® **Primary Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
AuditVare® **Supporting Fit**	Risk-based assurance, control design and effectiveness testing, evidence, findings and action 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**

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.
ERMVare® **Primary Fit**	Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership reporting.
InciVare® **Supporting 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**

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.
ERMCare® **Primary Fit**	Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership reporting.
InciCare® **Supporting 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 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.
ERMCare® **Primary Fit**	Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting.
AuditCare® **Supporting Fit**	Risk-based assurance, control testing, evidence, findings, approvals and remediation follow-up.
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**

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	**Corporate Governance Rules for Kuwaiti Banks** CBK	**Official Source**
02	**Strategic Cybersecurity Framework for the Banking Sector** CBK	**Official Source**
03	**Risk Management Framework for Digital Banks** CBK	**Official Source**
04	**Cyber and Operational Resilience Framework 2025** CBK	**Official Source**

THE NEXT STEP

Build a Connected GRC Operating Model for Kuwait.

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