POINT OF VIEW - SEPTEMBER 2026

Jordan: From Regulatory Obligation to Board-Ready Evidence.

Traceable risk and incident governance for Jordan

Jordan is strengthening financial-sector governance, cyber resilience and personal-data protection. Institutions need clear ownership, documented risk decisions, internal-control assurance and fast incident escalation across Central Bank and national requirements.

REGION
Middle East

REGULATORY HUB
JOR

Jordan

Country in Brief

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

01 Jordan Regulatory Landscape

Jordan is strengthening financial-sector governance, cyber resilience and personal-data protection. Institutions need clear ownership, documented risk decisions, internal-control assurance and fast incident escalation across Central Bank and national requirements.

CBJ

Central Bank of Jordan

Industries Regulated

Banking and lending, Regulated financial services

JSC

Jordan Securities Commission

Industries Regulated

Capital markets and listed companies

MODEE

Ministry of Digital Economy and Entrepreneurship

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 Bank governance and board accountability	02 Financial-sector cyber resilience
03 Cyber-incident coordination	04 Personal-data accountability

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 Jordan 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 Instructions for Banks No. 2 of 2023

CBJ

Applies To	Banks operating in Jordan
Operational Focus	Board and committee governance, control functions, risk oversight, independence and 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**

Cybersecurity Framework for the Financial Sector

CBJ

Applies To	Financial institutions within CBJ scope
Operational Focus	Cyber-risk governance, resilience capabilities, threat understanding, control evidence and sector response.
ERMVare® **Primary Fit**	Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership reporting.
AuditVare® **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**

Jo-FinCERT Incident Coordination

CBJ

Applies To	Financial and banking institutions
Operational Focus	Cyber-incident response, threat coordination, escalation and sector resilience.
InciVare® **Primary Fit**	Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail.
ERMVare® **Supporting Fit**	Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership reporting.
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. 24 of 2023

MODEE

Applies To	Data controllers processing personal data in Jordan
Operational Focus	Data governance, controller responsibilities, data-subject rights, complaints and documented response to breaches.
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	**Corporate Governance Instructions for Banks No. 2 of 2023** CBJ	**Official Source**
02	**Cybersecurity Framework for the Financial Sector** CBJ	**Official Source**
03	**Jo-FinCERT Incident Coordination** CBJ	**Official Source**
04	**Personal Data Protection Law No. 24 of 2023** MODEE	**Official Source**

THE NEXT STEP

Build a Connected GRC Operating Model for Jordan.

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