

# Jordan Regulatory Hub

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

JOR Regulatory Hub

Region: Middle East

## 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.

### JOR

Middle East governance, risk and compliance intelligence

### 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

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 Board Accountability**

**02**

## **Financial-Sector Cyber Resilience**

**03**

## **Cyber-Incident Coordination**

**04**

## **Personal-Data Accountability**

Regulatory Alignment

## **Jordan 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.

## **Jordan Regulation And Product Map**

### **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.

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.cbj.gov.jo/ebv4.0/root\\_storage/en/eb\\_list\\_page/financial\\_consumer\\_protection\\_report\\_2023.pdf](https://www.cbj.gov.jo/ebv4.0/root_storage/en/eb_list_page/financial_consumer_protection_report_2023.pdf)

### **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.

Platform Fit and Workflow Support: Primary fit Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership 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.cbj.gov.jo/EN/List/Instructions\\_and\\_Frameworks2NEW](https://www.cbj.gov.jo/EN/List/Instructions_and_Frameworks2NEW)

### **Jo-FinCERT Incident Coordination CBJ**

Applies To: Financial and banking institutions

Operational Focus: Cyber-incident response, threat coordination, escalation and sector resilience.

Platform Fit and Workflow Support: Primary fit Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail. Supporting fit Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership reporting. Boundary GRC workflow and evidence support only. The platforms do not replace technical security monitoring, detection or protection tools.

Source: Source

<https://www.cbj.gov.jo/EN/Pages/JoFinCert>

### **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.

Platform Fit and Workflow Support: Primary fit Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence. Supporting fit Privacy risks, controls, assessments, treatment actions, ownership, approvals and management reporting. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

[https://www.modereg.gov.jo/EN/Pages/Personal\\_Data\\_Protection\\_Unit?View=2201](https://www.modereg.gov.jo/EN/Pages/Personal_Data_Protection_Unit?View=2201)

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 | Jordan

## **Build a Connected GRC Operating Model for Jordan**

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