POINT OF VIEW - SEPTEMBER 2026

Morocco: From Regulatory Obligation to Board-Ready Evidence.

Integrated banking controls, cyber governance and personal-data assurance

Morocco's framework combines Bank Al-Maghrib supervision, AMMC capital-market governance, national cybersecurity legislation and CNDP privacy oversight. Organisations need linked risk, internal-control, audit, incident and remediation evidence.

REGION
Africa

REGULATORY HUB
MAR

Morocco

Country in Brief

4	**5**	**4**	**3**
Regulatory authorities profiled	Official regulatory sources mapped	Supervisory priorities operationalised	Connected TransVare platforms

01 Morocco Regulatory Landscape

Morocco's framework combines Bank Al-Maghrib supervision, AMMC capital-market governance, national cybersecurity legislation and CNDP privacy oversight. Organisations need linked risk, internal-control, audit, incident and remediation evidence.

BAM

Bank Al-Maghrib

Industries Regulated

Banking and lending

AMMC

Moroccan Capital Market Authority

Industries Regulated

Capital markets and listed companies

DGSSI

General Directorate of Information Systems Security

Industries Regulated

Capital markets and listed companies, Government and critical infrastructure

CNDP

National Commission for Personal Data Protection

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	Banking risk and internal controls
02	Market governance
03	Critical-system cybersecurity
04	Privacy and incident response

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 Morocco 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.

Banking Supervision Operational Framework

BAM

Applies To	Credit institutions and other supervised financial entities
Operational Focus	Risk-based supervision, board governance, internal controls, risk functions, internal audit and corrective measures.
ERMVare® **Primary Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
AuditVare® **Primary Fit**	Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and 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**

Banking Legal and Regulatory Framework

BAM

Applies To	Banks and credit institutions within the applicable framework
Operational Focus	Prudential governance, operational risk, outsourcing, control systems, reporting and supervisory assurance.
ERMVare® **Primary Fit**	Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight 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**

Capital-Market Regulations and Circulars

AMMC

Applies To	Issuers, listed companies and capital-market professionals
Operational Focus	Governance, risk controls, compliance, audit oversight, disclosure and regulator reporting.
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	Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.
Official Source	**Open Official Source**

Law No. 05-20 on Cybersecurity and Decree 2-21-406

DGSSI

Applies To	Government bodies, infrastructure of vital importance and sensitive information systems within scope
Operational Focus	Cyber governance, risk assessment, security controls, incidents, continuity, audit and third-party responsibilities.
ERMVare® **Primary Fit**	Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting.
InciVare® **Primary 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**

Law No. 09-08 on Personal Data Protection

CNDP

Applies To	Controllers processing personal data within scope
Operational Focus	Privacy governance, authorisation and notification, security controls, data-subject rights, incidents and remediation.
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	Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.
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	**Banking Supervision Operational Framework** BAM	**Official Source**
02	**Banking Legal and Regulatory Framework** BAM	**Official Source**
03	**Capital-Market Regulations and Circulars** AMMC	**Official Source**
04	**Law No. 05-20 on Cybersecurity and Decree 2-21-406** DGSSI	**Official Source**
05	**Law No. 09-08 on Personal Data Protection** CNDP	**Official Source**

THE NEXT STEP

Build a Connected GRC Operating Model for Morocco.

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

TransVare US: Delaware
8 The Green, Street R
Dover, Kent 19901, State of Delaware
United States of America

For Local Alliance Partner and Sales Contact:
Connect@TransVare.com
TransVare.com