

Morocco Regulatory Hub

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

MAR Regulatory Hub

Region: Africa

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.

MAR

Africa governance, risk and compliance intelligence

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

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

Banking Risk and Internal Controls

02

Market Governance

03

Critical-System Cybersecurity

04

Privacy and Incident Response

Regulatory Alignment

Morocco 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.

Morocco Regulation And Product Map

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.

Platform Fit and Workflow Support: Primary fit Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. Primary fit Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and follow-up. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://www.bkam.ma/en/Banking-supervision/Articles/Operational-framework-and-banking-control>

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.

Platform Fit and Workflow Support: Primary fit Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight 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.bkam.ma/en/content/view/full/15183>

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.

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 Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.

Source: Source

<https://www.ammc.ma/en>

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.

Platform Fit and Workflow Support: Primary fit Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting. Primary 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.dgssi.gov.ma/index.php/fr/decret-ndeg-2-21-406-du-4-hija-1442-15-juillet-2021-pris-pour-lapplication-de-la>

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.

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 Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.

Source: Source

<https://www.cndp.ma/>

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 Africa | Morocco

Build a Connected GRC Operating Model for Morocco.

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