

Saudi Arabia Regulatory Hub

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

KSA Regulatory Hub

Region: Middle East

Continuous GRC intelligence for Vision 2030 institutions

Saudi organisations operate across a layered regulatory environment led by the Saudi Central Bank, Capital Market Authority, National Cybersecurity Authority and Saudi Data and Artificial Intelligence Authority, alongside national data-protection requirements. The strongest operating model connects enterprise risk, independent assurance and incident evidence across these obligations.

KSA

Middle East governance, risk and compliance intelligence

SAMA

Saudi Central Bank

Industries Regulated

Banking and lending, Public and private organisations, Regulated financial services

CMA

Capital Market Authority

Industries Regulated

Capital markets and listed companies

NCA

National Cybersecurity Authority

Industries Regulated

Capital markets and listed companies, Government and critical infrastructure, Public and private organisations

SDAIA

Saudi Data and Artificial Intelligence Authority

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

Risk Appetite, Tolerances and Board Reporting

02

Risk and Control Assessment with KRI

03

Independent Risk-Based Internal Audit

04

Cyber Incident and Regulatory Escalation

05

Business Continuity and Third-Party Resilience

06

Personal-Data Accountability

Regulatory Alignment

Saudi Arabia 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.

Saudi Arabia Regulation And Product Map

Cyber Security Framework SAMA

Applies To: SAMA-regulated member organisations

Operational Focus: Cyber-risk governance, control maturity, KRIs, continuous monitoring and integration with enterprise risk management.

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 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://rulebook.sama.gov.sa/en/cyber-security-framework-2>

Business Continuity Management Framework SAMA

Applies To: Financial institutions supervised by SAMA

Operational Focus: Threat assessment, business-impact analysis, resilience, response, testing and independent assurance.

Platform Fit and Workflow Support: Primary fit Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up. Primary fit Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership reporting. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://rulebook.sama.gov.sa/en/business-continuity-management-framework-1>

Principles of Internal Auditing for Local Banks SAMA

Applies To: Local banks operating in Saudi Arabia

Operational Focus: Independent audit governance, risk-based planning, execution, reporting and issue follow-up.

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

Source: Source

<https://rulebook.sama.gov.sa/en/principles-internal-auditing-local-banks-operating-saudi-arabia>

Operational Risk Management SAMA

Applies To: Banks operating within SAMA's applicable scope

Operational Focus: Board-approved operational-risk programmes, risk and control matrices, internal controls, loss-event evidence and internal-audit review.

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://rulebook.sama.gov.sa/en/operational-risk-management>

Corporate Governance Regulations CMA

Applies To: Companies listed on the Saudi capital market

Operational Focus: Board oversight, risk management, internal controls, audit-committee responsibilities, corrective-action follow-up and governance 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 Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://cma.org.sa/en/RulesRegulations/Regulations/Pages/details.aspx?code=2>

Essential Cybersecurity Controls ECC 2-2024 NCA

Applies To: Government entities and organisations within the NCA's applicable scope

Operational Focus: Cybersecurity governance, asset and risk management, incident response, resilience, third-party controls, monitoring and audit evidence.

Platform Fit and Workflow Support: Primary fit Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting. Primary fit Risk-based assurance, control testing, evidence, findings, approvals and remediation follow-up. 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://nca.gov.sa/en/regulatory-documents/controls-list/ecc/>

Personal Data Protection Law and Implementing Regulations SDAIA

Applies To: Controllers and processors handling personal data within the Law's scope

Operational Focus: Privacy governance, processing records, risk assessment, processor oversight, breach assessment, notification workflows and corrective action.

Platform Fit and Workflow Support: Primary fit Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence. Primary 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://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/PDPL2/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfljo8ziPR1dzTwMgw2MDMOcTA3MjH39TE29jY0MQsz1w9EUhIZZAhUEGvI6OXoaGwQY60cRo98AB3A0IKTfi5ACoA-MinydfdP1owoSSzj0M_PS8vUjAlwCflyAlkfh1W5hjKEA039gBXg8UJAbGIHIkxbsma6oCAA-ytT9/dz/d5/L0IDUmITUSEhL3dHa0FKRnNBLzROV3FpQSEhL2Vu/

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 One on HUAWEI Cloud

Federated GRC on the Local Cloud. More Governance. Less Capital.

In Saudi Arabia, TransVare One runs live on HUAWEI Cloud. HUAWEI Cloud provides the infrastructure layer, while TransVare provides the trust layer.

Use a subscription model with no infrastructure to buy or refresh and no separate maintenance fee. Start with one discipline, onboard in weeks and add the next on the same federated foundation.

3

Flagship platforms live on the cloud

0

Infrastructure to buy, size or refresh

Weeks

To a live environment, not months

1

Shared data fabric across every domain

Risk Intelligence

Connect risks, controls and treatment plans with configurable KRIs, automated alerts, role-based heatmaps, board-ready reporting and AI-assisted risk drafting and classification.

Independent Assurance

Manage the audit universe, weighted risk assessment, agile annual planning, auditee evidence, follow-up and AI-assisted observation summaries, risk similarity and test steps.

Incident Response

Use one central incident register for reporting, investigation, root-cause analysis, escalation, notifications, corrective actions and closure tracking.

01

Control and assurance built in

Role-based access, multilevel approvals, Microsoft Entra ID single sign-on, multifactor authentication, encryption and a complete timestamped audit trail.

02

AI inside your own boundary

TransVare One AI operates within the customer tenancy on the local cloud. Risk data, audit evidence and incident records remain contained within the private environment.

Aligned with IIA Global Internal Audit Standards 2024, COSO ERM and ISO 31000.

TransVare Middle East | Saudi Arabia

Build a Connected GRC Operating Model for Saudi Arabia.

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