POINT OF VIEW - SEPTEMBER 2026

Saudi Arabia: From Regulatory Obligation to Board-Ready Evidence.

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 national data-protection requirements. The strongest operating model connects enterprise risk, independent assurance and incident evidence across these obligations.

REGION
Middle East

REGULATORY HUB
KSA

Saudi Arabia

Country in Brief

4	**7**	**6**	**3**
Regulatory authorities profiled	Official regulatory sources mapped	Supervisory priorities operationalised	Connected TransVare platforms

01 Saudi Arabia Regulatory Landscape

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

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

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 Risk appetite, tolerances and board reporting	02 Risk and control assessment with KRIs
03 Independent risk-based internal audit	04 Cyber incident and regulatory escalation
05 Business continuity and third-party resilience	06 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 Saudi Arabia 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.

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.
ERMCare® **Primary Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
AuditCare® **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**

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.
AuditCare® **Primary Fit**	Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up.
ERMCare® **Primary Fit**	Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership reporting.
Scope Boundary	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
Official Source	**Open Official Source**

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.
AuditVare® **Primary Fit**	Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and follow-up.
ERMVare® **Primary Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
Scope Boundary	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
Official Source	**Open Official Source**

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.
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**

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.
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**

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.
ERMVare® **Primary Fit**	Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting.
AuditVare® **Primary Fit**	Risk-based assurance, control testing, evidence, findings, approvals and remediation follow-up.
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**

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.
InciVare® **Primary Fit**	Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence.
ERMVare® **Primary 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 TransVare One on HUAWEI Cloud

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	0	Weeks	1
Flagship platforms	Infrastructure to buy	To a live environment	Shared data fabric

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.

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.

07 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	**Cyber Security Framework** SAMA	**Official Source**
02	**Business Continuity Management Framework** SAMA	**Official Source**
03	**Principles of Internal Auditing for Local Banks** SAMA	**Official Source**
04	**Operational Risk Management** SAMA	**Official Source**
05	**Corporate Governance Regulations** CMA	**Official Source**
06	**Essential Cybersecurity Controls ECC 2-2024** NCA	**Official Source**
07	**Personal Data Protection Law and Implementing Regulations** SDAIA	**Official Source**

THE NEXT STEP

Build a Connected GRC Operating Model for Saudi Arabia.

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