POINT OF VIEW - SEPTEMBER 2026

Kenya: From Regulatory Obligation to Board-Ready Evidence.

Banking resilience, listed-company governance and privacy evidence

Kenya's framework combines Central Bank prudential and cyber guidance, CMA corporate-governance rules and the Data Protection Act. Regulated enterprises need a connected operating model for risk appetite, control testing, incident response, third-party risk and board reporting.

REGION
Africa

REGULATORY HUB
KEN


Kenya

Country in Brief

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

01 Kenya Regulatory Landscape

Kenya's framework combines Central Bank prudential and cyber guidance, CMA corporate-governance rules and the Data Protection Act. Regulated enterprises need a connected operating model for risk appetite, control testing, incident response, third-party risk and board reporting.

CBK

Central Bank of Kenya

Industries Regulated

Banking and lending, Regulated financial services

CMA

Capital Markets Authority

Industries Regulated

Capital markets and listed companies

ODPC

Office of the Data Protection Commissioner

Industries Regulated

Cross-sector data controllers and processors

KE-CIRT

Kenya Computer Incident Response Team Coordination Centre

Industries Regulated

Government and critical infrastructure

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	Prudential risk management
02	Bank cyber resilience
03	Listed-company governance
04	Data breach notification

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 Kenya 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.

Prudential Guidelines for Institutions Licensed under the Banking Act
CBK

Applies To	Banks and financial institutions licensed under the Banking Act
Operational Focus	Corporate governance, risk management, internal controls, internal audit, outsourcing, continuity and supervisory reporting.
ERMVare® **Primary Fit**	Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting.
AuditVare® **Primary Fit**	Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and 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**

Risk Management Guidelines
CBK

Applies To	Banking institutions supervised by CBK
Operational Focus	Board risk oversight, appetite, identification, measurement, controls, stress testing, monitoring and 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**

Guidance Note on Cybersecurity for the Banking Sector
CBK

Applies To	Banks and other institutions within the guidance scope
Operational Focus	Cyber governance, threat and risk assessment, controls, incident response, regulatory reporting, recovery and audit.
ERMVare® **Primary Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board 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**

Code of Corporate Governance Practices for Issuers
CMA

Applies To	Issuers of securities to the public
Operational Focus	Board effectiveness, risk governance, internal controls, audit committees, disclosure and accountability.
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	Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.
Official Source	**Open Official Source**

Data Protection Act 2019
ODPC

Applies To	Data controllers and processors within scope
Operational Focus	Data governance, impact assessment, security, processor oversight, breach notification and compliance evidence.
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	**Prudential Guidelines for Institutions Licensed under the Banking Act** CBK	**Official Source**
02	**Risk Management Guidelines** CBK	**Official Source**
03	**Guidance Note on Cybersecurity for the Banking Sector** CBK	**Official Source**
04	**Code of Corporate Governance Practices for Issuers** CMA	**Official Source**
05	**Data Protection Act 2019** ODPC	**Official Source**

THE NEXT STEP

Build a Connected GRC Operating Model for Kenya.

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