POINT OF VIEW - SEPTEMBER 2026

Pakistan: From Regulatory Obligation to Board-Ready Evidence.

Connected banking governance, technology risk and market assurance

Pakistan's regulated sectors operate under State Bank governance and technology-risk frameworks, securities rules and national cybersecurity requirements. A connected model helps institutions manage risk appetite, control testing, internal audit, incidents, recovery and board reporting.

REGION
South Asia

REGULATORY HUB
PAK


Pakistan

Country in Brief

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

01 Pakistan Regulatory Landscape

Pakistan's regulated sectors operate under State Bank governance and technology-risk frameworks, securities rules and national cybersecurity requirements. A connected model helps institutions manage risk appetite, control testing, internal audit, incidents, recovery and board reporting.

SBP

State Bank of Pakistan

Industries Regulated

Banking and lending, Regulated financial services

SECP

Securities and Exchange Commission of Pakistan

Industries Regulated

Capital markets and listed companies

PKCERT

National Cyber Emergency Response Team

Industries Regulated

Government and critical infrastructure, Public and private organisations

MoITT

Ministry of Information Technology and Telecommunication

Industries Regulated

Telecommunications and digital services, Public and private organisations

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	Enterprise technology risk
02	Bank operational resilience
03	Corporate governance
04	Cyber incident coordination

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 Pakistan 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.

Enterprise Technology Governance and Risk Management Framework

SBP

Applies To	Banks, microfinance banks and development finance institutions within scope
Operational Focus	Board technology governance, risk management, controls, outsourcing, cybersecurity, continuity, incidents and audit.
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**

Operational Risk Management Framework

SBP

Applies To	Banks and development finance institutions within the applicable framework
Operational Focus	Operational loss events, risk and control assessment, indicators, scenario analysis, incident escalation and management reporting.
InciVare® **Primary Fit**	Incident reporting, triage, investigation, root cause, corrective action, escalation and closure.
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**

Corporate Governance Regulatory Framework
SBP

Applies To	Banking companies and financial institutions supervised by SBP
Operational Focus	Board oversight, risk committees, control functions, internal audit independence and remediation accountability.
ERM Vare® **Primary Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
Audit Vare® **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**

Listed Companies Code of Corporate Governance Regulations 2019
SECP

Applies To	Companies listed on a securities exchange in Pakistan
Operational Focus	Board composition, audit committees, internal controls, internal audit, risk oversight and governance reporting.
ERM Vare® **Primary Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
Audit Vare® **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**

National Cyber Security Policy

MoITT and PKCERT

Applies To	Public and private organisations within the national policy ecosystem
Operational Focus	Cyber governance, risk management, incident coordination, critical-infrastructure resilience and capability assurance.
ERMVare® **Primary Fit**	Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership 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**

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	**Enterprise Technology Governance and Risk Management Framework** SBP	**Official Source**
02	**Operational Risk Management Framework** SBP	**Official Source**
03	**Corporate Governance Regulatory Framework** SBP	**Official Source**
04	**Listed Companies Code of Corporate Governance Regulations 2019** SECP	**Official Source**
05	**National Cyber Security Policy** MoITT and PKCERT	**Official Source**

THE NEXT STEP

Build a Connected GRC Operating Model for Pakistan.

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

Karachi
Office No. 7, Silicon Valley, Building No. S2
Main Shahra-e-Faisal, NASTP 2, Karachi
Pakistan

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