POINT OF VIEW - SEPTEMBER 2026

Sri Lanka: From Regulatory Obligation to Board-Ready Evidence.

Operational resilience and accountable governance for Sri Lankan institutions

Sri Lanka's financial framework now includes detailed corporate-governance, technology-resilience, incident-reporting and outsourcing requirements. Regulated organisations need aligned risk ownership, tested controls, timely escalation and independent assurance.

REGION
South Asia

REGULATORY HUB
LKA


Sri Lanka

Country in Brief

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

01 Sri Lanka Regulatory Landscape

Sri Lanka's financial framework now includes detailed corporate-governance, technology-resilience, incident-reporting and outsourcing requirements. Regulated organisations need aligned risk ownership, tested controls, timely escalation and independent assurance.

CBSL

Central Bank of Sri Lanka

Industries Regulated

Banking and lending

SEC

Securities and Exchange Commission of Sri Lanka

Industries Regulated

Capital markets and listed companies

DPA

Data Protection Authority of Sri Lanka

Industries Regulated

Cross-sector data controllers and processors

Sri Lanka CERT

Sri Lanka Computer Emergency Readiness Team

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	Bank corporate governance
02	Technology resilience
03	IT and cyber incident reporting
04	Outsourcing controls

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 Sri Lanka 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.

Banking Act Direction 05 of 2024 on Corporate Governance

CBSL

Applies To	Licensed commercial banks and licensed specialised banks
Operational Focus	Board and committee governance, risk appetite, internal controls, compliance, internal audit and supervisory accountability.
ERMCare® **Primary Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
AuditCare® **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**

Banking Act Direction 16 of 2021 on Technology Risk Management and Resilience

CBSL

Applies To	Licensed banks in Sri Lanka
Operational Focus	Technology governance, risk assessment, critical systems, cybersecurity, incident response, continuity and independent review.
ERMCare® **Primary Fit**	Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership reporting.
InciCare® **Primary Fit**	Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail.
AuditCare® **Primary 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**

Circular 02 of 2025 on Reporting IT and Cybersecurity Incidents

CBSL

Applies To	Licensed banks within the circular's scope
Operational Focus	Incident classification, regulatory notification, progress reporting, root-cause analysis and closure evidence.
InciVare® **Primary Fit**	Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail.
ERMVare® **Supporting Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
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**

Banking Act Direction 01 of 2026 on Outsourcing

CBSL

Applies To	Licensed banks using outsourced services
Operational Focus	Third-party risk, due diligence, contracts, monitoring, concentration, exit plans, incidents and board oversight.
ERMVare® **Primary Fit**	Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting.
InciVare® **Primary Fit**	Incident reporting, triage, investigation, root cause, corrective action, escalation and closure.
Scope Boundary	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
Official Source	**Open Official Source**

Personal Data Protection Act No. 9 of 2022

DPA

Applies To	Controllers and processors within the Act's scope
Operational Focus	Data governance, impact assessment, security, processor oversight, breach response and accountability records.
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	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
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	**Banking Act Direction 05 of 2024 on Corporate Governance** CBSL	**Official Source**
02	**Banking Act Direction 16 of 2021 on Technology Risk Management and Resilience** CBSL	**Official Source**
03	**Circular 02 of 2025 on Reporting IT and Cybersecurity Incidents** CBSL	**Official Source**
04	**Banking Act Direction 01 of 2026 on Outsourcing** CBSL	**Official Source**
05	**Personal Data Protection Act No. 9 of 2022** DPA	**Official Source**

THE NEXT STEP

Build a Connected GRC Operating Model for Sri Lanka.

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