POINT OF VIEW - SEPTEMBER 2026

India: From Regulatory Obligation to Board-Ready Evidence.

One operating record across banking, securities, cyber resilience and privacy

India's regulatory environment combines Reserve Bank technology and operational-resilience expectations, SEBI governance and cyber-resilience requirements, national incident reporting and a developing digital-personal-data regime. Organisations benefit from connected risk, control, incident and assurance evidence.

REGION
APAC / South Asia

REGULATORY HUB
IND


India

Country in Brief

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

01 India Regulatory Landscape

India's regulatory environment combines Reserve Bank technology and operational-resilience expectations, SEBI governance and cyber-resilience requirements, national incident reporting and a developing digital-personal-data regime. Organisations benefit from connected risk, control, incident and assurance evidence.

RBI

Reserve Bank of India

Industries Regulated

Banking and lending

SEBI

Securities and Exchange Board of India

Industries Regulated

Capital markets and listed companies

CERT-In

Indian Computer Emergency Response Team

Industries Regulated

Government and critical infrastructure

MeitY

Ministry of Electronics and Information Technology

Industries Regulated

Telecommunications and digital services

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	IT governance and assurance
02	Operational resilience
03	Cyber incident reporting
04	Digital 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 India 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.

Commercial Banks Cybersecurity, Technology Risk, Resilience and Assurance Directions 2026

RBI

Applies To	Commercial banks within the Directions' stated scope
Operational Focus	Board technology governance, cyber and technology risk, resilience, third-party controls, incident management, independent assurance and regulatory reporting.
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.
Auditvare® **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**

Guidance Note on Operational Risk Management and Operational Resilience 2024

RBI

Applies To	RBI-regulated entities within the guidance perimeter
Operational Focus	Risk appetite, critical operations, dependency mapping, incidents, tolerances, scenario testing, third-party risk and board reporting.
ERMvare® **Primary Fit**	Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting.
Incivare® **Primary Fit**	Disruption reporting, escalation, investigation, corrective action, recovery tracking and closure evidence.
Scope Boundary	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
Official Source	**Open Official Source**

Cybersecurity and Cyber Resilience Framework 2024

SEBI

Applies To	SEBI-regulated entities
Operational Focus	Cyber governance, risk assessment, security operations, incident response, regulatory reporting, recovery and audit evidence.
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.
AuditVare® **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**

Listing Obligations and Disclosure Requirements Regulations

SEBI

Applies To	Listed entities within the regulations' scope
Operational Focus	Board and audit-committee oversight, risk-management committees, internal controls, disclosures and corrective-action accountability.
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	Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.
Official Source	**Open Official Source**

Digital Personal Data Protection Framework

MeitY

Applies To	Data fiduciaries and processors within the enacted framework
Operational Focus	Processing accountability, security safeguards, breach response, processor oversight and evidence supporting regulatory notifications.
InciVare® **Primary Fit**	Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence.
AuditVare® **Supporting Fit**	Risk-based assurance, control design and effectiveness testing, evidence, findings and action 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**

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	**Commercial Banks Cybersecurity, Technology Risk, Resilience and Assurance Directions 2026** RBI	**Official Source**
02	**Guidance Note on Operational Risk Management and Operational Resilience 2024** RBI	**Official Source**
03	**Cybersecurity and Cyber Resilience Framework 2024** SEBI	**Official Source**
04	**Listing Obligations and Disclosure Requirements Regulations** SEBI	**Official Source**
05	**Digital Personal Data Protection Framework** MeitY	**Official Source**

THE NEXT STEP

Build a Connected GRC Operating Model for India.

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