

India Regulatory Hub

Country-specific obligations, regulatory sources and product workflow mappings.

IND Regulatory Hub

Region: South Asia

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.

IND

South Asia governance, risk and compliance intelligence

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

Supervisory Priorities

What Regulated Organisations Need to Operationalise.

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

Regulatory Alignment

India Regulation and Product Map

Each row translates an official regulatory source into an operational GRC focus, then identifies only the platforms with a defensible workflow or evidence role.

Research Review

Official-source and product-fit review completed 1 September 2026.

Primary Fit

The platform directly manages a central process or evidence set described in the requirement.

Supporting Fit

The platform contributes linked evidence, oversight or follow-up but is not the main system for the requirement.

Not Shown

A weak or unsubstantiated product relationship is intentionally omitted.

India Regulation And Product Map

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.

Platform Fit and Workflow Support: Primary fit Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting. Primary fit Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail. Primary fit Risk-based assurance, control testing, evidence, findings, approvals and remediation follow-up. Boundary GRC workflow and evidence support only. The platforms do not replace technical security monitoring, detection or protection tools.

Source: Source

<https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=13643&Mode=0>

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.

Platform Fit and Workflow Support: Primary fit Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting. Primary fit Disruption reporting, escalation, investigation, corrective action, recovery tracking and closure evidence. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12679&Mode=0>

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.

Platform Fit and Workflow Support: Primary fit Operational-risk registers, critical-service assessments, controls, KRIs, treatments and leadership reporting. Primary fit Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail. Primary fit Risk-based assurance, control testing, evidence, findings, approvals and remediation follow-up. Boundary GRC workflow and evidence support only. The platforms do not replace technical security monitoring, detection or protection tools.

Source: Source

https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-csc-rf-for-sebi-regulated-entities-res-_85964.html

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.

Platform Fit and Workflow Support: Primary fit Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. Supporting fit Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up. Boundary Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.

Source: Source

https://www.sebi.gov.in/legal/regulations/jan-2026/securities-and-exchange-board-of-india-listing-obligations-and-disclosure-requirements-regulations-2015-last-amended-on-january-22-2026-_99423.html

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.

Platform Fit and Workflow Support: Primary fit Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence. Supporting fit Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up. Boundary Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.

Source: Source

<https://www.meity.gov.in/data-protection-framework>

This mapping is an implementation aid, not legal advice. It describes configurable workflow and evidence support, not automatic compliance. Always validate applicability, current versions, implementation dates and supervisory expectations with qualified advisers and the relevant authority.

Product Mapping Grounded in the 2026 Solution Briefs.

The mapping uses the capabilities documented in the current brochures. It does not extend the platforms beyond their stated functional scope.

Risk and Control Intelligence

Best suited to 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

Independent Assurance

Best suited to the audit universe, risk-based planning, engagement execution, RCM-linked design and effectiveness testing, evidence, findings, approvals and follow-up.

Risk-based audit planning

ToD and ToE test procedures

Working papers and evidence

GIAS 2024 observation drafting

Incident Response and Closure

Best suited to incident intake, triage, investigation, root-cause analysis, escalation, notifications, corrective and preventive actions, 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.

Connected Operating Model

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.

Risk intelligence

Independent assurance

Incident response

TransVare South Asia | India

Build a Connected GRC Operating Model for India

See how TransVare can support local regulatory readiness while preserving regional visibility and board oversight.