

Nepal Regulatory Hub

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

NPL Regulatory Hub

Region: South Asia

Prudential risk, digital controls and assurance for Nepalese institutions

Nepal's financial sector combines central-bank unified directives and risk guidance with securities supervision, electronic-transactions rules and privacy legislation. Institutions need traceable control ownership, internal audit, incident response and board-level monitoring.

NPL

South Asia governance, risk and compliance intelligence

NRB

Nepal Rastra Bank

Industries Regulated

Banking and lending, Regulated financial services

SEBON

Securities Board of Nepal

Industries Regulated

Capital markets and listed companies

NITC

National Information Technology Center

Industries Regulated

Telecommunications and digital services

MoCIT

Ministry of Communication 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

Bank Risk Governance

02

Unified Prudential Controls

03

Technology Incident Response

04

Privacy Accountability

Regulatory Alignment

Nepal 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.

Nepal Regulation And Product Map

Risk Management Guidelines 2018 NRB

Applies To: Banks and financial institutions within the guidelines' scope

Operational Focus: Board risk oversight, appetite, material-risk assessment, controls, monitoring, risk reporting and review.

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 Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://www.nrb.org.np/bsd/risk-management-guidelines-2018/>

Unified Directives for Banks and Financial Institutions NRB

Applies To: Licensed banks and financial institutions

Operational Focus: Governance, prudential controls, operational risk, internal audit, reporting, information security and corrective measures.

Platform Fit and Workflow Support: Primary fit Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. Primary fit Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and 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.nrb.org.np/category/unified-directives/>

Securities Regulatory Framework SEBON

Applies To: Listed entities, securities businesses and market participants

Operational Focus: Market governance, internal controls, disclosure, compliance monitoring and supervisory reporting.

Platform Fit and Workflow Support: Supporting 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.sebon.gov.np/>

Electronic Transactions Act MoCIT

Applies To: Electronic records, digital services and covered computer activities

Operational Focus: Electronic-record integrity, security responsibilities, cyber offences, incident evidence and response coordination.

Platform Fit and Workflow Support: Primary fit Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail. Supporting 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://lawcommission.gov.np/content/13397/>

Privacy Act Government of Nepal

Applies To: Public and private bodies processing personal information within scope

Operational Focus: Privacy governance, lawful handling, confidentiality, security, complaints and corrective response.

Platform Fit and Workflow Support: Primary fit Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence. Supporting fit Privacy risks, controls, assessments, treatment actions, ownership, approvals and management reporting. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://lawcommission.gov.np/>

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 | Nepal

Build a Connected GRC Operating Model for Nepal.

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