

Bhutan Regulatory Hub

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

BTN Regulatory Hub

Region: South Asia

Integrated governance, continuity and data protection for Bhutanese finance

Bhutan's Royal Monetary Authority maintains a clear suite of prudential, risk-management, business-continuity, cybersecurity and data-privacy requirements. Financial service providers can connect these obligations through shared risk, control, incident and assurance workflows.

BTN

South Asia governance, risk and compliance intelligence

RMA

Royal Monetary Authority of Bhutan

Industries Regulated

Banking and lending, Cross-sector data controllers and processors, Regulated financial services

GovTech

Government Technology Agency

Industries Regulated

Government and critical infrastructure

BtCIRT

Bhutan Computer Incident Response Team

Industries Regulated

Government and critical infrastructure

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

Corporate Governance

02

Enterprise Risk Management

03

Business Continuity

04

Cyber and Data Controls

Regulatory Alignment

Bhutan 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.

Bhutan Regulation And Product Map

Corporate Governance Rules and Regulations 2024 RMA

Applies To: Financial service providers within scope

Operational Focus: Board and committee responsibilities, risk oversight, internal controls, internal audit, conflicts and governance reporting.

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

Source: Source

<https://www.rma.org.bt/legislation/>

Risk Management Guidelines 2019 RMA

Applies To: RMA-regulated financial service providers

Operational Focus: Risk appetite, identification, assessment, limits, controls, monitoring, reporting and independent review.

Platform Fit and Workflow Support: Primary fit Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. Primary 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.rma.org.bt/legislation/>

Business Continuity Planning Guidelines 2022 RMA

Applies To: Financial service providers within the guideline's scope

Operational Focus: Business-impact analysis, recovery priorities, crisis response, testing, third-party dependencies and improvement actions.

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.rma.org.bt/legislation/>

Cybersecurity Directives for Banks RMA

Applies To: Banks supervised by RMA

Operational Focus: Cyber governance, risk controls, monitoring, incident response, continuity, regulatory reporting and audit.

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

Source: Source

<https://www.rma.org.bt/bank/notificationdirectives.jsp?id=9>

Guidelines on Data Privacy and Data Protection 2021 RMA

Applies To: Financial service providers handling customer and personal data

Operational Focus: Privacy governance, access controls, processing accountability, data incidents, retention and assurance.

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://www.rma.org.bt/legislation/>

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 | Bhutan

Build a Connected GRC Operating Model for Bhutan.

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