

Philippines Regulatory Hub

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

PHL Regulatory Hub

Region: APAC

Connected financial governance, cyber resilience and privacy accountability

The Philippines combines Bangko Sentral ng Pilipinas risk and technology supervision, Securities and Exchange Commission governance expectations, national cybersecurity policy and a mature privacy regime. Regulated organisations need connected risk ownership, internal controls, independent assurance, incident response and accountable corrective action.

PHL

APAC governance, risk and compliance intelligence

BSP

Bangko Sentral ng Pilipinas

Industries Regulated

Banking and lending, Regulated financial services

SEC

Securities and Exchange Commission

Industries Regulated

Capital markets and listed companies

NPC

National Privacy Commission

Industries Regulated

Cross-sector data controllers and processors

DICT

Department of Information and Communications Technology

Industries Regulated

Government and critical infrastructure, Public and private organisations

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

Enterprise Risk and Board Oversight

02

Internal Controls and Independent Audit

03

Technology and Third-Party Risk

04

Incident Escalation and Root-Cause Analysis

Regulatory Alignment

Philippines 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.

Philippines Regulation And Product Map

Manual of Regulations for Banks BSP

Applies To: Banks and other BSP-supervised financial institutions within the applicable provisions

Operational Focus: Corporate governance, risk appetite, enterprise risk management, internal controls, compliance, internal audit, board reporting and tracked remediation.

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.bsp.gov.ph/SitePages/Regulations/MORB.aspx>

Information Technology Risk Management Standards BSP

Applies To: BSP-supervised financial institutions within the standards' scope

Operational Focus: Technology governance, cybersecurity, outsourcing, continuity, incident recording, escalation, recovery testing and independent assurance.

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.bsp.gov.ph/SitePages/Regulations/RegulationsList.aspx>

Code of Corporate Governance for Public Companies and Registered Issuers SEC

Applies To: Public companies and registered issuers within the Code's scope

Operational Focus: Board and committee accountability, risk oversight, internal-control review, internal audit, disclosure and corrective-action monitoring.

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 Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.

Source: Source

<https://appointment.sec.gov.ph/mc-2019/mc-no-24-s-2019-code-of-corporate-governance-for-pub>

Data Privacy Act Implementing Rules and Regulations NPC

Applies To: Personal-information controllers and processors within scope

Operational Focus: Privacy governance, security measures, processor oversight, breach assessment, documentation, notification and remediation evidence.

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 Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.

Source: Source

<https://privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012/>

Personal Data Breach Reporting Procedures NPC

Applies To: Personal-information controllers subject to breach-notification duties

Operational Focus: Breach recording, risk assessment, regulatory escalation, affected-person communication, root-cause analysis and corrective actions.

Platform Fit and Workflow Support: Primary fit Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence. Primary 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://privacy.gov.ph/pips-and-pics/breach-reporting/>

National Cybersecurity Plan 2023 to 2028 DICT

Applies To: Government, critical infrastructure and participating organisations across the national cyber ecosystem

Operational Focus: Cyber-risk governance, resilience, coordinated incident response, information sharing, capability assurance and service continuity.

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. Boundary GRC workflow and evidence support only. The platforms do not replace technical security monitoring, detection or protection tools.

Source: Source

<https://dict.gov.ph/national-cyber-security-plan>

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 APAC | Philippines

Build a Connected GRC Operating Model for the Philippines

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