

Philippines Regulatory Hub

Country-specific obligations, regulatory sources and product workflow mappings. Source page: <https://transvare.com/en-ph/>

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.

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.

Philippine regulations mapped to TransVare platform workflows

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.

ERMVare (Primary fit): Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.

AuditVare (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: <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.

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.

CyberVare (Primary fit): Asset-centred cyber risk register, CIA-based assessments, control evidence, vulnerability exposure and accountable remediation.

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

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.

ERMVare (Primary fit): Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.

AuditVare (Primary fit): Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and follow-up.

GovernanceVare (Primary fit): Policies and governance documents, approval and renewal workflows, compliance checklists and board reporting.

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

Source: https://sec.gov.ph/wp-content/uploads/2020/02/2020PressRelease_SEC-raises-corporate-governance-standards-for-public-companies-registered-issuers_.pdf

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.

InciVare (Primary fit): Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence.

ERMVare (Supporting fit): Privacy risks, controls, assessments, treatment actions, ownership, approvals and management reporting.

ComplianceVare (Primary fit): Obligation register, applicability, compliance assessments, observations, KCIs and retained evidence.

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

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.

InciVare (Primary fit): Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence.

ERMVare (Primary fit): Privacy risks, controls, assessments, treatment actions, ownership, approvals and management reporting.

ComplianceVare (Supporting fit): Obligation register, applicability, compliance assessments, observations, KCIs and retained evidence.

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

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.

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.

CyberVare (Primary fit): Asset-centred cyber risk register, CIA-based assessments, control evidence, vulnerability exposure and accountable remediation.

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

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.

Brochure-Validated Capability

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.

ERMVare

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

AuditVare

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

InciVare

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

CyberVare

Cyber Risk and Control Evidence

Best suited to asset-centred cyber risk registers, confidentiality, integrity and availability assessments, control testing and evidence, vulnerability exposure and accountable remediation.

- Asset-centred risk register
- CIA-based risk assessment
- Control evidence and testing
- Vulnerability and observation follow-up

GovernanceVare

Policy and Board Governance

Best suited to policies, procedures and governance documents, approval and renewal workflows, compliance checklists, contract records and board reporting.

- Policy and document lifecycle
- Approval and renewal tracking
- Governance compliance checklists
- Board and committee reporting

ComplianceVare

Obligation and Compliance Management

Best suited to authority documents and obligation registers, applicability, compliance assessments, observations, KCIs, regulatory updates and evidence retention.

- Obligation and citation register
- Applicability and ownership
- Compliance assessments

- Observation and KCI 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.

ERMVare

Risk Intelligence

AuditVare

Independent Assurance

InciVare

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.

Contact: connect@transvare.com · <https://transvare.com/contact/>