POINT OF VIEW - SEPTEMBER 2026

# Philippines: From Regulatory Obligation to Board-Ready Evidence.

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.

**REGION**
APAC

**REGULATORY HUB**
PHL


Philippines

**Country in Brief**

| | | | |
|---|---|---|---|
| **4** | **6** | **5** | **3** |
| Regulatory authorities profiled | Official regulatory sources mapped | Supervisory priorities operationalised | Connected TransVare platforms |

Copyright 2026 @ TransVare Corporation

# 01 Philippines Regulatory Landscape

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.

### 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

Copyright 2026 @ TransVare Corporation

## 02 Supervisory Priorities

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 |
| 05 | Privacy breach notification |

## 03 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.

**04**

### Report to Leadership

Turn current operational evidence into traceable executive and board oversight.

Copyright 2026 @ TransVare Corporation

# 04 Philippines Regulation and Product Map

Each official requirement below is translated into an operational GRC focus. Only platforms with a defensible workflow or evidence role are shown as a primary or supporting fit.

## 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. |
| ERMCare® **Primary Fit** | Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. |
| AuditCare® **Primary Fit** | Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and follow-up. |
| **Scope Boundary** | Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers. |
| **Official Source** | **Open Official Source** |

## 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. |
| ERMCare® **Primary Fit** | Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting. |
| InciCare® **Primary Fit** | Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail. |
| AuditCare® **Primary Fit** | Risk-based assurance, control testing, evidence, findings, approvals and remediation follow-up. |
| **Scope Boundary** | GRC workflow and evidence support only. The platforms do not replace technical security monitoring, detection or protection tools. |
| **Official Source** | **Open Official Source** |

Copyright 2026 @ TransVare Corporation

## 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. |
| ERM Vare® **Primary Fit** | Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. |
| Audit Vare® **Primary Fit** | Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and follow-up. |
| **Scope Boundary** | Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration. |
| **Official Source** | **Open Official Source** |

## 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. |
| Inci Vare® **Primary Fit** | Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence. |
| ERM Vare® **Supporting Fit** | Privacy risks, controls, assessments, treatment actions, ownership, approvals and management reporting. |
| **Scope Boundary** | Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration. |
| **Official Source** | **Open Official Source** |

Copyright 2026 @ TransVare Corporation

## 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. |
| **Scope Boundary** | Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers. |
| **Official Source** | **Open Official Source** |

## 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. |
| **Scope Boundary** | GRC workflow and evidence support only. The platforms do not replace technical security monitoring, detection or protection tools. |
| **Official Source** | **Open Official Source** |

| Research Review | Primary Fit | Supporting Fit | Not Shown |
|---|---|---|---|
| Official-source and product-fit review completed 1 September 2026. | Directly manages a central process or evidence set. | Contributes linked evidence, oversight or follow-up. | Weak or unsubstantiated relationships are omitted. |

Copyright 2026 @ TransVare Corporation

# 05 Brochure-Validated Product Capability

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

ERMVare®

## Risk and Control Intelligence

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

Audit universe, risk-based planning, engagement execution, RCM-linked control testing, evidence, findings, approvals and follow-up.

Risk-based audit planning | ToD and ToE procedures | Working papers and evidence | GIAS 2024 observation drafting

InciVare®

## Incident Response and Closure

Incident intake, triage, investigation, root-cause analysis, escalation, notifications, corrective action, 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.

Copyright 2026 @ TransVare Corporation

# 06 Sources, Scope and Next Step

Official sources used in this report are linked directly from each regulation summary. The mapping is an implementation aid and not legal advice.

| | | |
|---|---|---|
| 01 | **Manual of Regulations for Banks**<br>BSP | **Official Source** |
| 02 | **Information Technology Risk Management Standards**<br>BSP | **Official Source** |
| 03 | **Code of Corporate Governance for Public Companies and Registered Issuers**<br>SEC | **Official Source** |
| 04 | **Data Privacy Act Implementing Rules and Regulations**<br>NPC | **Official Source** |
| 05 | **Personal Data Breach Reporting Procedures**<br>NPC | **Official Source** |
| 06 | **National Cybersecurity Plan 2023 to 2028**<br>DICT | **Official Source** |

TransVare provides configurable technology to support governance, risk, audit and incident-management processes. Platform use does not, by itself, constitute or guarantee regulatory compliance. Applicability depends on entity type, licence, sector and current legal requirements. Obtain professional advice before relying on any regulatory mapping.

THE NEXT STEP

## Build a Connected GRC Operating Model for Philippines.

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

**TransVare US: Delaware**
8 The Green, Street R
Dover, Kent 19901, State of Delaware
United States of America

**For Local Alliance Partner and Sales Contact:**
Connect@TransVare.com
TransVare.com