POINT OF VIEW - SEPTEMBER 2026

Taiwan: From Regulatory Obligation to Board-Ready Evidence.

Connected audit, cyber and privacy controls for regulated institutions

Taiwan's framework links financial internal-control and audit rules with a strengthened national cybersecurity regime and personal-data obligations. Institutions need clear control ownership, independent review, rapid incident escalation and verified corrective action.

REGION
APAC

REGULATORY HUB
TWN

Taiwan

Country in Brief

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

01 Taiwan Regulatory Landscape

Taiwan's framework links financial internal-control and audit rules with a strengthened national cybersecurity regime and personal-data obligations. Institutions need clear control ownership, independent review, rapid incident escalation and verified corrective action.

FSC

Financial Supervisory Commission

Industries Regulated

Public and private organisations, Regulated financial services

TWSE

Taiwan Stock Exchange

Industries Regulated

Capital markets and listed companies

NICS

National Institute of Cyber Security

Industries Regulated

Capital markets and listed companies, Government and critical infrastructure

PDPC

Personal Data Protection Commission Preparatory Office

Industries Regulated

Cross-sector data controllers and processors, Government and critical infrastructure

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	**Financial internal controls**
02	**Independent internal audit**
03	**Cyber incident escalation**
04	**Personal-data accountability**

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.

04 Taiwan 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.

Regulations Governing Internal Control and Auditing Systems

FSC

Applies To	Financial enterprises within the applicable sector rules
Operational Focus	Board-approved internal controls, independent audit, annual plans, findings, reporting and tracked remediation.
AuditVare® **Primary Fit**	Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and follow-up.
ERMVare® **Supporting Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
Scope Boundary	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
Official Source	**Open Official Source**

Cyber Security Management Act

Executive Yuan and cybersecurity authorities

Applies To	Government agencies and designated specific non-government agencies
Operational Focus	Cyber governance, risk programmes, incident response, reporting, audits and improvement measures.
ERMVare® **Primary Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board 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**

Cybersecurity Incident Reporting and Response Regulations

Cybersecurity authorities

Applies To	Entities designated under the Cyber Security Management Act
Operational Focus	Incident classification, time-bound reporting, response, status updates, investigation and corrective-action evidence.
InciVare® **Primary Fit**	Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail.
ERMVare® **Supporting Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
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**

Personal Data Protection Act

PDPC

Applies To	Government and non-government agencies processing personal data
Operational Focus	Purpose limitation, security safeguards, data-subject rights, incident accountability and damage prevention.
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.
Scope Boundary	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
Official Source	**Open Official Source**

Financial Operational Resilience on Cybersecurity Ecosystem Blueprint

FSC

Applies To	Financial institutions and industry bodies participating in the supervisory resilience programme
Operational Focus	Sector cyber governance, operational resilience, coordinated incident response, continuity, monitoring, exercises and assurance.
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.

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.

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	**Regulations Governing Internal Control and Auditing Systems** FSC	**Official Source**
02	**Cyber Security Management Act** Executive Yuan and cybersecurity authorities	**Official Source**
03	**Cybersecurity Incident Reporting and Response Regulations** Cybersecurity authorities	**Official Source**
04	**Personal Data Protection Act** PDPC	**Official Source**
05	**Financial Operational Resilience on Cybersecurity Ecosystem Blueprint** FSC	**Official Source**

THE NEXT STEP

Build a Connected GRC Operating Model for Taiwan.

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