

Taiwan Regulatory Hub

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

TWN Regulatory Hub

Region: APAC

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.

TWN

APAC governance, risk and compliance intelligence

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

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

Financial Internal Controls

02

Independent Internal Audit

03

Cyber Incident Escalation

04

Personal-Data Accountability

Regulatory Alignment

Taiwan 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.

Taiwan Regulation And Product Map

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.

Platform Fit and Workflow Support: Primary fit Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and follow-up. Supporting fit Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0390052>

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.

Platform Fit and Workflow Support: Primary fit Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board 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://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030297>

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.

Platform Fit and Workflow Support: Primary fit Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail. Supporting fit Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. Boundary GRC workflow and evidence support only. The platforms do not replace technical security monitoring, detection or protection tools.

Source: Source

<https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030305>

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.

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://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021>

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.

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://www.fsc.gov.tw/en/home.jsp?dataserno=202601280002&dtable=News&id=54&mcustomize=multimessage_view.jsp&parentpath=0%2C2

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 | Taiwan

Build a Connected GRC Operating Model for Taiwan.

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