

Australia Regulatory Hub

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

AUS Regulatory Hub

Region: APAC

Connected regulatory intelligence for Australian enterprises

Australia's governance landscape combines prudential risk management, operational resilience, breach reporting and listed-entity oversight. Regulated organisations need a traceable operating model that connects material risks, control effectiveness, incidents, assurance and board accountability.

AUS

APAC governance, risk and compliance intelligence

APRA

Australian Prudential Regulation Authority

Industries Regulated

Banking and lending, Insurance

ASIC

Australian Securities and Investments Commission

Industries Regulated

Capital markets and listed companies, Regulated financial services

ASX

Australian Securities Exchange

Industries Regulated

Capital markets and listed companies

OAIC

Office of the Australian Information Commissioner

Industries Regulated

Cross-sector data controllers and processors

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

Material-Risk Governance and Appetite

02

Operational Resilience and Service Providers

03

Reportable-Situation Workflows

04

Board and Audit-Committee Oversight

Regulatory Alignment

Australia 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.

Australia Regulation And Product Map

CPS 220 Risk Management APRA

Applies To: Authorised deposit-taking institutions and applicable insurers and groups

Operational Focus: A risk-management framework covering material risks, aligned with strategy and supported by clear accountability, review and reporting.

Platform Fit and Workflow Support: Primary fit Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. Supporting fit Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://www.apra.gov.au/standards/cps-220>

CPS 230 Operational Risk Management APRA

Applies To: APRA-regulated entities within the standard's scope

Operational Focus: Operational-risk management, critical-operation resilience, service-provider risk, incidents, near misses, controls and timely remediation.

Platform Fit and Workflow Support: Primary fit Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting. Primary fit Disruption reporting, escalation, investigation, corrective action, recovery tracking and closure evidence. Boundary Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.

Source: Source

<https://www.apra.gov.au/standards/cps-230>

CPS 234 Information Security APRA

Applies To: APRA-regulated entities and relevant group arrangements within the standard's scope

Operational Focus: Board accountability, information-security capability, control design and testing, material incidents, APRA notification and independent review.

Platform Fit and Workflow Support: 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.apra.gov.au/cps-234-information-security>

RG 78 Breach Reporting ASIC

Applies To: Australian financial services and credit licensees

Operational Focus: Identification, assessment, investigation, remediation and reporting of reportable situations within the applicable statutory regime.

Platform Fit and Workflow Support: Primary fit Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence. Supporting fit Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting. Boundary Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.

Source: Source

<https://www.asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-78-breach-reporting-by-afs-licensees-and-credit-licensees>

Corporate Governance Principles and Recommendations ASX

Applies To: Entities listed on the Australian Securities Exchange

Operational Focus: Board governance, risk oversight, internal-control review, internal audit, disclosure and accountable corporate conduct.

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.asx.com.au/about/regulation/corporate-governance-principles-and-recommendations>

Notifiable Data Breaches Scheme OAIC

Applies To: Privacy Act entities covered by the Notifiable Data Breaches scheme

Operational Focus: Eligible data-breach assessment, containment, documented decision-making, notification to the OAIC and affected individuals, and corrective action.

Platform Fit and Workflow Support: Primary fit Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence. Supporting fit Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up. Boundary Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.

Source: Source

<https://www.oaic.gov.au/privacy/notifiable-data-breaches>

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 | Australia

Build a Connected GRC Operating Model for Australia.

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