POINT OF VIEW - SEPTEMBER 2026

Australia: From Regulatory Obligation to Board-Ready Evidence.

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.

REGION	REGULATORY HUB	
APAC	AUS	 Australia

Country in Brief

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

01 Australia Regulatory Landscape

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.

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

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	**Material-risk governance and appetite**
02	**Operational resilience and service providers**
03	**Reportable-situation workflows**
04	**Board and audit-committee oversight**

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 Australia 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.

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.
ERMCare® **Primary Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
AuditCare® **Supporting Fit**	Risk-based assurance, control design and effectiveness testing, evidence, findings and action 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**

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.
ERMCare® **Primary Fit**	Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting.
InciCare® **Primary Fit**	Disruption reporting, escalation, investigation, corrective action, recovery tracking and closure evidence.
Scope Boundary	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
Official Source	**Open Official Source**

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.
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.
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**

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.
InciVare® **Primary Fit**	Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence.
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**

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.
ERMware® **Primary Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
Auditware® **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**

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.
Inciware® **Primary Fit**	Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence.
Auditware® **Supporting Fit**	Risk-based assurance, control design and effectiveness testing, evidence, findings and action 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**

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	**CPS 220 Risk Management** APRA	**Official Source**
02	**CPS 230 Operational Risk Management** APRA	**Official Source**
03	**CPS 234 Information Security** APRA	**Official Source**
04	**RG 78 Breach Reporting** ASIC	**Official Source**
05	**Corporate Governance Principles and Recommendations** ASX	**Official Source**
06	**Notifiable Data Breaches Scheme** OAIC	**Official Source**

THE NEXT STEP

Build a Connected GRC Operating Model for Australia.

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