MAPPING BRIEF

Using the Zscaler Zero Trust Exchange to Support Compliance with the Australian Prudential Standard CPS 234 – Information Security

©2026 Zscaler, Inc. All rights reserved.

Executive Summary

Supporting Your CPS 234 Compliance Journey

Prudential Standard CPS 234 Information Security establishes APRA's expectations that regulated entities maintain information security capabilities commensurate with the size and extent of threats to their information assets. The standard requires entities to implement controls to protect information assets based on criticality and sensitivity, systematically test the effectiveness of those controls, and notify APRA of material information security incidents.

CPS 234 places accountability for information security squarely with the Board of an APRA-regulated entity. Boards must ensure that information security capabilities support the continued sound operation of the institution and protect the confidentiality, integrity, and availability of information assets – including those managed by third parties.

Modern financial institutions operate in increasingly distributed environments characterised by hybrid workforces, SaaS adoption, public cloud workloads, encrypted traffic, and complex third-party ecosystems. Traditional perimeter-based architectures often rely on implicit trust and centralised infrastructure, which can increase exposure to lateral movement and reduce visibility across cloud and Internet traffic flows.

Zscaler's Zero Trust Exchange provides a cloud-native Security Service Edge (SSE) architecture designed to eliminate implicit trust, enforce identity-based least-privilege access, and inspect traffic inline across the Internet, SaaS, and private applications. Delivered through a globally distributed platform with service-level commitments for availability and performance, the architecture supports continuous visibility, consistent policy enforcement, and proactive threat prevention aligned with CPS 234 expectations.

This document maps CPS 234 requirements to capabilities within the Zscaler Zero Trust Exchange. It outlines how Zscaler's architecture may assist APRA-regulated entities in strengthening their information security posture while recognising that governance, risk ownership, and regulatory accountability remain with the regulated entity.

©2026 Zscaler, Inc. All rights reserved.

Zscaler Zero Trust Exchange Overview

The Zero Trust Exchange connects users, devices, and workloads directly to applications based on identity and contextual policy, without exposing the underlying network.

Core architectural principles include:

- Identity-based least-privilege access
- Inline inspection of encrypted and unencrypted traffic
- Application-level segmentation
- Centralised global policy enforcement
- Cloud-native distributed delivery

The platform supports CPS 234 objectives across five primary domains.

Data Protection

- Inline Data Loss Prevention (DLP)
- Exact Data Match and file fingerprinting
- Optical Character Recognition (OCR)
- Machine learning-based content classification
- API-based CASB inspection for SaaS data at rest

These capabilities support the protection of sensitive information assets across web, SaaS, and private applications.

Visibility and Monitoring

- Full SSL/TLS inspection across ports and protocols
- Real-time traffic inspection telemetry
- SaaS application discovery and risk scoring
- Administrator activity logging
- Integration with SIEM and SOAR platforms

These controls enhance visibility across the Internet, SaaS, and private application traffic flows.

Threat Prevention

- Secure Web Gateway (SWG)
- Cloud Firewall
- Intrusion Prevention System (IPS)
- DNS Security
- Advanced Sandbox
- AI-driven threat detection

These preventive controls reduce exposure to malware, ransomware, phishing, and command-and-control communications.

Access Control & Segmentation

- Zero Trust Network Access (ZPA)
- Application-level segmentation
- Device posture validation
- Multi-factor authentication integration
- Role-based access control (RBAC)

These capabilities enforce least-privilege access and reduce the risk of lateral movement.

©2026 Zscaler, Inc. All rights reserved.

Governance & Reporting Support

- Centralised policy engine
- Configuration change history
- Administrative audit trails
- Executive dashboards
- Zscaler Digital Experience (ZDX) monitoring

These features support oversight, monitoring, and assurance reporting.

How To Use This Guide

The following sections outline key CPS 234 requirements and describe how Zscaler Zero Trust Exchange capabilities may assist APRA-regulated entities in meeting information security obligations.

Zscaler provides technical controls, monitoring capabilities, and architectural enforcement that support CPS 234 objectives. Responsibility for governance, risk appetite, classification of information assets, independent testing, and regulatory notification remains with the regulated entity.

Zscaler Product Terminology

Industry Terminology	Zscaler Capability
Security Service Edge (SSE)	Zscaler Zero Trust Exchange
Secure Web Gateway	Zscaler Internet Access (ZIA)
Zero Trust Network Access	Zscaler Private Access (ZPA)
Cloud Access Security Broker	Zscaler CASB (Inline & API)
Data Loss Prevention	Zscaler DLP
Digital Experience Monitoring	Zscaler ZDX
Cloud Firewall	Zscaler Cloud Firewall

©2026 Zscaler, Inc. All rights reserved.

CPS 234 Information Security

Requirement Mapping to Zscaler Zero Trust Exchange

CPS 234 Requirement Mapping

The following pages map CPS 234 requirements (paragraphs 13–36) to supporting capabilities in the Zscaler Zero Trust Exchange. Each requirement also identifies the responsibilities that remain with the APRA-regulated entity.

- **CPS 234 Requirement:** The CPS 234 paragraph reference and a summary of the requirement.
- **Entity Responsibility:** Governance, accountability, risk ownership, independent testing and regulatory notification that remain with the regulated entity.
- **Zscaler Alignment:** Technical controls, monitoring, telemetry and architectural enforcement provided by the Zero Trust Exchange.

This guide is intended to support control design and evidence discussions. It does not replace an entity's legal, regulatory or prudential assessment of CPS 234.

CPS 234 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
ROLES AND RESPONSIBILITIES			
CPS234-13	The Board is ultimately responsible for information security and must ensure it is maintained commensurate with threats to information assets, enabling the continued sound operation of the entity.	Information security capability governance, resourcing decisions, and formal sufficiency assessments remain entity-owned.	ZTE operates a globally distributed, cloud-native proxy architecture (Zscaler Internet Access and Zscaler Private Access) in which all Internet, SaaS, and private application traffic is inspected inline. Full SSL/TLS decryption across ports and protocols enables deep inspection using Cloud Firewall, IPS, Advanced Threat Protection, DNS Security, and Advanced Sandbox. Inline Data Loss Prevention enforces policy on structured and unstructured data. Enforcement occurs at distributed service edges, reducing reliance on centralised perimeter appliances and supporting operational continuity.
CPS234-14	Clearly define roles and responsibilities for information security.	Governance framework definition, formal role assignment, and Board accountability remain entity-owned.	ZTE provides granular Role-Based Access Control, allowing segregation of administrative duties (e.g., policy authoring, DLP administration, read-only reporting access). All administrative activity is logged with user identity, timestamp, and configuration delta tracking. Audit logs can be exported to SIEM platforms for oversight and review.
INFORMATION SECURITY CAPABILITY			
CPS234-15	Maintain an information security capability commensurate with threats to information assets and ensure continued sound operation.	Enterprise-wide risk appetite setting and periodic capability benchmarking remain entity-owned.	Zscaler is a primary component of the entity's information security capability – providing always-on, cloud-native security that scales automatically with changes in the threat landscape. Zscaler delivers information security capability across internet access, private application access, cloud security, data protection, identity, and workload security – without hardware to maintain, patch, or upgrade. Threat intelligence, detection signatures, and policy engines are continuously updated, satisfying the obligation to "actively maintain capability with respect to changes in vulnerabilities and threats" without manual intervention.

©2026 Zscaler, Inc. All rights reserved.

CPS 234 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
CPS234-16	Assess the information security capability of related parties and third parties that manage information assets.	Third-party due diligence, contract negotiation, independent assurance reviews, and remediation enforcement remain entity-owned.	Zscaler will provide all relevant compliance certifications and attestations, along with cooperating with entities' third-party SaaS assessment processes.
CPS234-17	Actively maintain information security capability with respect to changes in vulnerabilities and threats.	Enterprise vulnerability scanning, patch management, and application-layer remediation remain entity-owned.	Zscaler supports continuously maintaining security capability as threats, vulnerabilities, users, applications, and infrastructure change, by moving security controls into a cloud-delivered zero trust architecture, where policy enforcement, threat protection, and access controls are updated centrally rather than through distributed hardware refresh cycles. ZIA provides inline inspection, SSL decryption, threat prevention, and data protection, while ZPA reduces application exposure and enforces identity- and context-based access. Combined with posture visibility, analytics, and risk insights, that helps customers demonstrate a more adaptive and operationally sustainable security model aligned to ongoing CPS 234 obligations.
POLICY FRAMEWORK			
CPS234-18	Maintain an information security policy framework commensurate with the entity's exposure to vulnerabilities and threats.	Formal policy documentation, Board approval, and lifecycle governance remain entity-owned.	Zscaler helps by giving customers continuous validation rather than point-in-time assurance. The Zero Trust Exchange enforces controls inline and generates detailed telemetry to show policy decisions, threat prevention, and data protection outcomes in real time. Risk360 and posture control capabilities help identify control gaps, misconfigurations, and drift across cloud and SaaS environments, so teams can continuously assess and improve effectiveness instead of relying only on periodic manual testing.
CPS234-19	Provide direction on responsibilities and compliance expectations within the policy framework.	Formal compliance monitoring processes and disciplinary governance remain entity-owned.	Zscaler supports governing appropriately skilled and functionally independent parties, so control assurance is objective and credible, by providing a cloud-native platform with centrally enforced controls, detailed logging, and measurable policy outcomes that can be independently reviewed by internal audit, risk, or third-party assessors. Because policy decisions, access activity, and threat events are visible through the platform, customers can more easily demonstrate control operation and support independent validation of their security posture.
INFORMATION ASSET IDENTIFICATION AND CLASSIFICATION			
CPS234-20	Identify and classify information assets, including those managed by related parties and third parties, by criticality and sensitivity.	Asset registers, classification methodologies, and formal ownership assignment remain entity-owned.	Zscaler helps organisations classify and protect information assets based on criticality and sensitivity by using data-aware security controls across users, apps, cloud workloads, and third parties. Through capabilities like data discovery, inline DLP, SaaS posture assessment, and workload segmentation, Zscaler can identify where sensitive data lives, how it's being accessed, and whether it's exposed internally or through related and third parties. That gives customers stronger visibility, more consistent policy enforcement, and better evidence that critical and sensitive assets are being handled appropriately across the full digital estate.

©2026 Zscaler, Inc. All rights reserved.

CPS 234 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
IMPLEMENTATION OF CONTROLS			
CPS234-21	Implement security controls proportionate to asset sensitivity and lifecycle stage.	Non-network lifecycle controls (e.g., backups, endpoint hardening, physical security, secure SDLC) remain entity-owned.	Zscaler helps by using a cloud-native zero trust platform that continuously enforces least-privileged access, inspects traffic inline, and protects users, workloads, and data across their full lifecycle. Instead of relying on broad network trust, Zscaler reduces attack surface, prevents lateral movement, and applies consistent controls based on who is accessing what, from where, and under what risk conditions. This gives organisations stronger, risk-aligned protection of information assets and helps demonstrate controls are commensurate with threats, vulnerabilities, and incident consequences.
CPS234-22	Evaluate the design of information security controls of related parties or third parties that manage information assets.	Independent third-party control testing and contractual audit rights remain the entity's responsibility.	Zscaler will provide all relevant compliance certifications and attestations, along with cooperating with entities' third-party SaaS assessment processes. The ZTE offers visibility into supported third-party platforms to expose data interaction patterns, API inspection results, DLP enforcement logs, and cloud activity monitoring, providing artefacts to support third-party oversight of control discussions.
INCIDENT MANAGEMENT			
CPS234-23	Detect and respond to information security incidents in a timely manner.	Incident response governance, executive escalation, and communications planning remain entity-owned.	Zscaler provides customers with continuous, real-time validation of how access, segmentation, and data protection policies are actually working. Because Zscaler sits inline and logs every user, app, and workload transaction, organisations can quickly identify control gaps, prove policies are being enforced, and generate audit-ready evidence. In short, Zscaler helps move control testing from periodic, manual checks to continuous assurance at scale, supported by correlated Threat Insights, aggregate IPS events, sandbox verdicts, DLP violations, DNS anomalies, and anomalous user behaviour. Logs can be integrated with SIEM/SOAR platforms for automated workflow execution. Detailed packet capture and session logs support forensic investigations.
CPS234-24	Maintain documented information security response plans.	Response plan documentation, approval, and maintenance remain entity-owned.	Zscaler helps by giving organisations immediate visibility into suspicious activity across users, devices, applications, and data flows. With real-time policy enforcement, threat detection, and detailed logging, security teams can identify incidents faster, investigate with better context, and respond more consistently. Zscaler's ZTE provides structured logging, policy export, and telemetry feeds to support operationalisation of response procedures and validation of detection coverage during exercises. In practice, Zscaler helps customers strengthen both the speed and effectiveness of their incident response obligations under CPS 234.
CPS234-25	Ensure response plans address escalation and communication requirements.	Formal communication protocols and stakeholder notification governance remain entity-owned.	Zscaler helps strengthen information security response plans by providing real-time visibility, inline controls, and rich telemetry across users, devices, applications, and data flows. That supports every stage of an incident – from early detection and investigation, to containment, response, recovery, and post-incident review. Because Zscaler captures detailed, actionable event data and integrates with SIEM, SOAR, and broader security operations workflows, teams can escalate incidents faster, coordinate response more effectively, and produce the evidence needed for internal reporting, Board updates, and regulatory notifications, including to APRA.

©2026 Zscaler, Inc. All rights reserved.

CPS 234 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
CPS234-26	Review and test response plans annually.	Test program governance, success criteria, and remediation tracking remain entity-owned.	Zscaler helps organisations annually test their information security response plans by providing real-time telemetry, detailed logs, and policy-driven controls that can be used to validate how response processes perform in practice. During tabletop exercises, simulations, or control testing, security teams can use Zscaler data to assess whether detection, escalation, containment, and recovery workflows are working as intended. Because Zscaler provides clear visibility across users, devices, applications, and data flows, it also helps identify gaps, measure response effectiveness, and support post-test reviews – ensuring response plans stay effective, current, and fit-for-purpose.
TESTING CONTROL EFFECTIVENESS			
CPS234-27	Test the effectiveness of information security controls.	Formal control testing program design and independence remain entity-owned.	Zscaler helps organisations test the effectiveness of their information security controls by providing continuous visibility, inline enforcement, and detailed telemetry across users, devices, applications, workloads, and data flows. That supports a more systematic testing program by allowing security teams to validate whether controls are operating as intended in real-world conditions, rather than relying only on periodic manual reviews. Because testing can be informed by live risk signals, asset criticality, changing threat exposure, and policy violations, organisations can adjust the nature and frequency of control testing to match the rate of vulnerability change and the potential business impact of a control failure. In practice, Zscaler helps customers move toward a more risk-based, evidence-driven approach to control assurance, with clear reporting to support remediation, governance, and audit readiness.
CPS234-28	Assess the effectiveness of third-party security control testing.	Independent assurance and formal testing of third-party controls remain the entity's responsibility.	Zscaler will provide all relevant compliance certifications and attestations, along with cooperating with entities' third-party SaaS assessment processes.
CPS234-29	Identify and report control weaknesses that are not promptly remediated.	Formal weakness reporting to the Board and remediation governance remain entity-owned.	Zscaler helps organisations identify and report material information security control deficiencies by providing continuous monitoring, real-time policy enforcement, and detailed telemetry across users, devices, applications, and data flows. When testing reveals a control gap or persistent policy weakness that cannot be remediated in a timely manner, Zscaler's logging, dashboards, and integrations with SIEM and reporting workflows help security teams clearly document the issue, assess its business impact, and escalate it to Board executives with supporting evidence. This gives leadership better visibility into unresolved control deficiencies, compensating controls, risk exposure, and remediation status – helping support stronger governance, risk acceptance decisions, and regulatory readiness.
CPS234-30	Ensure appropriately skilled and independent specialists conduct testing.	The selection of independent testers and the validation of independence remain the entity's responsibility.	Zscaler will provide all relevant compliance certifications and attestations, along with cooperating with entities' third-party SaaS assessment processes. Configuration exports, audit logs, and telemetry provide audit-ready artefacts to support independent review. Historical metrics and configuration baselines provide data inputs for evaluating testing adequacy and coverage.

©2026 Zscaler, Inc. All rights reserved.

CPS 234 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
CPS234-31	Review the sufficiency of testing programs.	Assurance sufficiency review governance remains entity-owned.	Zscaler will provide all relevant compliance certifications and attestations, along with cooperating with entities' third-party SaaS assessment processes. Configuration exports, audit logs, and telemetry provide audit-ready artefacts to support independent review. Historical metrics and configuration baselines provide data inputs for evaluating testing adequacy and coverage.
INTERNAL AUDIT			
CPS234-32	Internal audit must review the design and operating effectiveness of controls.	Audit planning, scope definition, and assurance conclusions remain the entity's responsibility.	Zscaler assists internal audit activities by giving organisations independent, evidence-based visibility into how information security controls are designed and how they operate in practice across users, devices, applications, workloads, and data flows. Because Zscaler enforces policy inline and captures detailed telemetry and logs, audit teams can review whether key controls are configured appropriately, consistently applied, and operating effectively over time. That same visibility can also support assurance over controls involving related parties and third parties, particularly where access to applications, data, or connected environments is mediated through the Zscaler platform. In practice, Zscaler helps strengthen information security control assurance by making it easier to validate control operation, identify gaps, support remediation tracking, and provide audit-ready evidence for internal governance and external review.
CPS234-33	Ensure information security control assurance is provided by appropriately skilled personnel.	Workforce capability development and staffing remain entity-owned.	Zscaler will provide all relevant compliance certifications and attestations, along with cooperating with entities' third-party SaaS assessment processes.
CPS234-34	Internal audit must assess the information security control assurance provided by related parties or third parties it intends to rely on.	Audit independence and reporting lines remain entity-owned.	Zscaler will provide all relevant compliance certifications and attestations, along with cooperating with entities' third-party SaaS assessment processes. Configuration exports, audit logs, and telemetry provide audit-ready artefacts to support independent review. Historical metrics and configuration baselines provide data inputs for evaluating testing adequacy and coverage.
APRA NOTIFICATION			
CPS234-35	Notify APRA of material information security incidents no later than 72 hours after becoming aware.	Determination of materiality thresholds and regulatory submission remains entity-owned.	Real-time alerting and consolidated logging enable rapid scoping of incident impact and affected assets. Session logs and DLP evidence assist materiality assessment.
CPS234-36	Notify APRA of material information security control weaknesses no later than 10 business days after becoming aware.	Formal regulatory notification and Board escalation remain the entity's responsibility.	Policy enforcement logs and recurring violation dashboards help identify systemic control weaknesses.

©2026 Zscaler, Inc. All rights reserved.

Next Steps

Zscaler works with APRA-regulated entities across Australia to align zero trust architecture with information security obligations. To discuss how Zscaler can support your CPS 234 compliance program, contact your Zscaler account team or visit zscaler.com/compliance.

Additional Resources

- **Zscaler Trust Site:** Real-time platform availability and performance metrics — trust.zscaler.com
- **Zscaler Customer Compliance Center:** Certifications, IRAP reports, and assurance documentation
- **CPS 230 Companion Guide:** Using the Zscaler Zero Trust Exchange to Support Compliance with CPS 230 Operational Risk Management

CONTRIBUTORS

Thomas Ferguson and Paul Krasey – Zscaler FSI Specialist team

DISCLAIMER

This document is provided for informational purposes only and does not constitute legal, regulatory, or prudential advice. APRA-regulated entities remain responsible for determining their own compliance obligations under Prudential Standard CPS 234 Information Security, including governance oversight, risk assessment, independent testing, and regulatory notification. Zscaler capabilities can support an entity's security architecture and control environment, but compliance remains an entity-specific determination.

zscaler™ | Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE–based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™, Zscaler Digital Experience, and ZDX™,and other trademarks listed at **zscaler.com/legal/trademarks** are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.