MAPPING BRIEF

Using the Zscaler Zero Trust Exchange to Support Compliance with the Australian Prudential Standard CPS 230 – Operational Risk Management

©2026 Zscaler, Inc. All rights reserved.

Executive Summary

Supporting Your CPS 230 Compliance Journey

Prudential Standard CPS 230 Operational Risk Management establishes APRA's expectations that regulated entities maintain resilience against operational risks and severe disruptions. The standard requires institutions to effectively manage operational risk, maintain critical operations within defined tolerance levels, and appropriately manage risks arising from service providers.

For banks and financial institutions, CPS 230 elevates operational resilience from a technology consideration to a prudential obligation directly linked to financial stability, customer outcomes, and Board accountability. Cyber incidents, cloud outages, ransomware events, concentration risk in digital platforms, and third-party failures are considered material operational risks that could disrupt critical banking services.

Modern financial institutions operate increasingly cloud-enabled, SaaS-dependent, and hybrid-workforce environments. Traditional perimeter-based network architectures rely on implicit trust, centralised infrastructure, and hub-and-spoke backhauling, which can introduce structural fragility and increase the likelihood that a cyber event escalates into a disruption of payments, customer access channels, claims processing, custody operations, or other designated critical operations.

Zscaler's Zero Trust Exchange provides a Security Service Edge (SSE) architecture designed to reduce operational risk by eliminating implicit network trust, enforcing identity-based least-privilege access, and inspecting 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 digital resilience rather than reliance on physical perimeter controls.

This document maps CPS 230 requirements to capabilities within the Zscaler Zero Trust Exchange. It outlines how Zscaler's architecture can help APRA-regulated entities strengthen operational risk management, resilience, transparency in governance, and oversight of service providers. Entities remain responsible for determining their own compliance obligations under CPS 230.

©2026 Zscaler, Inc. All rights reserved.

Zscaler Zero Trust Exchange Overview

The Zero Trust Exchange's core design principles include:

- Identity-based, least-privilege access
- Inline inspection of encrypted and unencrypted traffic
- Application-level segmentation
- Centralised policy enforcement
- Globally distributed cloud delivery

The platform supports CPS 230 objectives across four primary capability domains.

Threat Prevention & Technology Risk Controls

Zscaler provides inline inspection and enforcement across the Internet and SaaS traffic, including:

- Secure Web Gateway (SWG)
- Cloud Firewall
- Intrusion Prevention System (IPS)
- Advanced Sandbox
- DNS Security
- Full SSL/TLS inspection across ports and protocols

These capabilities operate as preventive controls that reduce exposure to ransomware, phishing, zero-day malware, command-and-control communications, and encrypted threats before they reach critical banking systems.

Data Protection

The Zero Trust Exchange includes:

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

These capabilities support data governance, reduce exfiltration risk, and enhance oversight of interactions with cloud service providers.

©2026 Zscaler, Inc. All rights reserved.

Monitoring & Risk Visibility

The platform provides:

- Centralised policy engine
- Granular role-based access control (RBAC)
- Administrator activity logging and change history
- Real-time telemetry
- SIEM and SOAR integration
- Zscaler Digital Experience (ZDX) monitoring

These features support transparency in governance, continuous monitoring, and enterprise risk reporting.

Resilience Architecture

Zscaler's architecture:

- Eliminates reliance on centralised VPN concentrators and perimeter appliances
- Provides direct-to-cloud connectivity
- Operates across globally distributed data centres
- Supports Private Service Edge deployment where required
- Segments access at the application layer

This model reduces single points of failure and limits lateral movement during breach scenarios.

How To Use This Guide

The following sections outline key CPS 230 requirements and describe how Zscaler Zero Trust Exchange capabilities may assist regulated entities in meeting operational risk management expectations.

Zscaler provides technical controls, monitoring capabilities, and architectural resilience features that support CPS 230 objectives. Governance accountability, risk appetite setting, tolerance definition, formal Board approvals, and regulatory notification responsibilities remain with the APRA-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 230 Operational Risk Management

Requirement Mapping to Zscaler Zero Trust Exchange

CPS 230 Requirement Mapping

The following pages map CPS 230 requirements to supporting capabilities in the Zscaler Zero Trust Exchange. Each requirement also makes the entity-owned governance or compliance responsibility explicit.

- **CPS 230 Requirement:** The CPS 230 paragraph reference and a summary of the requirement.
- **Entity Responsibility:** Governance, risk ownership, approvals and regulatory accountability that remain with the regulated entity.
- **Zscaler Alignment:** Technical controls, monitoring and architectural capabilities 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 230.

CPS 230 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
RISK MANAGEMENT FRAMEWORK			
CPS230-12	Effectively manage operational risk; maintain critical operations within tolerance; manage service provider risks.	Risk appetite definition, tolerance setting, and formal critical operations designation remain entity responsibilities	Zscaler enforces a cloud-native, zero trust architecture, proxying all traffic through a distributed security service edge. Full SSL/TLS inspection supports deep packet analysis to prevent malware and data exfiltration, while inline DLP and CASB ensure consistent governance over data at rest and in transit. A centralised policy engine further ensures that global security enforcement remains aligned with an entity's internal risk framework. **Maintaining Critical Operations within Tolerance** CPS 230 requires entities to maintain tolerance levels for critical operations. Zscaler's Business Continuity Cloud (BCC) ensures that operations remain within established parameters: • **Redundancy and Isolation:** BCC provides an isolated, customer-specific backup instance allowing seamless failover of connectivity during large-scale disruptions. • **Meeting RTOs and RPOs:** BCC ensures secure access to critical applications during cloud outages via ZIA and ZPA, supporting an entity's RTOs and RPOs. • **Resilient by Design:** Zscaler's architecture eliminates single points of failure to provide the operational resilience required by APRA, with presence in over 160 globally distributed data centres. **Service Provider Risk Management** Zscaler provides comprehensive security and compliance assurance, supporting entities' management of "material service provider" risk as required by CPS 230: • **Compliance Assurance:** Zscaler conducts regular IRAP assessments of its services at the PROTECTED level and maintains numerous other security compliance certifications such as ISO/IEC 27001 and SOC 2. Related documentation is available on Zscaler's Compliance Portal, facilitating entities' due diligence and monitoring obligations under CPS 230. • **SLAs and Governance:** Industry-leading SLAs for availability and performance facilitate fourth-party risk management and ensure governance remains within established tolerances. Live metrics are available on the Zscaler Trust Site.

©2026 Zscaler, Inc. All rights reserved.

CPS 230 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
CPS230-13	Identify, assess and manage operational risks that may result from inadequate or failed internal processes or systems, the actions or inactions of people or external drivers and events	Enterprise risk methodology and operational risk register remain entity-owned	Zscaler provides continuous telemetry across users, workloads, and applications. Correlated insights combine identity and behavioural signals to support dynamic risk scoring, while comprehensive logging and data export functions facilitate integration with risk platforms. **Managing Operational Risk** Zscaler supports entities in addressing "inadequate or failed internal processes or systems" with automated, policy-driven security: • **Identification:** Zscaler Risk360 continuously identifies control gaps and misconfigurations to provide a holistic risk score based on over 100 data points. • **Assessment:** The platform quantifies the financial and operational impact of process failures, enabling teams to prioritise remediation based on risk magnitude. • **Management:** Zscaler automates policy enforcement to reduce configuration errors. During system failures, BCC provides redundancy to maintain critical operations within established tolerances. **Insider Risk & Human Error** Zscaler's identity-based security model manages risks arising from the "actions or inactions of people", addressing both accidental human error and malicious insider threats: • **Identification:** Identity Threat Detection and Response (ITDR) identifies risky behaviours, such as credential theft or lateral movement, and flags inactions like the failure to use MFA. • **Assessment:** Dynamic risk scoring automatically triggers stricter access controls when user behaviour exhibits high-risk characteristics. • **Management:** By enforcing least-privileged access through ZPA, Zscaler ensures that human error or malicious intent does not result in systemic operational failure. **Cyberattack and Supply Chain Protection** Zscaler mitigates risks from "external drivers and events", including sophisticated cyberattacks and disruptions to supply chains and third-party providers: • **Identification:** Zscaler processes over 400 billion daily transactions, identifying global zero-day attacks and emerging threats before they reach entities' environments. • **Assessment:** ZDX provides end-to-end visibility to quickly isolate whether operational disruptions originate from ISPs, SaaS providers, or regional outages. • **Management:** ZPA minimises entities' attack surface by "cloaking" applications from the internet. Zscaler ensures connectivity even during major disruptions by automatically rerouting traffic through a network of over 160 data centers.
CPS230-14	To the extent practicable, prevent disruption to critical operations; adapt processes to continue to operate within tolerance levels and return to normal operations promptly after a disruption.	DR planning and operational recovery execution remain entity-owned	The Zero Trust Exchange (ZTE) supports the "prevent", "return" and "adapt" phases of addressing disruptions as per Requirement 14. Its architecture of over 160 data centres ensures 99.999% availability and high performance, even during regional outages. **Preventing Disruption** Zscaler maintains always-on connectivity through automated performance management: • **Dynamic Performance-based Selection:** Zscaler Client Connector (ZCC) monitors latency to autonomously reroute traffic to the most effective gateway, ensuring uninterrupted performance during brownouts.

©2026 Zscaler, Inc. All rights reserved.

CPS 230 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
			• **Global Cloud Footprint:** A network of over 160 data centres eliminates single points of failure and provides seamless connectivity failover during facility outages. • **Zscaler Resilience Audit:** This proactive service identifies configuration gaps and validates entities' BCP to ensure operational readiness. **Adapting During Disruption** During major disruptions, such as ISP failure, Zscaler maintains system operations within established tolerance levels while ensuring continuous enforcement of security controls: • **Data Centre Selection:** IT teams can manually or programmatically bypass specific regions or data centres to circumvent localised connectivity issues while maintaining continuous Zscaler protection. • **Zscaler Private Service Edge (PSE):** PSEs are local instances deployed on an organisation's premises providing a secure on-ramp during cloud outages and ensuring critical applications remain accessible. • **Disaster Recovery (DR) Mode:** During catastrophic failures, DR mode allows the platform to switch to policy-based access, ensuring that staff maintain secure connections to critical internal applications. **Return to Normal Operations** Following the mitigation stage, Zscaler ensures a controlled and stable return to standard operations: • **Customer-Controlled Restoration:** Administrators can use DNS TXT records to manage service restoration and prevent flapping, ensuring that traffic returns to the primary cloud only after the environment's stability is confirmed. • **Automated Stability Verification:** Zscaler's monitoring tools provide visibility into the health of the restored data centers, enabling a phased and verified return to normal traffic patterns while protecting the user experience.
CPS230-15	APRA entities must not rely on a service provider unless it can ensure that in doing so it can continue to meet its prudential obligations in full and effectively manage the associated risks.	Due diligence, contract terms, and regulatory oversight remain entity-owned	To comply with CPS 230 and similar global prudential regulations, organisations must balance platform efficiency with the mitigation of concentration risk. Zscaler's "Resilience-by-Design" architecture addresses this by ensuring the consolidated stack does not become a single point of failure: **Meeting Prudential Obligations** Zscaler supports compliance with operational resilience and third-party risk requirements through: • **Material Service Provider Management:** Where Zscaler would be considered as a "material service provider" under CPS 230, it can provide necessary transparency, assurance and SLAs to support entities' critical operations. • **Scenario-Based Testing:** Zscaler facilitates mandatory stress testing by simulating outages and triggering "DR mode", ensuring critical operations remain within established tolerance levels. • **Concentration Risk Assessment:** To support concentration risk requirements, Zscaler provides visibility into fourth-party dependencies, such as Tier-1 ISPs and infrastructure providers, enabling accurate systemic risk mapping. **ManagingConcentration Risk** Zscaler mitigates the risk of global outages through architectural decoupling and redundant service delivery: • **Architectural Redundancy:** A distributed architecture across 160+ data centres uses automatic BGP-based rerouting to ensure global availability

©2026 Zscaler, Inc. All rights reserved.

CPS 230 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
			if specific components or regions fail. • **Disaster Recovery (DR) Mode:** Zscaler Client Connector can transition to direct-to-app access using pre-defined emergency policies if the primary cloud becomes unreachable. • **Zscaler Private Service Edge (PSE):** Deploying local instances within customers' environments provides a secure on-ramp for sensitive operations, ensuring internal traffic remains within the perimeter during public cloud disruptions. **Substitutability and Exit Strategies** Zscaler facilitates prudential requirements for vendor transition and exit strategies through: • **Network Decoupling:** As a cloud-native overlay independent of physical network infrastructure, Zscaler enables organisations to revert to direct internet or alternative gateways without extensive network re-architecting. • **Standardised Interoperability:** Zscaler is committed to use of open standards, including SAML, SCIM, IPsec, and GRE, which prevents proprietary lock-in. This simplifies integration with or transition to alternative identity and security providers if required. **Operational Transparency and Continuous Audit** Zscaler provides the evidence of resilience required by regulators through: • **Zscaler Digital Experience (ZDX):** ZDX provides granular visibility into the entire connection path, enabling organisations to identify the precise origin of disruptions and demonstrate operational integrity to regulators. • **Third-party Assurance:** : Zscaler maintains extensive third-party security certifications and attestations which form the basis for operational risk assessments. Further details may be found on Zscaler's Compliance Portal.
CPS230-16	Risk Management frameworks: Oversight, profiling, controls, monitoring and business continuity planning	Risk appetite, BCP governance, and service provider policy ownership remain entity responsibilities	**Governance & Accountability** Zscaler facilitates Board and senior management oversight in accordance with Requirement 16 through: • **Shared Responsibility Model:** Zscaler's shared responsibility model clearly delineates duties between the provider and the regulated entity, supporting the Board in fulfilling its third-party risk oversight obligations. • **Audit-Ready Reporting:** Risk360 generates executive-level dashboards that provide senior management with high-level visibility into security posture and compliance status. • **Governance Data:** Zscaler telemetry integrates with enterprise GRC systems to provide the comprehensive data required for enterprise-wide risk oversight. **Risk Identification & Assessment** Zscaler enables entities to profile operational risks against their risk appetite through: • **Zscaler Risk360:** This risk quantification engine continuously profiles cyber-risk across the organisation. It evaluates over 100 data points to score risks across identity, data, applications, and devices. • **Vulnerability Profiling:** Using Cloud Native Application Posture Control (CNAPP), Zscaler profiles risks within cloud workloads, identifying misconfigurations and vulnerabilities that could lead to operational failure. • **Scenario-Based Assessment:** ZDX provides visibility into critical application paths, enabling entities to profile the potential impact of

©2026 Zscaler, Inc. All rights reserved.

CPS 230 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
			outages or cyberattacks. **Internal Controls and Risk Mitigation** Zscaler supports the risk mitigation component of Requirement 16 through: • **Zero Trust Architecture:** The Zero Trust Exchange (ZTE) enforces least-privilege access, acting as a primary internal control by ensuring users only connect to specific applications rather than the broad network. • **Inline Inspection:** Real-time inspection of encrypted and unencrypted traffic serves as a critical control against data exfiltration, malware, and unauthorised access. • **Identity-Based Controls:** ZPA prevents lateral movement through identity-centric policies, mitigating the risk of large-scale operational disruptions. **Monitoring Performance and Effectiveness** Zscaler enables organisations to monitor control effectiveness and report on their operational risk profile through: • **Continuous Controls Monitoring:** Zscaler provides real-time visibility into control effectiveness, immediately flagging policy bypasses or configuration changes. • **ZDX (Zscaler Digital Experience):** ZDX enables continuous monitoring of the end-to-end user experience. IT teams can track the performance of critical operations, as defined by CPS 230, and detect early indicators of system degradation. • **Automated Escalation:** Integration with SIEM and SOAR platforms automates the monitoring and response process, ensuring any deviations from the risk profile are escalated for management. **Business Continuity Planning** Zscaler supports entities' implementation of their BCP, ensuring availability of critical operations through: • **Zscaler Resilience™:** This suite includes the Business Continuity Cloud (BCC), which provides an isolated secondary data plane designed for CPS 230 compliance. • **Automated Failover:** During "severe but plausible" disruptions, traffic automatically fails over to the BCC. This ensures critical applications remain accessible within defined RTOs. • **Testing Resilience:** Zscaler enables organisations to simulate disruptions to verify that failover mechanisms maintain operational tolerance levels without manual intervention.
CPS230-17	Review operational risk management periodically in line with Requirement 16	Formal review process and sign-off remain entity-owned	Detailed configuration exports, logs, and performance reports provide essential evidence to facilitate risk assessment and governance. Zscaler further supports the review process through: • **Zscaler Risk360:** This executive-level engine provides the Board with a real-time view of the organisation's cyber-risk posture. By translating technical data into risk scores, it enables the Board to monitor alignment with defined risk appetite. • **Executive Reporting Dashboards:** These tools highlight material weaknesses and control gaps, supporting senior management in reporting significant operational risks to the Board as required by CPS 230. • **Shared Responsibility Model:** Clear documentation of duties between Zscaler and the regulated entity facilitates the review of the service provider management component of the risk framework. • **Dynamic Risk Profiling:** The platform automatically updates the risk profile in response to shifts in the threat landscape or internal environment. This ensures that the regular reviews mandated by

©2026 Zscaler, Inc. All rights reserved.

CPS 230 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
			Requirement 17 reflect current operational realities. • **Automated Control Validation:** The Zero Trust Exchange continuously monitors policy enforcement. Any attempts to bypass controls or instances of configuration drift are immediately logged for review. • **Zscaler Digital Experience (ZDX):** ZDX provides operating effectiveness data for critical operations. By isolating failures across internal systems, networks, or third-party providers, it provides the evidence required for formal effectiveness reviews. • **Audit-Ready Telemetry:** Granular transaction logs provide a comprehensive record of control performance. This allows internal and external auditors to verify that controls were operating effectively throughout the entire review period.
CPS230-18	Integrate operational risk into the overall risk management framework	Framework governance remains entity-owned	Zscaler ensures operational risk is integrated into the broader enterprise risk ecosystem, as mandated by Requirement 18, through: • **Zscaler Risk360:** Risk360 translates technical vulnerabilities into financial risk quantification. This allows operational risk to be reported in terms comparable to credit or market risk, facilitating its inclusion in the overall risk management framework. • **API-Driven Ecosystem:** Zscaler integrates with GRC, SIEM, and SOAR platforms via APIs. This ensures that operational risk telemetry is automatically incorporated into the organisation's primary risk management processes. • **Zscaler Digital Experience (ZDX):** ZDX provides a single source of truth for the health of critical operations. It ensures that real-time performance data consistently informs broader risk assessments and strategic decision-making. **Consistency with Recovery and Exit Planning** Zscaler Resilience™ ensures that business continuity plans do not conflict with or undermine recovery and exit planning, as specified in Requirement 18, through: • **Business Continuity Cloud (BCC):** This dedicated, customer-specific backup instance is logically and physically isolated from the primary cloud. It ensures that organisations' RTOs and RPOs are met during global disruptions, directly supporting recovery obligations. • **Policy & Control Consistency:** Unlike traditional methods that may bypass security controls to maintain connectivity, BCC maintains equivalent security policies and access controls during failover. This ensures continuity processes do not undermine the organisation's overall security posture. • **Exit Planning and Data Portability:** Zscaler facilitates orderly transitions through comprehensive audit logs and standardised data formats via the Nanolog Streaming Service. These tools provide a "golden record" of data and policies, ensuring that an exit can be managed without losing historical risk visibility.
CPS230-19	Independent review or remediation where weaknesses exist	Regulatory engagement and remediation program governance remain entity-owned	Refer to the response for Requirement 16 for details.

©2026 Zscaler, Inc. All rights reserved.

CPS 230 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
ROLES AND RESPONSIBILITIES			
CPS230-20-23	Board oversight of controls, risk management, roles and responsibilities	BCP approval and governance remain entity-owned, Impact decision-making remains entity-owned	Refer to the response for Requirement 16 for details.
OPERATIONAL RISK MANAGEMENT			
CPS230-25	Maintain sound IT capability and meet CPS 234	Asset lifecycle governance and CPS 234 program ownership remain entity-owned	Please refer to Zscaler's companion white paper addressing CPS 234 for further details.
CPS230-27	Assessment of operational risk	Scenario facilitation and documentation remain entity-owned	Zscaler provides a comprehensive suite of information systems to monitor, quantify, and report on operational risk: • **Zscaler Risk360:** Risk360 ingests billions of signals to provide a centralised view of the organisation's posture to provide an overview of operational risk. It continuously monitors over 100 risk indicators, such as misconfigured applications and compromised credentials, to satisfy operational risk mandates. • **Zscaler Digital Experience (ZDX):** ZDX monitors the operational health and performance of critical applications from the end-user perspective. It provides real-time availability and latency data, which are essential metrics for assessing operational resilience. • **AI-Powered Analysis:** Machine learning identifies patterns and anomalies across 400 billion daily transactions. This proactively detects emerging risks, including lateral movement attempts or SaaS provider performance degradation. • **Financial Risk Quantification:** Risk360 translates technical vulnerabilities into a financial impact view. By calculating the potential cost of operational failures, it enables risk teams to prioritise remediation based on business impact. • **Executive Dashboards:** These dashboards summarise complex data into Red/Amber/Green indicators and risk scores, allowing senior management to monitor alignment with the defined risk appetite at a glance. • **Trend Analysis and Benchmarking:** Zscaler supports Board reporting by providing longitudinal trend data and industry benchmarking. This context helps the Board determine if risk management performance is improving relative to the broader market. • **Automated Compliance Reporting:** The platform facilitates CPS 230 reporting requirements by generating audit-ready documentation on control effectiveness, incident history, and resilience monitoring.
CPS230-29	Design and implement internal controls	Control attestation remains entity-owned	Zscaler provides the foundational internal control framework for managing technology and data risks. By implementing a Zero Trust architecture, it replaces legacy perimeter security with more resilient, identity-centric controls: • **Least-Privileged Access:** ZPA enforces granular, identity-based controls. Users connect only to authorised applications rather than the broad network, mitigating risks of lateral movement and unauthorised data access. • **Application Cloaking:** Internal applications are made invisible to the public internet through ZPA. This control mitigates the risk of targeted

©2026 Zscaler, Inc. All rights reserved.

CPS 230 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
			attacks and vulnerability exploitation, addressing key external drivers of operational risk. • **Inline Data Protection:** ZIA provides real-time inspection of all traffic, including encrypted data, to prevent exfiltration and block malware. • **Continuous Controls Monitoring (CCM):** Real-time visibility into every transaction ensures that policy triggers or bypass attempts are logged instantly. This provides senior management with objective data on the operating effectiveness of the internal control environment. • **Risk360 Continuous Assessment:** Risk360 monitors over 100 indicators to score control effectiveness and provide a holistic view of the environment's health, identifying issues such as MFA bypasses or unpatched applications. • **Zscaler Digital Experience (ZDX):** ZDX monitors the operational health of the controls themselves. It ensures that security inspection does not degrade the performance of critical operations, verifying control effectiveness without impacting productivity. • **Guided Remediation:** Risk360 provides step-by-step instructions to address identified weaknesses, such as unsanctioned SaaS usage, before they result in a material operational event. • **Automated Policy Enforcement:** One-click policy updates allow for global remediation in seconds. This ensures faster responses than traditional manual firewall changes or infrastructure patching. • **Integration with ITSM/SOAR:** Integration with platforms like ServiceNow and Splunk creates a documented, closed-loop system. This demonstrates to regulators that gaps are identified and remediated in a structured and timely manner.
CPS230-30	Regularly monitor, review and test controls for design and operating effectiveness	Testing governance remains entity-owned	**Continuous Testing vs. Periodic Audits** Requirement 30 mandates that testing frequency align with the frequency of control operation. As security controls operate millions of times daily, Zscaler provides continuous validation through: • **Real-Time Policy Validation:** The Zero Trust Exchange validates controls, including identity, device posture, and data sensitivity, for every access request. Each instance, such as blocking an unauthorised user, is logged immediately as an automated test result for that transaction. • **Risk360 Control Scoring:** Risk360 continuously assesses the environment against over 100 indicators to verify both the existence and effectiveness of individual policies, such as identifying shadow IT applications that may be bypassing CASB controls, providing an ongoing assessment of control coverage across the internal environment. **Active Testing via Zscaler Deception** Zscaler supports the "active testing" of detection and response controls, as required by Requirement 30, through: • **Decoy-Based Testing:** By deploying honeytokens and decoys (fake applications, servers, or credentials), Zscaler provides a continuous test of an organisation's internal detection capabilities. Any interaction with these decoys serves as real-time validation of control effectiveness. • **Simulating Lateral Movement:** Monitoring decoy interactions provides empirical data on the effectiveness of least-privilege access controls. This approach delivers the adversarial testing that APRA expects for high-materiality risks, such as ransomware. **Testing Resilience and BCP Controls** Reflecting the focus on business continuity within CPS 230, Requirement 30 mandates the testing of controls that safeguard "critical operations":

©2026 Zscaler, Inc. All rights reserved.

CPS 230 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
			• **Resilience Audit Service:** Zscaler provides specialised services to assist entities in testing Business Continuity Cloud (BCC) failover. This enables organisations to simulate "severe but plausible" cloud outages and verify that failover controls perform as intended. • **ZDX Baselines:** ZDX serves as a "control group" for testing by establishing performance baselines for critical applications. This allows teams to determine if changes to the IT environment have degraded operational controls or impacted the user experience. **Evidence for Independent Testing** Requirement 30 often informs the work of internal and external auditors who must "test the testers": • **Granular Telemetry & Logging:** Zscaler provides high-fidelity, tamper-proof logs via the Nanolog Streaming Service. This provides external auditors with the "evidence of testing" to verify control effectiveness throughout the audit period, rather than a limited point-in-time snapshot. • **Configuration Change History:** Zscaler tracks every change made to security policies, allowing auditors to verify that only authorised personnel have modified the internal control environment.
CPS230-31	Remediate material weaknesses in its operational risk management, including control gaps, weaknesses and failures	Root cause governance remains entity-owned	**Timely Identification of Incidents** Requirement 31(a) stipulates that organisations must implement processes to "identify" incidents promptly to minimise impact. Zscaler facilitates a transition from reactive monitoring to proactive detection by identifying early indicators before they escalate into user-reported disruptions: • **Zscaler Digital Experience (ZDX):** ZDX is the primary tool for identifying operational availability or performance incidents. By monitoring the end-to-end path of critical operations, ZDX identifies application failure or performance degradation immediately, often before users are impacted. • **AI-Powered Threat Detection:** To address 'security-driven' operational incidents such as ransomware or data breaches, Zscaler's AI engine analyzes 400+ billion daily transactions to identify anomalies, lateral movement, or unauthorised data exfiltration in real-time. • **Identity Threat Detection and Response (ITDR):** ITDR identifies identity-based incidents, such as credential theft or privilege escalation, which are leading indicators of systemic operational failures. **Escalation and Notification** Under CPS 230, regulated entities must notify APRA of a material operational risk incident as soon as possible, and no later than 72 hours after becoming aware of the event: • **Automated Alerting & SIEM Integration:** Zscaler integrates with SIEM/SOAR platforms to automate escalation. High-severity detections trigger workflows to notify risk and compliance teams, ensuring the 72-hour regulatory window is managed effectively. • **Incident Impact Assessment:** Zscaler identifies the "blast radius" of an incident by detailing the affected users, applications, and datasets. This visibility assists senior management in determining whether an incident meets the "materiality" threshold for reporting. **Root Cause Analysis** Requirement 31(c) stipulates that entities to determine the root cause of incidents to prevent recurrence: • **Granular Telemetry & Forensic Logging:** The Nanolog Streaming Service (NSS) generates a detailed record of every transaction, enabling teams to examine the precise sequence of events during incident reviews. This high-fidelity evidence supports comprehensive root cause analysis,

©2026 Zscaler, Inc. All rights reserved.

CPS 230 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
			covering everything from initial connection attempts to final data flows. • **ZDX Deep Tracing:** For performance-related incidents, ZDX provides a hop-by-hop view of the network path. It can determine whether an incident was caused by an internal process failure, a third-party ISP, or a SaaS provider: a critical capability for meeting the service provider oversight requirements of CPS 230. **Remediation and Preventing Recurrence** The final component of Requirement 31 mandates that organisations remediate incidents and implement measures to prevent their recurrence. • **Dynamic Policy Updates:** Zscaler enables immediate, global policy updates once a root cause, such as an over-privileged user or an insecure application, is identified. This "closed-loop" remediation ensures that the vulnerability is closed across the entire enterprise in seconds. • **Risk360 Post-Incident Scoring:** Following incident resolution, Risk360 verifies the effectiveness of remediation efforts. By updating the organisation's risk score to reflect the enhanced control environment, it provides the Board and APRA with tangible evidence of 'lessons learned'.
CPS230-32	Operational risk incidents and near misses are identified, escalated, recorded and addressed in a timely manner	Incident management framework remains entity-owned	**Identifying "Severe but Plausible" Scenarios** Requirement 32 requires entities to identify specific events that could realistically disrupt critical operations. • **Zscaler Risk360:** Risk360 identifies an organisation's primary "control gaps", such as unpatched internet-facing assets or high-risk users. This data enables risk teams to construct realistic scenarios, including credential-stuffing attacks on primary SaaS providers or the total loss of legacy VPN infrastructure. • **Third-Party Risk Modeling:** Zscaler identifies "fourth-party" dependencies by mapping critical applications to their underlying cloud providers. This visibility allows entities to model systemic outages as 'severe but plausible' scenarios. **Assessing Control Adequacy** Requirement 32 stipulates that entities evaluate existing controls' sufficiency to handle major disruptions: • **Risk Mitigation Simulation:** Using Risk360, organisations can conduct "what-if" simulations to model how ransomware scenarios change when transitioning from flat networks to ZPA. By quantifying the resulting reduction in financial risk exposure, the platform provides empirical evidence of control adequacy. • **Deception Scenarios:** Zscaler Deception uses decoys and honeytokens to enable active scenarios that test organisational resilience. These simulations monitor the movement of a simulated attacker to validate whether detection and isolation controls are sufficient to stop an operational incident before it becomes material. **Testing Resilience via Simulation** Scenario analysis facilitates the validation of business continuity planning (BCP) as mandated elsewhere in CPS 230: • **Zscaler Resilience Audit:** Zscaler can assist entities in conducting disruption scenarios: by simulating primary cloud failures or major ISP outages, the service verifies that Business Continuity Cloud (BCC) failover mechanisms perform as designed. • **ZDX Scenario Modeling:** ZDX enables organisations to simulate performance 'blackouts' or 'brownouts' for critical operations such as payment gateways. This provides the data required to assess whether an entity can maintain "minimum service levels" as specified in Requirement 38c.

©2026 Zscaler, Inc. All rights reserved.

CPS 230 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
			Quantifying Impact for Board Reporting Requirement 32 requires that the results of scenario analysis inform the broader risk management framework and Board oversight: • **Financial Risk Quantification:** Zscaler converts technical scenarios into financial metrics. Teams can use these statistics to articulate the effectiveness and ROI of security initiatives, facilitating better-informed Board decisions. • **Objective Evidence:** Logs and reports generated during simulations provide the objective evidence required by APRA and internal auditors to validate that an entity is proactively testing resilience in accordance with Requirement 32.
BUSINESS CONTINUITY			
CPS230-34-37	Define critical operations, minimise disruption to critical apps, maintain BCP to tolerance levels and return to normal operations after a BCP event.	Critical operations register remains entity-owned	**Defining Critical Operations** CPS 230 Requirements 34 and 35 mandate that entities maintain a register of critical operations, defined as those having a material impact on customers or the financial system if disrupted. • **Zscaler Digital Experience (ZDX):** ZDX provides the real-time telemetry needed to build and validate the Critical Operations Register. By identifying enterprise applications, mapping dependencies, and quantifying usage, the platform enables risk teams to define critical operations objectively based on actual business traffic and impact. • **Dependency Mapping:** Zscaler identifies "fourth-party" risks by showing which critical operations depend on specific cloud providers or external networks, ensuring the register accounts for hidden systemic vulnerabilities. **Minimizing Disruption to Critical Apps** The Zero Trust Exchange's architecture is designed for high availability, minimising the likelihood that a disruption reaches a critical operation: • **Global Distributed Architecture:** With over 150 data centers globally, Zscaler's "Next-Hop" routing automatically bypasses localised internet outages or data center failures. • **Zscaler Resilience™:** The Zscaler Resilience suite includes Dynamic Path Selection to detect network 'brownouts' or performance degradation. The platform automatically reroutes traffic to healthier paths before user experiences or critical operations are significantly impacted. • **App Cloaking:** ZPA renders critical applications invisible to the public internet. This cloaking minimises disruptions caused by external threats such as DDoS attacks or targeted ransomware. **Maintaining BCP to Tolerance Levels** Requirement 34(c) mandates that entities maintain a BCP detailing how operations are managed within defined tolerance levels during disruptions. Zscaler facilitates these objectives through the following capabilities: • **Business Continuity Cloud (BCC):** Zscaler BCC provides a dedicated, customer-specific backup instance that is logically and physically isolated from the primary Zscaler cloud. In the event of a "severe but plausible" event, such as a global cloud provider outage, traffic fails over to the BCC. • **Sustaining Minimum Service Levels:** BCC maintains consistent security policies and access controls during failover. This ensures critical operations remain secure and aligned with an entity's risk appetite and tolerance levels, unlike traditional solutions which may "fail open", bypassing security controls.

©2026 Zscaler, Inc. All rights reserved.

CPS 230 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
			• **Real-time Tolerance Monitoring:** ZDX continuously monitors application performance against predefined thresholds. If a critical operation drops below its "minimum service level," ZDX triggers immediate alerts, allowing for rapid BCP activation. **Returning to Normal Operations** CPS 230 stipulates that entities establish clear processes for returning to normal operations following a disruption: • **Automated Failback:** Zscaler's architecture supports a seamless, automated "failback" process. Once the Zscaler Client Connector or App Connector detects that the primary cloud path is stable, it automatically reverts traffic from the BCC to the primary instance. • **Seamless User Experience:** The failback process is transparent to users and requires no re-authentication or system restarts. This ensures the return to normal operations does not cause secondary disruptions or impact productivity. • **Post-Event Evidence:** Granular logging provides a comprehensive record of the event, documenting the commencement of the disruption, failover performance, and the restoration of normal operations. This objective data supports the post-incident reviews mandated by CPS 230.
CPS230-38	Establish tolerance levels (time, data, service)	Tolerance definition remains entity-owned	**Defining Minimum Service Levels** Requirement 38(c) requires entities to specify the "minimum service levels" maintainedn while operating under alternative arrangements: • **Zscaler Digital Experience (ZDX):** ZDX provides the granular telemetry needed to define these baselines. By measuring metrics such as latency, page fetch time, and DNS resolution, ZDX allows organisations to set objective, data-driven minimum service levels for critical applications such as core banking systems or customer portals. • **ZDX Score:** The platform utilizes a standardised health score from 0 to 100 that maps directly to CPS 230 tolerance levels. This allows entities to define minimum service levels numerically, ensuring that any performance decline into 'poor' categories is immediately identified as a breach of tolerance. • **Real-User Monitoring (RUM):** ZDX provides continuous monitoring of service levels, ensuring that alternative arrangements such as remote work or failover paths actually meet defined performance thresholds. This replaces point-in-time audits with real-time validation of operational resilience. **Supporting Recovery Time Objectives (RTO)** Requirement 38(a) focuses on the maximum period of time an entity can tolerate a disruption, known as RTO: • **Zscaler Resilience™ & Business Continuity Cloud (BCC):** Zscaler BCC provides an isolated, secondary data plane that remains active and ready for immediate failover. This architecture assists entities in meeting aggressive RTOs by providing a pre-configured backup path for critical application access through ZIA/ZPA. • **Automated Failover/Failback:** By automating the transition to the BCC during severe but plausible events, the platform minimises the duration of disruptions. This ensures that essential security and connectivity services are restored within the defined tolerance window. **Maintaining Data Integrity** Requirement 38(b) mandates the maximum extent of data loss an entity will accept, also known as RPO. Zscaler supports the integrity of data throughout the recovery process:

©2026 Zscaler, Inc. All rights reserved.

CPS 230 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
			• **Inline Data Loss Prevention (DLP):** Zscaler ensures data remains protected during business continuity events or while operating under alternative arrangements. By preventing unauthorised exfiltration during disruptions, the platform ensures that recovery efforts do not lead to secondary data integrity or compliance failures. • **Encrypted Traffic Inspection:** The platform maintains comprehensive inspection of SSL and TLS traffic during failover. This prevents malicious actors from exploiting disruptions to corrupt or steal critical data, helping entities adhere to defined RPO standards. **Alerting and Compliance Reporting** CPS 230 mandates that boards and senior management are notified of any breaches to established tolerance levels: • **Dynamic Alerting:** Zscaler allows risk teams to configure Alert Rules based on their CPS 230 tolerance levels. Should performance or availability fall below minimum service levels, the platform triggers automated notifications via SIEM, SOAR, or ITSM systems. • **Risk360 Reporting:** Risk360 aggregates performance and security metrics into executive-ready dashboards. This provides boards with the objective evidence required to demonstrate that critical operations are managed within established tolerance levels during mandated regular reviews.
CPS230-40	Maintain credible BCP	BCP documentation and communication planning remain entity-owned	**Execution and Monitoring of Business Continuity Plans (BCPs)** Requirement 40 mandates that entities maintain the capability to execute BCPs, monitor compliance with tolerance levels, and report failures to the board alongside remediation plans: • **Execution Capability:** Zscaler facilitates BCP execution through documented escalation processes, operational guidance, and security features such as role-based access control and administrative auditability. These resources support controlled "break glass" procedures and emergency changes during disruptions. • **Resilience and Technology:** Zscaler provides detailed service documentation regarding its architectural resilience, supported by formal SLAs and real-time incident communications. These assets assist entities in refining their continuity planning and incident response playbooks. • **Tolerance Monitoring:** Zscaler delivers the telemetry and logs required to monitor performance against defined tolerance levels. Integration with ZDX and SIEM platforms enables entities to track critical indicators such as access success rates, latency, and service degradation. • **Reporting and Remediation:** Zscaler provides incident notifications, root-cause analyses, and support-case timelines to support board reporting and remediation planning. These materials enable entities to document impact versus tolerance while identifying contributing factors and corrective actions.
CPS230-41-43, 45, 46	BCP execution, testing, review and oversight	Exercise governance remains entity-owned	**Comprehensive Testing & Service Provider Integration** Requirements 41 and 42 mandate 'severe but plausible' testing that incorporates dependencies on material service providers: • **Zscaler Resilience Audit):** Zscaler provides a structured service to simulate "blackout" scenarios, such asa total loss of a cloud instance or regional ISP. This shifts testing from theoretical desktop exercises to physical failover validation, ensuring operational preparedness. • **Dependency Mapping:** ZDX maps the end-to-end path of critical operations, identifying dependencies on fourth-party providers such as AWS, Azure, or specific ISPs. This allows entities to include these external dependencies into BCP tests, verifying that the failover to the BCC

©2026 Zscaler, Inc. All rights reserved.

CPS 230 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
			bypasses these points of failure. **Analysing Results and Remediating Gaps** Requirement 43 mandates that entities investigate test failures and remediate identified gaps in a timely manner. • **Forensic Telemetry:** Should a BCP test fail to meet RTOs, ZDX provides the forensic telemetry required to identify the precise cause of the failure, such as DNS resolution delays or misconfigured backup paths. • **Closed-Loop Remediation:** Zscaler facilitates streamlined remediation through global policy updates. This ensures that corrective actions are documented and applied enterprise-wide, providing the audit trail of lessons learned, which supports the testing stipulated by Requirement 43. **Maintaining and Updating the BCP** Requirement 45 requires the BCP to be updated based on test results and changes in the operational environment. • **Automated Policy Sync:** Zscaler maintains the technical relevance of the BCP by synchronising security and access policies between the primary environment and the BCC. This prevents policy drift, ensuring that backup paths remain aligned with ongoing production changes. • **Material Change Triggers:** ZDX identifies the emergence of new critical applications or evolving traffic patterns. These insights provide risk teams with the data-driven triggers necessary to perform out-of-cycle BCP updates, as stipulated in Requirement 45. **Board and Senior Management Oversight** Requirement 46 mandates that the results of testing be reported to the board and senior management to facilitate effective oversight of operational resilience. • **Risk360 Resilience Scoring:** Risk360 converts technical test data, such as failover times, application health, and control effectiveness, into an executive-level Resilience Score. This metric provides a high-level overview of the entity's ability to maintain operations during a disruption. • **Audit-Ready Reporting:** Zscaler generates standardised reports that document test scenarios, performance against defined tolerance levels, and the status of any remediations. This provides the board with the objective evidence they need to fulfill governance obligations under CPS 230.
MANAGEMENT OF SERVICE PROVIDER ARRANGEMENTS			
CPS230-47-49	Service provider management and register, identification of material providers.	Register ownership remains entity-owned	Service Provider ManagementRequirement 47 expects entities to maintain a policy for identifying material service providers and managing the risks associated with those arrangements. Zscaler provides the necessary documentation to support the development and evidence of this policy, including security and privacy audit certifications, service specifications and operational process summaries. These resources enable entities to integrate Zscaler's resilience and availability information directly into their broader control frameworks: • **Supplier Agreement Lifecycle Planning:** Requirement 48(a) addresses the monitoring, substitution, and exit of service arrangements. Zscaler supports these requirements through comprehensive service descriptions, SLA terms, and telemetry export mechanisms for ongoing monitoring. To facilitate orderly transitions, the platform provides configuration export paths, logging retention options, and documented offboarding practices that inform customer exit strategies. • **Supplier Risk Management and Governance:** Under Requirement 48(b), entities must manage the operational risks associated with material service providers. Zscaler assists by providing platform features that

©2026 Zscaler, Inc. All rights reserved.

CPS 230 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
			reinforce governance controls, such as role-based administration, administrative auditing, and policy segmentation. Integration guidance for identity providers and SIEM/SOAR platforms ensures that entities can maintain robust monitoring, detection, and oversight capabilities. • **Fourth-Party Transparency:** Requirement 48(c) focuses on managing fourth-party risks. Zscaler provides transparency through formal subprocessor disclosures and established mechanisms for notifying customers of changes. This compliance documentation allows entities to assess and monitor the risks introduced by Zscaler's own dependencies effectively. • **Register of Material Service Providers:** Requirement 49 stipulates that entities maintain a centralised register of material service providers. Zscaler supplies the essential information required for these entries, including service scope, contractual attributes, data processing artefacts, and escalation models. This data enables entities to link register entries to their risk assessments, monitoring approaches, and BCP assumptions.
CPS230-53	Due diligence before material arrangements	Formal due diligence governance remains entity-owned	**Security and Privacy Assurance** Zscaler provides comprehensive security and privacy assurance documentation, including SOC 2 and ISO/IEC 27001 certifications and IRAP assessment reports, to support an entity's supplier risk assessments. These resources encompass platform architecture overviews, documented management processes for changes and incidents, and formal SLAs. Furthermore, Zscaler cooperates with entities' third-party SaaS assessment processes to ensure regulatory transparency and alignment with internal risk frameworks. Please visit Zscaler's Trust Site and Compliance Portal for further information. **Managing Single-Platform Concentration Risk** Zscaler mitigates risks that arise from single platform concentration, such as catastrophic global outages, through architectural decoupling and technical redundancy: • **Distributed Architectural Redundancy:** Unlike legacy single-instance solutions, Zscaler operates a distributed cloud across more than 160 data centres. In the event of a regional disruption, automated BGP-based rerouting directs traffic to the nearest healthy node, ensuring the platform remains globally available even if specific components fail. • **Disaster Recovery (DR) Mode:** Zscaler Client Connector includes a 'DR Mode' as a critical emergency capability. Should the primary cloud environment become unreachable, this feature enables secure, direct-to-application access based on pre-defined emergency policies, ensuring continuity during extreme scenarios. • **Zscaler Private Service Edge (PSE):** For highly sensitive operations, entities can deploy Zscaler Private Service Edge on private hardware or within private cloud environments. This provides a local on-ramp that ensures internal traffic remains within the organisational perimeter even if the public cloud is disrupted.
CPS230-54-55	Contractual requirements and APRA access	Contract negotiation and APRA access rights remain entity-owned	**Contractual Framework for Material Arrangements** Zscaler provides a formal contractual framework for "material arrangements" with an entity. Documentation included stipulates service levels, roles and responsibilities, and data handling protocols. The framework also establishes provisions for audit and assurance, dispute resolution, termination, and liability, while providing a structured approach for managing subcontracting: • **Agreement Documentation and Data Governance:** The contract suite comprises the service agreement, order forms, and specific product schedules. These documents delineate service levels and support

©2026 Zscaler, Inc. All rights reserved.

CPS 230 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
			commitments through formal SLAs. Additionally, data protection and privacy terms specify ownership, confidentiality, and retention policies, while security documentation clarifies the shared responsibility model and control frameworks. Formal subprocessor disclosures and notification mechanisms ensure ongoing transparency regarding third-party involvement. • **Regulatory Cooperation and Access:** Zscaler provides security and privacy assurance documentation which includes independently audited reports and certifications. These resources provide the objective evidence necessary to fulfil regulatory obligations and are accessible via Zscaler's Trust Site and Compliance Portal. Data export mechanisms in Zscaler services enable entities to produce information as requested by APRA. While on-site access provisions are subject to negotiation, Zscaler supports these commitments through agreed access mechanisms and evidence collection routes.
CPS230-56	Ongoing provider risk and exit	Exit governance remains entity-owned	**Risk Management in Material Arrangements** Requirement 56 mandates that entities identify and manage risks associated with material service providers to ensure ongoing service delivery and operational resilience. Zscaler supports these obligations through its secure, distributed architecture and independently audited certifications, which provide the transparency necessary to manage third-party risks: • **Security Architecture and Administrative Controls:** The Zscaler platform is securely architected with robust mechanisms for tenant isolation, encryption, key management and data protection, which are also detailed in customer-facing resources. Administrative features include audit logs and guidance on role-based access and least-privilege principles. Furthermore, integration documentation for Identity Providers (IdP) and SIEM platforms, alongside secure configuration hardening guides, ensures that entities can maintain a resilient and well-governed environment. • **Incident Management and Operational Continuity:** Operational resilience is supported by documented incident communication processes and real-time service status updates. Zscaler provides documentation detailing its BCP and DR controls including redundancy and operational support models. The ZTE platform offers telemetry and logging outputs, such as log streaming and SIEM integrations, which support proactive monitoring and oversight, facilitating rapid detection and triage. • **Exit Planning and Transition Support:** Zscaler provides configuration export APIs and tools designed to extract policies and administrative settings, which facilitates exit planning Log streaming capabilities ensure that evidentiary records are maintained during transition periods, while documented offboarding processes and data retention policies provide a clear framework for decommissioning. Architectural documentation further assists entities in developing comprehensive transition and substitution strategies.
CPS230-58	Monitor provider performance and controls	Compliance governance remains entity-owned	**Assessment of Performance** Zscaler enables entities to move beyond reliance on service providers' internal status pages by providing independent, real-time data on application performance. This transparency ensures that oversight is based on objective metrics rather than provider-reported availability: • **Objective Performance Monitoring:** ZDX generates an objective performance score for material service providers, such as Microsoft 365, Salesforce, and AWS, as well as bespoke applications. By monitoring the complete network path from the user to the application, ZDX provides comprehensive visibility into the end-to-end performance of critical

©2026 Zscaler, Inc. All rights reserved.

CPS 230 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
			services. • **Independent Verification and Evidence:** Entities can track specific metrics, including latency, packet loss, and DNS resolution times, associated with a service provider's infrastructure. This data provides the objective evidence required to verify uptime claims and address performance degradation, facilitating informed discussions with providers regarding SLA compliance. • **Granular Performance Alerting:** Requirement 57 stipulates that entities must monitor performance with reference to agreed service levels. ZDX supports this by allowing the configuration of custom alerts based on the precise thresholds defined in service contracts. These notifications provide immediate awareness if a provider's performance falls below stipulated levels, ensuring proactive governance and operational oversight. **Effectiveness of Controls** Zscaler provides the control mechanisms and visibility necessary to evaluate their performance. This dual capability supports the ongoing assessment of risk controls as mandated by the entity's operational risk framework: • **Zero Trust Connectivity and Monitoring:** ZPA enforces least-privileged connectivity for service providers requiring access to an entity's environment. The effectiveness of these controls can be monitored through detailed access logs, ensuring that lateral movement is prevented and that access remains restricted to authorised applications and segments. • **Data Protection and Governance:** Zscaler's CASB and DLP engines monitor data flows to third-party providers. Control effectiveness is assessed by reviewing the volume of sensitive data transfers that were blocked or sanitised in accordance with established risk policies, ensuring that data handling remains compliant with entities' risk policies. • **Security Posture and Configuration Integrity:** For entities utilising SaaS-based service providers, Zscaler SaaS Security Posture Management (SSPM) conducts regular scans of provider configurations, such as Microsoft 365 or ServiceNow. This process identifies configuration drift and ensures that the security controls within the provider's platform remain effective and aligned with the entity's risk appetite. • **Continuous Monitoring and Auditability:** CPS 230 emphasises the necessity of regular control assessments. Zscaler's centralised logging maintains a continuous audit trail, providing the reports necessary to demonstrate that security policies were active, threats were blocked, and encryption protocols were maintained throughout the assessment period.
CPS230-59	APRA notification of agreements/offshoring	APRA notification remains entity-owned	**Due Diligence and Security Assurance** Prior to notifying APRA of a new material arrangement, an entity must conduct rigorous due diligence to assess the service provider's suitability. Zscaler facilitates this requirement by providing comprehensive documentation and independent assessments that validate its security controls and operational maturity: • **IRAP Assessment:** Zscaler undergoes periodic IRAP assessments at the PROTECTED level, performed by a registered independent assessor. These assessment artefacts provide the necessary assurance that the platform adheres to the stringent security standards required by Australian government agencies and financial services organisations. • **Global Compliance Certifications:** Zscaler maintains an extensive portfolio of global compliance certifications, including SOC 2 Type II and ISO/IEC 27001. These reports provide entities with the objective evidence needed to evaluate Zscaler's control environment and ensure alignment

©2026 Zscaler, Inc. All rights reserved.

CPS 230 Requirement		Shared Responsibility & Zscaler Alignment	
Para	**Requirement**	**Entity Responsibility**	**Zscaler Alignment**
			with internal risk management policies. **Materiality and Operational Resilience** Under CPS 230, Zscaler is generally designated as a "material service provider", as it delivers critical security infrastructure essential for an entity's safe and continuous operation. To mitigate risks associated with this materiality, Zscaler provides the architectural resilience and contractual guarantees necessary to support an entity's operational risk profile: • **High Availability and Architectural Resilience:** The Zero Trust Exchange is a globally distributed cloud architecture designed to achieve 99.999% availability. This high-availability design supports an entity's operational resilience objectives by ensuring that critical security functions remain performant and available, even during periods of high demand or localised disruption. • **Service Level Agreements (SLAs):** Zscaler provides robust SLAs for latency and uptime, offering the verifiable metrics required to demonstrate to APRA that the service provider does not introduce unacceptable operational risk. **Offshoring & Data Sovereignty** Requirement 59(b) stipulates that entities must manage the specific risks associated with offshoring arrangements. Zscaler supports these requirements through: • **Local Infrastructure and Data Residency Controls:** Zscaler maintains a significant presence within Australia, with data centres located in Sydney, Melbourne, Canberra, Brisbane, Perth, and Adelaide. This local infrastructure, combined with configurable data residency controls, allows entities to specify where their data is processed and stored. These features provide the transparency necessary to accurately report on offshoring status to APRA. **Continuous Supply Chain Monitoring** CPS 230 mandates that entities continuously monitor their material service providers to ensure ongoing operational resilience. Zscaler facilitates this through a platform-wide approach to visibility and performance management. ZDX enables organisations to monitor the real-time performance of their entire digital ecosystem, including other material service providers such as SaaS applications, providing evidence to demonstrate broader supply chain oversight.
CPS230-60	Internal audit review of outsourcing	Audit independence and reporting remain entity-owned	**Audit Support and Evidence Collection** Zscaler provides all relevant compliance certifications and attestations while supporting an entity's supplier assessment processes. The platform enables the generation of audit-ready evidence such as through configuration exports, telemetry, and RBAC records. These resources streamline the assessment process, ensuring that entities can demonstrate a robust and well-governed control environment to both auditors and regulators.

©2026 Zscaler, Inc. All rights reserved.

Next Steps

Zscaler works with APRA-regulated entities across Australia to align zero trust architecture with operational resilience obligations. To discuss how Zscaler can support your CPS 230 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 234 Companion Guide:** Using the Zscaler Zero Trust Exchange to Support Compliance with CPS 234 Information Security

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 230 Operational Risk Management, including governance oversight, risk assessment, independent testing, and regulatory notification.

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.