Kiteworks

COMPLIANCE BRIEF

Kiteworks Supports Australia's Prudential Standard CPS 230 Operational Risk Management

Operational Resilience, Audit-Ready, for APRA-Regulated Entities

Solution Highlights

- Hardened Virtual Appliance
- Data Policy Engine with ABAC and RBAC
- Comprehensive Audit Logs With SIEM Feeds
- Real-Time Logs
- Data Sovereignty and Geofencing

Prudential Standard CPS 230 Operational Risk Management is made by APRA under the Banking Act 1959, Insurance Act 1973, Life Insurance Act 1995, Private Health Insurance (Prudential Supervision) Act 2015, and Superannuation Industry (Supervision) Act 1993. CPS 230 took effect 1 July 2025 under APRA's 2023 determination. APRA has since reissued it via Determination No. 1 of 2026 (23 April 2026, delegate Ian Beckett), revoking the 2023 determination as varied in 2024; the reissued standard commences 1 July 2026 as a refresh, not a new obligation. It applies to all APRA-regulated entities, including ADIs, foreign ADIs, general and life insurers, friendly societies, private health insurers, RSE licensees, and authorised NOHCs. For foreign ADIs, Category C insurers, and EFLICs, obligations apply only to Australian branch operations. CPS 230 specifies no monetary fines; APRA enforces via supervisory powers and mandatory 72-hour, 24-hour, and 20-business-day notification timelines. Here's how Kiteworks supports Australia's CPS 230 obligations:

Hardened Appliance for Sound IT Capability

Paragraph 24 of CPS 230 requires sound IT capability to support critical operations and manage technology risks; Paragraph 28 requires embedding internal controls to mitigate operational risk. Kiteworks addresses Paragraph 24 through the Virtual Appliance With Built-in Hardening and Defense in Depth: enterprise-grade encryption, an embedded network firewall and WAF with automated updates, intrusion detection, file integrity monitoring (FIM), and zero-trust exchange between services. The Comprehensive Dev SecOps "Shift Left" capability tracks third-party vulnerabilities and applies FIM-based detection and patching. For Paragraph 28, the Data Policy Engine enforces ABAC runtime policies aligned to the NIST CSF framework, letting admins define context-aware risk policies across data exchange channels: requiring SafeEDIT or SafeVIEW, blocking an action, or requiring approval. Authorization combines RBAC (permission sets) with ABAC (dynamic, attribute-based access).

Runtime Risk Policies and Service Provider Governance

CPS 230's remaining obligations span tolerance, governance, business continuity, and service provider oversight, which Kiteworks operationalizes as follows. Paragraph 13 (tolerance/disruption) is met through MFT Server cluster high availability without single points of failure, Hardened Virtual Appliance clustering, and cluster reboot/recovery. Paragraphs 15 (governance) and 26 (risk data monitoring) are addressed by ABAC runtime policies aligned to the NIST CSF framework and security analytics via the CISO dashboard and Splunk app. Business continuity duties, such as Paragraphs 33 and 40, draw on high availability, storage replication, database backup, and vault-to-vault integration. Service provider duties, such as Paragraphs 48 and 60, use vault-to-vault integration, repositories gateway, admin reporting, and data sovereignty/geofencing. Paragraph 31 applies AI-based intrusion and anomaly detection and embedded MDR. The remaining board oversight and service-provider policy duties, such as Paragraph 12 and Paragraph 44, stay organizational obligations administered directly.

From Real-Time Logs to APRA Notification Windows

CPS 230 sets strict notification duties: Paragraph 32 requires notifying APRA within 72 hours of a material incident; Paragraph 41, within 24 hours of a critical-operation disruption; Paragraph 60, within 20 business days of a critical service agreement change. Kiteworks supports the 72-hour window through log timeliness (entries append immediately, feeding syslogs and Splunk in real time) and comprehensive audit logs with SIEM feeds (unlike competitors that delay entries up to 72 hours), plus real-time threat intelligence notifications. For the 24-hour notification, service-down alerting and log timeliness supply the evidence. A broader set of paragraphs across tolerance, governance, IT capability, and business continuity, such as Paragraph 29 and Paragraph 33, carry tracking obligations, addressed through comprehensive audit logs with SIEM feeds (cleaned, normalized, aggregated into a real-time stream), the compliance report – audit log, security analytics, compliance summary reports, node health dashboards, connection usage monitoring, and admin reporting exportable via CSV, producing on-demand records for board and APRA accountability.

Kiteworks gives APRA-regulated entities a practical path through CPS 230's operational resilience obligations. The virtual appliance pairs enterprise-grade encryption, firewalls, and intrusion detection with Data Policy Engine controls that enforce risk policies at runtime. High availability, storage replication, database backup, and vault-to-vault integration keep critical operations running, while service provider governance and data sovereignty controls manage third-party risk. Real-time log timeliness, audit logs with SIEM feeds, and monitoring dashboards evidence incidents inside APRA's reporting windows. Kiteworks operates as one unified platform, turning CPS 230's requirements into repeatable, auditable practice.

Ready to Meet APRA's CPS 230 Notification Windows?

www.kiteworks.com

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.