AWS INCIDENT RESPONSE

APRA CPS 234 on AWS: Notification, Material Weakness, and the CPS 230 Overlay

APRA-regulated entities have 72 hours to notify a material information security incident — and 24 hours under CPS 230 if customer-facing operations are affected. This is the practical playbook for AWS workloads in ap-southeast-2 and ap-southeast-4.

AUSTRALIA

By Matt Gurr
12 May 2026

ghostvector.ai/guides

GHOST VECTOR — GUIDE

APRA CPS 234 on AWS: Notification, Material Weakness, and the CPS 230 Overlay

TL;DR

APRA Prudential Standard CPS 234 imposes a **72-hour notification** obligation for material information security incidents on Australian banks, insurers, and superannuation funds. CPS 230, effective from 1 July 2025, adds a **24-hour notification** for material operational risk events — which most cyber incidents now trigger. The 24-hour clock controls in practice. Hitting it on AWS requires a documented materiality model that an operations team can apply at 2am, a board-approved incident commander with standing notification authority, and an evidence stack in ap-southeast-2 or ap-southeast-4 that can quantify customer impact within hours. This guide covers what CPS 234 and CPS 230 actually require, how to read them together, and the AWS-specific operational changes that follow.

What CPS 234 actually requires

CPS 234 is the prudential standard governing information security for APRA-regulated entities. It has been in force since **1 July 2019** and applies to:

- Authorised Deposit-taking Institutions (ADIs) — banks, credit unions, building societies
- General insurers
- Life insurance companies
- Private health insurers
- Registrable Superannuation Entities (RSEs)
- Authorised Non-Operating Holding Companies

Two notification obligations sit at the heart of the standard:

Paragraph 35 — Incident notification (72 hours). Notify APRA as soon as possible and no later than 72 hours after becoming aware of an information security incident that:

- Materially affected, or had the potential to materially affect, the entity or the interests of depositors, policyholders, beneficiaries or other customers; **or**
- Has been notified to any other regulator, in Australia or any other jurisdiction.

Paragraph 36 — Material weakness notification (10 business days). Notify APRA no later than 10 business days after becoming aware of a material information security control weakness that cannot be remediated in a timely manner.

The "or" in paragraph 35 is the trap. Even an incident that you assess as not material to your operations becomes APRA-notifiable the moment you decide to notify any other regulator. A breach affecting Australian users that triggers OAIC notification is automatically APRA-notifiable under trigger (b), regardless of its impact on the institution itself.

The CPS 230 overlay — 24 hours for operational risk events

CPS 230 (Operational Risk Management) became effective **1 July 2025** and overlays CPS 234 in important ways.

Paragraph 41 — Material operational risk event (24 hours). An APRA-regulated entity must notify APRA within 24 hours of identifying an operational risk event that has had, or is likely to have, a material financial impact or a material impact on the entity's ability to maintain critical operations.

For cyber incidents specifically:

- A ransomware incident affecting customer-facing systems is both a CPS 234 incident (72 hours) and a CPS 230 event (24 hours)
- An S3 misconfiguration that exposes customer records is both a CPS 234 incident and an OAIC NDB notification — which then triggers CPS 234 paragraph 35(b)
- An IAM credential compromise that lets an attacker shut down a production payment system hits CPS 234, CPS 230, and any payment-system-specific notification (RBA, AusPayNet)

The practical consequence: the 24-hour CPS 230 clock now controls most cyber notification timelines for APRA-regulated entities. Plan for 24, not 72.

CPS 230 also formally introduces the **material service provider** classification, which captures AWS for any entity running core systems on it. This brings due diligence, ongoing oversight, exit planning, and concentration risk management obligations — relevant context for incident response because APRA will ask whether the AWS relationship was operating to standard at the time of the incident.

The incident notification matrix for AWS

Mapping common AWS-side incident scenarios to APRA notification triggers:

AWS-side incident	CPS 234 (72h)	CPS 230 (24h)	Other regulators
Ransomware on production EC2 affecting customer transactions	Yes	Yes	Possibly OAIC if personal data affected
Compromised IAM credentials with customer data access	Yes if material; or Yes via 35(b) if OAIC notified	Yes if customer-facing impact	OAIC, possibly overseas regulators
S3 bucket misconfiguration exposing customer records	Yes via 35(b) if OAIC notified	Possibly	OAIC almost certainly
DDoS taking down customer-facing API	Yes if material	Yes if critical operation affected	Possibly RBA / AusPayNet
Material control weakness discovered (e.g., MFA bypass)	Paragraph 36 (10 business days)	Not directly, unless event occurred	Internal audit, board
AWS region outage affecting critical operation	Possibly	Yes if material impact on critical operation	Possibly RBA / AusPayNet
Insider exfiltration of customer data	Yes	Yes if material	OAIC almost certainly
Third-party MSP breach affecting your AWS environment	Yes if material	Yes if material	Vendor-specific

The matrix is institution-specific in detail — the materiality threshold and the definition of critical operations are yours to set and document — but the structural shape is consistent.

The 24-hour APRA notification runbook on AWS

Designed against the CPS 230 24-hour clock, which is the binding deadline in practice for most cyber incidents:

Hour 0 — Awareness. The incident commander confirms that an event meeting the materiality test has occurred. Record the exact timestamp. *This is t=0 for both CPS 234 and CPS 230 clocks.*

Hours 0–2 — Mobilise and classify. Page the CISO, head of IT, CRO, and the APRA relationship contact. Open the war-room. Decide which clocks apply: CPS 234 alone, CPS 234 + CPS 230, or CPS 234 + CPS 230 + other regulators (OAIC, RBA, overseas).

Hours 2–6 — Contain and quantify. Run pre-staged containment automations. Isolate affected resources, snapshot evidence, rotate compromised credentials. In parallel, quantify customer impact — how many customers affected, what services degraded, what data at risk.

Hours 6–12 — Materiality assessment. Apply the documented materiality model. The threshold should be in your information security policy, signed off by the board, and reference customer impact, financial impact, operational impact, and reputational impact. Document the assessment and sign-off in the incident record.

Hours 12–18 — Draft notifications. Populate pre-staged templates for APRA and any other relevant regulator. The APRA notification should be factual, short, and explicit about what is known and unknown at the time. APRA does not expect forensic completeness in the first notification.

Hours 18–22 — Internal sign-off. Board chair or audit committee chair noted, CEO informed, formal sign-off by the named accountable person (typically the CISO).

Hours 22–24 — Submit. Send the CPS 230 notification to APRA via the established channel. If notifying OAIC or other regulators, send in parallel. Trigger the CPS 234 paragraph 35(b) notification simultaneously if not already done.

The 24-hour design leaves the second day for the deeper CPS 234 follow-up, OAIC assessment work, and the start of the longer-form post-incident report.

Pre-incident hardening — what to set up now

Four AWS-specific items separate APRA-regulated entities that handle notification cleanly from those that draw supervisory scrutiny.

1. A board-approved materiality model

CPS 234 and CPS 230 both require the entity to apply a materiality test. APRA expects the criteria to be:

- Documented in a board-approved policy
- Reference both quantitative thresholds (dollar amounts, customer counts) and qualitative factors (customer harm, regulatory exposure)
- Applied consistently across incidents
- Tested in tabletops

A common AWS-specific quantitative threshold is something like: "any incident affecting more than X customers, or causing more than Y minutes of unavailability on a critical customer-facing system, or involving unauthorised access to any production database containing customer financial information." Adapt to your institution's scale.

2. A pre-tested APRA notification path

CPS 230 in particular expects a documented, tested notification channel. Maintain:

- The supervisor's direct contact details, refreshed quarterly
- A documented after-hours notification procedure
- Standing authority for the CISO or COO to submit notifications without further internal approval (board pre-approval of this delegation is the cleanest approach)
- A tested template aligned to APRA's expected notification content

3. Logging and evidence baseline in ap-southeast-2 / ap-southeast-4

For the materiality assessment, the post-incident report, and the inevitable APRA on-site follow-up, you need substantial evidence:

- **CloudTrail** organisation trail with S3 destination in ap-southeast-2 or ap-southeast-4, ≥12 months retention with Object Lock in compliance mode
- **CloudWatch Logs** for application and infrastructure logs, ≥12 months retention

- **VPC Flow Logs** delivered to S3 in an Australian region
- **GuardDuty** enabled in every active region
- **Security Hub** aggregating findings across regions
- **AWS Config** recording configuration history — critical for the "was the control in place at time of incident" question
- **CloudTrail data events** on all production storage holding customer data

APRA's published guidance after recent enforcement actions emphasises chain-of-custody. Object Lock and AWS Config history together give you both.

4. CPS 230 material service provider documentation

Independent of any incident, you need an up-to-date material service provider register documenting AWS:

- Services consumed and regions used
- Concentration risk assessment
- Due diligence artefacts (AWS SOC reports, IRAP assessment, AWS APRA papers)
- Exit plan with technical and commercial detail
- Right-of-audit arrangements (the AWS Audit Manager program supports this)
- Periodic review evidence

This documentation is what APRA will ask for during any post-incident review involving AWS.

AWS region selection and Australian FSI considerations

Australia has two AWS regions: **ap-southeast-2 (Sydney)** since 2012 and **ap-southeast-4 (Melbourne)** since 2024. Both are within Australian sovereign data jurisdiction. Three IR-relevant points:

1. **Multi-region active-active across Sydney and Melbourne is now the APRA default expectation.** CPS 230's emphasis on operational resilience and ability to recover from disruption means single-region architectures attract more scrutiny than they used to. Both AWS Australian regions are independent enough to satisfy resilience expectations.
2. **IRAP-assessed services.** AWS Asia Pacific (Sydney) Region is IRAP-assessed to PROTECTED level for a substantial service catalogue. APRA does not formally require IRAP, but IRAP-assessed services are easier to defend in supervisory review.

3. **Direct Connect dependencies.** Most APRA-regulated entities operate hybrid architectures with Direct Connect from on-premises data centres into AWS. An incident that spans the on-premises and AWS environments — for example, lateral movement from a corporate workstation into AWS via a long-lived Direct Connect path — is one of the more common scenarios. Your runbook must cover it explicitly.

Common mistakes

Five patterns we see repeatedly when reviewing APRA readiness for AWS workloads:

- **Planning to the 72-hour CPS 234 clock and ignoring CPS 230.** Most cyber incidents now trigger both clocks, and the 24-hour CPS 230 deadline is binding. If your runbook is built around 72 hours, it is built around the wrong number.
- **Materiality model that lives in the CISO's head.** APRA expects a documented, board-approved, consistently applied model. Inconsistent application is a supervisory red flag in its own right.
- **Forgetting the paragraph 35(b) trigger.** A notification to OAIC automatically pulls APRA in within 72 hours. Many incidents reach OAIC first and miss this dependent notification.
- **No material service provider register for AWS.** Discovering during a supervisory review that you cannot produce CPS 230-compliant AWS oversight documentation is an avoidable problem.
- **Single-region production architectures.** Increasingly hard to defend under CPS 230's operational resilience expectations. Sydney + Melbourne is the standard answer.

What to do this week

If your entity is APRA-regulated and runs AWS workloads, three actions return the most value in the first week:

1. **Reconcile your runbook against the 24-hour CPS 230 clock.** If your current incident notification target is 72 hours, walk through what would need to change to hit 24 — the materiality decision, the notification authority, the template.
2. **Audit your AWS material service provider register.** If you don't have one, start. If you do, confirm it reflects current AWS usage including any new

regions, services, or accounts.

3. **Run a CPS 230 tabletop.** Use a realistic scenario — for example, a ransomware deployment via compromised IAM credentials in production. Time the materiality assessment and the notification path. Find out where 24 hours falls over before a live incident does.

CPS 234 and CPS 230 together make Australia one of the tighter cyber notification regimes for financial services in the world — not as fast as MAS's 1-hour rule, but substantially faster than the headline 72 hours suggests once the operational risk overlay is accounted for. Institutions that plan to the right number get this right consistently.

Related guides

- AWS Incident Response in APAC — Pillar guide — the regulatory and technical overview across Australia, Singapore, India, and ASEAN.
- OAIC Notifiable Data Breach scheme on AWS — the Australian privacy regulator parallel; OAIC notification automatically triggers CPS 234 paragraph 35(b).
- MAS TRM and AWS incident response — the Singapore FSI parallel with a 1-hour clock.
- Meeting CERT-In's 6-hour incident reporting rule on AWS — relevant for any APRA-regulated entity with Indian operations or customers.
- Ghost Vector managed detection — our managed detection service includes CPS 234 and CPS 230 notification workflows.