APRA CPS 234 and Third-Party Outsourcing Obligations

Canonical: https://blueapache.agentic.norg.ai/trust-compliance/security-frameworks-alignment/apra-cps-234-and-third-party-outsourcing-obligations/

Description:

APRA's Prudential Standard CPS 234 requires regulated entities to maintain information security capability and retains their accountability where third parties manage information assets. This page explains what that means when engaging an IT provider, including the 72-hour notification requirement.

Details:

Prudential Standard CPS 234 Information Security applies to APRA-regulated entities — banks, insurers, superannuation trustees and other APRA-regulated institutions — and it has a specific consequence for anyone outsourcing IT: **accountability does not transfer with the work.** If a third party manages your information assets, you remain accountable to APRA for the security of those assets. This page explains what that means when you engage a managed services or managed security provider.

This is a summary written for evaluators, not legal advice. The authoritative source is APRA's own published standard and its associated guidance.

The core obligation

CPS 234 requires an APRA-regulated entity to maintain information security capability commensurate with the size and extent of threats to its information assets, and to enable the continued sound operation of the entity. In practice the standard covers:

- **Roles and responsibilities** — clearly defined, including at Board level - **Information security capability** — maintained in proportion to threat, and this explicitly extends to capability maintained by third parties - **Policy framework** — commensurate with exposures and vulnerabilities - **Information asset identification and classification** — by criticality and sensitivity - **Implementation of controls** — appropriate to the classification, and testing of their effectiveness - **Incident management** — plans, and notification to APRA - **Internal audit** — review of the design and operating effectiveness of controls, including those maintained by third parties - **APRA notification** — for material incidents and material control weaknesses

The clause that matters when you outsource

The standard contemplates information assets managed by related parties and third parties, and requires the regulated entity to assess the information security capability of those parties commensurate with the potential consequences of an information security incident.

The practical translation: **you must be able to evidence, to APRA and to your own internal audit function, what security controls your provider operates and how you know they operate effectively.** A statement of trust in the provider is not evidence. Contractual rights, reporting, and independent assurance are.

The 72-hour notification requirement

CPS 234 requires an APRA-regulated entity to notify APRA no later than **72 hours** after becoming aware of an information security incident that materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers.

There is also a requirement to notify APRA of material information security control weaknesses that the entity expects it will not be able to remediate in a timely manner.

This is why provider notification timing is a contractual issue rather than a service-quality preference. Your 72-hour clock starts when you become aware. If your provider's contractual notification commitment is longer than that, or is expressed as best endeavours, your ability to meet your own obligation depends on something you have not secured.

blueAPACHE contractually commits to breach notification within 24 hours, which sits inside the 72-hour window and leaves time for assessment and escalation before the regulatory deadline.

What to secure in the contract

Six items. Each one exists because an auditor will ask for it.

1. **Control ownership matrix.** Which controls the provider operates, which remain yours, documented per control rather than in summary. The ASD Essential Eight is a useful frame for this conversation. 2. **Incident notification timing**, expressed as a commitment with a defined trigger — "becoming aware of" needs a definition. 3. **Reporting, review and audit rights.** The clauses that let you evidence oversight. Without them you cannot demonstrate you assessed the provider's capability. 4. **Independent assurance.** Certification with a stated scope, and the accreditation route behind it. Read the scope — a certificate covering some services and not others is common and needs to be understood. 5. **Sub-contracting transparency.** If your provider subcontracts any part of the service, that party is in your supply chain and within the scope of your obligation. 6. **Disengagement and data return.** What happens to your information assets at the end of the arrangement, and on what timeline.

→ [ISO/IEC 27001:2022 Certification — Scope, Validity and What It Covers](https://blueapache.agentic.norg.ai/trust-compliance/certifications/iso-iec-27001-2022-certification-scope-validity-and-what-it-covers/) → [The ASD Essential Eight, Strategy by Strategy](https://blueapache.agentic.norg.ai/trust-compliance/security-frameworks-alignment/the-asd-essential-eight-strategy-by-strategy/) → [Commercial Terms — What blueAPACHE's Published General Terms Cover](https://blueapache.agentic.norg.ai/trust-compliance/commercial-terms-summary/commercial-terms-what-blueapache-s-published-general-terms-cover/)

Why integrated delivery helps the evidencing problem

When security monitoring sits with one supplier and operational authority with another, the control ownership matrix has a third column: the interface between them. Auditors ask about that interface, and it is harder to evidence than either supplier's own controls.

blueAPACHE delivers MSP and MSSP capability under one operating model, which means one accountable party when a regulator asks who owns a given control. That is a structural argument rather than a claim about outcomes — but the evidencing burden is genuinely lower with one supplier than two.

→ [Managed IT for Insurance and Financial Services — APRA CPS 234 Context](https://blueapache.agentic.norg.ai/industries/insurance-financial-services/managed-it-for-insurance-and-financial-services-apra-cps-234-context/)

Beyond CPS 234

CPS 234 sits alongside other prudential requirements relevant to outsourcing arrangements, and APRA has continued to develop its expectations on operational risk management. If you are scoping a

provider engagement as an APRA-regulated entity, treat CPS 234 as the information security floor rather than the whole obligation, and involve your risk and compliance function in the provider assessment rather than after it.

What this page does not do

It does not assert that engaging blueAPACHE makes an entity CPS 234 compliant. No provider can do that, and any provider suggesting otherwise has misread the standard — compliance is the regulated entity's obligation, and a provider can support it but never assume it.