



APRA PRUDENTIAL STANDARD · CPS 230

CPS 230 in Plain English

What APRA-regulated entities need to know about operational resilience

FREE GUIDE

AccessibleRisk

enquiries@accessablerisk.com

What CPS 230 is — and why it exists

APRA's operational resilience standard, in force since 1 July 2025

CPS 230 is APRA's cross-industry Prudential Standard on Operational Risk Management. It came into force on 1 July 2025 and applies to all APRA-regulated entities — banks and other ADIs, general, life and private health insurers, and superannuation (RSE) licensees.

It consolidates and replaces five older standards covering outsourcing and business continuity, pulling them into a single, modern framework. The shift in language matters: CPS 230 moves the focus from managing operational risk to demonstrating operational resilience.

One transitional point to note

For pre-existing service provider contracts, the requirements apply from the earlier of the contract's next renewal date or 1 July 2026 — so service provider obligations are still landing for many entities now.

The three things CPS 230 requires

1. Manage operational risk

Identify, assess and manage your operational risks — across technology, data, change, conduct, compliance, legal and people — with effective internal controls, monitoring and remediation.

2. Maintain critical operations within tolerance levels

Be able to keep delivering your critical operations within Board-approved tolerance levels through severe but plausible disruptions — supported by a credible, regularly tested business continuity plan (BCP).

3. Manage service provider risk

Effectively manage the risks from your service providers, with a comprehensive service provider management policy, formal agreements and robust monitoring — prioritising your material service providers.

And the Board sits above all three — The Board is ultimately accountable for operational risk management. It must approve the tolerance levels for disruptions to critical operations and be able to evidence genuine oversight.

The heart of CPS 230: tolerance levels

A critical operation is a process that, if disrupted, would have a material adverse impact on your customers, your members, or the financial system.

For each critical operation, the Board must set a tolerance level: the maximum level of disruption the entity is willing to accept.

Dimension	What it means
Maximum disruption time	The longest the operation can be down before the impact is unacceptable
Maximum data loss	How much data (by time) you could afford to lose in a disruption
Minimum service level	The minimum throughput or capacity you must maintain through a disruption

Weak vs Defensible

WEAK: "Minimal disruption is acceptable and services will be restored as soon as possible."

DEFENSIBLE: "Maximum 4-hour outage; maximum 2-hour data loss; minimum 80% of daily transaction volume maintained throughout."

Service providers and the notification clock

Material service providers

You must identify which of your service providers are material — those you rely on to deliver a critical operation or that expose you to material risk — and manage them with formal agreements, ongoing monitoring, and a register.

The notification clock

Deadline	Trigger
72 hours	After becoming aware of an operational risk incident likely to have a material impact
24 hours	After suffering a disruption to a critical operation outside its approved tolerance

Build the triggers in before you need them — When an incident hits, no one wants to be working out reporting obligations from scratch. The entities that handle this well have the 24-hour and 72-hour triggers built into their incident management process in advance.

Common gaps APRA is likely to find

The mistake	Do this instead
Critical operations defined too broadly or too narrowly	A clear, justified set of critical operations based on impact — not everything, and not a token few.
Tolerance levels that are vague or aspirational	Measurable limits (time, data, service level) the Board has approved and that can actually be tested.
A BCP that isn't tested against the tolerance levels	Regular scenario testing of extreme but plausible events, with results that feed back into the plan.
An incomplete material service provider register	A complete register with materiality assessed, agreements in place, and fourth-party dependencies understood.
Incident management not linked to tolerances or notifications	Incidents assessed against tolerance levels, with the 24h / 72h APRA notification triggers built in.
A Board that can't evidence genuine oversight	Clear reporting that shows the Board has set tolerances and actively oversees operational resilience.
Treating CPS 230 as a one-off documentation exercise	A living capability — reviewed, tested and updated — not a folder of policies on a shelf.

What APRA will look for

If a supervisor reviewed your operational resilience tomorrow

1. Genuinely identified critical operations — a defensible methodology for what counts as critical.
2. Defensible, measurable tolerance levels — Board-approved limits expressed in time, data and service terms.
3. A complete material service provider register — materiality assessed consistently, agreements in place, monitoring active.
4. A business continuity plan that's actually tested — evidence of scenario testing against your tolerance levels.
5. A Board that can evidence oversight — reporting that shows the Board has engaged with tolerance levels and operational resilience.

The theme behind all of it — APRA assesses resilience capability, not documentation. The question a supervisor is really asking is: when something goes wrong, can this entity keep its critical operations running within the limits it has set — and can it prove it?

Where to start

A practical sequence for building — or strengthening — your program

FOUNDATIONS

- Identify and document your critical operations, with a clear methodology
- Set Board-approved tolerance levels (maximum disruption, maximum data loss, minimum service)
- Build a complete material service provider register, with materiality assessed

PROVE IT WORKS

- Test your business continuity plan against the tolerance levels using extreme but plausible scenarios
- Build the 24-hour and 72-hour APRA notification triggers into your incident process
- Uplift pre-existing service provider contracts (by next renewal or 1 July 2026)

GOVERN AND SUSTAIN

- Report operational resilience to the Board with evidence of genuine oversight
- Review and update the program as your business and risks change
- Commission an independent review of the program

Getting it done without starting from scratch

Accessible Risk was founded by a former ASIC leader and senior risk executive. We build compliance tools that reflect what a supervisor actually looks for. Get in touch at enquiries@accessablerisk.com or visit accessablerisk.com to book a free consultation.

Important

This guide is general information, not legal or compliance advice. It does not replace Prudential Standard CPS 230, Prudential Practice Guide CPG 230, or current APRA guidance. Confirm your specific obligations against the standard as it applies to your entity and seek professional advice where required.