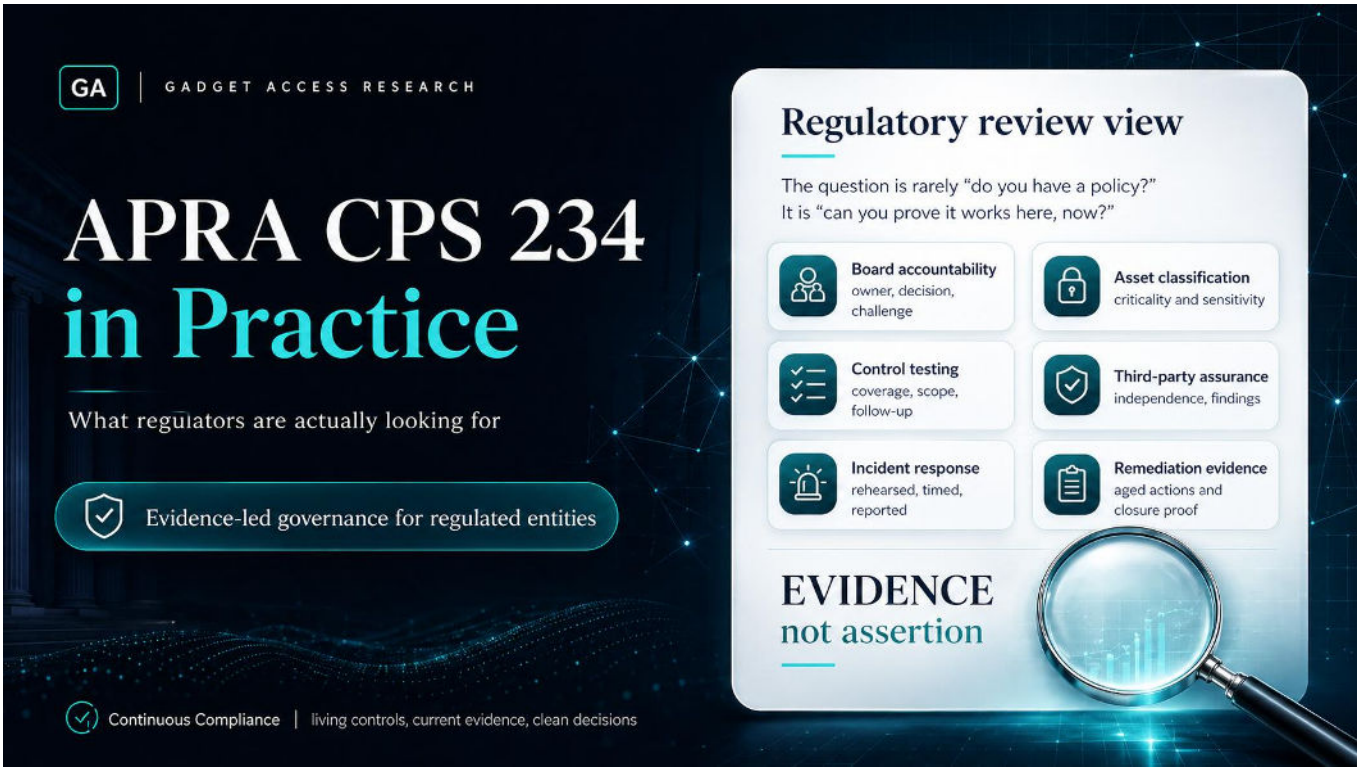

APRA CPS 234 in Practice: What Regulators Are Actually Looking For

A frank briefing on what APRA expects from regulated entities, based on supervisory review patterns and the practical reality of running cyber programs under pressure.

Gadget Access Research | 5 minute read

Briefing note: APRA is not looking for cyber theatre. It is looking for current, traceable and tested evidence that controls are commensurate with the entity's actual risk.

The short version from the trenches

APRA CPS 234 has a deceptively simple ambition: make regulated entities resilient against information security incidents, including cyber-attacks, by maintaining capability that is commensurate with the threats, vulnerabilities and sensitivity of their information assets. That sounds neat on paper. In practice, it asks one very uncomfortable question: can you prove that your security capability matches your actual risk?

That question matters because cyber risk is now a board-level and system-level concern. APRA's own 2025 stakeholder survey found cyber risk was the top business risk raised by banks, insurers and superannuation trustees. The regulator also supervises an ecosystem holding around $9.8 trillion in assets, so a weak control environment is not merely an internal technology problem. It can become a prudential problem, a customer harm problem and, on a very bad day, a financial stability problem.

The biggest mistake we see is treating CPS 234 as a compliance artefact. A policy pack, a risk register and a once-a-year penetration test may be useful ingredients, but APRA is looking for an operating model. It wants evidence that the board is informed, critical assets are known, controls are fit for risk, control testing is systematic, third parties are challenged, incident response is rehearsed and material issues are reported promptly. In other words, the regulator is looking for a living security system, not a folder with a heroic filename.

The evidence gap is where reviews get interesting

Most regulated entities can produce policies. The harder question is whether those policies survive contact with production reality. The policy may say assets are classified by criticality and sensitivity, but the asset register may not include the SaaS platform acquired by a business unit six months ago. The policy may say privileged access is controlled, but the service account inventory may be incomplete. The supplier may have a certificate, but the certificate may not cover the systems that actually hold customer data. This is the moment a CPS 234 review stops being a paperwork exercise and becomes a governance test.

APRA has been unusually clear about the patterns it keeps seeing. Its 2023 cyber security stocktake, drawn from CPS 234 tripartite assessments, identified recurring gaps in asset identification and classification, third-party control assurance, control testing, incident response testing, internal audit coverage and timely notification processes. Its 2024 and 2025 letters then put sharper edges on specific weaknesses such as backup isolation, configuration management, privileged access, security testing and authentication controls.

Those letters are not random cyber tips. They are supervisory breadcrumbs. When APRA writes to industry about multi-factor authentication, backup recoverability or privileged access, it is telling boards and executives where the next difficult questions are likely to land. The question is not simply whether MFA exists. It is whether the coverage is complete for privileged, remote and high-risk activities, whether exceptions are justified, whether the control is tested, and whether gaps could amount to a material control weakness.

What regulators are really testing

First, APRA tests traceability. Can the entity connect the dots from a customer-impacting service to the information assets that support it, to the data those assets hold, to the controls that protect them, to the control tests that prove they work? Traceability is the difference between saying "we are secure" and showing how a specific high-value asset is protected today. If the trail depends on three spreadsheets, two ticketing systems and the one person who is currently on leave, the trail is too fragile.

Second, APRA tests currency. CPS 234 is explicit that information security capability must be actively maintained as vulnerabilities, threats, information assets and the business environment change. A control that was appropriate last year may be inadequate after a cloud migration, a new outsourced service, a threat intelligence change, a merger, or an AI-enabled fraud campaign. Regulators do not expect clairvoyance. They do expect a mechanism that notices change and triggers reassessment.

Third, APRA tests independence and assurance. The standard requires systematic control testing by appropriately skilled and functionally independent specialists. APRA's public findings show that incomplete testing coverage, repeated testing of the same limited assets, weak test evidence and insufficient oversight of findings are recurring issues. A penetration test can be useful, but it is not a substitute for a control assurance program that covers the population of material controls over time.

Fourth, APRA tests escalation discipline. CPS 234 requires APRA notification within 72 hours for material information security incidents and within 10 business days for material information security control weaknesses that cannot be remediated in a timely manner. The regulator is not looking for perfection in the first hour of an incident. It is looking for a decision process that is fast, documented and connected to the board, accountable executives, legal, technology, operations, suppliers and regulators.

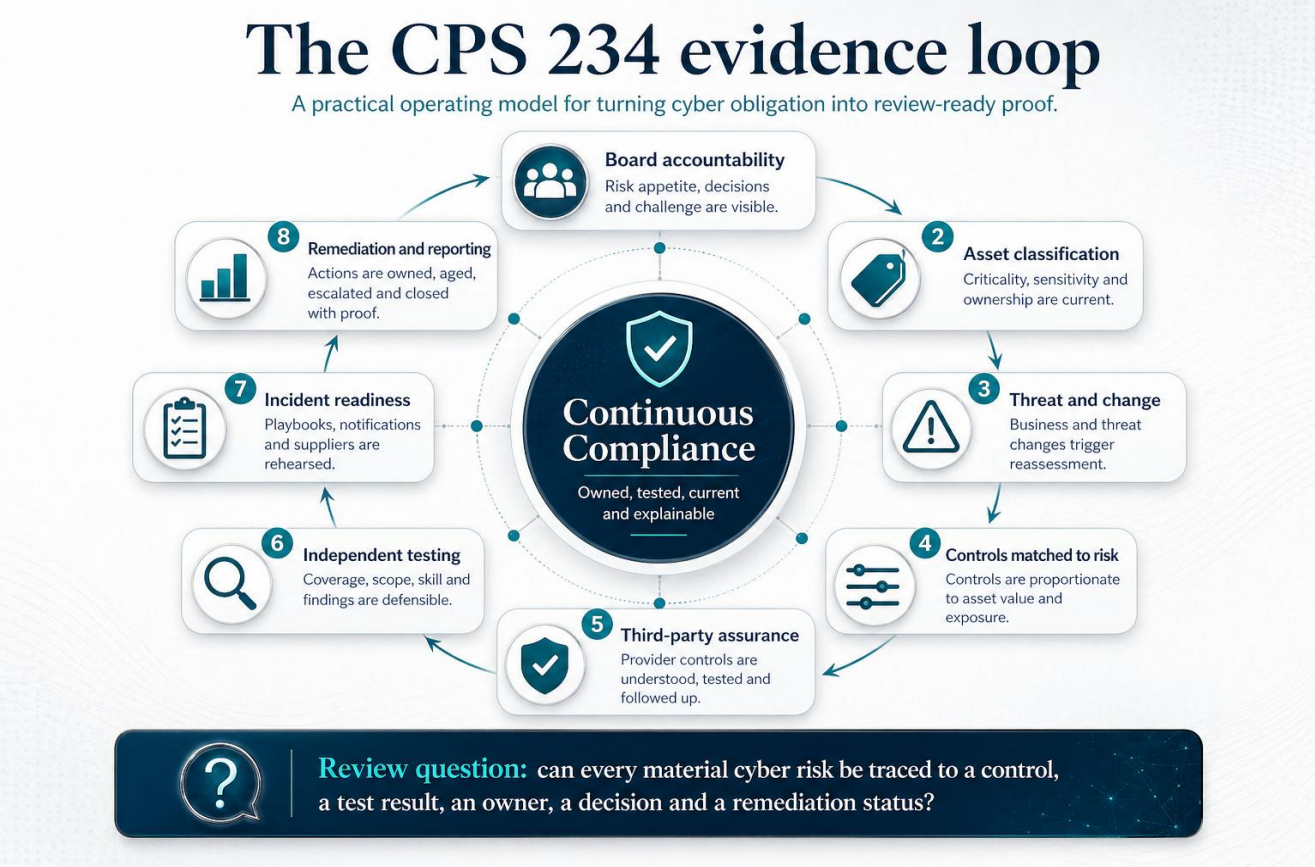

Figure 1. Common CPS 234 review assertions compared with the type of evidence that usually withstands scrutiny.

The board does not need firewall logs. It does need a grip on reality.

CPS 234 makes the board ultimately responsible for information security. That does not mean directors should approve every endpoint rule or know the CVSS score of every vulnerability. It means they need reporting that turns technical signals into decisions. They should be able to see material cyber exposures, risk appetite breaches, control weaknesses, test coverage, overdue remediation, supplier assurance issues and incident readiness in a form that supports challenge.

A board pack that says "green" across the page while remediation tickets age quietly in the background is not assurance. It is decoration. Good cyber reporting shows movement, exceptions and consequence. It explains why a control gap matters to customer outcomes and prudential standing. It records decisions, including risk acceptance, funding, prioritisation and escalation. With the Financial Accountability Regime now applying across banking, insurance and superannuation, APRA's 2025 request for RSE licensees to identify accountable persons for CPS 234 compliance is another sign that cyber governance is becoming more personal, more explicit and harder to delegate into the mist.

Third parties are not outside the tent

One of the most persistent CPS 234 traps is assuming that outsourced technology means outsourced accountability. It does not. CPS 234 extends to information assets managed by related parties and third parties. APRA expects entities to assess third-party information security capability, evaluate control design, understand the nature and frequency of control testing, and assess the assurance it receives where material customer or entity impacts are possible.

In plain English, "our provider handles that" is not a control. It is the start of a control conversation. What systems are in scope? What data is held? What subcontractors are involved? What incident reporting clauses exist? What independent assurance is available, and what are its limits? What evidence proves remediation happened? This is where cyber, procurement, legal, risk and operations need to operate as one team rather than a polite queue of handoffs.

What good looks like in practice

A strong CPS 234 program has a simple rhythm. Material information assets are identified and classified. Control obligations are mapped to those assets and services. Control owners understand what they own. Exceptions are recorded with rationale, compensating controls and expiry dates. Testing is scheduled against risk and change. Evidence is retained. Findings become remediation actions with owners, dates and status. Board reporting is tied to the same evidence base. Incident playbooks include notification decision points and third-party escalation paths. Nothing about this is glamorous, which is probably why it works.

This is the logic behind Gadget Access's Continuous Compliance framework. The goal is to stop treating compliance as an annual panic and start generating defensible evidence through normal operations. A security control is not "done" because it was implemented. It is current because it is owned, tested, monitored, challenged and improved. That mindset is particularly useful for CPS 234 because the standard is principles-based. It gives entities flexibility, but flexibility only helps when the entity can explain its decisions with evidence.

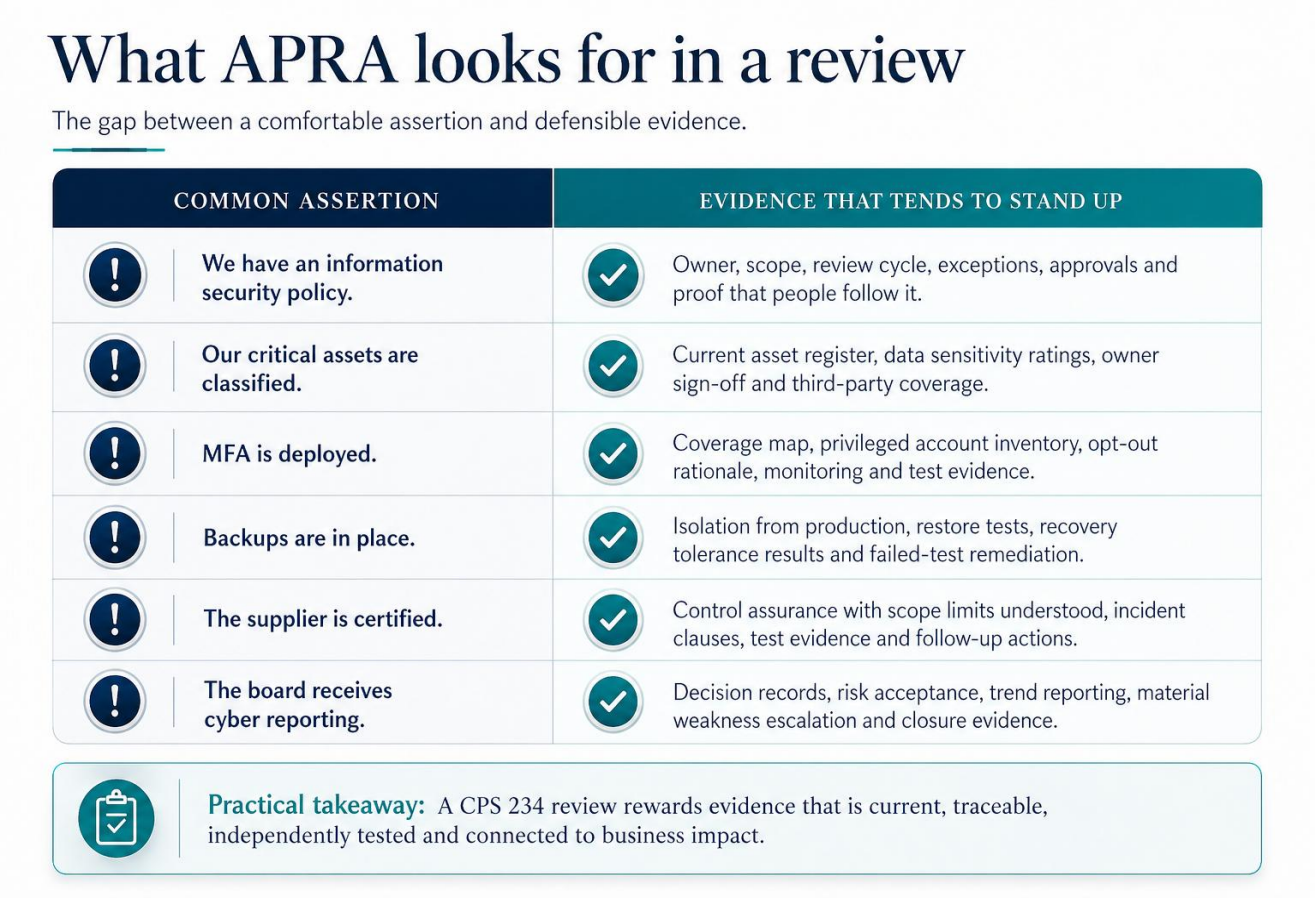

Figure 2. Continuous Compliance turns CPS 234 from a point-in-time exercise into a repeatable evidence loop.

Where AI and CiBRAI enter the picture

Agentic AI will not make a weak governance model magically compliant. It will, however, change what is possible for security teams drowning in telemetry. The regulatory value of modern cyber platforms is not just faster alert triage. It is the ability to preserve a clear chain from signal to context, from context to decision, from decision to action, and from action to audit trail.

That is the design space CiBRAI is built for. By bringing endpoint, cloud, identity and network signals into one operational view, adding an always-on AI analyst layer, guiding playbooks and producing board-ready summaries, platforms like CiBRAI can support the evidence discipline CPS 234 expects. The human accountable owners still make the decisions. The platform helps them see the incident story sooner, reduce noise, preserve the record and explain business impact without asking a sleep-deprived analyst to reconstruct the plot at midnight.

For regulated entities, the future is not a choice between advisory, tooling and governance. It is the integration of all three. Gadget Access brings the vCISO, compliance uplift, vendor management, testing, reporting and operating model experience. CiBRAI adds an AI-native security operations layer that can work with existing tools and support

sovereign deployment choices where data sensitivity and assurance demand them. Together, that is a pragmatic path from cyber obligation to operational clarity.

A final word for the next review

APRA is not asking every entity to look like a major bank. It is asking every entity to understand its own risk and prove that its controls are commensurate with that risk. Proportionality is not a permission slip for vagueness. It is a requirement to be precise about what matters most.

The best regulatory conversation is a calm one. When APRA asks what happens if a privileged account is compromised, a backup environment is attacked, a critical supplier is breached or a customer-facing system is unavailable, the answer should not begin with "let me check with IT". It should begin with an asset view, a tested scenario, a control map, a decision record and a remediation trail. That will not make the cyber threat disappear. It will make your organisation more resilient, and it will make your position defensible when the regulator comes looking for proof.

How Gadget Access helps

Gadget Access helps organisations translate cyber obligations into practical operating models. The team provides virtual CISO services, technical consulting, vendor management, testing, reporting and compliance uplift across frameworks such as Essential Eight, PSPF, ISM, ISO 27001:2022 and NIST. Our trademarked Continuous Compliance framework is designed to make control ownership, evidence, remediation and board reporting a continuous management discipline rather than a periodic audit scramble.

References and useful APRA materials

Selected source materials used in preparing this article:

- APRA Prudential Handbook: CPS 234 Information Security
- APRA Prudential Handbook: CPG 234 Information Security
- APRA: Cyber security stocktake exposes gaps
- APRA: Use of multi-factor authentication
- APRA: Security and adequacy of backups
- APRA: Additional insights on common cyber resilience weaknesses
- APRA Prudential Handbook: Letter to RSE licensees on information security obligations and critical authentication controls
- APRA Annual Report 2024-25
- APRA Corporate Plan 2025-26
- CiBRAI: Unified Security Platform with AI