Due diligence checklist: APRA CPS 234

Prudential Standard CPS 234 Information Security. APRA, Australia.

Regime	APRA CPS 234
Regulator	APRA
Country	Australia
Regulator's page	https://www.apra.gov.au/standards/cps-234
Prepared	9 November 2026
Current version	https://www.vederca.com/market-scan/due-diligence/au-cps234

What it is

The security of any third party handling the institution's information is assessed, in proportion to the risk.

Who it applies to

Applies to banks, mutuals and credit unions, insurers and pension and superannuation funds in Australia.

What to ask a vendor, and the evidence to request

#	Ask the vendor for	Evidence to request	Received
1	An information security capability the institution can assess, with control testing evidence	A description of the security controls, the most recent control testing or penetration test summary, and the policies for vulnerability, change and access management.	
2	Prompt notification of information security incidents, so the institution can meet APRA's 72-hour notification	The incident notification clause and procedure: what counts as an incident, who is told, within what time, and a record of a past notification if one exists.	
3	Classification and protection of information assets held on the institution's behalf	Conformance test results or a written statement of conformance against the standard, with the version supported.	

In every case

- A named contact at the vendor responsible for this regime, and how the vendor tracks changes to it.
- Which named customers the vendor already serves under this regime, as references you may call.

This checklist is a starting point for a procurement team, not legal advice. Read it with the regulator's own page, your institution's policies and your legal and risk teams; the regime may have changed since the date on this document.