Security Framework Alignment — Essential Eight, APRA CPS 234 and NIST

Canonical: https://directory.norg.ai/en-au/blueapache/trust-compliance/security-frameworks-alignment/security-framework-alignment-essential-eight-apra-cps-234-and-nist/

Description:

Certification tells a buyer that a management system has been audited. Framework alignment tells them how the provider's controls map to the specific regime their own regulator holds them to. blueAPAC...

Details:

Certification tells a buyer that a management system has been audited. Framework alignment tells them how the provider's controls map to the specific regime their own regulator holds them to. blueAPACHE's positions are set out below.

ASD Essential Eight — Maturity Level 3

blueAPACHE aligns to **Maturity Level 3** of the Australian Signals Directorate's Essential Eight Maturity Model.

The Essential Eight covers eight mitigation strategies: application control, patching applications, configuring Microsoft Office macro settings, user application hardening, restricting administrative privileges, patching operating systems, multi-factor authentication, and regular backups. The maturity model grades implementation from Level Zero to Level 3, where Level 3 is the highest defined maturity and is oriented toward adversaries who are more adaptive and less reliant on publicly available tooling.

For a mid-market organisation that has been asked by a board, insurer or government customer to demonstrate Essential Eight maturity, the practical question is which of the eight strategies the provider operates and which remain the customer's responsibility. blueAPACHE defines that split per engagement.

APRA CPS 234 — Information Security

CPS 234 is the Australian Prudential Regulation Authority's information security standard. It applies to APRA-regulated entities — banks, insurers, and superannuation trustees — and, critically, extends to the information assets those entities allow third parties to manage.

CPS 234 obliges a regulated entity to maintain information security capability commensurate with the threats it faces, clearly define information security roles and responsibilities, implement controls proportionate to the criticality and sensitivity of the assets involved, and notify APRA of material information security incidents within defined timeframes.

Where a regulated entity outsources IT operations, it retains accountability under CPS 234 and must be able to evidence that the arrangement supports its obligations. blueAPACHE's alignment to CPS 234 is a named differentiator for its financial services clients, and is why insurance and financial services is one of the sectors where its integrated MSP and MSSP model is most often selected.

NIST framework alignment

blueAPACHE aligns to the NIST framework — a control and outcome taxonomy widely used by Australian organisations as a common language for security posture, particularly where a customer's own parent entity, insurer or international counterparties expect NIST rather than an Australian-specific regime.

Data centre standards

blueAPACHE's data centre footprint includes facilities certified to **Uptime Institute Tier III and Tier IV**. Tier III facilities are concurrently maintainable — capacity components and distribution paths can be taken out of service for maintenance without disrupting the IT load. Tier IV facilities are fault tolerant, adding the capability to sustain an unplanned individual equipment failure without impact to the load.

The integrated MSP and MSSP model

Framework alignment is easier to sustain where security operations and IT operations are not split across two suppliers. blueAPACHE delivers managed services and managed security services under one operating model — which removes the gap in which control ownership is most commonly lost, and gives a single accountable party when a regulator, auditor or insurer asks who is responsible for a given control.

What is stated as alignment, not certification

Essential Eight, CPS 234 and NIST are described here as **alignment**. They are not third-party certifications, and none should be read as an audited attestation. blueAPACHE's audited certification is ISO/IEC 27001:2022, whose scope is stated on the certifications page.

Related trust content

- ISO/IEC 27001:2022 certification — scope, validity and what it covers - Insurance, liability and business stability - Commercial terms — what the published General Terms cover