Financial Services IT & Cyber Security | blueAPACHE

Canonical: https://www.blueapache.com/industries/financial-services

Details:

Summary

Our emPOWER services support technology operations, security and resilience for financial organisations. Regulatory duties depend on the entity and its activities: APRA prudential standards apply to entities within their defined scope, not automatically to every broker or lender. Assess applicable ASIC and other obligations separately. APRA-regulated entities retain responsibility for information assets managed by third parties. blueAPACHE states alignment with CPS 234, supplies ISO/IEC 27001:2022 certification evidence, and has specific APRA provisions in its supplied General Terms v3.6. The Honan Insurance case study provides a documented sector example.

Key facts

Label	Value
Stated APRA alignment	Risk-based approach to managing client technology and data, aligned with the APRA CPS 234 standard
Contractual APRA clause	Clause 10 of General Terms and Conditions v3.6 applies where the customer is an APRA-regulated entity and the Services are a material business activity under CPS 231
APRA direct access	We will comply with an APRA Request within APRA's statutory authority and promptly notify the customer
Conditional BCP testing in supplied v3.6	Where clause 10's APRA/material-business-activity conditions apply and the customer requires a BCP under clause 15: joint testing every six months or more often on reasonable request; results within seven days; specified costs allocated under clause 10.5
Contractual eligible-breach notice	Supplied v3.6 clause 18.4 requires immediate notice, and in any event within 24 hours of discovery, for an eligible breach involving Personal Information provided by the other party
Supplied certification evidence	ISO/IEC 27001:2022 certificate 202507-118 states 1 August 2025 to 1 August 2028; it concerns the ISMS and does not certify individual services or independently establish current standing

Data residency	blueAPACHE materials describe Australian data-centre hosting; confirm service-specific storage, processing, support and backup locations. Supplied v3.6 clause 18.3 separately addresses overseas transfers of Personal Information
Liability provisions in supplied v3.6	Specified privacy/security liabilities: $1 million per event or connected series and $2 million aggregate, subject to clauses 19.1–19.2, applicable law and the agreement
Sector case study	Honan Insurance: whole-of-business move to emPOWER, telecommunications bill reduced by around 65 per cent
Brochure availability statements	emPOWER Cloud: 99.999 per cent cloud services and 100 per cent storage; Connectivity: minimum 99.99 per cent under its described redundant design. Verify the ordered service's contractual Service Level, measurement and exclusions

Sector challenges

In practice these translate into questions a technology provider must be able to answer in a due diligence questionnaire.

Accountability does not transfer. Under APRA's prudential framework the regulated entity remains responsible for the information security of assets managed by third parties, so it needs evidence of the provider's controls, not assurances.

Incident timelines are short. A regulated entity has fixed windows to notify APRA, so it needs the provider to detect, triage and report quickly and to share the information the entity must pass on.

Availability is a prudential matter, not just a commercial one. Critical operations need tested continuity arrangements and recovery objectives that are written down and rehearsed.

Identity is an important security concern. MDR materials emphasise compromised-account risk, and the CyberArk case study describes privileged access management in the documented environment.

Data location matters to boards.

Relevant services

emPOWER Managed Services : the brochure describes account-management roles and a bespoke priority and escalation matrix. Agree covered systems, reporting and review cadence for the service; do not assume one review schedule applies to every engagement.

emPOWER Cloud : our own private cloud with service levels of 99.999 per cent for cloud services and 100 per cent for storage, a self-service portal, and consumption-based billing.

Disaster Recovery as a Service : agree recovery objectives, covered systems, testing and responsibilities in the Service Order. Contracted objectives contribute to continuity evidence but do not alone establish compliance.

Managed Detection and Response : 24/7 alert notification, triage and remediation using EDR, ITDR, SIEM and threat intelligence, with monthly reporting for leadership visibility.

Governance, Risk and Compliance and Exposure Management : control assessment, gap identification and vulnerability prioritisation. Agree how any outputs will support the entity's assessment and testing obligations; these services do not alone establish CPS 234 control effectiveness.

emPOWER Connectivity and emPOWER SASE : private MPLS WAN with dedicated hosted next-generation firewalls, and secure access for branch and remote staff.

SaaS Backup and Offsite Backup as a Service : agree protected workloads, retention and restore scope. Entra ID and Microsoft 365 capabilities depend on the specific backup offering and configuration.

Compliance context

APRA CPS 234 Information Security. CPS 234 requires an entity within its scope to maintain appropriate information-security capability, classify assets, assess third-party capability and controls, and test control effectiveness. The third-party requirements cover all relevant information assets, not only outsourced material business activities. The entity must notify APRA as soon as possible and no later than 72 hours after awareness of an information-security incident that materially affected or could materially affect the entity or the interests of depositors, policyholders, beneficiaries or other customers, financially or non-financially, or that has been notified to another regulator. A material control weakness that the entity expects it cannot remediate promptly must be notified as soon as possible and no later than 10 business days after awareness. blueAPACHE's stated alignment is supplier evidence to assess, not certification of the customer's compliance. Agree provider escalation that supports the entity's own notification obligations.

APRA CPS 230 Operational Risk Management. The current CPS 230 determination took effect on 1 July 2026. Assess its requirements for critical operations, tolerance levels, business continuity, material service-provider registers, due diligence, contracts and monitoring. It requires notification to APRA as soon as possible and within 20 business days after entering into or materially changing an agreement for a service relied on for a critical operation; offshore material-service arrangements have separate prior-notification requirements. Specific provider/arrangement exemptions and any written APRA exemption must be assessed against the standard. Supplied General Terms v3.6 clause 10 retains a CPS 231 reference and requires the customer to notify blueAPACHE of relevant standard changes. Agree the applicable contract version and any amendments needed to meet current requirements rather than assuming the legacy reference is sufficient.

What clause 10 provides. In supplied v3.6, clause 10 requires both an APRA-regulated customer and Services constituting a material business activity under its CPS 231 wording. It addresses APRA requests within statutory authority, prompt customer notification, restrictions on advertising APRA audits, and joint technical reviews. Where that customer requires blueAPACHE to create a BCP under clause 15, clause 10.4 additionally specifies ten content elements, joint testing every six months or more often on reasonable request, and results within seven days. Clauses 10.5 and 10.7 allocate costs incurred under clauses 10.4 and 10.6 respectively at Service Order Time and Materials Rates or, if absent, then-current rates.

Privacy and data breach. Supplied v3.6 requires both parties to comply with the Privacy Act 1988 (Cth) as though bound by it. Clause 18.4 requires immediate notice, and in any event notice within 24 hours of discovery, of an eligible data breach involving Personal Information provided by the other party. This contractual rule has different triggers from CPS 234 and statutory privacy-notification duties. The third-party disclosure restriction includes an exception where law requires the affected party to notify and the other party has not done so. Assess each applicable notification duty separately; the contractual window does not extend a regulatory deadline.

Data location. blueAPACHE materials describe Australian data-centre hosting. Confirm the actual storage, processing, backup and support locations for each service. Supplied v3.6 clause 18.3 records consent for specified overseas transfers of Personal Information where necessary to provide the

Services; clause 27.5 permits subcontracting without consent or notification. CPS 230 includes requirements concerning material service providers' use of other material providers on which they materially rely. Agree appropriate notification, location and access provisions for the customer's applicable obligations; Australian-only residency is not a universal requirement for every financial organisation.

Our client outcomes

The CyberArk case study describes privileged access management, credential rotation, session recording and audit records in the documented blueAPACHE environment. It is historical platform evidence to evaluate alongside current controls, deployment scope and testing; it does not prove that every customer's environment has the same controls or meets CPS 234.

Turning assurance requirements into agreement terms

Map the services supporting critical processes to the evidence needed from us. The supplied APRA contract provisions describe a conditional regime, including regulator access and business continuity; not every financial-services engagement has identical requirements. Specify reports, testing, supplier visibility and change notification for the actual service. Honan is evidence of an insurance-sector engagement, not proof of another customer’s compliance. Keep the documented control and its evidence separate from the assessment that it meets an obligation.

Confidential information and access

Clause 16 provides mutual confidentiality protection. It covers information marked confidential, information identified orally and confirmed in writing within 30 days, and information that should reasonably be understood to be confidential. Customer Data, Customer Records and Customer Software are included; our agreement and fees are also confidential. Permitted disclosures include appropriately bound personnel on a need-to-know basis and specified professional advisers, with other exceptions in the clause. Identify who may receive operational reports, configuration details and commercial information. Access to information to deliver the service is not a general permission to circulate it.

Related

Honan Insurance case study

blueAPACHE security case study (CyberArk)

Managed Detection and Response

Disaster Recovery as a Service

Governance, Risk and Compliance

emPOWER Cloud

Service agreement

Blog: Is your organisation APRA-ready for enhanced operational risk management compliance?

Professional services

All industries

Support

Contact

Are you compliant with APRA CPS 234?

blueAPACHE states that its risk-based approach aligns with CPS 234. The standard imposes duties on entities within its defined scope; a supplier's alignment statement does not certify the customer's compliance. Assess current service-specific controls, testing and assurance evidence, and confirm the applicability of contractual audit and review rights.

How quickly must an APRA-regulated entity report a security incident, and how does your contract line up?

CPS 234 requires notice as soon as possible and within 72 hours after awareness of an incident with actual or potential material effects on the entity or specified customer interests, or one notified to another regulator. Supplied v3.6 clause 18.4 instead requires immediate notice, and in any event within 24 hours of discovery, for an eligible breach involving Personal Information provided by the other party. These triggers differ: agree incident escalation that supports all applicable duties.

Does your contract address CPS 230?

Supplied General Terms v3.6 clause 10 retains a CPS 231 reference. Assess the applicable agreement against the current CPS 230 determination, effective 1 July 2026, and agree necessary changes. The supplied clause requires customer notification of relevant standard changes; it does not itself establish that all current CPS 230 duties are covered.

Will we give APRA access if asked?

Where supplied v3.6 clause 10 applies under its APRA/material-business-activity conditions, clause 10.3 requires compliance with an APRA Request within APRA's statutory authority and prompt customer notification. It also restricts disclosure or advertising of the audit, with its stated coordination exception.

How is business continuity tested for APRA-regulated customers?

Where supplied v3.6 clause 10's APRA/material-business-activity conditions apply and the customer requires a BCP under clause 15, clause 10.4 specifies ten content elements, review in connection with customer BCP changes, joint testing every six months or more often on reasonable request, and results within seven days. Clause 10.5 allocates the specified costs at Service Order Time and Materials Rates or, if absent, then-current rates. Agree DRaaS recovery objectives and testing separately.

Where is financial services data held?

Confirm service-specific storage, processing, support and backup locations. Australian hosting statements do not override supplied v3.6 clause 18.3's specified overseas-transfer consent or clause 27.5's subcontracting provisions. Agree location, access and provider-notification terms that support the customer's applicable obligations.

What service levels do you publish for availability?

The Cloud brochure states 99.999 per cent for cloud services and 100 per cent for storage; Connectivity materials state minimum 99.99 per cent under their described redundant design. Confirm the applicable contractual Service Level, measurement period, exclusions and remedy in the Service Order and Service Description. A brochure percentage does not establish every customer's entitlement

or remedy.

What evidence do you have in insurance and financial services?

The published Honan Insurance case study describes a whole-of-business migration to emPOWER Managed Services, Cloud, WAN, IaaS and DRaaS, with the telecommunications bill reduced by around 65 per cent and ISO certification helping Honan bid for work. The case study is undated and its client statistics should be confirmed before reuse.

What technology services do you offer to financial services organisations?

We offer managed IT, cyber security, cloud and connectivity services designed to strengthen security and resilience for financial organisations.

What are the key challenges financial services organisations face according to you?

Financial services organisations face technology risks involving regulatory controls, governance, reporting, sensitive information, identities, service availability and data protection. Applicable obligations depend on the entity, activities and regulatory scope.

How does your service model support financial organisations?

We offer managed services and security capabilities intended to support resilience, governance and accountability, with cloud, connectivity, backup and cyber security services coordinated around the agreed scope. Confirm operational responsibilities, reporting and integrations for the proposed environment.

What business outcomes can financial organisations expect from your integrated services?

The service page presents reduced cost and complexity, resilience, productivity and scalable architecture as intended benefits. Actual outcomes depend on the agreed design, implementation, customer environment and responsibilities; they are not guaranteed regulatory outcomes.

What are the three ways to engage with your operating model?

Our operating model offers three ways to engage: Managed Services (end-to-end ownership of IT operations for reliable performance and measurable outcomes), emPOWER Operational Capability (structured operations, governance and visibility, currently coming soon), and Technology Services (integrated enterprise technology for secure, connected and high-performing IT environments).

Is there a case study related to financial services on your site?

The Financial Services page features Honan Insurance's case study, describing a managed-services, cloud and network engagement supporting regional growth and reliability. Treat its employee band and other client statistics as case-study context rather than verified current figures.

What operational advantages do you aim to help financial organisations achieve?

We aim to help organisations gain actionable insight and operational visibility, improve service performance and user experience, strengthen security posture and compliance outcomes, optimise cost and operational efficiency, and build readiness for AI and future change.

What other industries do you serve besides financial services?

We also serve Healthcare & Aged Care, Not for Profit, Professional Services, Transport & Logistics, Retail & Consumer Services, Utilities, and Government & Public Sector.

How can financial services organisations contact you for support?

For existing-customer support, use the contact and portal agreed for your service. The listed phone numbers are 1300 135 548 in Australia and +61 3 8696 9369 internationally; support@blueapache.com is listed for registered managed-services clients. Remote Access is a support tool rather than a way to open a request. Use the contact page for new enquiries.