Service Overview

SynAck Solutions helps Australian organisations navigate the complex regulatory landscape governing information security. We assess your current posture against applicable requirements — APRA CPS 234, the Privacy Act 1988, SOCI Act, ASD Essential Eight, and PCI DSS — map existing controls to regulatory obligations, and develop practical remediation roadmaps that align security investment with compliance priorities across overlapping frameworks.

Business Value

- Identify and close compliance gaps before regulators or auditors find them
- Consolidate overlapping framework requirements into a unified control set
- Provide boards and executives with defensible evidence of compliance posture
- Reduce risk of regulatory penalties, enforcement actions, and mandatory notifications
- Prioritise security investment based on regulatory risk and business impact
- Accelerate preparation for external audits and prudential reviews
- Demonstrate due diligence to clients, partners, and cyber insurers

What's Included

- Regulatory applicability assessment identifying applicable frameworks
- Current-state compliance assessment against each applicable framework
- Control mapping across overlapping standards (CPS 234, ISO 27001, Essential 8)
- Gap analysis with findings rated by regulatory risk and remediation effort
- Remediation roadmap with specific actions, owners, and target timelines
- Policy and procedure review against regulatory requirements
- Third-party and supply chain risk assessment aligned to CPS 234 and SOCI Act
- Board-ready compliance summary with executive risk dashboard
- Guidance on regulatory notification obligations (NDB, CPS 234, SOCI Act)
- Evidence preparation assistance for regulatory reviews and auditor requests
- Advisory support during the remediation implementation period

Scope

Engagements cover all regulatory frameworks applicable to your industry, size, and operating model, examining people, process, and technology controls.

- APRA CPS 234 — information security capability, incident management, testing
- Privacy Act 1988 and APPs — personal information handling, NDB scheme compliance
- SOCI Act — critical infrastructure risk management programs and reporting
- ASD Essential Eight — maturity assessment and alignment
- PCI DSS v4.0 — cardholder data environment scoping and control assessment
- Industry-specific requirements as applicable (ACSC advisories, state frameworks)

What's Excluded

- Legal advice or formal legal opinions on regulatory interpretation
- QSA services for PCI DSS certification (referral available)
- Implementation of technical controls or security tooling
- Ongoing compliance monitoring beyond the engagement period
- Representation before regulators or in regulatory proceedings
- International frameworks (GDPR, SOX, HIPAA) unless specifically scoped

Methodology

Our methodology draws on ISO 27001:2022 for control framework structure and NIST CSF for maturity assessment. We map existing controls to regulatory obligations, identify gaps, and assess each against likelihood and impact. Priorities follow ISO 31000 and APRA prudential guidance.

Engagement Timeline

Engagements typically run four to eight weeks depending on the number of applicable frameworks. An applicability assessment is completed in the first week, with the full gap analysis and roadmap delivered within four to six weeks. Advisory support during remediation is available for up to twelve months.

Get Started

Contact SynAck Solutions to discuss your regulatory obligations and compliance priorities. We will assess your industry and applicable frameworks, then provide a tailored proposal.

info@synack.au | https://www.synack.au

ABN 88 667 784 956