Service Overview

SynAck Solutions provides cyber risk and compliance consulting that bridges the gap between technical security and governance. We work with your leadership, risk, and IT teams to establish risk management frameworks, conduct risk assessments, develop risk registers and treatment plans, and produce board-ready reporting — all grounded in deep familiarity with APRA CPS 234, the Privacy Act, the SOCI Act, and ISO 27001.

Business Value

- Establish a structured, repeatable cyber risk framework that satisfies regulatory expectations
- Identify and prioritise your most significant cyber risks based on likelihood and impact
- Demonstrate compliance to APRA, the OAIC, and the Cyber and Infrastructure Security Centre
- Provide board and executive leadership with clear, actionable cyber risk reporting
- Reduce audit and compliance costs through well-maintained documentation and evidence
- Align security investment with business risk for greatest risk reduction per dollar
- Satisfy third-party assurance requirements from clients, partners, and supply chain

What's Included

- Cyber risk management framework design or review, aligned with ISO 31000
- Comprehensive risk assessment covering threats, vulnerabilities, controls, and business impact
- Risk register development with ratings calibrated to your risk appetite
- Risk treatment plan with prioritised, costed actions linked to risk register entries
- Compliance gap analysis: APRA CPS 234, Privacy Act, SOCI Act, PCI DSS, Essential 8
- Policy and procedure review: information security, acceptable use, access control, IR
- Board and executive risk reporting with dashboards and strategic recommendations
- Stakeholder workshops to align risk appetite and validate assessment findings
- Third-party and supply chain risk assessment framework development
- Audit preparation and evidence packaging for internal and external audits

Scope

Engagements cover your organisation's cyber risk governance and regulatory obligations:

- Enterprise-wide cyber risk assessment across technology, people, and processes
- Regulatory compliance posture: APRA CPS 234, Privacy Act, SOCI Act, Essential 8, PCI DSS
- Information security policy framework covering core governance documentation
- Board and executive reporting requirements for cyber risk communication
- Third-party and supply chain risk management processes
- Integration with existing enterprise risk management and GRC tooling

What's Excluded

- Technical security testing: penetration testing, vulnerability scanning, red team assessments
- Legal advice or regulatory interpretation (we provide technical compliance guidance)
- Implementation of technical security controls (available via Remediation Assistance)
- Ongoing compliance monitoring or managed GRC services
- Financial risk, operational risk, or non-cyber risk domains

Methodology

Our methodology is grounded in ISO 31000 for risk framework design, ISO 27005 for cyber risk assessment, and ISO 27001 for ISMS alignment. We incorporate the NIST CSF for maturity benchmarking and apply APRA CPG 234 and ACSC Essential 8 guidance. Assessments are calibrated against current threat intelligence.

Engagement Timeline

A comprehensive engagement runs four to eight weeks depending on organisational size and regulatory complexity. Stakeholder workshops and document review complete in weeks one and two, with assessment and treatment planning over weeks three to six. Final deliverables provided within five business days of completion.

Get Started

Contact SynAck Solutions to discuss your cyber risk and compliance requirements. Whether preparing for regulatory review, building a risk framework, or seeking independent assurance, our consultants deliver practical, defensible outcomes.

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

ABN 88 667 784 956