Service Overview

SynAck Solutions guides organisations through the complete ISO 27001 certification journey — from initial gap analysis to certification readiness. We build practical, sustainable Information Security Management Systems aligned to ISO/IEC 27001:2022, focusing on genuine risk management and internal capability so your team can maintain the ISMS independently after certification.

Business Value

- Achieve ISO 27001 certification with a structured, milestone-driven program
- Demonstrate security maturity to clients, partners, regulators, and cyber insurers
- Satisfy contractual and tender requirements mandating ISO 27001 certification
- Establish risk-based security that prioritises investment where it matters most
- Build internal ISMS capability to maintain certification without external dependency
- Align with APRA CPS 234, SOCI Act, and international best practice
- Streamline compliance with overlapping frameworks using ISO 27001 as the foundation

What's Included

- ISMS scoping workshop to define context, interested parties, and boundaries
- Gap analysis against ISO/IEC 27001:2022 clauses and Annex A controls
- Risk assessment framework design with criteria and acceptance thresholds
- Information security risk assessment and risk treatment planning
- Statement of Applicability (SoA) mapping controls to identified risks
- ISMS policy suite — information security, access control, incident management
- Procedure documentation for internal audit, management review, and corrective action
- Control implementation guidance and validation for Annex A controls
- Internal audit program design and pre-certification audit execution
- Management review facilitation with documented outputs
- Stage 1 readiness assessment and Stage 2 preparation including mock audit

Scope

The engagement covers the full ISMS lifecycle from scoping through certification readiness. ISMS scope is defined collaboratively and typically covers:

- Organisational context analysis including internal/external issues (Clause 4)
- Leadership and governance structures for ISMS operation (Clause 5)
- Risk assessment and treatment processes (Clauses 6 and 8)
- All 93 Annex A controls across organisational, people, physical, and technology domains
- Operational processes: competence, awareness, communication (Clause 7)
- Performance evaluation: monitoring, internal audit, management review (Clause 9)

What's Excluded

- Certification body audit fees (paid directly to the certification body)
- Procurement or implementation of security technologies
- Ongoing ISMS management after certification (available as ISO 27000 Augmentation)
- Legal advice on regulatory interpretation or contractual obligations
- Penetration testing or technical vulnerability assessments
- Remediation of technical vulnerabilities (available as Remediation Assistance)

Methodology

Our methodology follows the Plan-Do-Check-Act cycle prescribed by ISO 27001:2022. Risk assessment follows ISO 27005 guidance, control selection is driven by the risk treatment plan mapped to Annex A. Internal audit methodology follows ISO 19011 guidelines, and readiness assessment mirrors accredited certification body processes.

Engagement Timeline

Engagements typically span three to six months depending on organisational size and control maturity. Gap analysis and roadmap are delivered within three weeks. Policy development and control implementation run in monthly sprints, with the pre-certification audit conducted in the final month.

Get Started

Contact SynAck Solutions to discuss your ISO 27001 certification objectives. We will assess your organisation's size, industry, and certification timeline, then provide a tailored implementation proposal.

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

ABN 88 667 784 956