Service Overview

SynAck Solutions provides rigorous, evidence-based assessment of your organisation's Essential Eight maturity across all eight ASD mitigation strategies. We perform hands-on technical validation — not just questionnaires — using criteria from the ASD Essential Eight Maturity Model, identify gaps against your target maturity level, and deliver a prioritised remediation roadmap. Increasingly mandated for Commonwealth entities and recommended by APRA and the ACSC.

Business Value

- Establish clear, evidence-based understanding of current Essential Eight maturity
- Identify specific technical and procedural gaps preventing maturity advancement
- Receive a prioritised remediation roadmap aligned with measurable maturity improvement
- Satisfy regulatory expectations from APRA, ACSC, and Commonwealth procurement
- Reduce exposure to ransomware, credential theft, and malicious code execution
- Demonstrate cybersecurity due diligence to boards, clients, and insurance underwriters
- Benchmark maturity against industry peers and ASD's recommended baselines

What's Included

- Scoping workshop to confirm target maturity level and assessment boundaries
- Technical assessment of all eight strategies against the ASD Maturity Model
- Application control validation — whitelisting enforcement and bypass resistance
- Patch management assessment for applications and operating systems
- Microsoft Office macro settings review — Group Policy and enforcement validation
- User application hardening — browser, OLE blocking, and PowerShell configuration
- Administrative privilege restriction — tiering, JIT/JEA, and credential exposure
- MFA assessment — coverage, strength, and phishing resistance
- Regular backups validation — coverage, integrity, offline storage, and restoration
- Current maturity scorecard with per-strategy ratings and evidence
- Prioritised remediation roadmap with effort estimates and quick wins

Scope

The assessment covers all eight ASD Essential Eight strategies. Scope is defined during the initial workshop and typically includes systems critical to business operations.

- Application control — policy configuration, enforcement, and rule integrity
- Patch applications — patching processes, vulnerability scanning, and SLA adherence
- Microsoft Office macro settings — execution policies and trust configuration
- User application hardening — browser settings, OLE, and PowerShell controls
- Restrict administrative privileges — account inventory, tiering, and PAM solutions
- Patch operating systems — scan coverage, SLA compliance, and EOL management
- Multi-factor authentication — deployment coverage and phishing-resistant methods
- Regular backups — scope, frequency, integrity verification, and recovery testing

What's Excluded

- Implementation of remediation actions (available as Remediation Assistance)
- Assessment of controls beyond the Essential Eight framework
- Penetration testing or adversary simulation (available separately)
- Procurement or deployment of security tooling or software
- Formal IRAP or ASD certification — this provides internal assurance

Methodology

Our methodology aligns to the ASD Essential Eight Maturity Model and ACSC assessment guidance. Each strategy is evaluated through technical testing, configuration review, and policy analysis. Maturity levels follow ASD criteria from Level Zero through Level Three, with remediation prioritised by effort and security uplift.

Engagement Timeline

Engagements typically span two to four weeks. Scoping and data collection complete in week one, technical assessment over one to two weeks, with the maturity scorecard and remediation roadmap delivered within five business days of completion. Reassessment available quarterly or six-monthly.

Get Started

Contact SynAck Solutions to discuss your Essential Eight maturity objectives. We'll assess your environment and regulatory context, then provide a tailored proposal.

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

ABN 88 667 784 956