



Service Overview

SynAck Solutions delivers end-to-end business continuity and disaster recovery consulting — from business impact analysis and risk assessment through to plan development, tabletop exercises, and simulation testing. Our approach integrates cyber resilience into traditional BCP/DRP frameworks, ensuring your organisation can maintain critical operations and recover within acceptable timeframes during any disruptive event.

Business Value

- Ensure critical functions continue operating during disruptions, minimising revenue loss
- Define and validate recovery time objectives (RTOs) and recovery point objectives (RPOs)
- Satisfy regulatory requirements under APRA CPS 232, SOCI Act, and ISO 22301
- Reduce financial impact through pre-planned response procedures that accelerate recovery
- Identify single points of failure and critical dependencies across the organisation
- Build confidence through regular testing and validation of continuity plans
- Demonstrate resilience to clients, partners, insurers, and regulators

What's Included

- Business impact analysis identifying critical functions, dependencies, and downtime thresholds
- Risk assessment of disruption scenarios: cyber incidents, natural disasters, supply chain failures
- Recovery strategy development for maintaining and restoring critical functions
- BCP documentation: activation criteria, roles, communications, and recovery workflows
- Disaster recovery plan for IT systems: failover, backup validation, and restoration sequences
- Crisis communication plan with stakeholder notification templates and escalation procedures
- Tabletop exercise design and facilitation using realistic disruption scenarios
- Plan maintenance framework with review cycles, update triggers, and accountability
- Gap analysis against ISO 22301 and APRA CPS 232 requirements
- Executive summary and board reporting pack with improvement recommendations

Scope

Engagements cover the people, processes, and technology required to maintain and recover critical business functions:

- Critical business function identification and prioritisation across all units
- IT disaster recovery for on-premises, cloud, and hybrid architectures
- Supply chain and third-party dependency analysis for critical providers
- Cyber incident scenarios including ransomware, data breach, and system compromise
- Workplace disruption scenarios including site inaccessibility and remote working
- Communication and stakeholder management during crisis events

What's Excluded

- Implementation of technical DR infrastructure (available via Disaster Recovery as a Service)
- Incident response execution during active security incidents (see Incident Response)
- Insurance procurement or claims management
- Legal advice on contractual or regulatory obligations during disruptions
- Ongoing plan maintenance — we establish frameworks; your organisation retains ownership

Methodology

Our methodology aligns with ISO 22301 for plan structure and lifecycle, NIST SP 800-34 for IT disaster recovery, and ISO 22317 for business impact analysis. Risk assessment incorporates ISO 31000 fundamentals. For APRA-regulated entities, we ensure alignment with CPS 232 and CPG 233.

Engagement Timeline

A comprehensive BCP engagement runs six to ten weeks depending on organisational complexity. BIA and risk assessment complete in weeks one through four, with plan development following. Tabletop exercises are scheduled after plan delivery. Annual review and exercise retainers are available.

Get Started

Contact SynAck Solutions to discuss your business continuity and disaster recovery requirements. We deliver practical, testable plans tailored to your operations and regulatory obligations.

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

ABN 88 667 784 956