



## Service Overview

SynAck Solutions' DRaaS provides cloud-based disaster recovery infrastructure, automated failover, and tested recovery procedures that ensure your organisation resumes critical operations within defined RTO and RPO targets. Our solution replicates critical workloads to geographically separated Australian cloud infrastructure, with automated failover orchestration and regularly validated runbooks — so recovery works in practice, not just theory.

## Business Value

- Ensure business continuity with defined, tested RTO and RPO targets for critical systems
- Eliminate capital expenditure of maintaining dedicated disaster recovery infrastructure
- Reduce recovery time from days to hours through automated failover orchestration
- Protect against ransomware with immutable, air-gapped backup replicas
- Satisfy audit requirements for DR testing under APRA CPS 232 and ISO 22301
- Minimise data loss with continuous replication to geographically separated infrastructure
- Provide board confidence through regular, documented DR test results

## What's Included

- DR architecture design and cloud replication infrastructure deployment
- Continuous data replication to Australian-hosted cloud infrastructure (AWS, Azure, or GCP)
- Automated failover orchestration with defined boot sequences and dependency mapping
- Recovery runbook development and maintenance for each protected workload
- Quarterly full failover testing with documented results for audit evidence
- Tabletop DR exercises with IT and business stakeholders
- RTO/RPO monitoring and alerting with real-time replication lag visibility
- Immutable backup copies with configurable retention for ransomware resilience
- Failback procedures and support for returning to primary infrastructure
- Monthly replication health report with RPO compliance metrics
- 24/7 failover activation support with defined escalation procedures

## Scope

DRaaS scope is defined by your critical workloads and recovery requirements identified through a Business Impact Analysis (BIA).

- Server workloads: physical and virtual servers (VMware, Hyper-V, KVM) replicated to cloud
- Cloud-native workloads: AWS, Azure, and GCP instances with cross-region replication
- Database systems: SQL Server, PostgreSQL, MySQL, Oracle with consistent replication
- File and object storage: critical file shares, document management, and object storage
- Active Directory and identity infrastructure required for failover authentication
- Network connectivity: VPN, DNS failover, and load balancer reconfiguration

## What's Excluded

- Endpoint device backup and recovery (laptops, desktops, mobile devices)
- Application-level high availability (active-active clustering, multi-site)
- BCP documentation beyond IT disaster recovery — available via our BCP service
- Telecommunications and voice system failover (PBX, contact centre platforms)
- Physical site recovery (alternate workspace, logistics, personnel mobilisation)
- Cloud infrastructure hosting costs — billed separately based on consumption

## Methodology

Our methodology aligns with ISO 22301, NIST SP 800-34, and APRA CPS 232. Recovery planning begins with a BIA to identify critical functions, maximum tolerable downtime, and data loss thresholds. RTO/RPO targets are defined per workload, and quarterly failover tests validate end-to-end recovery capability with auditable documentation.

## Engagement Timeline

Initial engagement — including BIA review, architecture design, and replication deployment — completes within four to eight weeks. First full failover test is conducted within twelve weeks. Ongoing service includes quarterly DR tests, monthly reporting, and annual strategy reviews on a twelve-month minimum term.

## Get Started

Contact SynAck Solutions to schedule a disaster recovery readiness assessment. We'll review your current capabilities, define RTO/RPO targets, and design a DRaaS solution that ensures rapid, confident recovery.

[info@synack.au](mailto:info@synack.au) | <https://www.synack.au>

ABN 88 667 784 956