


CredEntry

Powered by 

APPENDIX E.8

RECOVERY RUNBOOKS & CHECKLISTS

Contents

1. Purpose and Scope	2
2. General Incident Response & Management	2
2.1 Detection & Initial Triage Checklist	2
2.2 Escalation Checklist	2
2.3 Crisis Communication Checklist	2
3. Recovery Runbooks for Critical Functions	3
3.1 Complete Service Outage (Priority 1)	3
3.2 Regional Failover	3
3.3 Data Corruption/Loss	3
3.4 Security Breach Scenarios	3
3.5 PKI / Key Compromise.....	3
4. Regular Testing & Maintenance Checklists	4
5. Roles & Responsibilities (Recovery Operations)	4
6. External Dependencies & SLAs	4
7. Document Control	4

1. Purpose and Scope

This appendix defines the **operational recovery procedures and checklists** that underpin the Business Continuity and Disaster Recovery Plan (Appendix E.7).

These runbooks ensure that incident response, crisis communications, and disaster recovery are executed consistently and within the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) defined in:

- **Service Level Agreement (Appendix E.1)**
- **BCP/DRP (Appendix E.7)**
- **Escalation & Communications Templates (Appendix E.5)**

2. General Incident Response & Management

2.1 Detection & Initial Triage Checklist

- Continuous monitoring (Azure Monitor, Sentinel SIEM/SOAR, Event Hubs).
- Real-time alert review.
- 24/7 L1 Perth Support centre intake.
- Severity classification:
 - **Priority 1 (Critical):** Outage, verified breach, credential verification failure.
 - **Priority 2 (High):** Significant but contained degradation.
 - **Priority 3 (Moderate/Low):** Limited impact.

2.2 Escalation Checklist

- Notify **DPC Contract Manager within 15 minutes** for Priority 1 incidents.
- Escalation: L1 Perth Support → L2 Tech Lead → Incident Manager → Customer Contract Manager.
- Specialist teams engaged (Security IR, DevOps, Project Manager).
- Notify external dependencies (IdX, DTP, OEM wallets, CAs) as required.

2.3 Crisis Communication Checklist

- Notify internal leadership, legal, comms.
- Notify **DPC Contract Manager within 15 minutes (P1)**.
- OAIC notification within 72 hours if Privacy Act breach.
- Use **pre-approved templates (Appendix E.5)**.
- Seek DPC approval before public disclosure.

3. Recovery Runbooks for Critical Functions

3.1 Complete Service Outage (Priority 1)

- Trigger: Core outage (verification, revocation).
- Restore via Azure Front Door failover ($\leq 2\text{h}$ RTO, $\leq 15\text{m}$ RPO).
- Validate PostgreSQL, Storage, PKI synchronisation.
- Notify stakeholders with ETA.
- RCA post-restoration.

3.2 Regional Failover

- Trigger: Outage in one sovereign region.
- Redirect via Azure Front Door.
- Confirm replication of storage/DB, HSM integrity.
- Validate Redis, Service Bus, Functions.
- Restore service $\leq 4\text{h}$ RTO, zero data loss.

3.3 Data Corruption/Loss

- Trigger: Corruption, deletion, degradation.
- Isolate systems; restore PostgreSQL PITR / backups.
- Validate via hash checks.
- Notify stakeholders, conduct RCA.

3.4 Security Breach Scenarios

(a) **Ransomware/Malware** – Isolate, preserve logs, restore clean backups, run post-remediation scans.

(b) **DDoS Attack** – Engage Azure DDoS Protection Standard, apply rate limits, monitor abnormal traffic.

(c) **Insider Threat** – Immediately revoke access via JIT/RBAC, conduct forensic analysis, notify DPC.

For all: Notify OAIC if PII compromised; RCA + PIR within 5 business days.

3.5 PKI / Key Compromise

- Detect via Key Vault monitoring.
- Revoke compromised certs; generate new HSM keys.
- Publish updated trust lists.
- Re-issue affected credentials.
- Notify stakeholders and issuers.

4. Regular Testing & Maintenance Checklists

- **Monthly:** Backup restoration tests; service failover drills; vulnerability scans.
- **Quarterly:** Regional failover drills; IdX/ServiceWA integration tests.
- **Annual:** Full DR simulation; penetration test; third-party compliance audit.
- **Semi-Annual:** Tabletop exercises (decision-making & comms).
- **Secure Development:** Continuous SAST/DAST scans, code reviews, OWASP ASVS compliance.

5. Roles & Responsibilities (Recovery Operations)

Role	Responsibilities	Primary Contact	Alternate Contact
Incident Manager	Overall coordination, DPC liaison	Justin Hancock – Project Delivery Lead	Shelby Long – Implementation Specialist
Infrastructure Recovery Lead	Azure infrastructure, regional failover	Rodrigo Miranda – FullStack DevOps	Marcus Abreu – Senior Solution Architect
Application Recovery Lead	Application fixes, deployments	Marcus Abreu – Senior Solution Architect	Marisa Cardoso – Quality Assurance
Security & IR Lead	Containment, forensic analysis, OAIC notifications	Flavia C – Security & Compliance Officer	Shelby Long – Implementation Specialist
Data Recovery Specialist	Backup restore, DB validation	Zachariah Adams – Technical Support Lead	Credential Management / DB Admin (internal team)
Communications Lead	Stakeholder and DPC comms	Shelby Long – Implementation Specialist	WA Contract Manager (DPC)
Customer Approval	Formal government liaison	DPC Contract Manager	DPC Performance Manager

6. External Dependencies & SLAs

Dependency	Function	SLA / RTO	Contact Protocol
IdX/DTP	Identity verification	2h SLA	Notify via DGov channel
OEM Wallets	Wallet integration	4h SLA	Vendor support portal
Certificate Authorities	PKI trust	24h SLA	CA emergency hotline

7. Document Control

- **Version:** 2.0 (or latest)
- **Last Updated:** September 2025
- **Next Review:** December 2025 (quarterly); full annual review 2026
- **Owner:** WA Project Delivery Lead
- **Storage:** SharePoint ISMS (restricted access)
- **Approval:** DPC Contract Manager