


# CredEntry

Powered by 

## APPENDIX E.7

### BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY PLAN

## Table of Contents

1. Executive Summary and Governance Context .....	2
2. Standards and Regulatory Compliance.....	2
3. Scope and Coverage.....	2
4. Risk Assessment & Business Impact Analysis .....	2
5. Business Continuity Strategy .....	3
6. Service Levels & Recovery Objectives.....	3
7. Incident Response & Recovery .....	3
8. Roles & Responsibilities (Recovery Operations).....	4
9. Testing & Continuous Improvement.....	4
10. Organisational Capability.....	4
11. Compliance & Assurance .....	4
12. Commercial Considerations.....	5
13. Document Control .....	5

## 1. Executive Summary and Governance Context

This BCP/DRP establishes CredEntry’s approach to ensuring uninterrupted delivery of the WA Government Digital Wallet and Verifiable Credentials Solution.

- Supports Digital WA Strategy by ensuring seamless digital service delivery.
- Meets WA Cyber Security Policy requirements through defence-in-depth resilience.
- Enables ServiceWA Integration by ensuring continuous wallet functionality.
- Maintains citizen trust by protecting credential availability, security, and privacy during service disruptions.

Governed under clauses **47 (Business Continuity)** and **48 (Disaster Recovery)** of the Agreement.

## 2. Standards and Regulatory Compliance

Aligned with:

- ISO/IEC 22301:2019 (Business Continuity)
- ISO/IEC 27001:2022 (Information Security)
- ISO/IEC 18013-5:2021 / 18013-7:2024 (mDL standards)
- ISO/IEC 23220-1:2023 (mobile eID)
- ISO/IEC 12207:2017 (software lifecycle)
- ISO/IEC 29100:2024 (privacy)
- ISO/IEC 19790:2025 (crypto modules)
- ISO 9001:2015 / 90003:2018 (quality management)
- ACSC Essential Eight, IRAP PROTECTED, OWASP ASVS, W3C Verifiable Credentials, TDIF 4.8, eIDAS 2.0

**Certification roadmap:** ISO/IEC 27001 re-certification (Pilot Phase), IRAP PROTECTED alignment.

## 3. Scope and Coverage

**Within Scope:** SaaS wallet platform, SDK integration, credential lifecycle services, PKI, APIs (IdX, DTP), admin dashboard, monitoring, WA-based support, backup & recovery.

**Out of Scope:** ServiceWA app infrastructure (Adaptor), source systems, end-user devices, GovNext-IP.

## 4. Risk Assessment & Business Impact Analysis

**Critical Functions Priority Matrix**

Function	Criticality	Citizen Impact	Agency Impact	Priority
<b>Credential Verification</b>	Critical	High	High	1
<b>Real-time Revocation</b>	Critical	High	High	1
<b>Credential Issuance</b>	High	Medium	High	2
<b>SDK/API Endpoints</b>	High	High	Medium	2
<b>Admin Dashboard</b>	Medium	Low	Medium	3
<b>Analytics &amp; Reporting</b>	Low	Low	Low	4

**Threat Landscape:** APTs, ransomware, DDoS, supply chain risks (Azure SDKs), social engineering, Azure outages, database corruption, config errors, key staff unavailability.

#### Impact Scenarios:

- Complete Service Outage: RTO 2 hrs, RPO 15 min.
- Regional Failover: RTO 4 hrs, zero data loss.

## 5. Business Continuity Strategy

#### Resilience Architecture

- Multi-region active-active Azure deployment.
- Tenant isolation, per-agency cryptographic keys.
- Zero-trust model (MFA, RBAC, TLS 1.3, AES-256).
- Continuous monitoring (Microsoft Sentinel).

#### Data Sovereignty

- All data stored in Australian regions.
- Keys in Azure HSM (Australia only).
- Retention: 7 yrs logs, 35-day PITR.
- Testing: monthly restores, quarterly failovers.

## 6. Service Levels & Recovery Objectives

Service Component	Availability	RTO	RPO	Measurement
<b>Credential Verification</b>	99.95%	2 hrs	15 min	Monthly
<b>Revocation Services</b>	99.95%	2 hrs	5 min	Monthly
<b>Credential Issuance</b>	99.90%	4 hrs	15 min	Monthly
<b>SDK/API Endpoints</b>	99.90%	4 hrs	30 min	Monthly
<b>Admin Dashboard</b>	99.80%	24 hrs	1 hr	Monthly

## 7. Incident Response & Recovery

- **Priority 1:** Response 15 min, resolution 2–4 hrs.
- **Escalation path:** L1 Perth Support → L2 Tech Lead → Incident Manager → Customer Contract Manager.
- **Customer notification:** DPC Contract Manager informed within 15 min.
- **Failover:** Automatic Azure Front Door redirection; manual E2E verification.
- **Security response:** Immediate containment, forensic evidence, OAIC within 72 hrs if privacy breach.
- **Records:** Stored in SharePoint, retained per ISO/IEC 27001.

## 8. Roles & Responsibilities (Recovery Operations)

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

## 9. Testing & Continuous Improvement

- **Monthly:** Backup restores, service failover, vulnerability scans.
- **Quarterly:** Regional failover drills, tenant isolation checks, IdX/ServiceWA integration tests.
- **Annual:** DR simulation, external audit, penetration testing.
- **Post-incident:** RCA within 5 business days; BCP/DRP updated within 10 days.

## 10. Organisational Capability

- 24/7 WA-based support centre (Perth).
- Project Delivery Lead: WA-based, 15-min escalation.
- Certified Security IR team (CISSP/CISM).
- Development team 2-hr integration response.
- No subcontractors: full accountability.

## 11. Compliance & Assurance

- Privacy Act 1988 (APPs), Australian Digital ID Act 2024.
- Quarterly compliance reports (ISO, Essential Eight, pen test results).
- Regular assurance to DPC via governance forums.

## 12. Commercial Considerations

- Service credits for SLA breaches: 5–25% of monthly fee.
- Insurance: Cyber liability & professional indemnity up to \$50M.

## 13. Document Control

- Classification: OFFICIAL Sensitive
- Review Cycle: Quarterly; annual full review.
- Next Review: December 2025
- Owner: WA Project Delivery Lead
- Customer Approval: DPC Contract Manager