


# CredEntry

Powered by 

## APPENDIX E.6

## TESTING METHODOLOGY, RESULTS & IMPROVEMENT LOG

## Table of Contents

1. Purpose and Scope .....	2
2. Testing Methodology .....	2
2.1 Objectives .....	2
2.2 Testing Types & Frequency .....	3
2.3 Testing Environments .....	3
2.4 Standards Alignment.....	3
3. Results, Evidence & Reporting.....	3
3.1 Acceptance Criteria.....	3
3.2 Artefacts & Evidence Pack .....	3
3.3 Reporting (Appendix E.4 – Reporting Matrix).....	4
3.4 Stakeholder Communication (Appendix E.5 – Communications Templates & Emergency Escalation Contacts).....	4
4. Continuous Improvement.....	4
4.1 Issue Tracking & Root Cause Analysis.....	4
4.2 Corrective & Remedial Actions .....	4
4.3 Updates to Plans & Documents .....	4
4.4 Governance & Metrics .....	4
5. Dependencies & Readiness Gates .....	5

## 1. Purpose and Scope

This appendix defines CredEntry's structured approach to testing the resilience, security, performance, and operability of the Digital Wallet and Verifiable Credentials Solution.

It aligns with and is supported by:

- **Appendix E.1 – Service Level Agreement (SLA)** (availability, RTO/RPO, incident response, vulnerability remediation).
- **Appendix E.2 – Training Plan** (UAT readiness, role-based training linked to test outcomes).
- **Appendix E.3 – Release & Onboarding Process Flow** (release gates, pilot/production readiness testing).
- **Appendix E.4 – Reporting Matrix** (frequency, owners, recipients of test reports).
- **Appendix E.5 – Communications Templates & Emergency Escalation Contacts** (incident and test notification templates and escalation contacts).
- **Appendix E.7 – Business Continuity Plan & Disaster Recovery Plan** (resilience architecture, recovery objectives, continuity testing).
- **Appendix E.8 – Recovery Runbooks & Checklists** (step-by-step operational recovery procedures used during tests).
- **Appendix E.9 – Standards Compliance Mapping** (ISO/IEC 22301, 27001, 18013-5/-7, 23220-1, ACSC Essential Eight, TDIF, eIDAS 2.0).

## 2. Testing Methodology

### 2.1 Objectives

- Validate compliance with Business Continuity and Disaster Recovery requirements (per Appendix E.7).
- Ensure the solution meets functional, security, and integration expectations.
- Confirm SLA targets (availability, response/resolution, RTO/RPO) defined in Appendix E.1 are consistently met.
- Support continuous improvement and incident prevention.
- Demonstrate readiness for major events, onboarding milestones, and environmental changes (Appendix E.3).

## 2.2 Testing Types & Frequency

Frequency	Activities	Linked Evidence	Reporting Obligation (Appendix E.4)
<b>Monthly</b>	Backup restoration; partial failover simulation; vulnerability scanning	Recovery steps (Appendix E.8), SLA metrics (Appendix E.1)	SLA Compliance Report; Incident Notification (if triggered)
<b>Quarterly</b>	Regional failover drills; tenant isolation checks; ServiceWA/IdX integration tests	BCP/DRP alignment (Appendix E.7), runbook validation (Appendix E.8)	Vulnerability Scan Report; Continuous Improvement & Trend Analysis
<b>Annual</b>	Full DR simulation; third-party penetration test; system-wide UAT	BCP/DRP scenarios (Appendix E.7); Release gates (Appendix E.3)	Testing Results & Improvement Log; Annual Performance & Roadmap Review
<b>Ad hoc</b>	Cyber incident simulation; emergency failover; onboarding release verification	Crisis comms templates (Appendix E.5); Runbooks (Appendix E.8)	Cybersecurity Incident Report (CR-3); PIR (≤5 business days)

## 2.3 Testing Environments

- **Pre-Production Staging:** Mirrors production; used for all major tests and UAT.
- **Pilot/Test Infrastructure:** Used for SDK integration and onboarding validation (Appendix E.3).
- **Production:** Limited to monitoring and controlled failover testing.

## 2.4 Standards Alignment

Testing is aligned with standards documented in **Appendix E.9 – Standards Compliance Mapping**:

- ISO/IEC 27001:2022 – Information Security Management Systems
- ISO/IEC 22301:2019 – Business Continuity Management
- ISO/IEC 18013-5 & 18013-7 – Mobile Driving Licence standards
- ISO/IEC 23220-1:2023 – Mobile eID architecture
- ACSC Essential Eight; OWASP ASVS; TDIF 4.8; eIDAS 2.0; IRAP PROTECTED alignment

## 3. Results, Evidence & Reporting

### 3.1 Acceptance Criteria

A test cycle is successful if:

- Functional and technical specifications are met.
- SLA service levels (Appendix E.1) are achieved.
- RTO/RPO recovery objectives (Appendix E.7) are met.
- UAT and onboarding validation (Appendix E.3) is signed off.
- Runbooks (Appendix E.8) execute without deviation.

### 3.2 Artefacts & Evidence Pack

Evidence is maintained in SharePoint (per governance model in Appendix E.4) and includes:

- Test execution reports, defect logs, UAT sign-offs.
- Vulnerability scan and pen test results (linked to Appendix E.1 remediation timelines).
- DR drill timings vs RTO/RPO (Appendix E.7).
- Runbook execution checklists (Appendix E.8).
- PIRs, CAPs, PRPs (Appendix E.1 & E.5).

### 3.3 Reporting (Appendix E.4 – Reporting Matrix)

- **Testing Results & Improvement Log** – after each major cycle, annually consolidated. Owner: QA Lead.
- **SLA Compliance Report** – monthly; includes test data where relevant. Owner: Project Delivery Lead.
- **Vulnerability Scan Report** – quarterly and post-release. Owner: Security & Compliance Officer.
- **Continuous Improvement & Trend Analysis** – quarterly. Owner: Implementation Specialist.
- **Post-Incident Report (PIRs)** – ≤5 business days for Severity 1–2. Owner: Project Delivery Lead.
- **Cybersecurity Incident Reports** – ≤24 hours of detection. Owner: Technical Support Lead.

### 3.4 Stakeholder Communication (Appendix E.5 – Communications Templates & Emergency Escalation Contacts)

- Severity 1: notify Contract Manager within 15 minutes.
- Severity 2: notify within 30 minutes (business hours) or 2 hours after-hours.
- Security/Privacy incidents: ≤24h to DGov Security; ≤72h OAIC if Privacy Act breach.

## 4. Continuous Improvement

### 4.1 Issue Tracking & Root Cause Analysis

- All failures/incidents logged and triaged. RCA within 5 business days.
- Unresolved risks entered into the Risk Register (per Appendix E.7).

### 4.2 Corrective & Remedial Actions

- **Corrective Action Plans (CAPs)** for critical deviations (Appendix E.1).
- **Performance Remediation Plans (PRPs)** for repeat issues (Appendix E.1).

### 4.3 Updates to Plans & Documents

- BCP/DRP (Appendix E.7), Runbooks (Appendix E.8), and Training materials (Appendix E.2) updated within 10 days of a critical incident/test failure.
- Test plans reviewed annually or after major releases (Appendix E.3).

### 4.4 Governance & Metrics

Metrics (per Appendix E.4 governance forums):

- MTTD/MTTR, % tests passed first attempt, vulnerability ageing, DR drill timings.
- Persistent breaches → CAP/PRP under Schedule 6 and Appendix E.1 SLA.

## 5. Dependencies & Readiness Gates

Release and onboarding readiness gates (per Appendix E.3):

- QA sign-off, security clearance (Appendix E.1), continuity rehearsal (Appendix E.7/E.8), UAT approval, and training updates (Appendix E.2).

External dependencies: IdX, DTP, OEM wallets, and CAs, managed under Appendix E.8.

