


CredEntry

Powered by 

APPENDIX E.9

STANDARDS COMPLIANCE MAPPING

Table of Contents

1. Purpose and Scope	2
2. Business Continuity & Disaster Recovery Standards	2
3. Information Security & Cyber Resilience Standards	2
4. Digital Identity & Interoperability Standards	3
5. Privacy & Data Protection Standards	3
6. Quality & Software Engineering Standards	3
7. Technical Implementation Standards	3
8. Compliance Reporting & Assurance	3
9. Standards Compliance Mapping (Matrix View)	4
10. Diagram	6

1. Purpose and Scope

This appendix outlines CredEntry's alignment with **international standards, Australian frameworks, and WA Government requirements** relevant to the Digital Wallet and Verifiable Credentials Solution.

It demonstrates how CredEntry's Business Continuity Plan (BCP), Disaster Recovery Plan (DRP), and platform design meet — or are progressing towards — critical compliance obligations.

2. Business Continuity & Disaster Recovery Standards

- **ISO/IEC 22301:2019 – Business Continuity Management Systems**
CredEntry's BCP/DRP is explicitly structured around ISO 22301, with regular testing (monthly backup and failover, quarterly regional drills, annual full DR simulation). Post-incident reviews and continuous updates ensure ongoing alignment.
- **Digital Wallet and Verifiable Credentials Agreement (Clauses 47 & 48)**
CredEntry fulfils contractual obligations for Business Continuity and Disaster Recovery Services, with immediate notification, mitigation, and restoration. All costs for recovery actions arising from CredEntry systems are borne by CredEntry.

3. Information Security & Cyber Resilience Standards

- **ISO/IEC 27001:2022 – Information Security Management Systems**
Re-certification in progress (completion during Pilot Phase). ISMS practices include encrypted credential storage, RBAC, secure deletion, audit logging, and controlled SharePoint repositories.
- **WA Cyber Security Policy (2024)**
Defence-in-depth model with 24-hour incident reporting, interoperable open data formats, and configuration exportability.
- **ACSC Essential Eight**
MFA, patching, application control, and restricted admin privileges implemented to Maturity Level One (or equivalent), tracked quarterly.
- **IRAP PROTECTED**
Alignment in progress with ASD-accredited assessors engaged during Pilot Phase.
- **ISO/IEC 19790:2025 – Cryptographic Modules**
AES-256 and TLS 1.3 encryption, key rotation, HSM integration via Azure Key Vault.
- **OWASP ASVS & OWASP API Security Top 10**
APIs and SDKs tested for vulnerabilities, remediation targets defined in SLA.
- **Zero-Trust Architecture**
MFA, just-in-time RBAC, encryption, and continuous monitoring.
- **Secure by Design (ACSC Foundations)**
Secure release management and vulnerability remediation integrated into SLA.
- **Security Incident Response**
Immediate containment, forensic preservation, OAIC notification $\leq 72h$, RCA and PIR reporting.
- **Vulnerability & Penetration Testing**
Monthly automated scans, annual penetration tests, automated SAST/DAST in CI/CD.
- **Key Management**
Sovereign Azure HSM key lifecycle (generation, rotation, destruction). SaaS IACA PKI managed by CredEntry; Root CA oversight retained by DPC.

4. Digital Identity & Interoperability Standards

- **ISO/IEC 18013-5:2021 / 18013-7:2024 (Mobile Driving Licence)** – mDL-ready with offline/online presentation, OIDC4VP support.
- **ISO/IEC 23220-1:2023 (Mobile eID Architectures)** – Modular, supports revocation, polling, event-driven issuance.
- **W3C Verifiable Credentials & DID** – Rapid updates (<5 min), selective disclosure, DID resolution.
- **Trusted Digital Identity Framework (TDIF 4.8)** – Data minimisation, governance reporting.
- **eIDAS 2.0** – PKI trust, issuer revocation, schema templates, remote verification.
- **OID4VCI & OIDC4VP** – APIs/SDKs conform to issuance and presentation protocols.
- **Australian Digital ID Act 2024** – Designed for compliance with interoperability, audit trails, and roadmap for Auth Level 2 biometrics.

5. Privacy & Data Protection Standards

- **Privacy Act 1988 (Cth) & APPs** – Privacy-by-design, selective disclosure, OAIC notification ≤72h.
- **ISO/IEC 29100:2024 – Privacy Framework** – Data minimisation, purpose limitation, attribute-level selective disclosure.
- **GDPR** – Data minimisation, user dashboards, delegated credential rights.
- **Data Sovereignty** – All data and cryptographic material stored in Australian sovereign regions.
- **Data Minimisation & Consent** – Consent receipts, obfuscation of PII.

6. Quality & Software Engineering Standards

- **ISO 9001:2015 / 90003:2018** – Quality management aligned to onboarding and production readiness. Certification targeted by end of Pilot Phase.
- **ISO/IEC 12207:2017** – Software lifecycle processes aligned to development and maintenance. Certification targeted by end of Pilot.
- **ITIL v4** – Incident response, SLA management, remediation aligned to ITIL service practices.

7. Technical Implementation Standards

- **OpenAPI 3** – API documentation for all endpoints.
- **WCAG 2.2+** – Interfaces tested to WCAG 2.2 AA accessibility standards.
- **Webhooks** – Event-driven credential lifecycle support.
- **SAML 2.0** – Configurable alongside OIDC IdPs.

8. Compliance Reporting & Assurance

- **Quarterly Compliance Reports** – Covering ISO/IEC 27001 alignment, Essential Eight maturity, pen test results, privacy compliance.
- **Annual Security Certification** – Independent audit reports provided annually.
- **Proof-of-Operation & Pilot Evaluation** – Evaluated against technical, integration, security, privacy, and performance criteria.
- **Audit Trail Transparency** – Administrative and credential logs made available to DPC upon request.

9. Standards Compliance Mapping (Matrix View)

Standard / Framework	Requirement	CredEntry Evidence	Status
ISO/IEC 22301:2019 (Business Continuity)	Maintain BCP/DRP with testing & continuous improvement	Monthly backup/ failover tests, quarterly regional drills, annual DR simulation, RCA & updates	Aligned
WA Digital Wallet Agreement (Clauses 47 & 48)	Immediate notification, mitigation, restoration at no cost if CredEntry-related	Escalation process, DPC notified ≤ 15 min for P1 incidents	Aligned
ISO/IEC 27001:2022 (ISMS)	Secure ISMS with controls for access, logging, encryption	Encrypted credential storage, RBAC, audit logs, SharePoint record keeping	In progress: re-certification by end Pilot Phase
WA Cyber Security Policy (2024)	Defence-in-depth, 24h incident reporting, interoperability	Sentinel, MFA, interoperable formats, 24h reporting commitment	Aligned
ACSC Essential Eight	MFA, patching, restricted admin, app control	Implemented to Maturity Level One or equivalent; tracked quarterly	Aligned
IRAP PROTECTED	Alignment to PROTECTED controls	Independent ASD-accredited assessors engaged during Pilot Phase	In progress
ISO/IEC 19790:2025 (Crypto modules)	Secure cryptographic modules	AES-256, TLS 1.3, key rotation, HSM via Azure Key Vault	Aligned
OWASP ASVS / API Top 10	Secure coding & API hardening	SAST/DAST in CI/CD, API testing, SLA for remediation	Aligned
Zero-Trust Architecture	Strong identity & network segmentation	MFA, JIT RBAC, Sentinel monitoring	Aligned
ISO/IEC 18013-5 & -7 (mDL)	Mobile Driving Licence compliance (offline/online)	SDKs support OIDC4VP, offline presentation, mutable fields	Aligned
ISO/IEC 23220-1:2023 (Mobile eID)	Modular, interoperable identity architecture	Event-driven issuance, revocation, polling, PII minimisation	Aligned
W3C VCDM & DID	Verifiable Credentials model, DID resolution	VC issuance/revocation < 5 min, selective disclosure, DID support	Aligned
TDIF 4.8	Digital ID interoperability & governance	Admin dashboards, reporting, data minimisation	Aligned
eIDAS 2.0	Trust, revocation, mutable fields, remote verification	PKI trust mgmt, schema templates, eIDAS conformance testing	Aligned
OID4VCI / OIDC4VP	Credential issuance & presentation protocols	APIs/SDKs align to OID4VCI & OIDC4VP workflows	Aligned

Standard / Framework	Requirement	CredEntry Evidence	Status
Australian Digital ID Act 2024	Interoperability, audit trails, optional biometrics	Wallet auditability, Auth Level 2 roadmap	Aligned
Privacy Act 1988 (APPs)	Privacy-by-design, OAIC notification $\leq 72h$	Selective disclosure, consent logs, OAIC compliance	Aligned
ISO/IEC 29100:2024 (Privacy Framework)	Data minimisation, purpose limitation	Attribute-level selective disclosure, PII obfuscation	Aligned
GDPR	Data protection, purpose limitation, audit logs	Transaction dashboards, consent management	Aligned
Data Sovereignty (WA Govt)	Local data hosting	All data in Australian sovereign Azure regions	Aligned
ISO 9001:2015 / 90003:2018	QMS for software & onboarding	Onboarding aligned; certification targeted end Pilot Phase	In progress
ISO/IEC 12207:2017	Software lifecycle alignment	Development, testing, maintenance practices aligned	Aligned
ITIL v4	Incident mgmt & remediation SLAs	Draft SLA framework with explicit remediation timelines	Aligned
OpenAPI 3	Standard API documentation	All platform APIs documented via OpenAPI spec	Aligned
WCAG 2.2+	Accessibility compliance	Web interface tested to WCAG 2.2 AA	Aligned
Webhooks	Event-driven issuance & storage	Webhooks for credential lifecycle	Aligned
SAML 2.0	Standards-based IdP integration	Configurable alongside OIDC IdPs	Aligned
Quarterly Compliance Reports	Provide updates to DPC	Reports on ISO, Essential Eight, penetration tests, privacy	Committed
Annual Security Certification	Independent certification provided to DPC	Annual ISO/Essential Eight/IRAP audit	Committed
Proof-of-Operation / Pilot Evaluation	Demonstrate operational readiness	Conformance testing against technical & security criteria	In progress

10. Diagram

