CredEntry

Powered by

APPENDIX L
CREDENTRY PROJECT PLAN

Contents

1. Executive Summary

The WA Government is deploying a secure, privacy-preserving Digital Wallet and Verifiable Credentials Solution within the ServiceWA app to empower citizens with control over their identity data while enabling seamless service access.

CredEntry has been selected to deliver the solution, leveraging its Organisation Wallet Platform hosted in Microsoft Azure Australian sovereign regions. This Project Execution Plan (PEP) defines the framework, methodologies, governance, and controls required to deliver the project successfully.

Key delivery pillars:

- Secure, standards-aligned implementation: ISO/IEC, eIDAS 2.0, W3C VC, OIDC4VP
- Phased, gated execution model: PoO → Pilot → Production → Continuous Improvement.
- Robust governance and compliance: Ensuring operational integrity and data sovereignty.
- Future-ready architecture: Supporting biometric authentication, mDL, and evolving standards.

2. Project Objectives and Drivers

2.1 Objectives

- Deliver a digital wallet platform fully integrated into ServiceWA.
- Enable citizens to securely store, present, and revoke credentials.
- Ensure compliance with international and Australian privacy/security standards.
- Provide a scalable, modular architecture that supports future enhancements.

2.2 Strategic Drivers

- Align with WA Government's Digital Identity Strategy.
- Simplify citizen onboarding and verification processes.
- Improve security through cryptographic proofs, PKI-backed credentialing, and selective disclosure.
- Enhance inter-agency interoperability via WA Identity Exchange (IdX).

3. Project Scope and Methodology

The solution will be delivered in **four stages** with gated acceptance criteria at each phase:

1. Proof of Operation (PoO)
2. Pilot Phase (Implementation, Restricted Pilot, Preview Pilot)
3. Evaluation
4. Full Production Transition

3.1 Stage 0 – Proof of Operation (PoO)

Objectives:

- **Demonstrate Platform Readiness**
    - Prove that the **CredEntry Organisation Wallet Platform** can issue, manage, present, and revoke verifiable credentials seamlessly.
- **Validate SDK Integration**
    - Ensure the SDK functions correctly with ServiceWA APIs and app frameworks.
- **Showcase Security & Privacy Compliance**
    - Demonstrate encryption, PKI lifecycle management, selective disclosure, and data minimisation.
- **Enable Early Stakeholder Confidence**
    - Provide WA Government evaluators with a **hands-on demonstration** of wallet capabilities, security workflows, and integration flexibility.
- **Prepare for Pilot Execution**
    - Identify and address technical, operational, and compliance gaps ahead of the Pilot Phase.

Key Activities

A) Environment Provisioning

- **Azure Deployment**
    - Stand up a sandbox environment in Microsoft Azure sovereign regions (Australia East and Central) for PoO testing.
    - Enable isolated tenancy to separate PoO activities from Pilot and Production environments.
- **Credential Lifecycle Infrastructure**
    - Deploy Azure PostgreSQL for credential storage and lifecycle metadata.
    - Configure Azure Key Vault with HSM-backed encryption for PKI management
    - Integrate Azure Certificate Services to issue and rotate signing certificates securely.
- **Security Hardening**
    - Enable Azure Front Door and Web Application Firewall (WAF) to secure SDK endpoints.
    - Activate Advanced Threat Protection and intrusion detection monitoring.

B) SDK Deployment & Integration

- Deliver the CredEntry SDK with comprehensive developer guides, API schemas, and code samples
- Enable SDK integration into the ServiceWA DTP sandbox environment:
    - Configure authentication flows with OIDC4VP and OpenID4VCI protocols
    - Set up data exchange pathways between wallet, ServiceWA APIs, and IdX.
- Establish developer support channels:
    - Technical walkthrough sessions.
    - Dedicated issue-tracking workflows for integration debugging.

C) Credential Lifecycle Demonstration

- **Issuance Workflows**
    - Deploy a **generic demonstration credential** schema for PoO.
    - Showcase wallet issuance, credential storage, and delivery into ServiceWA app or OEM wallets.
- **Presentation & Verification**
    - Simulate verifier workflows using ServiceWA APIs and third-party endpoints.
    - Demonstrate **selective disclosure** for attribute-level data sharing.

- **Revocation & Updates**
  - Prove real-time credential revocation (<5 minutes) with status updates pushed to wallets.

D) Security & Privacy Validation

- **Cryptographic Integrity Testing**
  - Validate credential signatures using trusted PKI workflows.
- **Selective Disclosure Compliance**
  - Ensure user-controlled consent for credential attributes.
- **Privacy Safeguards**
  - Obfuscate PII within all PoO demonstration records.
- **Penetration Testing**
  - Perform sandbox security assessments simulating unauthorised access attempts.
- **ISO & eIDAS Conformance Check**
  - Assess PoO workflows against ISO/IEC 18013, ISO/IEC 23220, eIDAS 2.0, and W3C Verifiable Credentials frameworks

E) Stakeholder Demonstration

- Host structured **demo sessions** for WA Government evaluators:
  - Walkthrough of SDK integration, credential lifecycle, and security posture.
  - Live demonstration of issuing, presenting, and revoking credentials.
- Provide **interactive testing environments** for evaluators to simulate verifier interactions.

Dependencies:

- **ServiceWA Development Partner**
  - Sandbox access and developer support for SDK integration.
- **WA Government**
  - Access to evaluators and relevant test credentials.
- **Identity Exchange (IdX)**
  - Sandbox configuration for verifier workflows.
- **OEM Wallet Providers**
  - Apple and Google developer profiles for testing push-to-wallet integration.

Deliverables:

- Fully deployed sandbox wallet environment within Azure sovereign regions.
- CredEntry SDK package with developer documentation and integration playbooks.
- Architecture diagrams detailing all components, APIs, and credential flows.
- Security and Compliance Report summarising encryption workflows and PKI management.
- PoO Demonstration Report outlining findings, testing results, and refinements.

3.2 Stage 2 – Pilot Phase (12 Months)

The Pilot Phase is the most critical delivery stage, validating technical feasibility, security, user experience, and operational readiness prior to a full production rollout. It is structured into four sub-stages, each with defined objectives, activities, deliverables, dependencies, risks, and acceptance gates.

Stage 2.1 – Implementation & Integration (Months 1-2)

Objective:

To deploy the CredEntry Organisation Wallet Platform within the WA Government's ServiceWA Digital Trust Platform (DTP) environment, establish secure integrations, and prepare the solution for live pilot testing.

Key Activities:

1. Environment Deployment

- Provision dedicated Azure sovereign environments (Australia East/Central).
- Set up multi-tenant SaaS architecture for pilot users and agencies.
- Configure identity segregation through Azure Active Directory (AAD) and tenant-level encryption keys.

2. Secure Integration Setup

- Integrate SDKs with ServiceWA APIs.
- Enable PKI and certificate lifecycle management via Azure Key Vault with HSM-backed encryption
- Configure endpoints for issuing, presenting, and revoking verifiable credentials, fully aligned with OpenID4VCI and OIDC4VP standards

3. Monitoring & Logging

- Enable Azure Monitor, Event Hubs, and Log Analytics for:
    - Credential issuance and verification success rates.
    - Latency tracking and API response monitoring.
    - Security event logging for real-time anomaly detection.

4. Testing Preparation

- Develop an Acceptance Test Plan (ATP) covering:
    - SDK integration testing.
    - End-to-end wallet workflows (issuance → presentation → revocation).
    - API performance under concurrent load.
    - Security validation against ISO and OWASP benchmarks.

5. Documentation Delivery

- Prepare detailed technical documentation, including:
    - Architecture diagrams.
    - SDK developer guides.
    - API schemas and integration playbooks.

Dependencies:

- ServiceWA development partner must provide API access and DTP endpoints.
- WA Government must approve SDK deployment within staging environment.

Deliverables:

- Integrated wallet platform within ServiceWA DTP.
- Signed-off ATP document.
- Security and architecture documentation.

Stage 2.2 – Restricted Pilot (Months 3-5)

Objective:

To validate the digital wallet functionality and SDK/API integrations with a controlled group of ~50 government testers using a single designated credential.

Key Activities:

1. Wallet Deployment

- Roll out the wallet to nominated government testers via ServiceWA app.
- Ensure smooth onboarding with step-by-step user guides and in-app support.

2. Credential Issuance & Verification

- Deploy one designated credential to testers.
- Execute credential lifecycle operations:
    - Issue → Store → Present → Revoke → Reissue.

3. OEM Wallet Integration

- Validate compatibility with Apple Wallet and Google Wallet.
- Ensure push-to-wallet flows comply with platform guidelines.

4. Security & Privacy Validation

- Conduct penetration testing focused on:
    - Credential storage encryption.

  - API endpoint vulnerabilities.
  - Data minimisation and selective disclosure scenarios.
- Validate compliance with ISO/IEC 18013-5, ISO/IEC 23220, and eIDAS 2.0 standards

5. Feedback Capture

- Establish structured channels to capture user experience insights:
  - Online surveys.
  - In-app analytics dashboards.
  - Weekly tester feedback workshops.
- Deploy the wallet to ~50 nominated government testers.
- Validate OEM wallet compatibility (Apple/Google).
- Execute **penetration testing** and **compliance validation** against ISO/IEC 18013 and 23220

Dependencies:

- WA Government to supply designated credential data.
- Access to ServiceWA analytics for UX insights.

Deliverables:

- Restricted Pilot Test Report.
- OEM Wallet Compatibility Report.
- Signed-off ATP results.

Stage 2.3 – Preview Pilot (Months 6-12)

Objectives:

To test scalability, interoperability, and user experience in a controlled live environment with ~200+ participants and multiple agencies.

Key Activities:

1. Participant Expansion

- Onboard ~200+ users, including citizens and agency stakeholders.
- Roll out onboarding campaigns with FAQs, guides, and assisted workshops.

2. Multi-Agency Integration

- Enable cross-agency credential workflows via WA IdX integration.
- Incorporate Department of Transport (DoT) credentials to test multi-source issuance and verification.

3. Usability & Accessibility

- Conduct full UX/UI accessibility reviews against WCAG 2.2 AA standards.
- Execute structured usability testing across user personas and demographics.
-

4. Real-Time Analytics

- Monitor issuance and verification volumes across geographies.
- Capture and analyse error logs, latency metrics, and user adoption trends.

Dependencies:

- IdX configuration and access credentials.
- Integration agreements with DoT.

Deliverables:

- Preview Pilot Evaluation Report.
- UX Insights Dashboard.
- Refined SDK and API integration documentation.

3.4 Phase 2 – Pilot Evaluation & Iteration

Objective:

To consolidate findings from the pilot, address identified issues and confirm readiness for full production rollout.

Key Activities:

- Execute comprehensive Acceptance Test Plans (ATPs) across SDK, wallet, APIs, and IdX integrations.
- Prepare consolidated Pilot Evaluation Report summarising:
  - Technical findings.
  - Security test results.
  - UX/UI insights and refinements.
- Host workshops with key stakeholders.
- Execute ATPs across SDK, wallet, and ServiceWA APIs.
- Deliver consolidated Pilot Evaluation Report.
- Present Go/No-Go recommendation to Evaluation Panel

Deliverables:

- Final Pilot Evaluation Report.
- Updated ATP results.
- Evaluation Panel Go/No-Go decision.

3.5 Stage 3 – Full Production Transition

The successful completion of the Pilot Phase (Stage 2) will provide a tested, validated solution ready for statewide deployment. Stage 3 focuses on scaling the CredEntry Organisation Wallet Platform into a production-grade service, enabling multi-agency integrations, supporting high transaction volumes, and establishing long-term operational readiness.

Objectives:

- **Scale the Solution**
  - Transition from a controlled pilot environment to a fully operational, production-ready SaaS platform hosted within Microsoft Azure sovereign regions.
- **Integrate Additional Agencies and Credentials**
  - Onboard new agencies, expanding the range of verifiable credentials available to WA citizens.
- **Establish Enterprise-Grade Operational Management**
  - Implement a 24/7 support model aligned with Service Level Agreements (SLAs).
  - Set up incident management, service monitoring, and capacity planning frameworks.
- **Ensure Compliance and Security Continuity**
  - Maintain adherence to ISO27001, ISO/IEC 18013, ISO/IEC 23220, W3C VC, OIDC4VP, eIDAS 2.0, and Privacy Act 1988 requirements
- **Prepare for Continuous Improvement**
  - Establish a foundation for future feature enhancements, including biometric authentication and mobile driver licence (mDL) support.

Key Activities:

A) Production Environment Deployment

- **Infrastructure Scaling**
  - Deploy production environments in Azure Australia East and Central for high availability and disaster recovery (DR) capability.
  - Enable multi-region redundancy to achieve SLA targets (>99.8% uptime).
- **Platform Hardening**
  - Apply security hardening to all services:
    - Web Application Firewall (WAF) configuration
    - Advanced Threat Protection via Microsoft Defender for Cloud
    - Data encryption at rest (AES-256) and in transit (TLS 1.3).

- **Capacity Planning**
    - Conduct load and performance testing to validate concurrent credential issuance, verification, and revocation under production-scale demand.

B) Multi-Agency Credential Onboarding

- Establish a Credential Onboarding Framework in collaboration with WA Government:
    - Prioritise agencies for early adoption (e.g. DoT, Health, Education).
    - Define credential schemas and issuance workflows.
    - Conduct data mapping and integration with each agency's backend systems.
- Configure secure APIs and integration gateways for:
    - WA Identity Exchange (IdX) interoperability.
    - Third-party service providers and verifiers.

C) Operational Readiness Framework

- **Support Models**
    - Establish Service Desk with defined tiered escalation paths:
        - Tier 1: Citizen support
        - Tier 2: Agency integration issues
        - Tier 3: Platform-level escalations.
- **Incident Management**
    - Implement ITIL-aligned workflows for incident detection, triage, and root cause resolution.
- **Monitoring & Reporting**
    - Enable continuous monitoring for:
        - Credential issuance/verification latency.
        - API availability and performance.
        - Security events, logged centrally via Azure Monitor and Log Analytics.

D) Security & Compliance Assurance

- Conduct full independent security audits prior to go-live, including:
    - Penetration testing
    - Data sovereignty validation
    - ISO/IEC and eIDAS alignment reviews.
- Implement ongoing conformance testing against emerging standards, such as ISO/IEC 23220-3 and OIDC4VP enhancement
- Establish a Data Breach Response Framework, aligned with the Notifiable Data Breaches (NDB) scheme.

E) Change Management & Stakeholder Engagement

- Run agency readiness workshops to:
    - Train technical teams on SDK integration.
    - Align operational responsibilities between CredEntry and WA Government.
- Update stakeholder communication plans to support statewide rollout:
    - Executive briefings.
    - Public communications via ServiceWA.

Dependencies:

- **ServiceWA Development Partner**:
    - Final delivery of production-ready ServiceWA app release.
- **WA Government Agencies**:
    - Timely provision of credential data schemas and issuance requirements.
- **Identity Exchange (IdX)**:
    - Finalisation of integration architecture and testing timelines.
- **Cybersecurity Teams**:
    - Approval of platform hardening measures prior to go-live.

Deliverables

- **Production-Ready Wallet Platform**
  - Fully deployed, security-hardened SaaS platform within Azure sovereign regions.
- **Credential Onboarding Framework**
  - Process, schema definitions, and technical integration guides.
- **Operational Readiness Pack**
  - SLA frameworks, incident response plans, monitoring dashboards.
- **Independent Security Audit Report**
  - Certification of compliance across ISO, W3C, and eIDAS standards.
- **Go-Live Readiness Report**
  - Signed off by Evaluation Team

Key Performance Indicators

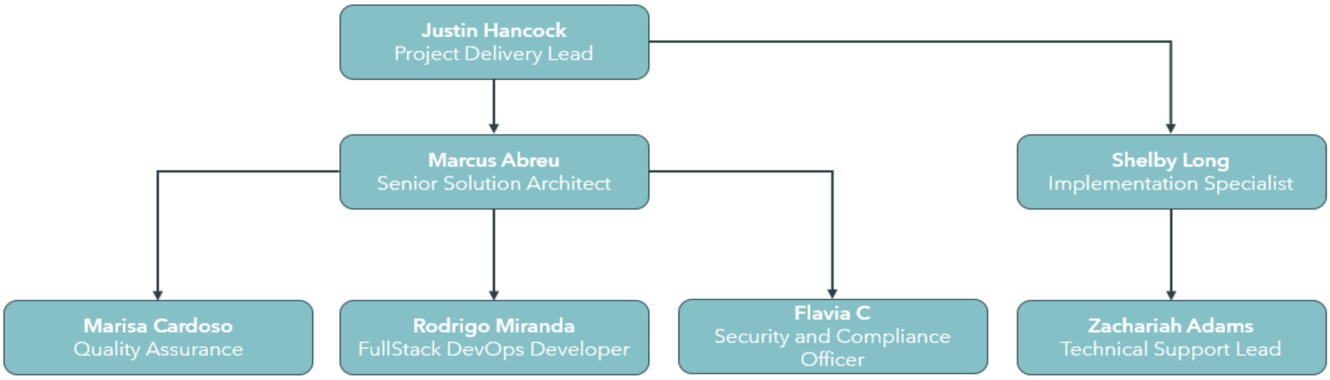
The below table summarises the KPIs that CredEntry will be aiming for throughout each of the phases.

Metric	PoO Target	Pilot Target	Production Target
Functional Completeness	80%	95%	99%
System Availability	95%	99%	99.8%
API Response Time	< 500ms	< 200ms	< 100ms
User Satisfaction	N/A	> 70%	> 85%
Support Ticket Resolution	N/A	< 24 hours	< 4 hours
Security Incidents	0	< 2 minor	0 critical
Documentation Completeness	70%	90%	100%
Test Coverage	60%	80%	90%

4. Governance, Roles & Responsibilities

4.1 Organisational Chart

Below details the project organisational chart for the Project:



4.2 Roles and Responsibilities

Project Sponsor – WA Government

- Provides strategic direction and ensures project objectives align with WA Digital Identity initiatives.
- Approves key milestones, funding allocations, and stage gate decisions.
- Engages with ministerial offices and other government stakeholders.
- Holds ultimate accountability for project outcomes and citizen trust.

Project Delivery Lead

- Leads overall delivery of the Digital Wallet and Verifiable Credentials program.
- Manages project scope, schedule, and budget across all phases.
- Coordinates with the WA Government, ServiceWA, and technical teams.
- Drives stakeholder engagement, ensuring alignment across multiple agencies.
- Reports to Project Sponsor on progress, risks, and issues.

Senior Solutions Architect

- Owns end-to-end wallet/credentials solution architecture and non-functional requirements (security, scale, HA).
- Designs API & SDK integration patterns with ServiceWA/IdX; leads technical design reviews.
- Establishes PKI, crypto, and standards alignment (W3C VC/DID, OpenID4VCI/OIDC4VP, ISO/IEC 18013 & 23220).
- Leads developers on patterns, code quality, and performance; approves release architecture.

Implementation Specialist

- Runs the day-to-day implementation and rollout, coordinating CredEntry, ServiceWA dev partner, and agencies.
- Leads requirements & readiness workshops, builds onboarding playbooks and training.
- Orchestrates pilot cohorts, cutover/checklists, and business change communications to agencies/users.
- Tracks adoption KPIs and issues, driving resolution with tech/QA/security leads.

Quality Assurance (Tester)

- Authors the Acceptance Test Plan (ATP); manages functional, regression, UAT, performance & accessibility testing.
- Verifies SDK/APIs & credential lifecycle (issue/present/revoke), with traceability from requirements to results.
- Runs security/OWASP-aligned checks with Security Officer; gates release readiness and evidence capture.
- Reports defects/risks, drives triage to closure, and signs test exit criteria.

Full Stack DevOps Developer

- Builds and maintains SDKs, APIs, and microservices, enabling wallet + verifier integrations.
- Owns CI/CD, IaC (e.g., Azure DevOps/Terraform), observability, and performance tuning.
- Implements secure coding and privacy-by-design; supports offline flows and mobile/OEM wallet behaviours.
- Supports the Solution Architect on scalability and with QA on automated test coverage

Security and Compliance Officer

- Operates the ISO 27001-aligned ISMS, risk register, and audit-ready artefacts (IRAP/ISM, Privacy Act).
- Runs vulnerability assessments & pen testing; tracks remediation to closure.
- Oversees credential security controls (PKI, key management, revocation status, data minimisation).
- Delivers PIAs/SIAs, release security sign-off, and breach/incident response procedures

Technical Support Lead

- Designs and manages L1/L2/L3 support, ticketing/escalations, and SLA reporting.
- Maintains the knowledge base and user enablement materials; leads problem/RCA cycles.
- Coordinates incident comms and service status with agencies; feeds issues back to Dev/QA for fixes.
- Monitors wallet issuance/verification support metrics and drives CX improvements

All Staff

All project team members are expected to:

- Act Professionally – Treat colleagues, stakeholders, and partners with respect, fairness, and integrity.
- Maintain Confidentiality – Protect sensitive information and citizen data in line with privacy, security, and compliance requirements.
- Adhere to Code of Conduct – Follow organisational policies, values, and workplace standards at all times.
- Prioritise Safety & Wellbeing – Comply with health, safety, and risk management procedures.
- Perform to a High Standard – Take ownership of tasks, deliver quality work, and meet agreed deadlines.
- Collaborate & Support – Work openly with others, share knowledge, and contribute to a positive team environment.

5. Resourcing Continuity & Knowledge Sharing

CredEntry is committed to maintaining a skilled, experienced, and readily available workforce to ensure uninterrupted delivery of the Digital Wallet and Verifiable Credentials Project throughout the Term.

5.1 Access to Skilled Backup Personnel

- **Trusted Subcontractor Network**: CredEntry maintains a **vetted panel of trusted subcontractors** who can be engaged as needed to support specific scopes of work or during periods of high workload.

- **Casual Support Pool**: We maintain a dedicated pool of trained casual personnel to provide additional capacity, particularly to support the Technical Support Lead and Security & Compliance Officer roles when required.

- **Recruitment Partner**: CredEntry partners with Vitil People Solutions, a trusted recruitment provider, to rapidly source and onboard suitably skilled personnel should the project require additional resourcing.

5.2 Proactive Resource Planning

- **Structured Project Scheduling**: Our project management framework and delivery schedule are designed to identify potential resourcing gaps early and enable forward planning for workload peaks.

- **Knowledge Sharing & Documentation**: All processes, configurations, and delivery activities are fully documented and stored in centralised knowledge repositories. This ensures seamless handover of tasks, rapid onboarding of new personnel, and continuity of operations even if team members change.

- **Cross-Functional Handover**: Regular briefings, shared workspaces, and structured documentation ensure that knowledge is retained across all project phases.

5.3 Rapid Response Capability

CredEntry’s delivery model ensures we can mobilise backup resources within minimal response times by leveraging:

- Pre-established subcontractor agreements.
- Pre-screened casual staff for surge support.
- A proactive recruitment framework for scaling the team as required.

By combining resourcing flexibility, structured documentation, and robust knowledge-sharing practices, CredEntry ensures the project maintains a skilled and experienced workforce, achieves continuity of service, and meets all delivery milestones without delays or compromise to quality.

6. Interface Management & Stakeholder Engagement

Effective and transparent interface management between CredEntry, the WA Government, ServiceWA, and other project stakeholders is critical to the successful delivery of the Digital Wallet and Verifiable Credentials Project.

CredEntry's approach ensures open communication, timely decision-making, and alignment of expectations across all parties.

6.1 Kick Off Meeting

A formal project kick-off meeting will be conducted at the commencement of the project to:

- Introduce key personnel from CredEntry, the Department, ServiceWA, and other partners.
- Provide a comprehensive project overview, including scope, objectives, deliverables, and success criteria.
- Align expectations across all parties, including timelines, resourcing, governance, and acceptance gates.
- Confirm the project schedule, reporting cadence, escalation pathways, and points of contact.
- Establish a collaborative environment to ensure all parties are working towards a shared vision.

Format: Preference for in-person attendance; hybrid or virtual attendance will be supported via Microsoft Teams if required.

6.2 Project Meetings

To maintain alignment, CredEntry proposes regular project meetings with the Department, ServiceWA, and key stakeholders:

- **Frequency:** Fortnightly (or as agreed with the Department).
- **Attendees:** Project team members, Department representatives, ServiceWA developers, and other relevant stakeholders.
- **Format:** Preference for face-to-face meetings at the Department's office; hybrid/virtual meetings via Microsoft Teams will be available when required.

Purpose:

- Track progress against milestones and deliverables.
- Identify and resolve emerging issues and risks.
- Manage dependencies across multiple agencies and technical teams.
- Ensure all stakeholders are informed and aligned on upcoming priorities.

Outputs:

- Meeting agendas shared in advance.
- Minutes recorded and circulated within 24 hours.
- Action items assigned, tracked, and reviewed in subsequent meetings.

6.3 Project Reporting

CredEntry will provide structured project reporting to the Department to ensure transparency and timely decision-making:

- **Frequency:** Fortnightly or monthly (to be confirmed by the client).
- **Content:**
  - Progress updates against key milestones and deliverables.
  - Budget, resourcing, and schedule tracking.
  - Risk and issue registers with escalation recommendations.
  - Stakeholder engagement updates and decision dependencies.
- **Format:**
  - **Dashboard-style reporting** with executive summaries.
  - Detailed appendices for technical progress, compliance status, and test results where required.
- **Distribution:** Delivered to the Department, Steering Committee, and relevant project stakeholders.

6.4 Project Office

To facilitate efficient engagement, real-time decision-making, and direct access to key stakeholders, CredEntry proposes to:

- Co-locate core delivery personnel within the allocated Department project office for the duration of the project.
- Ensure CredEntry's Project Director, Implementation Specialist, and Security/Compliance Officer are on-site during critical phases, including Proof of Operation, Pilot deployment, and Production transition.
- Leverage co-location to:
  - Accelerate issue resolution and decision cycles.
  - Support knowledge sharing between CredEntry and Department teams.
  - Improve collaboration with ServiceWA developers and agency representatives.
- Maintain flexibility by combining on-site presence with virtual engagement tools (e.g., Microsoft Teams, shared workspaces) to ensure stakeholders remain connected regardless of location.

7. Project Schedule

See Appendix D – Product Development Roadmap

8. Security, Privacy & Compliance Framework

CredEntry adopts a defence-in-depth approach to security and privacy, underpinned by the ISO/IEC 27001 Information Security Management System (ISMS) framework and aligned with WA Government cybersecurity policies. Our solution is architected to protect citizen data, meet compliance obligations, and maintain stakeholder trust across all delivery stages.

8.1 Secure Hosting & Architecture

- The Digital Wallet and Verifiable Credentials platform is hosted in Microsoft Azure IRAP-assessed sovereign regions (Australia East and Australia Central) to ensure compliance with WA Government security policies and data sovereignty requirements.
- The platform employs AES-256 encryption at rest and TLS 1.3 encryption in transit for all communications, ensuring end-to-end data protection.
- Public Key Infrastructure (PKI) is managed using Azure Key Vault with HSM-backed keys, providing hardware-level security for credential issuance, revocation, and verification.

8.2 Compliance Alignment

The platform is fully aligned with:

- ISO/IEC 27001 – Information Security Management System.
- ISO/IEC 27035 – Information Security Incident Management.
- ISO/IEC 18013 & 23220 – Mobile Driver Licence and Verifiable Credentials standards.
- W3C Verifiable Credentials and OpenID4VCI/OIDC4VP protocols.

- Australian Privacy Principles (APPs) – Protection of Personally Identifiable Information (PII).
- WA Government Cyber Security Policy and the Digital Identity 2024 Trust Framework.

8.3 Security Assurance

- Independent Security Assessments – Annual penetration testing and vulnerability scanning are conducted by accredited third-party specialists.
- ISO27001 Recertification – The ISMS is reviewed and recertified annually to maintain compliance.
- Privacy Impact Assessments (PIAs) – Conducted at each delivery stage to assess, mitigate, and manage privacy risks.

8.4 Incident Response & Breach Management

- Real-time monitoring via Microsoft Sentinel SIEM detects abnormal activity across wallet endpoints, SDK integration points, and ServiceWA APIs.
- A dedicated Security Incident Response Team (SIRT) manages detection, containment, and remediation of incidents.
- The Department is notified within two hours of any confirmed data breach involving PII and provided with an impact assessment within four hours.
- A formal Security Incident Report is delivered within five business days, including root cause analysis, remediation steps, and preventive measures.

9. Testing, QA/QC & Acceptance Criteria

CredEntry adopts a comprehensive, layered testing strategy to ensure the Digital Wallet and Verifiable Credentials solution meets all technical, security, accessibility, and compliance requirements.

9.1 Acceptance Test Plan (ATP)

A detailed **ATP** is co-designed with the Department and defines:

- Testing objectives, roles, and responsibilities.
- Entry and exit criteria.
- Acceptance thresholds for each stage: PoO, Pilot, and Production.

9.2 Testing Approach

- **Functional Testing**: Validates the full credential lifecycle: issuance, storage, presentation, selective disclosure, updates, and revocation.
- **Integration Testing**: Ensures seamless interoperability between the wallet SDK, ServiceWA APIs, IdX, and agency credential systems.
- **System Testing**: Validates real-world scenarios to ensure consistent, intuitive user experiences for citizens, verifiers, and administrators.
- **Security Testing**: Includes penetration testing, vulnerability assessments, and privacy reviews, performed independently and remediated prior to release.
- **Performance & Load Testing**: Simulates statewide concurrency scenarios to confirm scalability and uptime objectives (>99.8% availability).
- **Accessibility Testing**: Validates compliance with WCAG 2.1 AA standards to support citizens of all abilities.

9.3 Compliance Testing

- Conformance validation across ISO/IEC 18013, ISO/IEC 23220, W3C VC, and OpenID4VCI/OIDC4VP frameworks.
- Department sign-off is secured at each stage upon meeting agreed acceptance criteria.

10. Project Controls

10.1 Project Budget

The project budget is defined as per the DPC2142 Attachment 4 - Schedule 7 - Pricing and Payment.

10.2 Contract Variation Requests

CredEntry applies a robust change control framework to manage all contract variations:

- A Variation Register will be maintained, capturing:
    - Description of the variation.
    - Financial impacts.
    - Schedule impacts.
    - Approval status and supporting documentation.
- Variations impacting the critical path or total project cost are escalated to the Project Delivery Lead approval before initiating a formal variation request with the Department.
- Supporting evidence, impact analyses, and decision logs are archived for audit purposes.

The variation process between the two parties is as follows:

1. **Raise and Discuss** – Any potential material change is initially raised at regular project meetings for discussion between CredEntry and the Department.
2. **Document in Project Reports** – All potential variations are recorded in project progress reports.
3. **Submit Change Proposal** – Once discussed, CredEntry will submit a formal change request letter to the Department outlining:
    - Description of the change.
    - Supporting information (technical, commercial, or operational drivers).
    - Proposed changes to relevant pricing and milestone schedules.
4. **Mutual Agreement** – All changes will be mutually agreed and signed off by both parties, with documentation captured via the Department's Contract Goods Amendment template.

10.3 Project Schedule Revisions

The project schedule will be updated fortnightly by exception and formally issued to the Department monthly with the project report.

11. Risk Management & Mitigation

The project will be governed under the framework outlined in ***Appendix E – Support & Maintenance Framework***, with oversight and escalation pathways defined in **Schedule 10 – Governance** of the Agreement. A centralised Risk Register outlined in ***Appendix M – Risk Register*** will track technical, operational, and compliance risks, including data sovereignty, standards alignment, and BCP/DRP obligations. Risks and mitigations will be reviewed regularly in line with the processes detailed in ***Appendix F – Implementation Plan*** and ***Appendix E.7 – Business Continuity Plan & Disaster Recovery Plan (BCP/DRP)***

12. Training & Knowledge Transfer

CredEntry ensures all stakeholders, technical, operational, and citizen-facing are fully enabled to manage, support, and use the solution effectively.

12.1 Training Delivery

- Delivered at least four weeks prior to Pilot commencement.
- Covers Department staff, ServiceWA developers, agency verifiers, and citizen-facing support teams.
- Training models include:
    - Instructor-led workshops.
    - Interactive e-learning modules.
    - Demonstration videos and practical exercises.

12.2 Knowledge Management

- All SDK documentation, integration guides, and administrative playbooks are stored in a centralised Knowledge Management Database.
- Ensures rapid onboarding of new personnel and continuity of service.
- Continuous feedback loops update training content as the platform evolves.

13. Transition to Operations & Continuous Improvement

CredEntry ensures a smooth transition from project delivery to operational management while maintaining flexibility for future enhancements.

13.1 Operational Readiness

- Establish SLA frameworks, escalation pathways, and 24/7 operational monitoring.
- Conduct formal handover sessions with Department teams and ServiceWA developers.

13.2 Continuous Improvement

- Support onboarding of new credentials and agencies via controlled SOW processes.
- Deliver quarterly performance, security, and compliance reports to maintain transparency.
- Apply a continuous improvement framework based on operational insights, citizen feedback, and emerging standards.