CredEntry

Powered by

APPENDIX H.8

TECHNICAL STANDARD

RELEASE MANAGEMENT

Table of Contents

Technical Standard PRM Release Management

Requirement

PRM-1: Supplier must provide an approach to onboarding customers, configuring platforms for their requirements and achieving production readiness.
Classification: Must
Reference Standards: ISO 9001, ISO/IEC 27001

Implementation by CredEntry

CredEntry follows a structured Release and Onboarding Management Process aligned to ISO 9001 (Quality Management) and ISO/IEC 27001 (Information Security Management). This ensures every customer is onboarded in a controlled, secure, and repeatable manner, with clear milestones for achieving production readiness.

1. Onboarding Preparation

- Establish customer requirements and objectives through discovery workshops.

- Confirm compliance obligations (e.g., ISO/IEC 27001 controls, WA Government policies).

- Allocate dedicated onboarding team (project manager, solution architect, security lead).

- Define scope, timelines, and acceptance criteria in a formal onboarding plan.

2. Environment Provisioning

- Deploy segregated environments (Development, Staging, Production) within Azure Australia East/Central.

- Apply baseline security controls, including encryption, access management, monitoring, and logging.

- Configure logical multi-tenancy and PKI/identity partitions to align with customer requirements.

3. Platform Configuration

- Customise identity providers, PKI, credential schemas, and branding per customer specifications.

- Implement role-based access control (RBAC) and segregation of duties.

- Integrate with customer systems (HR, CRMs, or registries) using APIs or secure connectors.

- Validate configuration against **CredEntry standard configuration checklists**.

4. Testing and Validation

- Conduct functional testing (credential issuance, revocation, wallet integration).

- Perform security validation (penetration testing, vulnerability scanning).

- Execute conformance testing against ISO/IEC 18013, ISO/IEC 23220, eIDAS 2.0 where applicable.

- Document results and remediate any issues before go-live.

5. Training and Knowledge Transfer

- Provide administrator and end-user training sessions.

- Deliver tailored operational guides and runbooks.

- Ensure customer security and compliance teams are trained in incident response and reporting workflows.

6. Go-Live and Production Readiness

- Conduct Go-Live Readiness Review with customer stakeholders.

- Validate data migration, cutover, and rollback procedures.

- Approve production release through change management board.

- Transition into steady-state operations under agreed SLAs.

7. Post-Go-Live Support and Continuous Improvement

- Monitor system stability and performance during hypercare period (typically first 4–6 weeks).

- Capture lessons learned and incorporate into continuous improvement cycle.

- Provide ongoing patching, vulnerability remediation, and feature upgrades under the CredEntry Release Schedule.

- Ensure compliance and certification renewals remain current throughout the contract.