Project Initiation Document (PID)

SentralQ Proof of Concept (POC)

Project Name	SentralQ Hybrid Evidence POC
Version	1.1
Status	Approved for Execution
Project Type	Proof of Concept / Prototyping
Document Date	23 December 2025

1. Project Background & Objective

Financial institutions face "Audit Fatigue" due to the manual effort required to correlate technical telemetry with regulatory documentation. Current solutions offer either static document storage (GRC tools) or technical monitoring (Observability tools), but fail to link the two.

Primary Objective: To validate the technical feasibility of a "Hybrid Evidence Lakehouse" for SentralQ. The POC must demonstrate the ability to ingest, correlate, and retrieve both Machine-Generated Data (Syslogs/API) and Documentary Evidence (PDFs/Policies) to generate regulator-ready "Assurance Packs."

2. Scope Definition

2.1 In-Scope Capabilities

The POC will deliver a functional prototype demonstrating:

• **Multi-Format Ingestion:** Simultaneous ingestion of machine logs and PDF documents.

• **Immutable Storage:** Hashed storage of all raw inputs (The "Raw Vault").

• **Automated Linkage:** Using Dojo Mapper to mathematically link a log event to a specific document clause.

• **Natural Language Retrieval:** Using Telescope for evidence navigation.

• **Assurance Output:** Generation of a time-bound, immutable Assurance Pack.

Disclaimer: This assurance pack supports attestation readiness by providing structured, time-bound evidence. It does not constitute certification, regulatory approval, or compliance sign-off.

2.2 Exclusions / Out of Scope

• **Write Access:** The system will operate strictly in Read-Only mode. No control actions will be sent back to payment systems.

• **Automated Judgement:** The system will not make compliance decisions. Telescope provides evidence retrieval and navigation, surfacing relevant, time-bound evidence aligned to defined controls. Control judgement and attestation decisions remain with auditors and risk owners.

• **Live Production Data:** The POC will utilize sanitized or synthetic data representative of live environments.

3. Technical Solution Architecture

To adhere to the baseline guidance, the solution utilizes a 3-Layer Lakehouse Architecture powered by internal tooling.

Layer 1: The Raw Vault (Ingestion)

• **Function:** Secure, immutable entry point.

• **Pipeline A (Telemetry):** Listeners for SWIFT Alliance Access, Payment Gateway, and Firewall logs.

• **Pipeline B (Artefacts):** Secure upload zone for Policy PDFs, Audit Reports, and Configuration files.

• **Security Control:** SHA-256 hashing upon entry to establish chain-of-custody.

Layer 2: The Normalisation Engine (Dojo Mapper)

• **Function:** Contextualisation and Linking.

• **Role of Dojo Mapper:** Acts as the "Universal Translator."

• - Parses technical logs (e.g., Event ID 4625).

• - Indexes document metadata (e.g., Security Policy, Para 12.1).

• **Core Logic:** Creates a unified "Evidence Object" that links the Technical Reality (Log) to the Regulatory Requirement (Document).

Layer 3: The Evidence Layer (Telescope)

• **Function:** Retrieval and Packaging.

• **Role of Telescope:**

• - Telescope provides evidence retrieval and navigation, surfacing relevant, time-bound evidence aligned to defined controls.

• - It assembles the "Assurance Pack" (Log extracts + Governing Documents) based on auditor queries.

• **Note:** Control judgement and attestation decisions remain with auditors and risk owners.

4. Operational Workflow Simulation

To demonstrate strict regulatory compliance capability, the POC will execute the following generic simulation:

• **Entity:** Global Mid-Tier Commercial Bank.

• **Regulatory Context:** Simultaneous compliance with SWIFT CSP (Global) and Regional Cyber Security Frameworks.

Execution Flow:

1. **Input:** Risk Team uploads "Corporate Access Control Policy v2.pdf" (Document). System ingests raw Authentication Server logs (Data).

2. **Processing:** Dojo Mapper correlates the Policy requirement for "Two-Factor Authentication" with specific log attributes (MFA_Status=Success).

3. **Query:** Internal Auditor asks Telescope: "Show proof of MFA enforcement on SWIFT terminals for Q3."

4. **Output:** System generates an Assurance Pack containing the Policy PDF (highlighting the clause), the 90-day log extract, and a verification hash.

5. Project Deliverables & Phasing

Phase	Milestone Name	Description / Deliverable
Phase 1	Hybrid Ingestion Foundation	Dashboard demonstrating live ingestion of a Syslog stream side-by-side with PDF upload.
Phase 2	Dojo Configuration	Demonstration of a "Raw Log" being automatically mapped to a specific "Regulatory Control" via Dojo.
Phase 3	Telescope Logic Integration	Implementation of Natural Language interface for evidence retrieval (non-judgemental).
Phase 4	Assurance Output Generation	Functionality to generate and download a zipped "Assurance Pack" with integrity hashes. Includes disclaimer: Supports attestation readiness; does not constitute certification.

6. Acceptance Criteria

The POC is considered complete and successful upon the validation of the following checklist:

■ **Ingestion:** System successfully ingests a raw Machine Log AND a Documentary Artefact.

■ **Immutability:** Both inputs are hashed and visibly stored in the "Raw Layer."

■ **Linkage:** Dojo Mapper creates a visible link between a Log entry and a Document clause.

■ **Retrieval:** Telescope retrieves the correct Log and Document based on a user query (e.g., "Show evidence for last 90 days").

■ **Output:** System generates a downloadable "Assurance Pack" containing the evidence trail.

7. Assumptions & Risks

- **Assumption:** Sample data (logs and dummy policies) will be provided or generated by the delivery team.
- **Risk:** Complexity in parsing non-standard PDF structures. *Mitigation:* POC will focus on standard searchable PDFs initially.
- **Risk:** Ambiguity in natural language queries. *Mitigation:* Telescope will be scoped to specific banking/compliance vocabulary.

8. Delivery Schedule & Execution Lock

Delivery Date	06 January 2026
Execution Lock	This document locks the scope. No changes permitted without Change Request.
Acceptance Gate	POC accepted only when all items in the SentralQ POC Acceptance Checklist (Section 6) are met.

This Project Initiation Document represents the formal agreement between project stakeholders and establishes the governance framework for the SentralQ POC delivery.