Loggie

CMMC Evidence Integrity Pilot

Statement of Work

Independent integrity validation for audit-critical records within regulated defense workflows.

Duration: 90 days
Scope: Single control family, single workflow
Deployment: Customer-controlled environment

Prepared by Loggie | Loggie Labs
Draft — For Discussion Purposes

1. BACKGROUND AND PURPOSE

Defense contractors operating under CMMC requirements face increasing pressure to demonstrate the integrity of compliance evidence. Policy documents, incident reports, security control attestations, and access change records must be maintained with verifiable provenance and non-repudiation throughout their lifecycle.

Current approaches rely on system-controlled audit trails that lack structural independence. When integrity is questioned during assessment, there is no neutral mechanism to verify that evidence has not been modified, backdated, or reconstructed.

This pilot deploys the Loggie integrity layer within a single compliance workflow to evaluate its effectiveness as independent cryptographic proof infrastructure for audit-critical records.

2. PILOT OBJECTIVES

- Demonstrate independent integrity anchoring for CMMC compliance evidence
- Validate deployment within a customer-controlled environment with no external data exposure
- Measure reduction in evidence preparation and audit response time
- Evaluate integration footprint and operational overhead

3. SCOPE OF WORK

3.1 Target Workflow

The pilot will target a single CMMC control family within the customer's existing compliance workflow. Recommended initial scope:

- Access Control (AC) policy revision tracking and attestation anchoring
- Incident Response (IR) report integrity and timestamping
- Configuration Management (CM) policy version lineage

Final workflow selection will be determined in collaboration with the customer's compliance and security teams during the onboarding phase.

3.2 Deployment Model

- Loggie deploys within the customer-controlled environment
- All processing occurs internally — no sensitive data leaves the enclave
- Optional anchor layer available but not required for pilot
- Air-gapped deployment supported if required

3.3 Exclusions

The following are explicitly outside the scope of this pilot:

- Replacement of existing storage, SIEM, or document management systems
- Modification of existing compliance processes or control implementations
- Access to classified or operationally sensitive mission data
- Public blockchain anchoring (unless explicitly requested)

4. PILOT TIMELINE

PHASE	DURATION	ACTIVITIES
Phase 1	Weeks 1–2	Onboarding, workflow selection, environment setup
Phase 2	Weeks 3–4	Integration, configuration, initial anchoring tests
Phase 3	Weeks 5–10	Operational deployment, evidence anchoring in workflow
Phase 4	Weeks 11–12	Evaluation, reporting, expansion assessment

5. DELIVERABLES

- **Environment:** Deployed Loggie integrity layer within customer environment
- **Evidence Anchoring:** Anchored compliance records for selected control family with cryptographic timestamps and identity binding
- **Verification Capability:** Independent verification of record integrity demonstrable to assessors
- **Final Report:** Pilot summary including integrity metrics, integration assessment, and expansion recommendations

6. SUCCESS METRICS

- 100% of target workflow records anchored with cryptographic integrity proof
- Zero sensitive data transmitted outside customer-controlled environment
- Measurable reduction in evidence preparation time for anchored records
- Independent verification of record integrity confirmed without reliance on source system
- Integration completed without modification to existing operational systems

7. SECURITY BOUNDARY

The following security constraints govern all pilot activities:

- All Loggie components deploy within the customer-controlled environment
- No raw data, telemetry, documents, or operational records leave the enclave
- Only cryptographic commitments (hashes) may optionally cross a controlled boundary
- Customer retains full control of all cryptographic key material
- No external key custody or key escrow
- Air-gapped operation available — no external connectivity required

8. RESOURCE REQUIREMENTS

8.1 From Customer

- Designated compliance workflow owner as primary point of contact
- Access to target compliance records (non-classified)
- Deployment environment (server or container infrastructure)
- IT/security coordination for environment provisioning

8.2 From Loggie

- Loggie integrity layer deployment and configuration
- Integration support for target workflow
- Technical documentation and onboarding guidance
- Pilot summary report and evaluation

9. COMMERCIAL TERMS

Pilot pricing, licensing terms, and any associated costs will be defined in a separate commercial agreement executed prior to pilot initiation. This Statement of Work defines scope, timeline, and technical parameters only.

Post-pilot expansion pricing and enterprise licensing will be addressed in the final evaluation phase based on deployment scale and workflow coverage.

10. CONFIDENTIALITY

All information exchanged during this engagement is treated as confidential. Loggie will not disclose customer identity, workflow details, or pilot results without written authorization. A mutual NDA is recommended prior to pilot initiation.

Loggie

Independent integrity infrastructure for high-trust systems.

Prepared for discussion purposes. Subject to mutual agreement.