Implementation Plan

Cloud Governance Foundation – Phase One

---

1. Purpose of This Plan

This Implementation Plan defines the sequenced execution approach for Phase One of the Cloud Governance Foundation project. The plan outlines approved actions, execution order, dependencies, validation criteria, and evidence expectations while preserving governance intent and scope guardrails.

2. Execution Approach

Phase One execution follows a governance-first, evidence-driven approach:

- Intent is defined before validation
- Validation is observational, not interventionist
- Evidence is captured via CLI only
- Decisions and risks are documented as execution progresses

Execution is divided into four controlled workstreams, sequenced to reduce risk and rework. This implementation plan reflects governance validation activities and does not authorize or direct engineering changes.

---

3. Implementation Sequence Overview

Sequence	Workstream	Dependency
1	Governance Design and Framing	Project Charter approved
2	Identity Governance Validation	Governance intent defined
3	Logging Governance Validation	Identity baseline understood
4	Evidence Consolidation and Review	All validations complete

This sequence ensures intent is established before technical validation and evidence capture.

---

4. Detailed Implementation Steps

4.1 Governance Design and Framing

Objective
Establish governance intent, scope boundaries, and success criteria prior to validation activities.

Planned Actions

- Define governance objectives for identity and logging
- Document control intent separate from technical implementation
- Confirm Phase One scope boundaries and guardrails

Dependencies

- Approved Project Charter
- Approved Scope and Guardrails

Validation Criteria

- Governance objectives documented and internally consistent
- Control intent clearly separated from implementation detail

Evidence Produced

- Governance intent narrative
- Scope and guardrails document

4.2 Identity Governance Validation

Objective
Validate the existence and structure of identity controls without modifying configurations.

Planned Actions

- Identify access categories (administrative, read-only, audit)
- Define role-based access intent without policy engineering
- Validate presence of IAM and IAM Identity Center constructs using AWS CLI

- Capture sanitized JSON outputs demonstrating identity state
- Document access lifecycle expectations

Dependencies

- Governance design completed
- CLI access available

Validation Criteria

- Identity constructs confirmed to exist
- Evidence captured and sanitized
- No production changes introduced

Evidence Produced

- Sanitized CLI outputs (identity validation)
- Identity governance narrative

4.3 Logging and Monitoring Governance Validation

Objective
Validate that logging controls exist and align with governance expectations.

Planned Actions

- Confirm CloudTrail is enabled at the account level
- Identify governance-relevant event categories
- Validate logging presence using CLI evidence capture
- Define log retention intent and accountability

Dependencies

- Identity governance validation completed

Validation Criteria

- CloudTrail presence confirmed

- Governance relevance documented
- Evidence captured without configuration changes

Evidence Produced

- Sanitized CLI outputs (CloudTrail validation)
- Logging governance narrative

4.4 Evidence Consolidation and Review

Objective
Ensure evidence completeness, traceability, and portfolio safety.

Planned Actions

- Organize evidence artifacts by phase and purpose
- Verify sanitization and public safety compliance
- Link evidence to governance objectives and framework mappings
- Prepare execution narrative suitable for interviews

Dependencies

- All validation activities completed

Validation Criteria

- Evidence set complete and reviewable
- No sensitive identifiers present
- Traceability between intent, validation, and evidence established

Evidence Produced

- Evidence index
- Consolidated governance execution narrative

---

5. Risk and Decision Integration

Throughout execution:

- Identified risks are logged in the Risk Register
- Scope or execution tradeoffs are recorded in the Decision Log
- Deviations from plan are documented rather than improvised

This ensures execution remains governed and auditable.

---

6. Execution Guardrails

- Read-only operational posture enforced
- CLI-only evidence collection
- No engineering redesign or enforcement
- Public-safe documentation maintained at all times

---

7. Phase One Completion Criteria

Phase One execution is complete when:

- All planned actions are executed or formally deferred
- Evidence artifacts are captured and organized
- Governance intent and framework mappings are documented
- Execution narratives are interview-ready
- Phase closeout activities are initiated