Project Charter

Cloud Governance Foundation – Phase One

1. Project Purpose

The purpose of this project is to establish a defensible cloud governance foundation by defining, validating, and documenting identity and logging controls in an AWS environment. The project focuses on governance intent, evidence capture, and audit readiness rather than infrastructure buildout or deep technical configuration.

---

2. Project Objective

The objective of Phase One is to achieve governance readiness and audit defensibility by validating the existence and intent of identity and logging controls, mapping them to recognized security frameworks, and producing sanitized, evidence-based documentation suitable for interviews and public portfolio review.

---

3. Project Timeframe

- **Start:** December 2025
- **End:** January 2026
- **Duration:** Approximately 6 weeks
- **Completion Condition:** Phase One governance objectives validated, documented, and formally closed.

---

4. High-Level Scope

In Scope (Phase One Only)

Governance Design and Framing

- Define governance objectives for identity and logging at the AWS account level
- Document control intent separate from technical implementation
- Establish Phase One scope boundaries and success criteria

Identity Governance (Conceptual and Evidence-Based)

- Identify access categories (administrative, read-only, audit)
- Define role-based access intent without custom policy engineering
- Validate existence of IAM and IAM Identity Center constructs using AWS CLI
- Capture sanitized JSON outputs demonstrating identity state
- Document access lifecycle expectations (request, approval, removal)

Logging and Monitoring Governance

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

Framework Alignment

- Map governance intent to:
    - NIST RMF (control selection and implementation intent only)
    - NIST CSF (Identify and Protect categories)
    - AWS Shared Responsibility Model (customer vs AWS boundary)

Evidence and Documentation

- Produce audit-defensible artifacts including:
    - Sanitized CLI outputs
    - Governance narrative
    - Role responsibility mapping
- Prepare interview-ready execution narrative for Phase One

Out of Scope (Explicit Exclusions)

Technical Engineering

- Custom IAM policy authoring

- Permission boundary design
- SCP creation or enforcement
- CloudTrail advanced configuration
- CloudWatch alarms or dashboards
- Automated remediation or guardrails

Infrastructure and Operations

- Workload deployment
- Network configuration
- Application logging integration
- CI/CD pipelines
- Cost optimization or billing analysis

Organizational Maturity

- Multi-account architecture
- Organization-wide governance enforcement
- Formal audit execution
- Risk quantification or scoring
- Incident response execution

Compliance Expansion

- FedRAMP, HIPAA, or ISO certification readiness
- AI governance controls
- Continuous monitoring automation

---

5. Constraints and Assumptions

Constraints

1. **Read-Only Operational Posture**
   All validation activities are observational. No destructive or production-impacting changes are permitted.

2. **CLI-Only Evidence Collection**
   All verification must be performed using AWS CLI with sanitized outputs. Console screenshots are excluded.
3. **Portfolio and Public Safety Constraint**
   All deliverables must be safe for public GitHub publication with deterministic redaction of sensitive data.

Assumptions

- The AWS account already contains baseline IAM and CloudTrail configurations
- Access to AWS CLI is available for validation purposes

---

6. Key Roles and Stakeholders

- **Project Manager**
  Maintains scope discipline, tracks deliverables, and ensures Phase One objectives are met.
- **Cloud Account Owner**
  Ultimately accountable for governance posture and strategic decisions.
- **Cloud Administrator**
  Implements IAM and logging configurations outside the scope of this phase.
- **GRC Analyst**
  Defines control intent, maps governance to frameworks, and reviews evidence.
- **Security Auditor**
  Consumes evidence and assesses governance design effectiveness.

---

7. Project Authorization

This project is authorized as a standalone Phase One governance initiative. The Project Manager is accountable for execution, documentation, and formal closure of Phase One within the defined scope and constraints.

---

8. Success Criteria (Phase One)

The project is considered successful when:

- Governance intent for identity and logging is clearly documented
- Control existence is validated through sanitized CLI evidence
- Framework mappings are complete and defensible
- Deliverables are organized, reviewable, and portfolio-safe
- Phase One closure documentation is completed and approved by the Project Manager.