Scope and Guardrails

Cloud Governance Foundation – Phase One

---

1. Purpose of This Document

This document defines the approved scope boundaries and execution guardrails for Phase One of the Cloud Governance Foundation project. Its purpose is to ensure disciplined execution, prevent scope creep, and clearly separate governance validation work from technical engineering or operational ownership.

2. In-Scope Activities (Phase One Only)

The following activities are explicitly approved and treated as in scope for Phase One execution.

2.1 Governance Design and Framing

- Define governance objectives for identity and logging at the AWS account level
- Document control intent independently from technical implementation details
- Establish Phase One success criteria and completion conditions

---

2.2 Identity Governance (Conceptual and Evidence-Based)

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

---

2.3 Logging and Monitoring Governance

- Confirm CloudTrail is enabled at the AWS account level

- Identify which event types are governance-relevant
- Validate logging presence through CLI-based evidence capture
- Define log retention intent and accountability at a governance level

---

2.4 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 responsibility boundaries)

2.5 Evidence and Documentation

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

---

3. Explicitly Out-of-Scope Activities

The following activities are explicitly excluded from Phase One. These exclusions are intentional and non-negotiable.

3.1 Technical Engineering

- Custom IAM policy authoring
- Permission boundary design
- Service Control Policy creation or enforcement
- Advanced CloudTrail configuration (data events, insights, organization-wide trails)

- CloudWatch alarms, dashboards, or metric tuning
- Automated remediation or preventative guardrails

3.2 Infrastructure and Operations

- Workload or application deployment
- Network configuration (VPCs, subnets, routing, security groups)
- Application-level logging integration
- CI/CD pipeline design or execution
- Cost optimization or billing analysis

3.3 Organizational Maturity and Compliance Expansion

- Multi-account architecture design
- Organization-wide governance enforcement
- Formal audit execution
- Risk quantification or scoring
- Incident response execution
- Compliance certification readiness (FedRAMP, HIPAA, ISO)
- AI governance controls
- Continuous monitoring automation

---

4. Execution Guardrails

The following guardrails govern how Phase One work is performed.

4.1 Read-Only Operational Posture

- All validation activities are observational
- No destructive or production-impacting changes are permitted

---

4.2 CLI-Only Evidence Collection

- All verification must be performed using AWS CLI
- Console screenshots and manual attestations are excluded
- Evidence must preserve structure while removing sensitive identifiers

---

4.3 Portfolio and Public Safety Constraint

- All artifacts must be suitable for public GitHub publication
- No account IDs, ARNs, or sensitive metadata
- Deterministic redaction only, with structure preserved

---

5. Scope Change Control

Any activity outside the defined in-scope items requires:

- Explicit documentation in the Decision Log
- Impact assessment on scope, risk, and timeline
- Formal approval before execution

Unapproved activities remain out of scope by default.

---

6. Phase One Completion Criteria

Phase One is considered complete when:

- All in-scope activities are executed or formally deferred
- Evidence artifacts are captured, sanitized, and organized
- Governance intent and framework mappings are documented
- Scope boundaries and exclusions are preserved
- Phase One is formally closed