Risk Register

Cloud Governance Foundation – Phase One

---

1. Purpose of this Risk Register

This Risk Register identifies, assesses, and tracks risks associated with Phase One execution of the Cloud Governance Foundation project. Risks are evaluated at a governance and execution level, not at a deep engineering or operational level, in alignment with project scope and guardrails.

---

2. Risk Rating Scale

Rating	Definition
Low	Minimal impact, easily managed
Medium	Moderate impact, requires monitoring
High	Significant impact, requires mitigation or escalation

---

3. Risk Register

Risk ID	Risk Description	Category	Likelihood	Impact	Response Strategy	Status
R-01	Governance scope expands into engineering configuration work, causing role confusion and scope creep	Scope / Role	Medium	High	Explicit scope guardrails documented; deviations require decision log entry and approval	Open

R-02	Identity or logging controls exist but are inconsistently implemented, limiting the strength of governance conclusions	Technical / Governance	Medium	Medium	Frame findings as readiness assessment, not enforcement; document gaps without remediation	Open
R-03	CLI evidence contains sensitive identifiers, creating portfolio or public-sharing risk	Compliance / Security	Low	High	Apply deterministic sanitization process; peer review evidence before publication	Open
R-04	Limited time availability delays documentation or evidence consolidation	Schedule	Medium	Medium	Prioritize core deliverables; defer non-critical enhancements to later phases	Open
R-05	AWS service behavior or permissions restrict CLI validation access	Dependency / Access	Low	Medium	Document access limitations; record assumptions and constraints transparently	Open
R-06	Framework mapping (NIST RMF / CSF) is interpreted as compliance certification readiness	Interpretation / Expectation	Medium	Medium	Clearly state mapping is intent-level only; exclude certification claims in documentation	Open
R-07	Interviewers misinterpret the project as purely theoretical due to limited implementation	Perception	Low	Medium	Emphasize executed validation steps, evidence capture, and controlled actions in narratives	Open

R-08	Over-documentation reduces clarity for non-technical stakeholders	Communication	Low	Low	Provide executive summaries and structured navigation in deliverables	Open

---

4. Risk Monitoring Approach

- Risks are reviewed during execution and status reporting
- New risks are added as execution progresses
- Risk responses are adjusted if likelihood or impact changes
- Closed risks are documented during phase closeout

---

5. Risk Ownership

- Project Manager owns risk identification, documentation, and tracking
- Technical risks are framed and documented without assuming remediation authority
- Escalation occurs through documented decisions, not ad hoc changes

---

6. Phase One Risk Closure Criteria

A risk may be marked Closed when:

- The risk is no longer applicable due to completed work

- The risk has been formally accepted and documented
- The risk is deferred to a future phase with rationale recorded
- All risks remain Open at Phase One close due to their relevance to future phases or ongoing governance oversight.