Risk Management Plan

Phase 0: Foundation & Planning

Sovereign AI Infrastructure Project

Document:	Risk Management Plan (Phase 0)
Version:	1.0
Date:	February 11, 2026
Status:	Draft for Review
Owner:	Project Manager / Risk Manager
Standard:	ISO 31000:2018; IEEE 1540-2001; PMBOK

1. Executive Summary

This Risk Management Plan establishes the framework, methodology, and governance for identifying, assessing, and mitigating risks throughout the Sovereign AI Infrastructure project lifecycle. The project involves deploying a complex, multi-model AI orchestration system with strict data sovereignty requirements, hardware constraints, and novel architectural patterns (bicameral GPU/CPU separation, Prolog-based constitutional routing).

> **Key Risk Areas Identified:**
>
> - **Technical Risks:** Model quality, hardware constraints, integration complexity
> - **Schedule Risks:** Novel architecture complexity, Prolog learning curve
> - **Resource Risks:** GPU memory limitations, model availability
> - **Security Risks:** Data sovereignty, prompt injection, validation bypass
> - **Operational Risks:** Deployment complexity, monitoring requirements

2. Risk Management Strategy

2.1 Risk Management Approach

The project adopts a **proactive, continuous risk management approach** integrated with the development lifecycle:

- **Phase 0 (Foundation):** Identify preliminary risks during technical analysis and architecture design
- **Phase 1 (Design):** Deep-dive technical and security risk assessments
- **Phase 2+ (Implementation):** Weekly risk monitoring and mitigation tracking
- **Phase 3 (Operations):** Operational risk register and incident response

2.2 Risk Appetite Statement

> **Organizational Risk Appetite:** The Sovereign AI Infrastructure project operates in a **low-risk tolerance environment** due to:
>
> - Regulatory compliance requirements (HIPAA, GDPR, SOC 2)
> - High-stakes use cases (healthcare, finance, legal)
> - Data sovereignty mandates (no external dependencies)
> - Novel architecture with unproven integration patterns
>
> **Decision Rule:** When in doubt, prefer risk mitigation over risk acceptance. High-severity risks must be mitigated before proceeding to subsequent phases.

2.3 Risk Categories

Category	Description	Examples
Technical	Risks related to technology, architecture, and implementation	Model quality insufficient, hardware constraints, integration failures
Schedule	Risks affecting project timeline and milestones	Complexity underestimation, learning curve delays, scope creep
Cost	Risks affecting budget and resource allocation	Hardware procurement delays, additional tooling costs
Resource	Risks related to personnel, skills, and availability	Prolog expertise gap, ML engineering capacity
Security	Risks related to data protection and system security	Prompt injection, data exfiltration, validation bypass

Compliance	Risks related to regulatory and legal requirements	Audit trail incompleteness, data sovereignty violations
External	Risks from external dependencies and vendors	Model availability, llama.cpp updates, dependency vulnerabilities

3. Risk Assessment Methodology

3.1 Probability Scale

Rating	Probability	Description
1	Rare	<10% likelihood; may occur only in exceptional circumstances
2	Unlikely	10-30% likelihood; not expected but possible
3	Possible	30-50% likelihood; could occur under certain conditions
4	Likely	50-70% likelihood; expected to occur at some point
5	Almost Certain	>70% likelihood; will probably occur

3.2 Impact Scale

Rating	Impact	Technical	Schedule	Cost
1	Negligible	Minor issue, easily fixed	<1 week delay	<$1K
2	Minor	Workaround available	1-2 week delay	$1K-$5K
3	Moderate	Significant rework required	2-4 week delay	$5K-$20K
4	Major	Architecture redesign needed	1-2 month delay	$20K-$50K
5	Catastrophic	Project failure or abandonment	>2 month delay	>$50K

3.3 Risk Assessment Matrix

Risk Score = Probability × Impact (Range: 1-25)

	Impact 1 (Negligible)	Impact 2 (Minor)	Impact 3 (Moderate)	Impact 4 (Major)	Impact 5 (Catastrophic)
Prob 5 (Almost Certain)	**5**	**10**	**15**	**20**	**25**

Prob 4 (Likely)	4	8	12	16	20
Prob 3 (Possible)	3	6	9	12	15
Prob 2 (Unlikely)	2	4	6	8	10
Prob 1 (Rare)	1	2	3	4	5

Risk Level Classification:

- **Critical (Score 15-25):** Immediate action required; escalate to steering committee
- **High (Score 10-14):** Mitigation plan required before phase progression
- **Medium (Score 5-9):** Monitor and mitigate as resources allow
- **Low (Score 1-4):** Accept and monitor periodically

4. Roles and Responsibilities

Role	Risk Responsibilities	Authority
Project Sponsor / Steering Committee	Approve risk appetite; resolve escalated risks; authorize contingency reserves	Accept/escalate Critical risks
Project Manager / Risk Manager	Maintain risk register; facilitate risk reviews; track mitigation progress; report status	Accept Low risks; assign Medium risk owners
Technical Lead	Identify technical risks; assess feasibility; propose mitigations; validate assumptions	Accept technical Low risks
Solutions Architect	Assess architectural risks; design risk mitigations; validate technology choices	Recommend technical risk treatments
Security Architect	Identify security threats; conduct threat modeling; define security controls	Mandate security mitigations
Product Lead	Assess business impact; prioritize risk mitigations; manage scope trade-offs	Accept schedule/cost risks
Risk Owners (Assigned)	Execute mitigation plans; monitor risk triggers; report status changes	Implement approved mitigations

5. Escalation Procedures

5.1 Escalation Triggers

Trigger	Action	Timeline
New Critical risk identified	Immediate notification to Project Manager and Technical Lead	Within 4 hours
Risk score increases to Critical	Escalate to Steering Committee; halt affected work if necessary	Within 24 hours
Risk mitigation fails	Reassess risk; escalate if residual risk remains High/Critical	Within 48 hours
Multiple Medium risks materialize	Convene risk review meeting; assess cumulative impact	Within 1 week
Risk owner unavailable	Reassign to backup; notify Project Manager	Immediate

5.2 Escalation Path

1. **Level 1:** Risk Owner → Project Manager (for Medium risks, mitigation issues)
2. **Level 2:** Project Manager → Technical Lead + Product Lead (for High risks, cross-functional issues)
3. **Level 3:** Technical/Product Lead → Steering Committee (for Critical risks, strategic decisions)
4. **Level 4:** Steering Committee → Executive Sponsor (for project-threatening risks)

6. Review and Reporting Cadence

Activity	Frequency	Participants	Outputs
Risk Identification	Continuous	All team members	New risk entries in register
Risk Assessment Updates	Weekly (Phase 2+)	Risk Owners, PM	Updated risk scores
Risk Review Meeting	Bi-weekly	Core team, leads	Risk status report
Steering Committee Report	Monthly	PM, Steering Committee	Executive risk summary
Phase Gate Review	Per phase	All stakeholders	Phase risk clearance

7. Risk Treatment Strategies

Strategy	When to Use	Examples
Avoid	Risk impact is unacceptable; alternative approach exists	Remove feature, change technology, simplify architecture
Mitigate	Risk can be reduced to acceptable level with effort	Add validation, increase testing, add redundancy
Transfer	Risk is better managed by third party	Insurance, outsourcing, vendor SLAs
Accept	Risk impact is low or cost of mitigation exceeds benefit	Monitor only; contingency plan if materializes

8. Tools and Templates

8.1 Risk Register Template

The Initial Risk Register (companion document) uses the following fields:

- Risk ID, Date Identified, Risk Description, Category
- Probability, Impact, Risk Score, Risk Level
- Mitigation Strategy, Mitigation Actions, Risk Owner
- Target Date, Status, Residual Risk, Contingency Plan

8.2 Tools

Purpose	Tool
Risk Register Storage	Git repository (Markdown/CSV)
Risk Tracking	GitHub/GitLab Issues with risk labels
Reporting	Markdown reports, PDF exports
Collaboration	Slack/Teams for urgent notifications

9. Integration with Project Lifecycle

Phase	Risk Activities	Deliverables
Phase 0: Foundation	Establish risk framework; identify preliminary risks; create initial register	Risk Management Plan, Initial Risk Register
Phase 1: Design	Technical risk assessment; security threat modeling; update register	Technical Risk Assessment, Security Risk Assessment
Phase 2: Implementation	Weekly risk monitoring; track mitigation progress; identify new risks	Risk Monitoring Log
Phase 3: Operations	Operational risk identification; incident-based risk updates	Operational Risk Register
Phase 4: Knowledge Transfer	Post-implementation risk review; lessons learned	Post-Implementation Risk Review

10. Success Criteria

This Risk Management Plan is considered successful when:

1. All Critical and High risks from Phase 0 are identified and have mitigation plans
2. Risk register is populated with at least 80% of foreseeable risks before Phase 1
3. Risk review meetings occur on schedule with documented outcomes
4. No unidentified Critical risks materialize during implementation
5. Risk escalation procedures are tested and understood by all team members

Risk Management Plan | Phase 0: Foundation & Planning | Version 1.0

Document maintained per ISO 31000:2018 and IEEE 1540-2001 standards