
template_id: risk_assessment_v1 iso_clauses: ["6.1","Annex C"] ai_act:
["Annex IV §6"] version: "1.0.0" language: "en" generated_at:
"2025-10-18T08:23:11.917532+00:00"

Risk Management Plan — Test System

Based on ISO/IEC 42001 clause 6.1 and Annex C.

Organization: On-Chain Labs Governance

System: Test System

Domain: testing

AI Act Classification: minimal

Generated: 2025-10-18T08:23:11.917532+00:00

1. Purpose

Identify, analyse, evaluate and treat risks related to AI systems operated by On-Chain Labs Governance.

2. Scope

All AI systems operated by On-Chain Labs Governance, including the Test System system, pilots and third-party models.

3. Methodology

- ISO 31000 principles (Identify → Analyse → Evaluate → Treat → Monitor).
- Risk register maintained in this document; update after incidents or significant model changes.

4. Roles and Responsibilities

Role	Responsibility
AI Governance Lead	Maintains the risk register; reports to top management.
System Owner	Identifies operational risks; owns mitigation actions.
Compliance Officer	Aligns risks with legal/ethical requirements.

5. Risk Register (example rows)

ID	Risk	Likelihood	Impact	Level	Mitigation	Owner	Status
R-001	Bias in training data	M	H	High	Fairness metrics, re-sampling, threshold review	ML Lead	Open
R-002	Data leakage	L	H	Med	DLP controls, access review, secrets scanning	Data Steward	Mitigated
R-003	Model drift	M	H	High	Weekly PSI checks, retrain triggers, rollback	MLOps	Ongoing

6. Monitoring & Review

Quarterly review or after incidents; metrics: open risks, MTTR, residual risk trend.

7. References

ISO/IEC 42001 §6.1; ISO/IEC 23894; EU AI Act Annex IV §6.