# First Agent Spec v1.0

## 1. Problem / Use case

## 2. User and trigger

## 3. Success criteria

## 4. Scope and boundaries

## 5. Agent Loop

## 6. State schema

## 7. Tool Contracts

## 8. Data Source Register

## 9. State / Memory / Logging

## 10. Human Approval Matrix

## 11. Guardrails and limits

## 12. Test set and results

## 13. Pilot Scorecard

## 14. Open risks

## 15. vNext roadmap

## 16. Production readiness gaps

- auth/identity
- permissions
- secrets
- monitoring/alerts
- retries/idempotency
- audit trail
- recovery/rollback
- support owner

- legal/security checks for target systems