

SAMPLE DELIVERABLE · READINESS ASSESSMENT

Agent Governance Readiness Assessment

Maturity scoring against the 12 Principles for Agent Runtime Governance, with prioritized roadmap to Level 3 (Governed).

PREPARED FOR	Acme Capital
SECTOR	Financial Services (Illustrative)
ENGAGEMENT	Agent Governance Readiness Assessment
SCOPE	Enterprise AI agent platform (18 agents in production)
DELIVERED	March 2026

01 Executive Summary

Current-state maturity assessment of Acme Capital's AI agent governance posture, measured against the 12 principles of Agent Runtime Governance.

OVERALL MATURITY SCORE: LEVEL 1.6 (IDENTIFIED, APPROACHING CONTROLLED)

Acme Capital has made significant progress on agent identity (Level 3) and logging infrastructure (Level 2). However, runtime governance, delegation tracking, and execution lineage remain at Level 1 or below. The organization has strong IAM foundations but lacks the runtime evaluation layer required to safely scale agent adoption beyond current pilots. **The path to Level 3 (Governed) is estimated at 4–6 months with focused investment.**

Headline Findings

AGENTS IN SCOPE 18 production + 7 staging	CURRENT MATURITY Level 1.6 / 5.0
TARGET MATURITY Level 3.0 (Governed)	PRINCIPLES AT LEVEL ≥ 3 2 of 12
CRITICAL GAPS IDENTIFIED 5	PATH TO LEVEL 3 4–6 months

Critical Governance Gaps

- No runtime policy evaluation on agent actions** GAP

Agents operate under static IAM roles assigned at deployment. No mechanism exists to evaluate intent, context, or delegation chain at the moment of action. Violates Principle 7 (Runtime Policy Enforcement).
- Long-lived credentials across 15 of 18 agents** GAP

Most agents hold API keys and service tokens with 90-day TTLs and broad scope. No capability-token broker exists. Violates Principle 11 (Tool and Service Governance).
- No delegation chain tracking for multi-agent workflows** GAP

Three production workflows involve orchestrator-to-worker agent delegation. Authority flows freely without scope narrowing or cryptographic verification. Violates Principle 3.

02 Maturity Scorecard

Current-state scoring against each of the 12 principles. Levels range from 0 (Unmanaged) to 5 (Optimized). Target state is Level 3 (Governed) or higher for all principles.

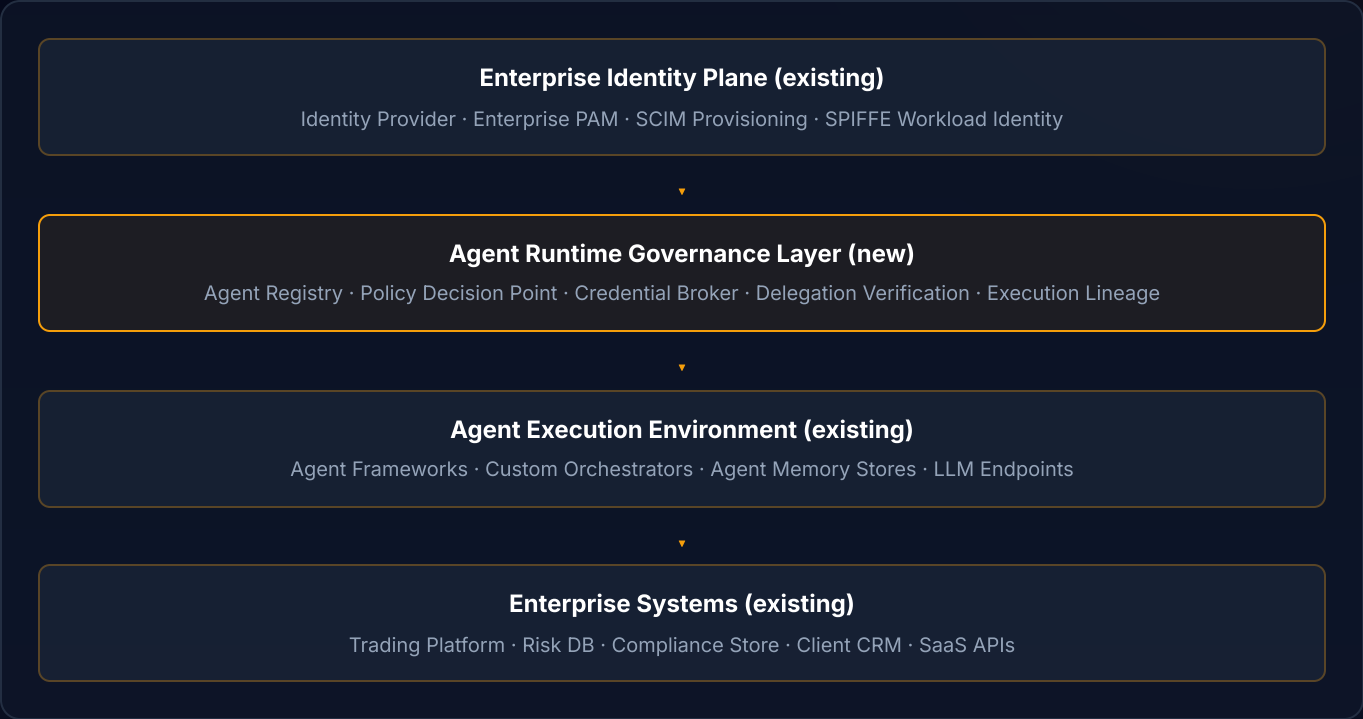
1. Agent Identity Is Mandatory	FOUNDATIONS		3.0
2. Explicit Purpose, Goals, Intent	FOUNDATIONS		1.0
3. Authority Is Scoped & Time-Bound	FOUNDATIONS		1.0
4. Deterministic Control Planes	EXECUTION		1.0
5. Plan-Act-Observe Lifecycle	EXECUTION		2.0
6. Human-in-the-Loop as Capability	EXECUTION		2.0
7. Runtime Policy Enforcement	EXECUTION		0.5
8. Governed Memory and State	OPERATIONS		2.0
9. Observability and Auditability	OPERATIONS		2.5
10. Safe Failure Semantics	OPERATIONS		1.0
11. Tool and Service Governance	OPERATIONS		1.0
12. Multi-Agent Coordination	OPERATIONS		1.0

OVERALL MATURITY

Level 1.6 / 5.0 · Acme Capital demonstrates strong foundations in agent identity and logging. Governance gaps concentrate in runtime enforcement, delegation tracking, and credential management. These gaps represent focused, addressable areas of investment rather than systemic issues.

03 Target Reference Architecture

Recommended target architecture for Acme Capital to reach Level 3 (Governed) maturity. Integrates with existing identity, PAM, and SIEM infrastructure.



Integration Points

IDENTITY SOURCE Enterprise IdP + SCIM	POLICY LANGUAGE Cedar (recommended)
CREDENTIAL BACKEND Enterprise PAM + Vault	OBSERVABILITY SINK SIEM + OTel bridge
EVENT TRANSPORT NATS JetStream	DEPLOYMENT TARGET Kubernetes (existing clusters)

Key Integration Notes

- Leverage existing enterprise IdP (OIDC) for agent identity provisioning through SCIM extensions
- Use the existing PAM backend for short-lived capability tokens
- Policy authoring in Cedar with the existing GitOps workflow for policy versioning
- Stream execution lineage events to the SIEM platform via the existing OpenTelemetry collector
- Deploy the ARG control plane to the existing platform Kubernetes clusters with autoscaling enabled

04 Prioritized Roadmap

Path to Level 3 (Governed) maturity, sequenced to deliver risk reduction incrementally. Quick wins in the first month, strategic capabilities over 4–6 months.

MONTH 1 · QUICK WINS

Visibility & Hygiene

- Complete agent registry (P1)
- Document ownership for all 25 agents
- Rotate all long-lived credentials
- Enable intent declaration (P2)
- Baseline behavioral logging (P9)

MONTH 2–3 · FOUNDATION

Runtime Governance

- Deploy ARG control plane
- Author Cedar policies for top 5 workflows
- Integrate with enterprise IdP
- Enable policy evaluation (P7)
- Pilot on 3 non-critical agents

MONTH 4–5 · CREDENTIALS

Broker & Delegation

- Deploy credential broker (P11)
- Migrate all production agents
- Retire long-lived tokens
- Cryptographic delegation chains (P3)
- Scope narrowing enforcement

MONTH 6 · OPERATIONS

Lineage & Readiness

- Execution lineage graph (P9)
- Multi-agent coordination (P12)
- Compliance reporting
- Level 3 readiness review
- Runbook and on-call setup

Expected Maturity Progression

MILESTONE	MONTH 1	MONTH 3	MONTH 5	MONTH 6
Overall Maturity	1.8	2.3	2.7	3.0
Foundations (P1-P3)	2.5	3.0	3.3	3.5
Execution (P4-P7)	1.3	2.3	2.8	3.0
Operations (P8-P12)	1.5	1.8	2.3	2.8

Detailed implementation guidance, resource requirements, and specific Cedar policy examples are provided in Appendices A through E.