

GovAgent: Governance Framework

PUBLIC STANDARD FOR AGENTIC AI INTEGRITY & RISK MANAGEMENT

Framework Purpose

GovAgent establishes a transparent, open-source protocol for the deployment of autonomous systems. By shifting from "Black Box" operations to **Verifiable Governance**, the framework enables organizations to scale AI capabilities while maintaining strict adherence to financial, ethical, and operational guardrails.

1. Governance-as-Code

The framework utilizes declarative manifests (YAML) to define the operational boundaries of an agent. This ensures that governance is not a manual oversight process but a hard-coded technical constraint.

2. Risk Mitigation Matrix

Control Area	Mechanism	Enterprise Outcome
Financial	Real-time Circuit Breakers	Elimination of runaway API costs.
Operational	Confidence-based Escalation	Reduction in hallucination-led errors.
Compliance	Forensic Telemetry Ledger	Audit-ready logs for SOC2/ISO review.

3. Accountability & Transparency

As a public standard, GovAgent provides a cryptographically verifiable trace of agentic decisions. This enables a 'Right to Explanation' for automated actions, bridging the gap between innovation and regulatory requirements.

AUTHORIZED FRAMEWORK SPECIFICATION

Framework: GovAgent v0.1.0 (Public Release)

Status: Active / Open-Source Standard

Release Date: 28 April 2026

Compliance: Designed for Enterprise-Grade Accountability