Runtime Governance for Enterprise AI

Executive Briefing

Dan Mercede
Founder — Orion Intelligence Agency

orionintelligenceagency.com/book

THE PROBLEM

Enterprise AI Fails on Control, Not Capability.

72%

of enterprise AI deployments stall before production due to unresolved governance gaps

$4.2M

average cost of a single agentic failure in regulated environments

< 3%

of organizations enforce governance at runtime — the rest rely on policy documents

Execution outruns governance. The result: compounding risk with no deterministic containment.

THE ENFORCEMENT STACK

Four-Layer Control-Plane Architecture

01	**AUTHORITY GATE** *Intent Boundary*	Execution depends on authority. Fail-closed halt if authority cannot be verified.	*No execution without explicit authority.*
02	**IMMUTABLE RECEIPTS** *Mutation Attestation*	Every state change cryptographically attested. Append-only receipt ledger.	*No mutation without attestation.*
03	**DRIFT GUARD** *Behavioral Constraint*	Containment across time. Authority decays. No standing execution paths.	*No behavior without constraint.*
04	**GATED SUBSTRATE** *Physical Isolation*	Capability removed, not restricted. Workload isolation at the substrate.	*No capability without isolation.*

Each layer is necessary. None is sufficient alone.

LAYER 1

Authority Gate — Intent Boundary

WITHOUT AUTHORITY GATE	WITH AUTHORITY GATE
• Agent receives instruction	• Agent receives instruction
• Executes immediately	• Intent evaluated at boundary
• No authority verification	• Authority verified deterministically
• State mutated without constraint	• Fail-closed halt if unverified
• Damage discovered post-hoc	• Zero unauthorized state mutations

Key Metric: Unauthorized execution rate → 0%

LAYERS 2–3

Immutable Receipts + Drift Guard

IMMUTABLE RECEIPTS

Mutation Attestation Layer

ACTION → Cryptographic hash
↓
HASH → Append-only ledger
↓
LEDGER → Non-repudiation proof
↓
PROOF → Audit-ready artifact

DRIFT GUARD

Behavioral Constraint Layer

- Authority decay enforcement
- No standing execution paths
- Privilege creep detection
- Behavioral deviation containment
- Time-bounded session constraints

Audit Coverage: **12% → 97%** | *Logs are telemetry. Receipts are enforcement artifacts.*

LAYER 4

Gated Substrate — Physical Isolation

Capability must be removed, not restricted.

Workload Isolation

- Execution environment containment
- No shared substrate between agents
- Resource boundary enforcement

Tool Boundary Redesign

- Capability surface minimization
- Tool access scoped per-session
- No inherited permissions

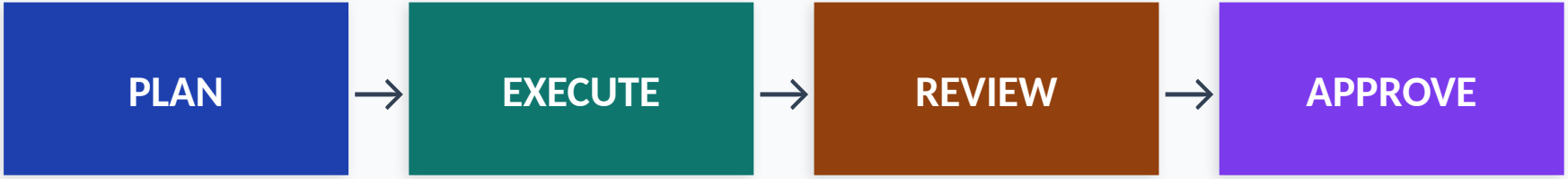
Routing Prevention

- Intelligence cannot route itself
- Physical separation of control
- Governance outside the execution path

Blast Radius: **Contained to single execution boundary**

ENFORCEMENT PIPELINE

Gate Pipeline Flow



Intent declared.
Authority evaluated.

Bounded action.
Receipt generated.

Drift assessed.
Constraints checked.

Attestation issued.
State committed.

- Authority Gate evaluates intent before execution begins
- Receipt ledger attests every state mutation at execution boundary
- Drift Guard constrains behavioral deviation across time
- Gated Substrate isolates execution environment physically

ROI PROOF

Measured Impact of Runtime Governance

67%

Cost Reduction

Per successful AI task after enforcement deployment

94%

Escalation Reduction

Human-in-the-loop interventions eliminated

97%

Audit Coverage

From 12% baseline to full attestation coverage

4.2x

Throughput Increase

Governed task completion rate vs. ungoverned baseline

< 48hrs

Time to Evidence

From incident to complete attestation chain delivery

$0

Unauthorized Mutations

Financial exposure from ungoverned state changes

Composite metrics from anonymized design-partner engagements.

ENGAGEMENT MODEL

From Readiness Scan to Hardened Production

Readiness Scan

Complimentary

45-minute assessment

- Control-plane gap map
- Failure-mode heatmap
- Evidence & attestation checklist
- Prioritized 30/60/90 roadmap

AI Readiness Sprint

$7,500

2 weeks

- Full enforcement audit
- Priority hardening plan
- Quick-win implementation
- Stakeholder risk brief

AI Hardening Engagement

$25K - $40K

6–10 weeks

- 4-layer enforcement deployment
- Runtime governance integration
- Compliance evidence generation
- Production readiness certification

Every engagement produces enforcement artifacts — not advisory documents.

Schedule Your Readiness Scan

45 minutes. Four enforcement layers assessed.
Actionable roadmap delivered.

orionintelligenceagency.com/book

dan@orionapexcapital.com | linkedin.com/in/danmercede | danmercede.com

If governance isn't enforced at runtime, it isn't governance.