

REGULATOR VIEW

Agentic Execution - Tool-Chained Authority Expansion

World: Agentic Execution Governance **Outcome:** ESCALATE **Evidence Pack ID:** JSP-PUBLIC-20260302-AGENTIC_EXEC-0001

1. What action happened

Agent requests production write access mid-run.

2. Who held authority

Primary authority	Platform Owner
Secondary authority	Security Approver
Escalation roles	Platform Owner, Security Approver
Authority principle	No consequential action proceeds without named human authority.

3. What was enforced at runtime

Outcome	ESCALATE
Bounds enforced	<ul style="list-style-type: none">- exact scope required (namespace-scoped)- TTL \leq 30 minutes- reversible actions only- no secret access unless explicitly approved
Escalation path	Route to named platform owner + security approver (dual control). If denied or timed out, SAFE DEGRADE to read-only tools.

4. What would happen if confidence dropped

Without governance: Agent could gain broad write authority and execute multi-system drift before review.

Prevented failure mode: privilege expansion by momentum

Illustrative exposure: production incident + credential misuse

Note: exposure figures are illustrative; the structural claim is that the system intercepts and governs at the moment before consequence.

Evidence & Integrity

5. Evidence minimums and signals

- requested_tool
- requested_scope
- ttl_requested
- current_delegation_token
- secret_access_in_scope
- blast_radius_estimate

6. Portable artefacts included in this pack

evidence_pack.json	Top-level decision record and links.
authority_contract.json	Who can authorise what, with what bounds.
policy_trace.ndjson	Versioned doctrine checks evaluated.
audit_export.ndjson	Runtime event log for audit ingestion.
provenance_chain.json	Illustrative model/prompt/tool-call chain integrity.
manifest.json + signature	Tamper-evident integrity for this entire bundle.

7. Integrity verification

Run **verify_manifest.py** in the root folder to recompute SHA-256 hashes and verify the signature (when cryptography or OpenSSL is available).

Expected output: **PASS** (no files changed).

This proof object is designed to be inspected without access to the originating systems.

Contact: founder@judgementspine.com | <https://judgementspine.com/>