

BOARD VIEW

Agentic Execution - Tool-Chained Authority Expansion

Suite: Platform Runtime Control Suite **World:** Agentic Execution Governance **Outcome:** ESCALATE

What happened (execution intent)

Agent requests production write access mid-run.

Status quo	IAM governs static roles, not dynamic delegation drift; mid-run privilege expansion becomes an unowned trust boundary.
AI shift	Agents chain tools and tokens, expanding capability across systems; authority can drift with each tool call.
Judgement Spine difference	Judgement Spine enforces 'no authority expansion by momentum' at execution time. Privilege elevation becomes a governed MTM requiring dual control, scoped TTL, and signed approval tokens before the tool call can execute.
Impact	Stops authority creep (the defining risk of agentic systems) while preserving planning velocity.

Decision summary

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.

Proof you can produce in 60 seconds

1. Open WOW_PACK/OPEN_ME.html (offline).
2. Select this scenario and click Replay (90 seconds).
3. Open Regulator View and Dispute Pack PDFs.
4. Run verify_manifest.py to confirm integrity (hashes + signature if available).

Evidence Pack ID: JSP-PUBLIC-20260302-AGENTIC_EXEC-0001 **Control plane demos:**

<https://judgementspine.com/control-plane-demos>

Note: This is a public, redacted, illustrative pack. The structural claim is about runtime authority, bounded autonomy, and proof written before consequence.