



Pattern C - Agent Tool Wrapper (Agentic Era)

Use when agents can call tools that change infra, IAM, data, or security state.

Implementation steps

1. Wrap agent tool calls so each privileged action triggers a governance decision before execution.
2. Bind delegation rules: scope, TTL, and non-negotiable blocks (no mid-run escalation of privilege).
3. On ESCALATE, pause execution and request a signed approval token from named authorities.
4. Resume run only inside the approved scope + TTL. If denied or timed out, degrade safely to read-only.
5. Mint evidence capturing attempted expansion, approvals, and enforced bounds.

Minimal adapter contract (illustrative)

```
{
  "intent": { "action": "request_prod_write", "scope": "payments-prod/*", "ttl": "30m" },
  "world": "Agentic Execution Governance",
  "context": { "secrets_in_scope": true, "blast_radius": "wide" }
}
```

Outputs you should produce

- Runtime outcome returned (ALLOW / BOUNDS / ESCALATE / BLOCK / SAFE DEGRADE)
- Enforcement applied in the target system
- Evidence pack minted (intent, authority, bounds, doctrine version, rationale, integrity refs)

Contact: founder@judgementspine.com