

ASPHODEL + TIRESIAS-ZT • AGENT WALKTHROUGH

The Compliance Officer. The last signature in the chain.

A single governed agent sits at the terminal node of ACME's showcase workflow — synthesizing every upstream hand-off into an auditable sign-off, and escalating to frontier reasoning when the stakes demand it.

● Asphodel + Tiresias-ZT • ACME Corporation

Automation without a paper trail is just faster risk.

When 367 agents act on your behalf, the question is never "did they work?" — it is "can you prove what they did, and who is accountable for the result?" The compliance-officer agent exists to answer that question by design, not after the fact.

Terminal	Last node of the hand-off DAG Every upstream finding funnels here before anything is signed	node 7 / 7
Accountable	Sign-off + ROI synthesis Reconciles the workflow's outputs and its economics into one record	deny-by-default
Provable	Every action lands in a signed audit chain SoulKey Ed25519 signatures, durable WAL, shipped to the control plane	Ed25519

THE GOVERNED WORKFORCE

367 agents, one policy fabric, zero implicit trust.

The compliance officer is one identity inside a real, live zero-trust deployment
— mapped like-for-like onto ACME's actual org and enforced on every call.

367 GOVERNED AGENTS	7 SHOWCASE DAG AGENTS	360 FLEET AGENTS • 28 DEPTS	325,154 DIRECTORY PRINCIPALS
---	---	---	--

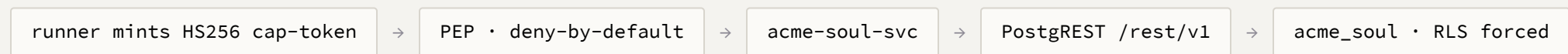
The directory behind the fleet is not synthetic: 120,120 humans and 205,034 non-human identities across 28 departments, 10 regions and 626 roles, synced from a real Samba-AD tree into the control-plane identity store.

Source: ARCHITECTURE-FACTS.md • Plane 1 (Directory) + Plane 5 (Runner)

THE SLICE THAT MATTERS HERE

Nothing this agent does is taken on faith.

Every governed call the compliance officer makes crosses the enforcement plane before it touches data. Deny-by-default is the resting state; an allow is an explicit, signed event.



WHAT THE PEP CHECKS

Validates the tenant X-Tiresias-API-Key and the per-call X-Capability-Token, evaluates policy, and only then forwards the request *verbatim* to the agent's own soul-svc tenant backend.

WHAT ISOLATION GUARANTEES

Each agent is its own soul-svc tenant with FORCE row-level security on Cloud SQL. The compliance officer cannot read another agent's memory — even a postgres superuser is subject to forced RLS.

Source: ARCHITECTURE-FACTS.md · Governed request flow + Plane 4 (Data)

LIVE PROOF

This is a running instance, not a diagram.

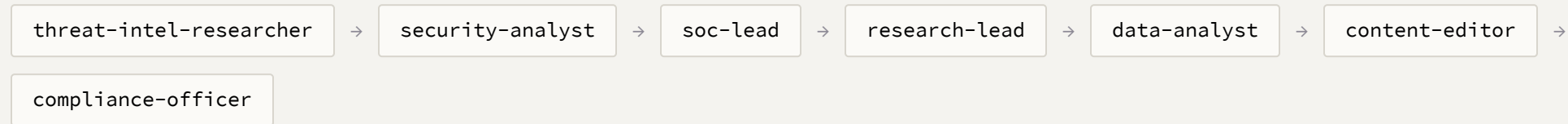
The compliance officer's calls are observable on the same published surfaces an auditor would use to check them — right now, on the acme-demo host.

SURFACE	WHERE	WHAT IT PROVES
PEP · governed data plane + /admin	:8343	every allow/deny + audit chain
Asphodel management console	:3001	agents, memory / CoT review, policy
Grafana · ROI economics board	:3000	per-model \$/1M-token cost
Loki · SoulWatch SIEM sink	:3100	behavioral drift + syslog audit
Promtail · syslog ingest	:1514	RFC5424 SIEM feed

Source: ARCHITECTURE-FACTS.md · Port map + Plane 6 (Observability). Host: acme-demo (34.133.17.162).

Seven agents hand off. The buck stops at node seven.

The showcase workflow is a 14-edge topological hand-off DAG. Upstream agents research, analyze and draft; the compliance officer is where their outputs converge for sign-off.



By the time work reaches this node, six agents have already acted — and every one of their calls is already in the chain the compliance officer signs against.

When the words say "breach," the model tier changes.

Each showcase agent runs with a home tier, a ceiling and a floor. The compliance officer's keyword-escalation triggers on the highest-stakes signals — +incident, +breach, +critical — and routes the reasoning up to the frontier model.

Trigger	Regulatory / incident keywords in the brief +incident · +breach · +critical push the request toward the ceiling tier	escalate
Ceiling	Frontier reasoning for the sign-off opus-4.8 — the paid OpenRouter tier reserved for the hardest calls	score 100
Floor	Fallback-to-floor on LLMError The agent degrades to a reliable tier rather than failing the job	no silent drop

Cost follows consequence: routine synthesis stays cheap; a suspected breach buys the most capable model in the roster — on purpose, and on the record.

One governed job, start to signed finish.

On its schedule, the compliance officer runs a regulatory-watch brief. The job is not special-cased — it travels the exact governed path every agent uses, and lands as a durable, isolated write.

01	Domain brief in Regulatory-watch prompt enters the tiered LLM router	runner.py
02	Capability token minted Per-agent HS256 token from a 64-hex capability secret	HS256
03	Governed through the PEP Api-key + cap-token validated, policy evaluated, deny-by-default	:8343
04	Governed CoT + memory write ContentInspection requires source_type + authored_by on every write	/v1/memory/write
05	Usage reported Tokens + cost flow to tzt_usage and the ROI board	/cp/usage/report

The audit story the compliance officer both writes and lives inside.

This agent's authority rests on the same machinery that watches it. Its sign-offs are only as trustworthy as the chain that records them — and that chain is cryptographic, durable, and continuously monitored.

SIGNED AUDIT CHAIN

Every governed call is signed into a SoulKey Ed25519 audit chain with a durable WAL at /data/audit-wal, then shipped to the control plane. Verify it from the PEP /admin console.

SOULWATCH DRIFT → QUARANTINE

Behavioral drift trips SoulWatch, which auto-quarantines the offending agent via the shared postgres store. A compliance officer that started misbehaving would be contained, not trusted.

SIEM	RFC5424 syslog → Promtail → Loki	:1514 → :3100
The full audit feed is queryable alongside every other agent's		
Review	PEP /admin: audit/verify, soulwatch, quarantine, analytics	pdp.tiresias.watch
Role-token gated — trajectory, model_baseline, campaign, drift		

The sign-off carries a number, and the number is measured.

Part of this agent's job is ROI synthesis — and the Grafana ROI board (uid acme-roi-economics) gives it real per-call economics to reconcile. The frontier tier it escalates to is the most expensive line by three orders of magnitude.

MODEL TIER	PROVIDER	\$/CALL	RELATIVE
opus-4.8 (escalation ceiling)	OpenRouter paid	\$0.19	
sonnet-4.5	OpenRouter paid	\$0.03	
deepseek-v4-pro	Ollama Cloud	\$0.002	
gpt-oss:120b	Ollama Cloud	\$0.0015	
Llama-3.3-70B	HuggingFace	\$0.0012	
gemma-4-31b:free	OpenRouter free	\$0	

Source: ARCHITECTURE-FACTS.md • Plane 6 (ROI dashboard, observed \$/1M-token economics)

THE CLOSE

Accountable by construction.

The compliance officer is what a governed workforce looks like when it takes its own governance seriously: a terminal sign-off node that escalates to frontier reasoning under pressure, writes into a signed chain it cannot forge, and reconciles the economics of the whole workflow — every call deny-by-default, every action provable.

7 / 7 TERMINAL DAG NODE	100 ESCALATION SCORE → FRONTIER	Ed25519 SIGNED AUDIT CHAIN	367 AGENTS UNDER ONE POLICY
---	---	--	---