

One production AI system. One file. A closed 90-day book — or the reason it isn't.

An underwriter approves the system that is actually in production, for the next policy period, when three things are visible: the dangerous things it is allowed to do were tested on the right frameworks, **a named person is on the hook**, and the last 90 days are a closed book — exceptions happened, someone owned them, and they ended. **A beautiful empty pack is a referral**. The Control File is what goes inside the pack.

IN THE EVIDENCE PACK TODAY

The file and the fleet page

Schema 1.2 — Midnight Evidence layout, 11 sections.

- ▶ **Evidence Pack PDF + JSON** per registered system, with an integrity page and verify hashes
- ▶ **AI System Schedule** — every production system on one page
- ▶ **Measured results** — latest Security run preferred; questions answered by category, no scores
- ▶ **Signed attestation**, countersign, **escalation chains**, and the **Risk Acceptance Ledger**

ADDING IN ACT-077 · SCHEMA 1.3 · IN REVIEW

The meat of the file

Fills the sections that print “not assessed” today.

- ▶ **Key binding** — each field key records the system, provider, model, and prompt hash
- ▶ **Binding check on every field run** — match, model mismatch, prompt mismatch, or not attested
- ▶ **Run reason** — startup, intraday, or manual; never inferred from the clock
- ▶ **90-day exception log** with owner, time to acknowledge, and disposition
- ▶ **Drift tables** — behavior, binding changes, signed evidence left behind

How it works: one key, one implementation

1 · Bind

The customer binds one key to one system, one LLM, one prompt hash.

2 · Attest

On every field run the client reports the model, the prompt hash, and why it ran.

3 · Compare

We compare and store the result. A mismatch is recorded, never refused.

4 · Log

Every mismatch, miss, veto, or open item becomes a row in the exception log.

Eight gates. The cover sentence prints only when all eight pass.

G1

Production

Production environment, active status.

G2

Security in window

A completed Security run in the last 90 days.

G3

Startup and the day

Security field runs on startup and intraday.

G4

Prompt and model

Latest field run and tested run match the binding.

G5

Owner signed

Unexpired attestation; countersign when required.

G6

Closed book

No open row in the exception log.

G7

No unanswered drift

Each drift row has a retest or signed acknowledgment.

G8

Human stop

Kill switch and a named person when it can act.

“Security ran on startup and through the window, the prompt and model are the ones we tested, the owner signed, the 90-day exception log is closed, and nothing material moved without a new test.”

If any gate fails, the cover prints the failed gates instead — never a softer paraphrase. The fleet page sorts by the CFO failure-cost band, then open exceptions, so the files that can hurt you are read first.

The Control File is

- Evidence that each gate passed, with the record behind it
- A 90-day exception log where an empty log says so in one line
- One file per system, plus one fleet page for the portfolio

The Control File is not

- An approval, a binder, a premium, or a certification
- Independent proof of the prompt — the customer attests, we compare
- A penetration test — Security means measured behavioral responses

Before the next underwriter conversation — one test.

Hand the underwriter two files for the same system: one clean, one with a seeded exception — a prompt change with no retest, or an item left open past the clock. **Ask them to find it**. If they can, the file does its job.