

## AUDIT-12 — Scope

**Stand:** 2026-05-18

### Forensische Frage-Klassen

Wir testen unsere Reproduzierbarkeit gegen fünf Frage-Klassen, die eine Marktüberwachungsbehörde in 5–10 Jahren stellen könnte:

| ID | Frage-Klasse                  | Beispiel                                                                                       |
|----|-------------------------------|------------------------------------------------------------------------------------------------|
| F1 | Konfigurations-Identifikation | „Mit welchem Doc-Set wurde diese Akte erstellt? Hash?“                                         |
| F2 | Modell-Identifikation         | „Welches KI-Modell mit welcher Version hat Aussage X formuliert?“                              |
| F3 | Lookup-Stand-Identifikation   | „Welche Norm-Klausel-Pool-Version wurde zum Erstellungs-Zeitpunkt verwendet?“                  |
| F4 | Rekonstruktion                | „Erzeuge die Akte mit dem damaligen Stand erneut — ist der Inhalt identisch?“                  |
| F5 | Audit-Trail-Lückenlosigkeit   | „Welche Schreiber/Lektor/Aggregator-Schritte sind durchlaufen worden, in welcher Reihenfolge?“ |

### In-Scope Test-Vektoren

| Vektor                                      | Was wir prüfen                                                         |
|---------------------------------------------|------------------------------------------------------------------------|
| W1 — CM-1 vorhanden in jeder Final-Akte     | Pytest gegen sample Final-Akten                                        |
| W2 — CM-1-Hash deterministisch              | Re-Berechnung über Original-Doc-Set ergibt selben Hash                 |
| W3 — Doc-Set-Snapshot ist hash-stempelbar   | Backup-Restore + Re-Hash → identischer Hash                            |
| W4 — Modell-Provenance pro Schreiber-Output | <code>state.audit.modell_provenance[ ]</code> lückenlos                |
| W5 — Lookup-Versions-Snapshot               | <code>state.audit.lookup_versionen</code> enthält Hash pro Lookup-yaml |
| W6 — Audit-Log append-only                  | keine Mutation in <code>audit_log.jsonl</code>                         |

| Vektor                          | Was wir prüfen                                                            |
|---------------------------------|---------------------------------------------------------------------------|
| W7 — 10-Jahres-Archiv-Hash      | Akten im Archiv mit SHA-256-Stempel + Manifest                            |
| W8 — Live-Rekonstruktions-Übung | echte V.4-Akte aus 2026-05 mit Stand 2031 neu rendern (siehe 03_evidence) |

## Out-of-Scope

| Bereich                                   | Wo geprüft                 |
|-------------------------------------------|----------------------------|
| Pipeline-Reife (Akkuranz pro Archetyp)    | Reifegrad-Seite + AUDIT-04 |
| LLM-Modell-Drift (Cross-Provider-Konsens) | AUDIT-06                   |
| Backup-Verfügbarkeit                      | AUDIT-05                   |

## Bezugsnormen

- EU-MV 2023/1230 Art. 11 + Anhang IV (10-J-Aufbewahrungspflicht, Hersteller)
- ISO 9001:2015 §8.5.2 (Identifikation + Rückverfolgbarkeit)
- ISO/IEC 27001:2022 A.12.4 (Logging + Monitoring)
- DIN EN ISO 19011:2018 (Auditing-Methodik)