AI Claims & Governance Watch: Monitoring Method and Handoff Guide

ILLUSTRATIVE MONITORING METHOD GUIDE | PUBLIC-SOURCE AND SERVICE METHODOLOGY

No completed client matter is represented. This document demonstrates questions, evidence requirements, limitations and possible deliverables. It contains no verified findings about a named buyer or company. A matter, source access, fixed fee and timing require separate written acceptance.

Monitoring decision

What *materially changed* since the last verified source snapshot that could alter: Can vendor AI assertions be traced to evidence that supports the buyer's decision?

Watch subjects: named entities and the agreed records about `model card`, `vendor technical document` and `NIST AI RMF`.

Thresholds to agree

- Major record change: dated filing, order, licence, material ownership/provenance event or published correction; verify with original issuer before alert.
- Identity-related event: name, owner, operator or controlling-entity change confirmed by an applicable register.
- Contradiction: `unreplicable accuracy claim`, `missing evaluation population` or `unsupported security promise` becomes supported by a new original document.
- No material change: explicitly say coverage windows and sources; never imply a universal negative.
- Inaccessible record: note the access failure, source refresh lag, date and whether escalation is warranted.

Report layout

Field; Required manuscript content

Baseline source; Publisher, original record ID, capture date, scope and retention law

New source; URL/document ID, issue/effective/retrieval dates and exact changed fact

Proposed alert; One sentence explaining which client decision might be altered

Contradiction test; Compare at least one independent adverse or old-version record

Confidence and limits; Supported/partial/contradicted/unresolved + known source lag

Reviewer; Human disposition and date

Candidate monitoring sources

Ref; Primary source / comparator; Link; Evidence limitation and status

EU-AI-2026; European Commission AI Act Service Desk: AI Act staged enforcement and application; https://ai-act-service-desk.ec.europa.eu/en/ai-act/faq/when-does-enforcement-start; WEB CHECKED 2026-10-12. The dates differ by obligation; do not treat all AI Act requirements as simultaneously applicable

NIST-AI; U.S. NIST: AI risk management framework; https://www.nist.gov/itl/ai-risk-management-framework; WEB CHECKED 2026-10-12. Voluntary risk management framework; not an AI certification

Commissioning: Watch frequency, event severity, authorised recipients, privacy permissions, source spend, fee, data retention, renewal and termination must be specified in a separate written agreement. No live watch is running because this manuscript exists.

Limits: No AI certification, conformance assessment, penetration testing or blanket accuracy guarantee.

Release controls

- Confirm the appointing client, exact research question, relevant location, decision date, conflicts, privacy, sanctions and licensing.
- Check original source identity, authority, issue date, effective date, retrieval timestamp, version and lawful access.
- Reproduce important calculations and compare at least one plausible contrary explanation.
- Keep allegations, regulatory findings, historical claims and unresolved matches distinct.
- Mark each proposed finding supported, partially supported, contradicted, unresolved or outside mandate; include missing-source requests.
- Confirm that illustrations do not imply a real engagement, completed investigation, certified outcome or affiliation with named comparators.
- Obtain final human sign-off on accuracy, legal boundaries, confidentiality, claims and publication version before release.

Professional boundaries: Independent research support only. No legal, tax, investment, audit, valuation, brokerage, investigation requiring a specific professional licence or regulated opinion is implied. No confidential material should be sent before instructions.