AIGovXRay
-REPORT-

System: `claims-assistant-eu`

Evidence Source: `Uploaded evidence pack`

Report ID: `bundle_ea56bc818a3d8216`

Generated at: `2026-05-19T20:02:08.730888+00:00`

Run ID: `job_20260519T200207Z_f4beea0b54`

> Evidence-Pack Scan: findings are limited to the uploaded logs and records supplied for this run.

> This full-detail report is generated for immediate delivery only.
>
> Uploaded source logs are deleted after analysis, and the hosted service does not retain this full-detail report after download.

Delivery & Continuity Note

- Assessment mode: `single transient assessment`
- Drift readout: `not applicable unless the upload includes prior-scan evidence`
- Source evidence handling: raw uploaded logs are deleted after analysis and are not retained by AIGovXRay.
- Continuity expectation: if future reference or drift analysis is required, retain this report and any prior-scan evidence in your own records because a later upload must carry that material explicitly.

Scan Context

This report was generated for system `claims-assistant-eu` from a `Uploaded Logs Scan`.

System Snapshot

- System identifier: `claims-assistant-eu`
- Scan type: `Uploaded Logs Scan`
- Evidence Source: `Uploaded evidence pack`
- Findings emitted: `10`
- Highest observed severity: `high`
- Observed evidence domains: `Human Oversight`, `Supplier Assurance`, `Post-Market Monitoring`, `Technical Documentation`

Pilot Readout

This page is designed to answer the first pilot question quickly: do we have a usable, evidence-based view of this AI system?

- **Current risk signal:** `high`
- **Most affected domain:** `Human Oversight`
- **Framework projection mode:** `multi_framework_overlay`
- **Forensic depth available:** `0` candidate chain(s)

A good pilot outcome is not 'perfect compliance'. It is a clearer answer to what can be proven now, where evidence is weak, and what to review next.

Executive Summary

Executive Risk Snapshot

Overall Risk Level: `high`

Audit Readiness: `Not demonstrable`

Control Demonstrability: Key governance controls cannot be demonstrated across oversight, supplier assurance, monitoring, and runtime traceability.

Why this level was assigned: Overall risk is `high` because the run produced 10 finding(s) (4 high, 6 medium), with highest reported severity `high` under `low` evidence fragility.

Primary Concern: 10 finding(s) require review (4 high, 6 medium), with highest reported severity `high` under `low` evidence fragility.

Business Impact:

- The current findings indicate governance review work, but the available evidence still limits scope certainty.

Recommendation Priority: Immediate review recommended

What We Observed

- Oversight record is incomplete for flow-3 (missing: required_role).
- Supplier registry record is incomplete for sup-02 (missing: security_contact).
- Post-market monitoring record is incomplete for pm-101 (missing: verification_status).

Why It Matters

- Responsibility cannot be attributed, weakening audit defensibility.
- Supplier dependency scope, assurance, or accountability cannot be defended in audit review.
- Ongoing performance or remediation assurance lacks demonstrable verification evidence.
- The available evidence does not support a defensible control demonstration.
- Control scope remains ambiguous, weakening review of affected systems and actors.

What We Could Not Prove

- Accountable human oversight cannot be demonstrated.
- Third-party governance cannot be evidenced.
- Monitoring and corrective-action verification cannot be proven.
- The governed system boundary cannot be demonstrated.
- Runtime correlation cannot be proven.

Evidence Strength

- Highest reported severity: `high`
- Max evidence tier: `Direct structured evidence`
- Overall fragility: `low`
- Confidence is strongest where direct runtime or captured-page evidence was available.

Regulatory Signal Mapping

Signal-oriented crosswalk only. This report is not a compliance certification or legal attestation. _This section reflects the evidence-first core findings projected across the available governance frameworks for this report._

Finding Category	Regulation / Lens	Signal
Accuracy Robustness Evidence Gap	Governance baseline	Control evidence signal
Boundary Bypass Or Undefined Boundary	Governance baseline	Control evidence signal
Documentation Linkage Gap	Governance baseline	Control evidence signal
Human Oversight Gap	EU AI Act	Human review control signal
Post Market Monitoring Gap	Governance baseline	Control evidence signal
Runtime Correlation Gap	Governance baseline	Control evidence signal
Supplier Assurance Gap	Governance baseline	Control evidence signal
operational_accountability_gap	DORA	Ambiguous ownership, actor attribution, oversight, or delegation evidence may weaken proof of accountable ICT governance and operational control under DORA (observed severity: medium).
operational_accountability_gap	DORA	Ambiguous ownership, actor attribution, oversight, or delegation evidence may weaken proof of accountable ICT governance and operational control under DORA (observed severity: high).
ict_control_documentation_gap	DORA	Incomplete documentation or recordkeeping evidence may weaken proof that ICT controls, procedures, and risk decisions are documented and reviewable under DORA (observed severity: medium).

NIST AI RMF Posture

Projection method: deterministic rule-based mapping from evidence-derived findings into NIST AI RMF functions. Absence of a signal means the function was not evidenced in this run, not that it is satisfied.

Function	Status	Notes
GOVERN	Partial	Evidence projected to transparent policies, procedures, controls, and evidence linkage, human-ai configuration, oversight, and escalation clarity.
MAP	Not evidenced	System context, intended use, and boundary evidence were not evidenced in this run.
MEASURE	Not evidenced	Monitoring, evaluation, or telemetry evidence was not evidenced in this run.
MANAGE	Partial	Evidence projected to operational guardrails, override, and safe disengagement, post-deployment monitoring, appeals, recovery, and change management.

Recommended Actions

Immediate Actions

- For `fx_2db1fc043891` (Human Oversight Gap), Document the human review checkpoint that must occur before the workflow can proceed or be released.
- For `fx_421e028a51f3` (Supplier Assurance Gap), Review the finding with the responsible owner and confirm the missing control evidence for this run.
- For `fx_6f76bf191692` (Post Market Monitoring Gap), Review the finding with the responsible owner and confirm the missing control evidence for this run.

NIST Function Actions

- Improve GOVERN by assigning named roles, approval checkpoints, and communication paths for AI-assisted actions.
- Improve MAP by documenting system purpose, intended use, boundaries, dependencies, and affected actors for the scanned system.
- Improve MEASURE by adding telemetry, monitoring criteria, and evaluation evidence for observed AI behavior and control effectiveness.
- Improve MANAGE by defining mitigation, override, incident response, and recovery workflows tied to observed AI-related risks.

Finding-Specific Follow-up

- For `fx_2db1fc043891`, collect or validate: Reviewer identity, approval timestamp, or escalation record showing human oversight.
- For `fx_2db1fc043891`, assign follow-up to the risk, compliance, or control owner.
- For `fx_421e028a51f3`, collect or validate: The missing governance evidence needed to validate or close this finding.
- For `fx_421e028a51f3`, assign follow-up to the system owner.
- For `fx_6f76bf191692`, collect or validate: The missing governance evidence needed to validate or close this finding.
- For `fx_6f76bf191692`, assign follow-up to the system owner.

Evidence Posture

- Max evidence tier: `Direct structured evidence`
- Overall fragility: `low`

Coverage By Evidence Domain

Evidence Domain	Normalized Events	Findings
Human Oversight	4	4
Post-Market Monitoring	4	2
Supplier Assurance	4	2
Technical Documentation	3	2

Top Gaps By Domain

- **Human Oversight**: 4 finding(s), highest severity `high`.
- Example gap: Oversight record is incomplete for flow-3 (missing: required_role).
- **Post-Market Monitoring**: 2 finding(s), highest severity `high`.
- Example gap: Post-market monitoring record is incomplete for pm-101 (missing: verification_status).
- **Supplier Assurance**: 2 finding(s), highest severity `high`.
- Example gap: Supplier registry record is incomplete for sup-02 (missing: security_contact).
- **Technical Documentation**: 2 finding(s), highest severity `medium`.
- Example gap: Technical documentation cannot be correlated to a model or runtime version for doc-sales-02.

Governance Sections

Human Oversight

- Oversight record is incomplete for flow-3 (missing: required_role).
- Human oversight boundary is undefined or incomplete for flow-2.
- Human oversight boundary is undefined or incomplete for flow-3.
- ... and 1 more finding(s) in this domain.

Post-Market Monitoring

- Post-market monitoring record is incomplete for pm-101 (missing: verification_status).
- Accuracy or robustness monitoring evidence is incomplete for pm-101.

Supplier Assurance

- Supplier registry record is incomplete for sup-02 (missing: security_contact).
- Supplier registry record is incomplete for sup-03 (missing: dependency_type, assurance_type).

Technical Documentation

- Technical documentation cannot be correlated to a model or runtime version for doc-sales-02.
- Technical documentation record is incomplete for doc-sales-02 (missing: linked_model_version).

Lens Signals

The following signals are derived from the `multi_framework_overlay` framework projection layer over the same evidence set. They do not imply compliance or non-compliance.

- **DORA | Governance and organisation | Accountable governance, authority, escalation, and ownership | operational_accountability_gap**
- Ambiguous ownership, actor attribution, oversight, or delegation evidence may weaken proof of accountable ICT governance and operational control under DORA (observed severity: medium).
- Target: Governance and Accountability (Management Accountability and Operational Control)
- Audit objective: Show that ICT operational decisions, delegations, escalations, and corrective actions are attributable to accountable owners.
- Triggered by findings: `fx_2db1fc043891`, `fx_f5d8e942da00`
- **DORA | ICT risk management | Documented ICT controls, procedures, and audit records | ict_control_documentation_gap**
- Incomplete documentation or recordkeeping evidence may weaken proof that ICT controls, procedures, and risk decisions are documented and reviewable under DORA (observed severity: medium).
- Target: ICT Risk Management (ICT Risk Management Framework)
- Audit objective: Retain reviewable documentation and records for ICT controls, operating limits, and risk decisions.
- Triggered by findings: `fx_f58c91dc3692`
- **DORA | ICT third-party risk management | Supplier assurance, contractual visibility, and dependency register completeness | ict_third_party_assurance_gap**
- Incomplete supplier, dependency, or disclosure-path evidence may weaken proof of ICT third-party risk management and register-of-information completeness under DORA (observed severity: medium).
- Target: ICT Third-party Risk (ICT Third-party Risk and Register of Information)
- Audit objective: Demonstrate that ICT third-party services, important dependencies, and disclosure paths are identified and governed.
- Triggered by findings: `fx_421e028a51f3`, `fx_ad65b3ad8947`
- **DORA | Digital operational resilience testing | Traceable testing, recovery, rollback, and remediation closure | resilience_testing_and_recovery_gap**

- Evidence gaps in rollback, runtime correlation, audit-chain continuity, or timeline reconstruction may weaken proof of digital operational resilience testing and recovery readiness under DORA (observed severity: medium).
- Target: Resilience Testing (Digital Operational Resilience Testing and Recovery Evidence)
- Audit objective: Demonstrate that resilience tests, recovery paths, corrective actions, and operational timelines are traceable.
- Triggered by findings: `fx_f304733a3cc0`
- **EU AI Act | Article 11 | Technical documentation completeness | documentation_gap**
- Technical documentation linkage evidence is incomplete (observed severity: medium).
- Target: Article 11 (Technical Documentation)
- Audit objective: Maintain technical documentation sufficient to explain design, purpose, and limits.
- Triggered by findings: `fx_f58c91dc3692`
- **EU AI Act | Article 14 | Human oversight and execution boundary clarity | oversight_ambiguity**
- Undefined execution boundary may impact demonstrable human oversight.
- Target: Article 14 (Human Oversight)
- Audit objective: Show that human oversight responsibilities and intervention boundaries are defined.
- Triggered by findings: `fx_cf5bde216604`, `fx_def8c2191601`
- **EU AI Act | Article 14 | Human oversight and fallback controls | oversight_gap**
- Human oversight or fallback evidence is incomplete (observed severity: medium).
- Target: Article 14 (Human Oversight)
- Audit objective: Demonstrate that appropriate human review, escalation, or fallback exists where required.
- Triggered by findings: `fx_2db1fc043891`, `fx_f5d8e942da00`
- **EU AI Act | Article 72 | Post-market monitoring and corrective action | post_market_gap**
- Post-market monitoring or corrective-action evidence is incomplete (observed severity: high).
- Target: Article 72 (Post-Market Monitoring)
- Audit objective: Demonstrate ongoing monitoring, issue detection, and corrective follow-up after deployment.
- Triggered by findings: `fx_6f76bf191692`
- **ISO/IEC 42001 | Clause 10.1 | Corrective action and post-deployment improvement | continual_improvement_gap**
- Incomplete post-deployment monitoring evidence may weaken proof that AI issues trigger corrective action and continual improvement within the AIMS (observed severity: high).
- Target: Clause 10.1 (Improvement)
- Audit objective: Ensure AI issues trigger corrective action and continual improvement.
- Triggered by findings: `fx_6f76bf191692`
- **ISO/IEC 42001 | Clause 5.3 | Roles, responsibilities, and human review paths | oversight_accountability_gap**
- Incomplete human oversight evidence may weaken proof of assigned roles, responsibilities, and escalation paths for AI decisions (observed severity: medium).
- Target: Clause 5.3 (Roles and responsibilities)
- Audit objective: Assign and demonstrate accountable roles, responsibilities, and human oversight.
- Triggered by findings: `fx_2db1fc043891`, `fx_f5d8e942da00`
- **ISO/IEC 42001 | Clause 7.5 | Documented information and technical documentation linkage | documented_information_gap**
- Incomplete technical documentation linkage may weaken required documented information for trustworthy AI governance and review (observed severity: medium).
- Target: Clause 7.5 (Documented information)
- Audit objective: Maintain reliable documented information for AI governance and auditability.
- Triggered by findings: `fx_f58c91dc3692`

- **ISO/IEC 42001 | Clause 8.1 | Operational control over external providers and dependencies | supplier_control_gap**
- Incomplete supplier assurance evidence may weaken operational control over external AI dependencies and services used within the AIMS (observed severity: medium).
- Target: Clause 8.1 (Operational planning and control)
- Audit objective: Control outsourced or dependent AI services within operational governance.
- Triggered by findings: `fx_421e028a51f3`, `fx_ad65b3ad8947`
- **NIS2 | Governance Accountability | Management accountability and escalation | oversight_accountability_gap**
- Incomplete oversight evidence may weaken accountability for high-impact review and escalation paths (observed severity: medium).
- Target: Governance Accountability (Governance Accountability and Escalation)
- Audit objective: Demonstrate accountable review and escalation paths for high-impact decisions.
- Triggered by findings: `fx_2db1fc043891`, `fx_f5d8e942da00`
- **NIS2 | Supply Chain Security | Supply chain dependency oversight | supplier_assurance_gap**
- Incomplete supplier evidence may limit defensibility of supply-chain security posture and dependency oversight (observed severity: medium).
- Target: Supply Chain Security (Supply Chain Security)
- Audit objective: Demonstrate that suppliers and dependencies are governed through current assurance mechanisms.
- Triggered by findings: `fx_421e028a51f3`, `fx_ad65b3ad8947`
- **NIST AI RMF | GOVERN 1.4 | Transparent policies, procedures, controls, and evidence linkage | documentation_traceability_gap**
- Incomplete documentation linkage may weaken proof that AI risk management controls and outcomes are transparent, reviewable, and traceable under NIST AI RMF GOVERN 1.4 (observed severity: medium).
- Target: GOVERN 1.4 (Transparent risk management process)
- Criterion: Transparent and documented governance controls
- Audit objective: Establish transparent risk management processes and outcomes through policies, procedures, and documented controls.
- Triggered by findings: `fx_f58c91dc3692`
- **NIST AI RMF | GOVERN 3.2 | Human-AI configuration, oversight, and escalation clarity | human_ai_oversight_gap**
- Incomplete human oversight evidence may weaken proof that human-AI roles, review responsibilities, and escalation paths are defined under NIST AI RMF GOVERN 3.2 and related roadmap guidance on human-AI teaming (observed severity: medium).
- Target: GOVERN 3.2 (Human-AI roles and oversight)
- Criterion: Human oversight and human-AI teaming
- Audit objective: Define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems.
- Triggered by findings: `fx_2db1fc043891`, `fx_f5d8e942da00`
- **NIST AI RMF | GOVERN 6.1 | Third-party software, data, and model dependency governance | third_party_ai_risk_gap**
- Incomplete supplier assurance evidence may weaken proof that third-party AI services, data, or model dependencies are governed under NIST AI RMF GOVERN 6.1 and AI RMF profile guidance on value-chain integration (observed severity: medium).
- Target: GOVERN 6.1 (Third-party AI risk policies)
- Criterion: Third-party and value-chain governance
- Audit objective: Address AI risks associated with third-party entities, software, data, and other supply chain issues.
- Triggered by findings: `fx_421e028a51f3`, `fx_ad65b3ad8947`
- **NIST AI RMF | MANAGE 2.4 | Operational guardrails, override, and safe disengagement | boundary_control_gap**
- Undefined or bypassed execution boundaries may weaken proof that the organization can override, disengage, or safely constrain AI behavior under NIST AI RMF MANAGE 2.4 (observed severity: medium).
- Target: MANAGE 2.4 (Supersede, disengage, or deactivate unsafe behavior)
- Criterion: Safe fallback and intervention capability

- Audit objective: Ensure mechanisms and responsibilities exist to supersede, disengage, or deactivate AI systems that operate inconsistently with intended use.
- Triggered by findings: `fx_cf5bde216604`, `fx_def8c2191601`
- **NIST AI RMF | MANAGE 4.1 | Post-deployment monitoring, appeals, recovery, and change management | post_deployment_monitoring_gap**
- Incomplete post-deployment monitoring evidence may weaken proof that deployed AI systems are continuously monitored and managed through change, incident, and recovery processes under NIST AI RMF MANAGE 4.1 (observed severity: high).
- Target: MANAGE 4.1 (Post-deployment monitoring and change management)
- Criterion: Continuous monitoring and incident response
- Audit objective: Implement post-deployment monitoring plans, incident response, override, recovery, and change management mechanisms.
- Triggered by findings: `fx_6f76bf191692`
- **SOC 2 Type II | Security / Vendor Governance | Third-party control oversight | third_party_assurance_gap**
- Incomplete supplier assurance evidence may weaken demonstrability of third-party control oversight for SOC 2 Type II review periods (observed severity: medium).
- Target: CC9 (Vendor and Supply Chain Governance)
- Criterion: CC9
- Audit objective: Demonstrate that vendor dependencies are governed with current assurance evidence.
- Triggered by findings: `fx_421e028a51f3`, `fx_ad65b3ad8947`
- **SOC 2 Type II | Processing Integrity / Documentation | Documented system behavior and operating limits | documentation_control_gap**
- Incomplete technical documentation evidence may weaken proof that system behavior and operating limits were documented for review periods (observed severity: medium).
- Target: PI1 / CC2 (Documentation and Control Communication)
- Criterion: PI1 / CC2
- Audit objective: Demonstrate that system behavior, boundaries, and control expectations are documented.
- Triggered by findings: `fx_f58c91dc3692`

Technical Appendix

Technical Findings

Accuracy Robustness Evidence Gap (1)

- **fx_a55c895e799f**
- Audit readiness: Not demonstrable
- Severity: high
- Summary: Accuracy or robustness monitoring evidence is incomplete for pm-101.
- Audit statement: Monitoring and corrective-action verification cannot be proven.
- Impact: The available evidence does not support a defensible control demonstration.
- Action: Attach the missing control evidence identified for this finding.
- Confidence: high | 0.89 | direct
- Confidence notes: Directly observed in supplied governance evidence.
- Evidence posture: tier=Direct structured evidence | fragility=low
- Time resolution: unresolved
- Actor resolution: unresolved

- Evidence refs: Post-Market Monitoring:normalized_events.json#13

Boundary Bypass Or Undefined Boundary (2)

- **fx_cf5bde216604**
- Audit readiness: Partially demonstrable
- Severity: medium
- Summary: Human oversight boundary is undefined or incomplete for flow-2.
- Audit statement: The governed system boundary cannot be demonstrated.
- Impact: Control scope remains ambiguous, weakening review of affected systems and actors.
- Action: Define the system boundary and attach evidence that ties controls to that boundary.
- Confidence: high | 0.89 | direct
- Confidence notes: Directly observed in supplied governance evidence.
- Evidence posture: tier=Direct structured evidence | fragility=low
- Time resolution: unresolved
- Actor resolution: unresolved
- Evidence refs: Human Oversight:normalized_events.json#5
- **fx_def8c2191601**
- Audit readiness: Partially demonstrable
- Severity: medium
- Summary: Human oversight boundary is undefined or incomplete for flow-3.
- Audit statement: The governed system boundary cannot be demonstrated.
- Impact: Control scope remains ambiguous, weakening review of affected systems and actors.
- Action: Define the system boundary and attach evidence that ties controls to that boundary.
- Confidence: high | 0.89 | direct
- Confidence notes: Directly observed in supplied governance evidence.
- Evidence posture: tier=Direct structured evidence | fragility=low
- Time resolution: unresolved
- Actor resolution: unresolved
- Evidence refs: Human Oversight:normalized_events.json#6

Documentation Linkage Gap (1)

- **fx_f58c91dc3692**
- Audit readiness: Partially demonstrable
- Severity: medium
- Summary: Technical documentation record is incomplete for doc-sales-02 (missing: linked_model_version).
- Audit statement: Runtime applicability of documentation cannot be verified.
- Impact: The documentation may not be attributable to the system or version being reviewed.
- Action: Link documentation to the specific system, model, runtime, or release version.
- Confidence: high | 0.90 | direct
- Confidence notes: Directly observed in supplied technical documentation evidence.
- Evidence posture: tier=Direct structured evidence | fragility=low
- Time resolution: unresolved
- Actor resolution: unresolved
- Evidence refs: Technical Documentation:normalized_events.json#2

Human Oversight Gap (2)

- **fx_2db1fc043891**
- Audit readiness: Partially demonstrable
- Severity: medium
- Summary: Oversight record is incomplete for flow-3 (missing: required_role).
- Audit statement: Accountable human oversight cannot be demonstrated.
- Impact: Responsibility cannot be attributed, weakening audit defensibility.
- Action: Define and assign the reviewer role and approval checkpoint for this workflow.
- Confidence: high | 0.90 | direct
- Confidence notes: Directly observed in supplied oversight evidence.
- Evidence posture: tier=Direct structured evidence | fragility=low
- Time resolution: unresolved
- Actor resolution: resolved
- Evidence refs: Human Oversight:normalized_events.json#6
- **fx_f5d8e942da00**
- Audit readiness: Not demonstrable
- Severity: high
- Summary: Oversight record is incomplete for flow-2 (missing: approved_by, fallback_trigger).
- Audit statement: Accountable human oversight cannot be demonstrated.
- Impact: Responsibility cannot be attributed, weakening audit defensibility.
- Action: Define and assign the reviewer role and approval checkpoint for this workflow.
- Confidence: high | 0.90 | direct
- Confidence notes: Directly observed in supplied oversight evidence.
- Evidence posture: tier=Direct structured evidence | fragility=low
- Time resolution: unresolved
- Actor resolution: unresolved
- Evidence refs: Human Oversight:normalized_events.json#5

Post Market Monitoring Gap (1)

- **fx_6f76bf191692**
- Audit readiness: Not demonstrable
- Severity: high
- Summary: Post-market monitoring record is incomplete for pm-101 (missing: verification_status).
- Audit statement: Monitoring and corrective-action verification cannot be proven.
- Impact: Ongoing performance or remediation assurance lacks demonstrable verification evidence.
- Action: Attach monitoring event, metric, corrective action, and verification-status evidence.
- Confidence: high | 0.90 | direct
- Confidence notes: Directly observed in supplied post-market monitoring evidence.
- Evidence posture: tier=Direct structured evidence | fragility=low
- Time resolution: unresolved
- Actor resolution: unresolved
- Evidence refs: Post-Market Monitoring:normalized_events.json#13

Runtime Correlation Gap (1)

- **fx_f304733a3cc0**
- Audit readiness: Partially demonstrable
- Severity: medium
- Summary: Technical documentation cannot be correlated to a model or runtime version for doc-sales-02.
- Audit statement: Runtime correlation cannot be proven.
- Impact: Governance evidence cannot be tied to a concrete runtime or system boundary.
- Action: Link governance records to system identifiers, runtime versions, or operational telemetry.
- Confidence: high | 0.89 | direct
- Confidence notes: Directly observed in supplied governance evidence.
- Evidence posture: tier=Direct structured evidence | fragility=low
- Time resolution: unresolved
- Actor resolution: unresolved
- Evidence refs: Technical Documentation:normalized_events.json#2

Supplier Assurance Gap (2)

- **fx_421e028a51f3**
- Audit readiness: Partially demonstrable
- Severity: medium
- Summary: Supplier registry record is incomplete for sup-02 (missing: security_contact).
- Audit statement: Third-party governance cannot be evidenced.
- Impact: Supplier dependency scope, assurance, or accountability cannot be defended in audit review.
- Action: Complete supplier registry evidence with owner, dependency scope, assurance type, and recency.
- Confidence: high | 0.90 | direct
- Confidence notes: Directly observed in supplied supplier registry evidence.
- Evidence posture: tier=Direct structured evidence | fragility=low
- Time resolution: partially_resolved
- Actor resolution: unresolved
- Evidence refs: Supplier Assurance:normalized_events.json#9
- **fx_ad65b3ad8947**
- Audit readiness: Not demonstrable
- Severity: high
- Summary: Supplier registry record is incomplete for sup-03 (missing: dependency_type, assurance_type).
- Audit statement: Third-party governance cannot be evidenced.
- Impact: Supplier dependency scope, assurance, or accountability cannot be defended in audit review.
- Action: Complete supplier registry evidence with owner, dependency scope, assurance type, and recency.
- Confidence: high | 0.90 | direct
- Confidence notes: Directly observed in supplied supplier registry evidence.
- Evidence posture: tier=Direct structured evidence | fragility=low
- Time resolution: partially_resolved
- Actor resolution: unresolved
- Evidence refs: Supplier Assurance:normalized_events.json#10

Evidence Traceability

This section maps report conclusions back to the exact uploaded evidence locations that contributed to them where structured line or record references are available.

Oversight record is incomplete for flow-3 (missing: required_role).

- Why this evidence matters: The evidence does not show a clear human review or intervention checkpoint for the observed workflow.
- Evidence location: `oversight//app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/oversight/approval_flows.json:record 3` via `normalized_events.json#6`
- Observed signal: Evidence from `oversight` contributed to this conclusion.
- Event type: `oversight_record`
- Supporting evidence summary: A supporting source excerpt indicated: "EventPayload(data={'file': '/app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/oversight/approval_flows.json', 'index': 2, 'flow_id': 'flow-3',...".
- Raw reference: `normalized_events.json#6`

Supplier registry record is incomplete for sup-02 (missing: security_contact).

- Why this evidence matters: The available evidence points to a governance control gap that still requires operator review.
- Evidence location: `suppliers//app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/suppliers/supplier_registry.json:record 2` via `normalized_events.json#9`
- Observed signal: Evidence from `suppliers` contributed to this conclusion.
- Event type: `supplier_registry_record`
- Observed at: `2024-09-02`
- Supporting evidence summary: A supporting source excerpt indicated: "EventPayload(data={'file': '/app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/suppliers/supplier_registry.json', 'index': 1, 'supplier_id': 's...".
- Raw reference: `normalized_events.json#9`

Post-market monitoring record is incomplete for pm-101 (missing: verification_status).

- Why this evidence matters: The available evidence points to a governance control gap that still requires operator review.
- Evidence location: `post_market//app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/post_market/monitoring_events.json:record 2` via `normalized_events.json#13`
- Observed signal: Evidence from `post_market` contributed to this conclusion.
- Event type: `post_market_record`
- Supporting evidence summary: A supporting source excerpt indicated: "EventPayload(data={'file': '/app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/post_market/monitoring_events.json', 'index': 1, 'monitoring_eve...".
- Raw reference: `normalized_events.json#13`

Accuracy or robustness monitoring evidence is incomplete for pm-101.

- Why this evidence matters: The available evidence points to a governance control gap that still requires operator review.
- Evidence location: `post_market//app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/post_market/monitoring_events.json:record 2` via `normalized_events.json#13`
- Observed signal: Evidence from `post_market` contributed to this conclusion.
- Event type: `post_market_record`

- Supporting evidence summary: A supporting source excerpt indicated: "EventPayload(data={'file': '/app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/post_market/monitoring_events.json', 'index': 1, 'monitoring_eve...".
- Raw reference: `normalized_events.json#13`

Supplier registry record is incomplete for sup-03 (missing: dependency_type, assurance_type).

- Why this evidence matters: The available evidence points to a governance control gap that still requires operator review.
- Evidence location: `suppliers//app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/suppliers/supplier_registry.json:record 3` via `normalized_events.json#10`
- Observed signal: Evidence from `suppliers` contributed to this conclusion.
- Event type: `supplier_registry_record`
- Observed at: `unknown`
- Supporting evidence summary: A supporting source excerpt indicated: "EventPayload(data={'file': '/app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/suppliers/supplier_registry.json', 'index': 2, 'supplier_id': 's...".
- Raw reference: `normalized_events.json#10`

Human oversight boundary is undefined or incomplete for flow-2.

- Why this evidence matters: The available evidence points to a governance control gap that still requires operator review.
- Evidence location: `oversight//app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/oversight/approval_flows.json:record 2` via `normalized_events.json#5`
- Observed signal: Evidence from `oversight` contributed to this conclusion.
- Event type: `oversight_record`
- Supporting evidence summary: A supporting source excerpt indicated: "EventPayload(data={'file': '/app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/oversight/approval_flows.json', 'index': 1, 'flow_id': 'flow-2',...".
- Raw reference: `normalized_events.json#5`

Human oversight boundary is undefined or incomplete for flow-3.

- Why this evidence matters: The available evidence points to a governance control gap that still requires operator review.
- Evidence location: `oversight//app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/oversight/approval_flows.json:record 3` via `normalized_events.json#6`
- Observed signal: Evidence from `oversight` contributed to this conclusion.
- Event type: `oversight_record`
- Supporting evidence summary: A supporting source excerpt indicated: "EventPayload(data={'file': '/app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/oversight/approval_flows.json', 'index': 2, 'flow_id': 'flow-3',...".
- Raw reference: `normalized_events.json#6`

Technical documentation cannot be correlated to a model or runtime version for doc-sales-02.

- Why this evidence matters: The available evidence points to a governance control gap that still requires operator review.
- Evidence location: `tech_docs//app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/tech_docs/system_cards.json:record 2` via `normalized_events.json#2`
- Observed signal: Evidence from `tech_docs` contributed to this conclusion.
- Event type: `tech_docs_record`
- Supporting evidence summary: A supporting source excerpt indicated: "EventPayload(data={'file': '/app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/tech_docs/system_cards.json', 'index': 1, 'doc_id': 'doc-sales-0...".

- Raw reference: `normalized_events.json#2`

Technical documentation record is incomplete for doc-sales-02 (missing: linked_model_version).

- Why this evidence matters: The available evidence points to a governance control gap that still requires operator review.
- Evidence location: `tech_docs//app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/tech_docs/system_cards.json:record 2` via `normalized_events.json#2`
- Observed signal: Evidence from `tech_docs` contributed to this conclusion.
- Event type: `tech_docs_record`
- Supporting evidence summary: A supporting source excerpt indicated: "EventPayload(data={'file': '/app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/tech_docs/system_cards.json', 'index': 1, 'doc_id': 'doc-sales-0...".
- Raw reference: `normalized_events.json#2`

Oversight record is incomplete for flow-2 (missing: approved_by, fallback_trigger).

- Why this evidence matters: The evidence does not show a clear human review or intervention checkpoint for the observed workflow.
- Evidence location: `oversight//app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/oversight/approval_flows.json:record 2` via `normalized_events.json#5`
- Observed signal: Evidence from `oversight` contributed to this conclusion.
- Event type: `oversight_record`
- Supporting evidence summary: A supporting source excerpt indicated: "EventPayload(data={'file': '/app/data/outputs/_queued_inputs/job_20260519T200207Z_f4beea0b54/oversight/approval_flows.json', 'index': 1, 'flow_id': 'flow-2',...".
- Raw reference: `normalized_events.json#5`

Continuity Capsule

Scan this page and upload it with new logs, or upload the original report PDF, to detect possible system drift.

The encoded block below is machine-readable continuity data. It is intentionally not human-readable.

```
AIGOVXRAY_STATE_CAPSULE_V1_BEGIN
eyJhYWQiOnsic3lzdGVtX2lkIjoic3lzdGVtX2NsYWltc19hc3Npc3RhbnRfZXVfMDBlMWU5
NDgiLCJ1c2VyX2lkIjoidXNlcl9qdmFuZG91bF81Njg3YmM2ZiJ9LCJjYXBzdWxlX3ZlcnNp
b24iOiIxIiwiY2lwaGVydGV4dCI6InBHMG01RWE1dGRnckplbkl4SElGWG9reXd5TXB0YWdS
Y0o0SlFuUlVybXZ0TkFCSnl1YzkteWZoTkNTZlllQ1N2dHRMYTZpUjlSSkhrZ0d5SjRIZWFG
RXBCUmZPV21QMHRSbjF2YlRSdWJjaEQwUVRaY1I5OVFfRld5aTI3ejlyRTNfQXNnQTRFOXZY
RFdNT2F2VjRuZXJiNzdYZFhGTkloMEVZeWZYUkZYLXFtNl9BbE1qbVRDVVdvRTFWYjZUYVN3
WHY4NzUtOV84V0hHTnZCdWVaeVBxelRWNXZOR01GTHd1eXUwd0l3bWZRdGN0Q0dxT3VCekdi
LU5RQ05jNGp4djRxRG11UDRYR2JfaUtvUGJPQm9EU1FPbHJ3ZFBiaXVSUlNqamxONVphWDMz
OF9NOS1XcHE2S2J5VWlBSG5zT1ZaUlJhYkpWWnlFdzNrQlZtQzNyeEMxb3NJOENHVWd4VnhO
c0RqYl9tdldDSjNaTVRqRWltUFdsUXg4VktWckpqZUktWGoyNUNnc2VZLUdmTE9GZmNId2F5
OElqWGxVTWdoNlZ6Z3Z6WVU5QXZlU1k1WE85TDl5ZVhtY0MyRWwxcGpTMWlRcXZLY2NUS2lf
UG44NTdlNTZVaDlzUUhwMTVNOTNBMWFCLTZJUWt3bUZZOGRyRXdta0JScHFVUFM1YWV3MmR1
eWFJQndPbTExLWtPS1dwOVU3b3hxQnluTUR0TTVKeXZFQVVjLXVWNnZrNmNxTXFtSDFhQXY0
c2NoUDYyQnM0ZWkydWtfTHVPT1MxbUJsTndBNUpGSHFCVm5xU1VveGo1ekV4Y3M0WXhQV0Nn
dVdjc1BxV1dKTERMVWJpM2VtTTExTzlVTV9RN0o0QXBETEtramwwNUFIZFh1SkdTaUhsc3l1
Ui11VldwaW9Dc1k1SV81aDdNRjJBdkZqWVBXTkpyZ0ZOZGFReFpSX19tQ0pURmpBNDFaUjFQ
bk9VamRTVHVpYktLVVRSRmQ0U1cycElEMXg5UTk4aHdZQks1ZTFhdTlHZ3RpdnBvTFpWc05l
QUZDUFBSeUplOVQ0bVhQc1JSdWsxQjZmSzNaT0VURXloT2wzbmZaMDJLd21iYzE5YjdTOFhk
UTVMTWZWbWRKS2IteWVaWDhGSVlKRFJWTUpMOEExNGFoNjVxWTNFUnFHVW5Iem4tM0ZXWE1I
eFA5dXM1LXI4TTBsdWlxODEyZHBnajdHcmZJY3hSWDlTbUwwUGpXRmhaZE9BR3AycGZxTmNn
SmozelprN3pSTU1jN01ZU3AwSTJTbnV1SHBUazlfYnMwdm1ZR19WMTRXeXNHRmJqUU9QTDJ5
WHR6MDJOLVhHOXZjekpxSzFjWTNiNjlTaGlobFV1NElXNGRiUWhEOHFYc281SDRrcWdvbU5O
NFdMLVFDNm9OMGZhZWtZTjVRamRnMUxIbHRXNlhjc1d5YjRzcXk0TUVOa3ZmZ0pOUklLT2VY
WDVZQUhySW9DY1c2Zm1XSjN5aU5qNThwX0EyQ3VJVHhYQUlTMXFTc3dsN0JhWm1aUHZQaFkx
Q2pjR1dFcTdSLVYwaHpZVk13YkU2cnVSWFlxdDR4UUZ0b0pkNmFNVlJ4aFQwRmx0eWY3R3A1
SVZTZ2pnN3ZqUktuT25tcTBSQnFtU1M3Z215OGt0cFVWRElzUUtGaW52Wm5Pd0FmWDJQZkFw
TXFfYWJRRWN4S0ZVcS1oRTM3QUJUSnppbVBuRU5nNXR0VHc2UHg5UDJiQ0p4NGVhc0FLWVJJ
eVdRTWZRdXhVYVFoTlZaZFlhZDdWSUdBeEhQTG1RZklnRkNYcnVEZFJJS0lUd2twbUlGcmdO
Yl9ZNGhHY2NwSGNfRXpuN0N6aHVfVmxDZFBJbTNpRDdkVDFnT3RlRFFwUzk0ZnJCVHliVER3
dmtqTm9TR1lEclJBOWNUV2l2ZE44R1JRSDNzTzlUNWVmR3lLTEVzNGc4WGFpVlBzblJZbzdi
bndyMWVYMHQ5MDRiN1hVeTR2TU9xZTI1akthXzdDWVdVejAyTDhBWGlGeURHZUJFX1dHTVFE
bElvcU9kYUFZcW5WX0hNbFg4X2FobWxKX0lmenFsNjNyRTM5QmJJbDN3S0N3SUdmSVJRNWZi
M2NJcm0yTVdXUW1hWUwyS0VPSXg3VUs5Ry1EdWUzOGtrT1l4c3JuNnN3ZmFTUmhWbXk0TlFW
MVFOdFhmMlNCYVRub1U1Q0pZbWdOZkdIQmJBTlBTVkRqeGhLUzZqbXNvbElGZnJZbFlTbTFz
VHpVU1R5bW1iR29PbGg5Mk1jd184NjVYbTIxRFZNZnJtYUJvdEZ2VHc1QlQzb05ES2Z3eWVq
SGxCdC1TQ1d6VnBJMmdGViIsIm5vbmNlIjoiNnJUemM2MEI2Q2NzaW9PRyIsInRhZyI6IlZ3
UHA4ZldyYnpqb1NxQVA3WGJtYmcifQ
AIGOVXRAY_STATE_CAPSULE_V1_END
```