INFOSECURED.AI EVIDENCE LIBRARY

AML AI Assurance Evidence Pack

Methodology and Source Notes

OWNER-AUTHORIZED PUBLIC RESEARCH PROTOTYPE

A structured Excel research prototype for organizing AML AI system context, alert-review and escalation documentation, human-oversight references, model and data events, evidence sources, limitations, and consistency checks.

Artifact ID	ISAI-ART-000005
Public version	v0.2 Public Research Prototype
Canonical file	infosecured_aml_ai_assurance_evidence_pack_v0_2_public_research_prototype.xlsx
Verification authority	PH3-PUB-WP02-R1 - PASS
Verification date	July 20, 2026
Publication boundary	Independent educational/research prototype only

Required public warning

Independent educational/research prototype only. Professional review, legal review, privacy/security review, AML review, audit/evidence-methodology review, records-management review, and model-risk review were not performed. OSG-009 remains open as a publication limitation. Use synthetic or non-sensitive information only. Do not enter real customer, employee, account, transaction, alert, case, investigation, filing, model, dataset, vendor-confidential, production, or security-sensitive information. This artifact is not legal, compliance, audit, regulatory, model-validation, privacy, security, or AML advice. It is not approved for production or operational use.

This document describes design methodology and source treatment. It does not provide professional interpretation or approval.

1. Purpose, intended use, and design objectives

Purpose and intended use

The artifact is a public downloadable research prototype for organizing synthetic AML AI assurance documentation prompts, evidence and source references, limitations, examples, and bounded consistency checks. It is intended for education, research, structured demonstrations, and evaluation of documentation practices.

It may help users examine how documentation objects relate across system context, monitoring methods, alert review, escalation, human-oversight references, data and model events, evidence notes, limitations, and follow-up. It does not determine whether a particular organization, system, process, model, control, or decision is adequate or compliant.

Intended audience

Potential users include AML and financial-crime personnel, compliance and AI-governance teams, technology-risk and GRC teams, internal audit and model-risk personnel, privacy and security teams, researchers, and practitioners studying evidence-management practices. Organization-specific applicability was not assessed.

Design objectives

- Make evidence relationships visible without presenting them as proof of adequacy or effectiveness.
- Separate descriptive prompts, controlled values, research rationale, and manual-review limitations.
- Support traceable synthetic demonstrations across related worksheets and identifiers.
- Use formulas and validations for technical consistency prompts rather than assurance conclusions.
- Preserve explicit public-use warnings, review boundaries, and unresolved publication limitations.

Publication status

The owner authorized publication as a research prototype without satisfying the professional-review gate. No professional reviewer decision was used to create the public artifact. No R2 was created, and no license was selected.

2. Evidence-first assurance approach and workbook architecture

Evidence-first assurance approach

The workbook treats assurance-oriented documentation as a set of linked records rather than a single narrative assertion. Users can record context, evidence references, source references, limitations, review states, dates, and follow-up information. This structure can make missing documentation and unresolved questions easier to identify, but record presence is not evidence quality, sufficiency, acceptance, or control effectiveness.

Human review is represented through alert-review fields, escalation records, handoff prompts, and optional companion references. These records document relationships and workflow context only. They do not establish competent, independent, meaningful, effective, sufficient, legally adequate, audit-adequate, or compliant human oversight.

Workbook architecture

- README and Pack_Profile establish identity, status, use boundaries, and pack-level context.
- System_Use_Case and Monitoring_Method_Context capture synthetic system purpose, use limits, methods, assumptions, and source references.
- Alert_Review_Escalation, Oversight_References, and Reviewer_Handoff record descriptive review, escalation, reference, and handoff information.
- Data_Gaps_Workarounds and Model_Data_Events organize synthetic gaps, workarounds, dataset, model, and event-definition context.
- Date_Lineage_Lag, Observation_Performance, and Analyst_Feedback organize chronology, measurement windows, metrics, and feedback records.
- Model_Data_Limitations and Evidence_Source_Notes capture limitations and bounded evidence/source references.
- Example_Scenarios and Consistency_Checks support fictional demonstrations and formula-driven documentation prompts.
- Field_Guide, Value_Guide, Research_Source_Notes, and Changelog provide public field decisions, controlled values, research notes, and release history.

Standalone design

The public workbook contains no live dependency on a companion workbook. Human Oversight companion references are optional relationships requiring manual verification when a separately reviewed companion artifact becomes available.

3. Field, controlled-value, and synthetic-data architecture

Field architecture

The Field_Guide records public field identifiers, internal keys, components, public worksheet placement, labels, definitions, requirement treatment, disposition, review holds, organization-configurability, caution text, source basis, and notes. Visible user-entry fields are bounded public derivative fields; technical-note and excluded decisions are not presented as primary user-entry requirements.

Requirement treatments such as Core prompt, Conditional, and Optional organize the prototype. They are not universal legal, regulatory, supervisory, AML, audit, model-risk, or industry requirements.

Controlled-value architecture

The Value_Guide is the source for public dropdown lists. Some values are retained literals; others are explicitly organization-configurable starter values. The lists do not constitute universal classifications or approved taxonomies. Users must define and govern organization-specific meanings outside this prototype.

Synthetic demonstration-data approach

- Existing demonstration records are fictional and explicitly synthetic.
- Synthetic identifiers are used to illustrate record relationships and consistency prompts.
- Reviewer examples are workflow demonstrations, not evidence of identity, credentials, review, approval, or signoff.
- The artifact is not a secure repository and must not receive real operational or security-sensitive information.

Data-entry boundary

Do not enter real customer, employee, account, transaction, alert, case, investigation, filing, model, dataset, vendor-confidential, production, or security-sensitive information. This limitation applies whether the workbook is used locally, uploaded to a collaboration platform, or attached to another system.

4. Formula, validation, and consistency-check approach

Formulas and validations

Formulas calculate bounded technical results from the entered demonstration information. Validation lists constrain selected fields to Value_Guide options. Conditional formatting highlights selected states. These mechanisms support consistency and navigation; they do not establish correctness of the underlying interpretation or evidence.

- Preserve formula cells, validation definitions, table ranges, worksheet names, table names, and stable identifiers.
- Treat cached and displayed formula results as documentation prompts that may depend on dates and entered values.
- Use a separate working copy for experimentation; retain an unchanged reference copy.

Consistency checks

A Pass indicates only that a formula detected no issue under the entered data. Manual review indicates that the workbook cannot resolve the question automatically. The checks are not compliance tests, audit conclusions, AML determinations, regulatory assessments, model validations, or control-effectiveness conclusions.

Verified technical profile

Visible worksheets	20
Structured tables	19
Implemented public data-entry columns	166
Formulas	148
Validation rules	60 across 14 worksheets
Conditional formatting	Five rules across three ranges
Macros or VBA	None
External links or live connections	None
Embedded files	None
Hidden sheets, rows, or columns	None
Real or sensitive operational data	None identified during verification

The technical profile is a verification result, not professional approval, audit readiness, regulatory readiness, compliance, validation, or assurance of effectiveness.

5. Source hierarchy and interpretation boundaries

Source hierarchy

The public artifact separates source roles to avoid converting research rationale into official authority. Research_Source_Notes contains bounded academic and research support. Field_Guide and Evidence_Source_Notes link fields and claims to source categories and limitations. The public workbook does not publish internal source-processing identifiers.

Academic and research-source role

Academic and research sources provide design rationale, not official authority. They support ideas such as documentation, traceability, human-workflow context, data quality, evidence relationships, and transparent limitations. Their findings, frameworks, and examples remain bounded by their methods, samples, jurisdictions, domains, and publication dates.

Official-source candidate research role

RB-01 official-source research preserves warnings and limitations but does not constitute professional interpretation or approval. Candidate official sources were not assigned canonical ISAI source IDs in the public workbook. No candidate source should be treated as establishing applicability to an organization or use case without qualified interpretation.

Professional-interpretation boundary

- No professional reviewer decision was used to create the public artifact.
- Professional, legal, privacy/security, AML, audit/evidence-methodology, records-management, and model-risk reviews were not performed.
- Organization-specific applicability was not assessed.
- Source inclusion does not establish adequacy, acceptance, or compliance.

Public-use treatment

Citations should be presented as academic or research support only. Source limitations and claim boundaries must remain visible. The artifact must not state or imply that a cited article, conference paper, framework, or candidate official source approved the workbook.

6. Public research-source inventory (1 of 2)

The entries below reproduce the public source inventory in condensed form. Each source supports bounded design rationale only and is not official authority.

ISAI-SRC-000002	Muhammad, Yow, and Alsenan (2026), Audit-as-code: a policy-as-code framework for continuous AI assurance. DOI 10.3389/frai.2026.1759211.
ISAI-SRC-000004	Königstorfer and Thalmann (2022), AI Documentation: A path to accountability. DOI 10.1016/j.jrt.2022.100043.
ISAI-SRC-000005	Diaz et al. (2025), Dynamic Trust Modulation and Human Oversight in AI-Driven AML Systems. DOI 10.14569/IJACSA.2025.0161209.
ISAI-SRC-000006	Trapani et al. (2026), Human Oversight in the AI Act: From Legal Obligation to Operational Safeguards for Fundamental Rights. DOI 10.5220/0014300100004052.
ISAI-SRC-000008	Goncalves and Correia (2026), XAI-Compliance-by-Design. DOI 10.3390/jcp6020043.
ISAI-SRC-000009	Fritz-Morgenthal, Hein, and Papenbrock (2022), Financial Risk Management and Explainable, Trustworthy, Responsible AI. DOI 10.3389/frai.2022.779799.

Common limitation themes

The cited work includes conceptual frameworks, qualitative studies, reviews, perspective papers, technical demonstrations, and domain-specific implementations. Limitations include small or context-specific samples, jurisdictional and sector boundaries, synthetic demonstrations, evolving tools, untested generalizability, and the absence of evidence that documentation artifacts alone establish legal sufficiency, effective oversight, audit sufficiency, or regulatory acceptance.

7. Public research-source inventory (2 of 2)

The entries below reproduce the public source inventory in condensed form. Each source supports bounded design rationale only and is not official authority.

ISAI-SRC-000010	Mora-Cantallops et al. (2021), Traceability for Trustworthy AI: A Review of Models and Tools. DOI 10.3390/bdcc5020020.
ISAI-SRC-000012	Kalokyri et al. (2025), AI Model Passport: Data and system traceability framework for transparent AI in health. DOI 10.1016/j.csbj.2025.09.041.
ISAI-SRC-000015	Kawakami, Wilkinson, and Chouldechova (2024), Do Responsible AI Artifacts Advance Stakeholder Goals? Four Key Barriers Perceived by Legal and Civil Stakeholders. DOI listed as unknown in the workbook.
ISAI-SRC-000017	Oztas et al. (2024), Transaction Monitoring in Anti-Money Laundering: A Qualitative Analysis and Points of View from Industry. DOI 10.1016/j.future.2024.05.027.
ISAI-SRC-000018	Pyper and Wiese (2026), An Exploratory Study of Sociotechnical Issues for Anti-Money Laundering Workers. DOI 10.1145/3772318.3791584.
ISAI-SRC-000019	Gupta et al. (2022), Data Quality Issues Leading to Sub Optimal Machine Learning for Money Laundering Models. DOI 10.1108/JMLC-05-2021-0049.

Common limitation themes

The cited work includes conceptual frameworks, qualitative studies, reviews, perspective papers, technical demonstrations, and domain-specific implementations. Limitations include small or context-specific samples, jurisdictional and sector boundaries, synthetic demonstrations, evolving tools, untested generalizability, and the absence of evidence that documentation artifacts alone establish legal sufficiency, effective oversight, audit sufficiency, or regulatory acceptance.

8. Publication decision, limitations, and verification history

Owner-authorized publication decision

The owner-authorized publication decision permits research-prototype publication only. It does not satisfy or replace professional review, create professional approval, resolve source applicability, or authorize production or operational use.

OSG-009 publication limitation

OSG-009 remains open. It is an owner-accepted publication limitation and must remain visible on the artifact page, supporting documents, and implementation checklist. No R2 was created.

Privacy, security, access, retention, and download-use limitations

- Use synthetic or non-sensitive information only; the workbook is not a secure repository.
- Access controls, retention schedules, records-management requirements, and collaboration-platform suitability were not assessed.
- Retain an unchanged reference download and use a separate working copy.
- Do not rely on browser preview or conversion if it changes the XLSX package.
- No separate license was selected; no separate reuse or redistribution permission is granted.

Human-oversight limitation

The workbook can document review, escalation, handoff, and companion-reference information. It does not determine whether oversight is meaningful, effective, sufficient, competent, independent, legally adequate, audit-adequate, or compliant.

No-production-use boundary

The artifact is not approved for production or operational use and must not be integrated into live AML, investigation, filing, model, data, case-management, or security workflows.

Verification history

PH3-PUB-WP02-R1 independently re-verified the bounded correction and issued PASS on July 20, 2026: 249 controls passed, with zero failures and zero blocking observations. The verified XLSX matched SHA-256 fdb420723b8e0a330b93f4c8cda405e2756e388a7add47221b8749a3b5d8129b and size 349,926 bytes. This is technical verification only.

Version and public changelog summary

v0.2 Public Research Prototype — Owner-authorized publication derivative of the independently verified Review Draft R1 baseline. Public-status wording, warnings, publication limitations, Evidence Library notes, and related consistency checks were updated for research-prototype publication. Professional, legal, privacy/security, AML, audit/evidence-methodology, records-management, and model-risk reviews were not performed. OSG-009 remains open. No R2 was created. No license was selected. Not approved for production or operational use.

Remaining limitations

Professional and domain reviews remain unperformed; OSG-009 remains open; organization-specific applicability is unassessed; source applicability and interpretation remain unresolved; the artifact is synthetic-data-only; no production or operational approval exists; no R2 exists; and no license or separate reuse permission was selected.