Clausi

AI Compliance Audit Report

test_sample_project

Regulation: EU-AIA
Scan Date: 2026-01-02 22:14:57

Audit Readiness

Not Audit Ready

8 blocking issue(s) must be resolved before proceeding.

Executive Summary

FILES SCANNED **0**	TOTAL FINDINGS **20**
BLOCKING ISSUES **8**	HIGH RISK GAPS **7**
REMEDIATION EFFORT **Significant**	REGULATIONS **EU-AIA**

Top Risk Themes

4 Article-13

4 Article-10

3 Article-15

Findings Summary

Total Findings:	20
Critical Severity:	8
High Severity:	7
Medium Severity:	5
Low Severity:	0

Detailed Findings

Article-10 MEDIUM MEDIUM COMPLEXITY MEDIUM CERTAINTY ENGINEERING

LOCATION

`src/data_processor.py (lines 195-220)`

ISSUE

Data collection lacks explicit data quality validation and governance measures for AI training data

RECOMMENDATION

Add explicit data quality validation including checks for completeness, accuracy, and representativeness before storing data for AI training purposes

Article-12 MEDIUM MEDIUM COMPLEXITY MEDIUM CERTAINTY ENGINEERING

LOCATION

`src/data_processor.py (lines 149-159)`

ISSUE

Audit logging exists but lacks automatic event logging capabilities required for AI system traceability

RECOMMENDATION

Implement automatic logging for all AI-relevant events including model inputs, outputs, and system state changes with immutable storage

Article-10 CRITICAL MEDIUM COMPLEXITY HIGH CERTAINTY ENGINEERING

LOCATION

`src/model_handler.py (lines 16-27)`

ISSUE

Training function lacks data quality checks, bias detection, and data governance measures

RECOMMENDATION

Implement comprehensive data validation including quality checks, bias detection, data provenance tracking, and statistical analysis before training

Article-11 HIGH MEDIUM COMPLEXITY HIGH CERTAINTY ENGINEERING

LOCATION

`src/model_handler.py (lines 16-75)`

ISSUE

No technical documentation generated during model training, deployment, or updates

RECOMMENDATION

Implement automated documentation generation covering model architecture, training data characteristics, performance metrics, intended use, and known limitations per Annex IV requirements

Article-12 CRITICAL MEDIUM COMPLEXITY HIGH CERTAINTY ENGINEERING

LOCATION

`src/model_handler.py (lines 53-60)`

ISSUE

Logging function is empty and does not capture required event data

RECOMMENDATION

Implement comprehensive automatic logging including timestamps, input data hashes, model version, decision outputs, confidence scores, and context

Article-13 HIGH MEDIUM COMPLEXITY HIGH CERTAINTY ENGINEERING

LOCATION

`src/model_handler.py (lines 62-68)`

ISSUE

No explainability system implemented for AI decisions

RECOMMENDATION

Implement explainability mechanisms such as SHAP, LIME, or attention-based explanations that describe the main factors influencing decisions

Article-14 CRITICAL MEDIUM COMPLEXITY HIGH CERTAINTY ENGINEERING

LOCATION

src/model_handler.py (lines 29-39)

ISSUE

No human oversight mechanisms implemented for model deployment or operation

RECOMMENDATION

Implement human-in-the-loop controls including deployment approval workflows, intervention capabilities, override mechanisms, and real-time monitoring dashboards

Article-15 CRITICAL MEDIUM COMPLEXITY HIGH CERTAINTY ENGINEERING

LOCATION

src/model_handler.py (lines 29-39)

ISSUE

No accuracy validation or robustness testing before deployment

RECOMMENDATION

Implement mandatory pre-deployment validation including accuracy benchmarks, adversarial robustness testing, and security assessments

Article-15 HIGH MEDIUM COMPLEXITY HIGH CERTAINTY ENGINEERING

LOCATION

src/model_handler.py (lines 79-84)

ISSUE

Quality assessment function returns unknown quality without actual metrics

RECOMMENDATION

Implement comprehensive quality assessment including accuracy, precision, recall, F1 score, and domain-specific metrics with quantifiable thresholds

Article-10 CRITICAL MEDIUM COMPLEXITY HIGH CERTAINTY ENGINEERING

LOCATION

`src/model_handler.py (lines 87-92)`

ISSUE

Bias detection function always returns false without actual analysis

RECOMMENDATION

Implement actual bias detection using fairness metrics (demographic parity, equalized odds, etc.) across protected attributes

Article-16 CRITICAL MEDIUM COMPLEXITY HIGH CERTAINTY ENGINEERING

LOCATION

`src/model_handler.py (lines 94-98)`

ISSUE

No conformity assessment, technical documentation, or CE marking procedures implemented

RECOMMENDATION

Implement complete conformity assessment workflow including technical documentation generation, self-assessment or third-party audit depending on risk category, declaration of conformity, and CE marking procedures

Article-9 MEDIUM MEDIUM COMPLEXITY MEDIUM CERTAINTY ENGINEERING

LOCATION

`src/risk_manager.py (lines 68-120)`

ISSUE

Risk assessment is performed but lacks continuous iterative monitoring and update mechanisms

RECOMMENDATION

Add scheduled re-assessment triggers, risk metric monitoring dashboards, and automated alerts when risk indicators change

Article-13 CRITICAL MEDIUM COMPLEXITY HIGH CERTAINTY ENGINEERING

LOCATION

`src/user_interface.py (lines 14-23)`

ISSUE

AI decisions shown without transparency about AI involvement or decision logic

RECOMMENDATION

Display clear AI involvement indicator, confidence scores, key factors in decision, and option to request human review

Article-13 HIGH MEDIUM COMPLEXITY HIGH CERTAINTY ENGINEERING

LOCATION

`src/user_interface.py (lines 25-31)`

ISSUE

User notification about AI interaction is not implemented

RECOMMENDATION

Implement clear, prominent notification at the start of AI interactions informing users they are interacting with an AI system

Article-13 HIGH MEDIUM COMPLEXITY HIGH CERTAINTY ENGINEERING

LOCATION

`src/user_interface.py (lines 33-38)`

ISSUE

Explanation capability returns unavailable response

RECOMMENDATION

Integrate with explainability backend to provide meaningful explanations of decision factors, data used, and model reasoning

Article-14 CRITICAL MEDIUM COMPLEXITY HIGH CERTAINTY ENGINEERING

LOCATION

`src/user_interface.py (lines 40-46)`

ISSUE

Human review mechanism is not implemented

RECOMMENDATION

Implement human review workflow including request submission, queue management, qualified reviewer assignment, and response tracking

Article-12 MEDIUM MEDIUM COMPLEXITY HIGH CERTAINTY ENGINEERING

LOCATION

`src/user_interface.py (lines 69-75)`

ISSUE

User interaction logging lacks required event data

RECOMMENDATION

Add timestamp, AI system identifier, session context, decision references, and user consent status to interaction logs

Article-9 MEDIUM MEDIUM COMPLEXITY HIGH CERTAINTY ENGINEERING

LOCATION

`tests/test_basic.py (lines 13-23)`

ISSUE

Risk assessment tests lack proper validation of risk classification accuracy

RECOMMENDATION

Add comprehensive test cases validating correct risk level assignment for various input scenarios including edge cases and high-risk conditions

Article-10 HIGH MEDIUM COMPLEXITY HIGH CERTAINTY ENGINEERING

LOCATION

`tests/test_basic.py (lines 26-37)`

ISSUE

Data processing tests do not verify consent verification or data protection compliance

RECOMMENDATION

Add tests for consent verification, data minimization, purpose limitation, and rejection of data collection without valid consent

Article-15 HIGH MEDIUM COMPLEXITY HIGH CERTAINTY ENGINEERING

LOCATION

`tests/test_basic.py (lines 40-47)`

ISSUE

Missing tests for bias detection, security measures, and robustness

RECOMMENDATION

Add test suites for bias detection validation, security measure verification, transparency feature testing, and human oversight mechanism validation

---