AI Governance Compliance Report

EU AI Act, ISO 42001 & POLA Compliance

Report Metadata

Organization: EXAMPLE COMPANY
Report Version: 1.0.0
Generated: 2/9/2026, 2:22:27 AM
Reporting Period: 2/14/2025 - 2/9/2026

Section 1: AI Systems Inventory

Comprehensive inventory of all AI systems in use within the organization

Compliance Requirements:

- EU AI Act: Article 52 (Limited Risk Classification - General Purpose AI Systems)
- ISO 42001: Clause 4.3 (Determining Scope of AIMS)
- POLA: APP 1.2 (Managing Personal Information), APP 5 (Notification), APP 8 (Cross-border Disclosure)

Purpose: Define AI systems covered by AI Management System scope

System Name	Provider	Risk Class	Role	Users	Use Cases
Claude	Anthropic	Limited Risk	Deployer	20	Research; Code Development; Data Analysis
Chatgpt	OpenAI	Limited Risk	Deployer	12	Content Creation; Research; Code…
Perplexity	Perplexity AI	Limited Risk	Deployer	2	Research; Data Analysis
Gemini	Google	Limited Risk	Deployer	2	Content Creation; Research; Document…
Bing Chat	Microsoft	Limited Risk	Deployer	18	Search AI services
Google Search	Google	Limited Risk	Deployer	21	Search AI services
Canva	Canva	Limited Risk	Deployer	4	Design AI services
NotebookLM	Google	Limited Risk	Deployer	5	Research AI services
GitHub Copilot	GitHub	Limited Risk	Deployer	2	Coding AI services
Vireo Sentinel	Vyklow	Limited Risk	Deployer	32	AI governance; Compliance monitoring

Section 2: Risk Assessment & Treatment Plan

ISO 42001 Clause 6.1.2 (Risk Assessment) & 6.1.3 (Risk Treatment)

Compliance Requirements:

- EU AI Act: N/A (Limited-risk systems - transparency obligations only)
- ISO 42001: Clause 6.1.2 (AI Risk Assessment), Clause 6.1.3 (AI Risk Treatment)
- POLA: APP 11 (Security Safeguards), Privacy Impact Assessment Requirements

Purpose: Document identified organizational risks and implemented controls

2.1 Identified Organizational Risks

Risk ID	Risk Name	Category	Initial Level	Regulatory Impact
RISK-001	Data Leakage to Third-Party AI…	Data Protection	HIGH	GDPR Article 5, Article 32 - Data…
RISK-002	Privacy Violation Risk	Privacy / GDPR…	HIGH	GDPR Article 6, Article 28 - Lawfulnes…
RISK-003	Intellectual Property Exposure	Intellectual…	MEDIUM	Trade Secrets Directive (EU) 2016/943

2.2 Risk Treatment Controls

Control ID	Control Name	Type	Status	ISO 42001 Annex
CTRL-001	Real-time Content Monitoring	Detective	Operational	A.8.2 (Information Classification an…
CTRL-002	User Intervention Workflows	Preventive	Operational	A.7.1 (Human Oversight)
CTRL-003	Override Justification Requirements	Accountability…	Operational	A.8.3 (Incident Management), A.7.2…
CTRL-004	Comprehensive Audit Trail	Detective /…	Operational	A.8.4 (Record Management)

2.3 Assessment Methodology

Risk assessment performed using ISO 31000 principles: likelihood × impact analysis with consideration of regulatory requirements (GDPR, EU AI Act Article 52) and business impact.

Review Frequency: Quarterly risk review and annual comprehensive assessment
Last Reviewed: 2/9/2026

Section 3: Control Effectiveness Evidence

ISO 42001 Clause 8.2 (Operational Control) & 9.1 (Monitoring and Measurement)

Compliance Requirements:
- EU AI Act: N/A (Voluntary governance controls)
- ISO 42001: Clause 8.2 (Operational Planning and Control), Clause 9.1 (Monitoring and Measurement)
- POLA: APP 11 (Security - Demonstrable Effectiveness), Accountability Principle

Purpose: Evidence that risk treatment controls are operational and effective

3.1 Control Operation Evidence

Metric	Value
Total AI Interactions Monitored	4188
Users Protected	24
Monitoring Uptime	99.9%

3.2 Detection Effectiveness

Risk Level	Detections
High-Risk Content	296
Medium-Risk Content	97
Low-Risk Content	3795

3.3 Overall Control Effectiveness

Note: Control effectiveness measures whether users make informed, conscious decisions when interacting with sensitive content. Success = user was informed + made a decision (protective action, acknowledged risk, or justified override).

Metric	Value
Interventions Required	293
Informed Decisions	275
Control Effectiveness Rate	93.9%
Control Bypasses	3

3.4 Protective Actions

Note: Actions where risk was eliminated: content edited to remove sensitive info, action cancelled, or automatic redaction applied

Metric	Value
Total Protective Actions	21

Content Modified	15
Actions Cancelled	0
Auto Redactions	6
High-Risk Content Eliminated	18

3.5 Informed Risk Acceptance

Note: Instances where user made conscious decision to proceed: mandatory file upload acknowledgments, justified business overrides, or proceeded after reviewing risk warning. These demonstrate control working correctly.

Metric	Value
Total Informed Acceptances	355
File Uploads Acknowledged	33
Justified Overrides	225
Proceeded After Review	97

3.6 Human Oversight

Note: Percentage of override decisions with documented business justification

Metric	Value
Justified Overrides	225
Total Overrides	225
Justification Compliance Rate	100.0%

3.7 Detection Accuracy

Metric	Value
False Positives Identified	67
False Positive Rate	22.6%

Section 4: Residual Risk Assessment

ISO 42001 Clause 6.1 (Actions to Address Risks) - Post-Control Risk Evaluation

Compliance Requirements:

- EU AI Act: N/A (Voluntary risk management)
- ISO 42001: Clause 6.1 (Actions to Address Risks) - Residual Risk Assessment
- POLA: APP 11 (Ongoing Security Assessment), Breach Notification Considerations

Purpose: Document actual unmitigated risks after control implementation

Regulatory Risk Context

System Classification: LIMITED RISK | Residual Risk Level: LOW

Regulatory Basis: EU AI Act Article 52 - General Purpose AI platforms

Rationale: Monitoring controls active, user awareness maintained, audit trail complete

4.1 Risk Assessment After Controls

Risk ID	Risk Name	Initial Level	Residual Level	Bypass Events
RISK-001	Data Leakage to Third-Party AI…	HIGH	LOW	3
RISK-002	Privacy Violation Risk	HIGH	LOW	3
RISK-003	Intellectual Property Exposure	MEDIUM	LOW	0

4.2 Sensitive Content Detection Observations

Control Workflow Bypass Events: 3
Total High-Likelihood Detections: 293
User Engagement Rate: 99.0%

Important Distinction:

Vireo's content scoring detects POTENTIAL sensitive information for user review. Detection does not confirm actual regulatory risk or compliance violation. These events represent control workflow observations, not confirmed risk events.

Detection Criteria: High likelihood of sensitive information (PII, confidential data, proprietary content)

Control Effectiveness Indicators:

' Detection system operating (293 high-likelihood patterns identified)
' Audit trail maintained (all events recorded for review)
' Majority of users engage with interventions (99.0% engagement rate)
& Improvement opportunity: 3 users bypassed workflow (training/refinement needed)

Section 5: Continuous Improvement

ISO 42001 Clause 10 (Continual Improvement of AIMS)

Compliance Requirements:
- EU AI Act: N/A (Voluntary improvement)
- ISO 42001: Clause 10 (Continual Improvement of AIMS)
- POLA: APP 1 (Privacy Policy Review), Accountability - Continuous Improvement

Purpose: Demonstrate ongoing AIMS effectiveness and improvement actions

5.1 AIMS Performance Review

Review Date: 2/9/2026
Overall Status: Effective

Key Findings:

- Real-time monitoring controls operational with 99.9% uptime
- Control effectiveness rate of 93.9% - users making informed, conscious decisions
- 21 protective actions eliminated risk (edited content, cancelled actions, auto-redactions)
- 355 informed risk acceptances demonstrate control working correctly (file acknowledgments, justified overrides, proceeded after review)
- 3 control bypasses identified (no user action despite intervention)

Areas for Improvement:

- Review false positive patterns to refine organizational risk criteria
- Develop use-case-specific guidance for high-frequency scenarios
- Consider platform-specific policies based on usage patterns

5.2 Improvement Actions Planned

Action ID	Area	Proposed Action	Responsibility	ISO 42001
ACT-001	Risk Criteria…	Review override reasons quarterly to refin…	Compliance Officer /…	Clause 6.1 (Risk…
ACT-002	User Guidance…	Develop use-case-specific AI usage…	Department Managers…	Clause 7.3 (Awareness)