ISO 27001 vs ISO 42001

The 47 AI-Specific Controls You're Missing

⚠️ **Audit Alert:** If your organization uses AI systems and only has ISO 27001 certification, you have critical governance gaps that auditors are beginning to identify.

Why This Matters Now

Your ISO 27001 certification covers general information security management. But if you're using AI systems—whether it's customer-facing chatbots, predictive analytics, automated decision-making, or even GitHub Copilot—you have **47 additional controls** that ISO 27001 doesn't address.

These gaps aren't theoretical. Auditors, regulators, and enterprise customers are specifically asking about AI governance. Without ISO 42001 alignment, you're exposed.

93
Total ISO 27001 Controls

47
AI-Specific Controls

46
Shared with ISO 27001

Framework	Total Controls	AI-Specific	Covers AI Risk?
ISO 27001:2022	93 controls	0	✗ No
ISO 42001:2023	38 controls	38	✓ Yes

🚨 What Happens During Your Next Audit

- **SOC 2 Audits:** Auditors now ask "How do you manage AI model risk?" and "Show me your AI system inventory." If you can't answer, expect findings.
- **Customer Security Reviews:** Enterprise customers are adding AI governance questions to vendor questionnaires. No documented AI controls = lost deals.
- **Regulatory Compliance:** EU AI Act enforcement begins in 2025. Financial services, healthcare, and government contractors face sector-specific AI regulations now.
- **Insurance & Legal Risk:** Cyber insurance policies are starting to exclude AI-related incidents unless governance is documented.

The 47 Controls You're Missing

ISO 27001 has 93 controls for information security. ISO 42001 adds AI-specific requirements across critical areas. Here's what your organization needs to implement:

1 AI System Lifecycle Management (8 Controls)

5.2 **AI Policy**

Establish organizational AI governance policy covering acceptable use, risk tolerance, ethical principles, and accountability structures for AI systems.

6.2.1 **AI System Inventory**

Maintain comprehensive inventory of all AI systems including purpose, data sources, model types, risk classification, and responsible parties.

6.2.2 **AI Impact Assessment**

Conduct impact assessments for AI systems evaluating risks to individuals, organizations, and society before deployment.

6.2.3 **AI System Objectives**

Define and document specific objectives, success criteria, and performance metrics for each AI system aligned with business goals.

8.9 **AI System Development Lifecycle**

Implement structured development lifecycle including design, training, validation, deployment, monitoring, and decommissioning stages.

8.10 **AI System Versioning**

Maintain version control for AI models, training data, configurations, and documentation to enable rollback and change tracking.

8.32 **AI System Retirement**

Establish processes for safe decommissioning of AI systems including data archival, model preservation, and transition planning.

9.2 **AI Continuous Improvement**

Implement feedback mechanisms and continuous monitoring to improve AI system performance, safety, and alignment with objectives.

2 Data Governance for AI (12 Controls)

5.12 **Data Classification for AI**

Classify training, testing, and operational data based on sensitivity, regulatory requirements, and potential bias implications.

8.3 **Training Data Management**

Implement controls for training data quality, provenance, representativeness, and protection throughout the AI lifecycle.

8.4 Data Quality for AI

Establish data quality standards including accuracy, completeness, consistency, and timeliness requirements for AI systems.

8.11 Data Minimization

Collect and retain only data necessary for AI system purposes, implementing automated deletion and anonymization where appropriate.

8.12 Data Provenance

Track and document data sources, transformations, and lineage throughout AI development and operation.

8.13 Synthetic Data Controls

If using synthetic data, document generation methods, validation approaches, and limitations compared to real data.

8.14 Data Labeling

Implement quality controls for data labeling including annotator training, inter-rater reliability, and bias monitoring.

8.15 Test Data Segregation

Maintain separation between training, validation, and test datasets to prevent data leakage and ensure valid performance evaluation.

8.16 Data Poisoning Prevention

Implement controls to detect and prevent malicious data injection that could compromise AI system integrity.

8.33 **AI Data Retention**

Define retention periods for AI training data, model artifacts, and outputs based on regulatory and business requirements.

8.34 **Data Subject Rights**

Implement mechanisms to honor data subject rights (access, deletion, portability) in AI contexts including model retraining.

8.35 **Automated Decision-Making Transparency**

Provide mechanisms for individuals to understand, challenge, and obtain human review of automated decisions affecting them.

3 AI Model Risk & Testing (9 Controls)

6.2.4 **AI Risk Assessment**

Conduct comprehensive risk assessments covering technical risks, operational risks, ethical risks, and regulatory compliance risks.

8.17 **Model Validation**

Validate AI models against performance criteria, bias metrics, and safety requirements before production deployment.

8.18 **Performance Metrics**

Define and monitor key performance indicators including accuracy, precision, recall, fairness metrics, and business outcomes.

8.19 **Bias Testing**

Test AI systems for bias across protected characteristics and implement mitigation strategies for identified disparities.

8.20 **Adversarial Testing**

Conduct adversarial testing to identify vulnerabilities to manipulation, evasion attacks, and edge cases.

8.21 **Safety Testing**

Test AI systems under various scenarios including failure modes, unexpected inputs, and safety-critical situations.

8.22 **Model Robustness**

Evaluate and improve AI system robustness to input variations, distribution shifts, and environmental changes.

8.29 **Model Drift Detection**

Implement monitoring to detect performance degradation, concept drift, and data drift in production AI systems.

9.1 **AI Performance Monitoring**

Continuously monitor AI system performance against baseline metrics with automated alerting for anomalies.

4 Transparency & Explainability (6 Controls)

5.6 **AI Transparency Requirements**

Define transparency requirements for AI systems including disclosure to affected parties and documentation standards.

8.23 Model Explainability

Implement explainability techniques appropriate to AI system risk level, enabling stakeholders to understand decision factors.

8.24 AI Documentation

Maintain comprehensive documentation including model cards, data sheets, system architecture, and known limitations.

8.25 User Communication

Communicate to users when they're interacting with AI systems and provide appropriate context about capabilities and limitations.

8.26 Decision Auditability

Log AI decisions with sufficient detail to enable auditing, investigation of complaints, and regulatory compliance.

8.27 Stakeholder Communication

Establish communication protocols for informing stakeholders about AI system changes, incidents, and performance issues.

5 Human Oversight & Accountability (5 Controls)

5.3 AI Roles & Responsibilities

Define clear roles and responsibilities for AI governance including AI owner, data steward, and ethics review board.

6.2.5 Human Oversight Requirements

Define level of human oversight required based on AI system risk, including human-in-the-loop and human-on-the-loop approaches.

7.2 AI Competence Requirements

Define competency requirements for personnel developing, deploying, and overseeing AI systems including technical and ethical training.

8.28 Human Review Process

Implement processes for human review of AI decisions, particularly for high-stakes or contested outcomes.

8.36 AI Ethics Review

Establish ethics review board or process to evaluate AI systems for alignment with organizational values and societal norms.

6 Third-Party AI Management (4 Controls)

5.19 Third-Party AI Services

Establish vendor risk management process for third-party AI services including due diligence and ongoing monitoring.

5.20 AI Supply Chain Risk

Assess and manage risks in AI supply chain including data providers, model providers, and infrastructure dependencies.

5.21 Third-Party AI Agreements

Include AI-specific requirements in vendor contracts covering liability, performance standards, and audit rights.

8.30

AI Vendor Monitoring

Monitor third-party AI service providers for compliance with contractual obligations and performance standards.

7 AI Incident Response (3 Controls)

5.24

AI Incident Response Plan

Develop incident response procedures specific to AI failures, bias incidents, security breaches, and safety issues.

5.25

AI System Shutdown Procedures

Define criteria and procedures for emergency shutdown or rollback of AI systems showing unsafe behavior.

8.31

AI Incident Logging

Log AI-related incidents including false positives, bias incidents, security events, and performance degradation.

What This Means for Your Organization

If you're using AI and only have ISO 27001...

You're compliant with information security basics, but you have zero documented controls for:

- How you inventory and classify your AI systems
- How you assess AI-specific risks (bias, model failure, adversarial attacks)
- How you validate model performance and fairness

- How you monitor for model drift and degradation
- How you ensure explainability and transparency
- How you manage AI vendor risk differently from traditional vendors
- How you handle AI incidents and emergency shutdowns

Real-World Impact

Organizations are experiencing:

- **Lost enterprise deals** because they can't answer AI governance questions in security reviews
- **SOC 2 audit findings** for "no documented AI risk management process"
- **Regulatory inquiries** from sector regulators (FINRA, FDA, FTC) about AI systems
- **Executive liability concerns** as boards ask "how do we know our AI is safe?"
- **Insurance coverage gaps** for AI-related incidents

Don't Wait for an Audit Finding

Get a free 30-minute AI Governance Gap Assessment. We'll review your current ISO 27001 program and show you exactly which of these 47 controls apply to your AI systems.

Schedule Your Gap Assessment

DeuraInfoSec.com | AI Governance Pioneer-Practitioners
ISO 42001 • EU AI Act • NIST AI RMF
hd@deurainfosec.com | www.deurainfosec.com