WEBINAR RECORDED

PECB

# Is AI Still Under Control? What ISO/IEC 42001 and ISO/IEC 27001 Reveal

DECEMBER 18 | 03:00 PM CET

## Nathalie Claes

Security Governance Expert,
Management Consultant and Auditor

*#GlobalLeadingVoices*

# Agenda

- Why AI control is suddenly a board-level issue
- Where traditional security and compliance fall short
- What ISO IEC 42001 adds to ISO IEC 27001
- How organizations regain control over AI systems
- What auditors, regulators, and customers now expect
- How certification supports trust and readiness

PECB

# Why this question matters now

AI adoption has outpaced governance

Many organizations have AI in production without knowing it

Regulators are catching up fast EU AI Act, NIS2, CRA

# What we mean by “under control”

- Clear ownership and accountability
- Known risks and documented decisions
- Traceability from design to deployment
- Ability to stop, change, or explain AI behavior

Control is not about blocking AI. It’s about being able to answer hard questions with confidence.

PECB

# The typical AI reality in organizations

- Shadow AI tools in business teams
- AI embedded in SaaS and suppliers
- No central AI inventory
- Security, privacy, ethics handled separately

**Most AI risk is structural, not technical**

# Why existing controls fall short

- ISO 27001 focuses on information, not decisions
- Risk management stops at data security
- Human impact and bias are often ignored
- Model behavior is rarely governed

# What is ISO/IEC 42001

## ISMS thinking applied to AI

First international AI Management System standard

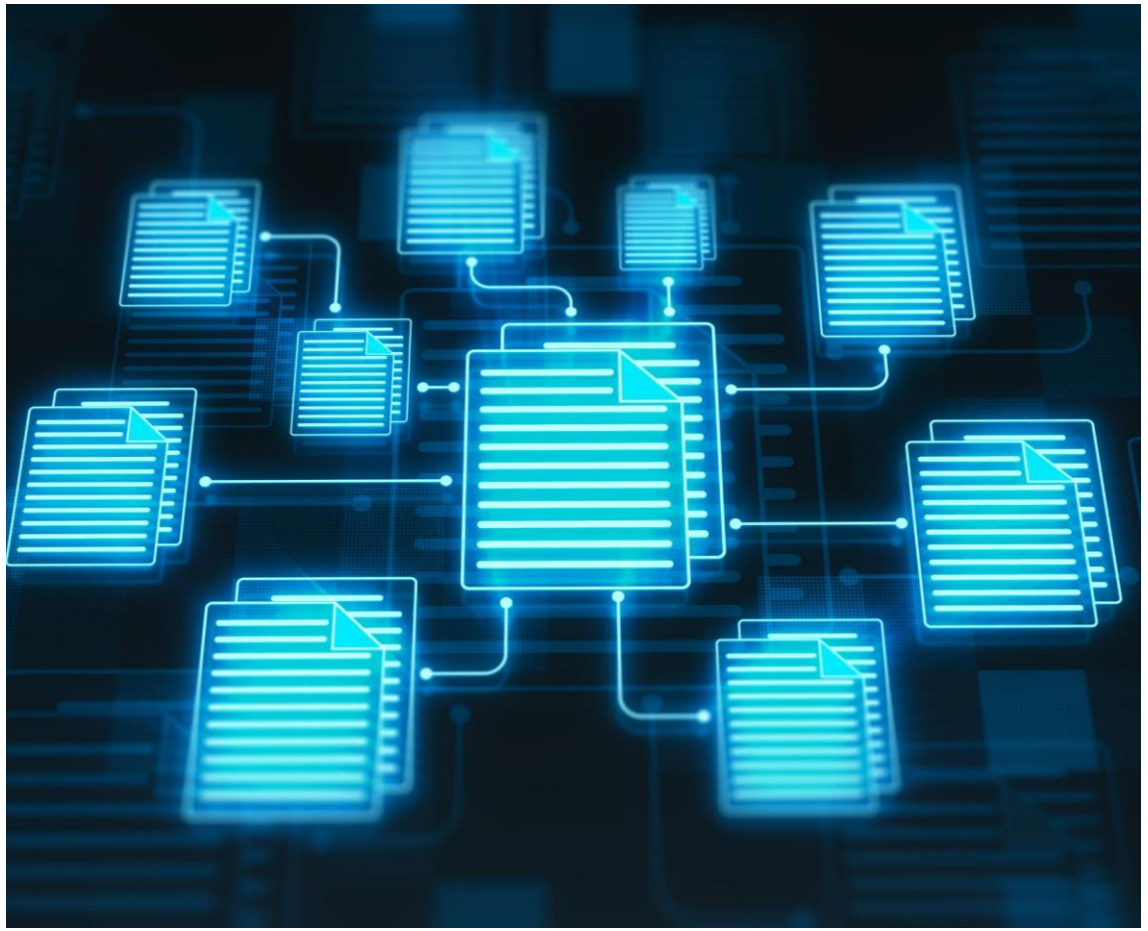
Focus on governance, risk, and accountability

Covers the full AI lifecycle

Designed to work with existing management systems

PECB

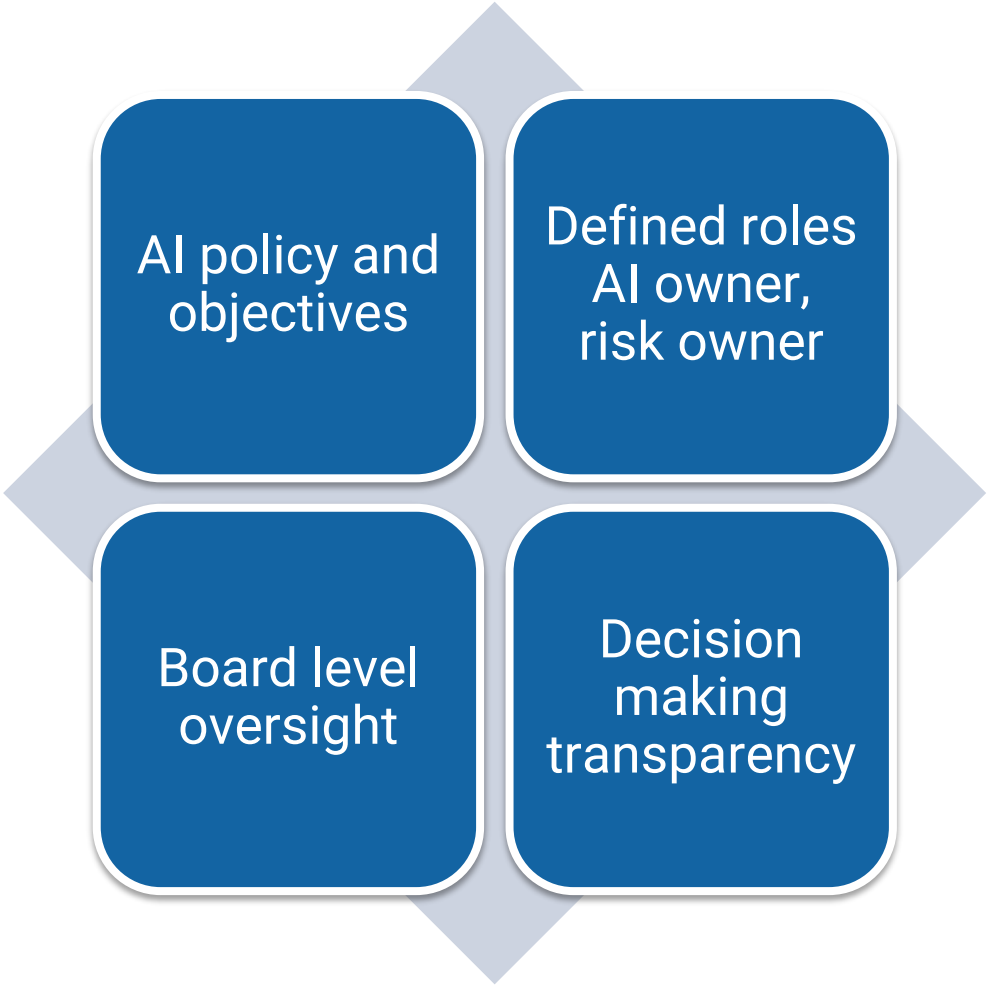
# Comparing ISO 27001 and ISO 42001



- Both standards share a common structure based on Annex
- ISO 27001 focuses on protecting information security
- ISO 42001 governs AI behaviour across its full lifecycle
- Both emphasise risk management, leadership, and continual improvement
- Together, they ensure comprehensive management of data and AI risks

PECB

# Control area 1: Governance and leadership



# Control area 2: AI Risk Management

Identify AI use cases and models

Assess impact on people, business, society

Consider bias, misuse, drift, over reliance

Document risk acceptance

Same logic as ISO 27001 risk treatment, broader impact.

PECB

# Control area 3: Data and Model Controls

Training data quality and provenance

Model validation and testing

Monitoring performance and drift

Change management for models

AI doesn’t fail once. It fails slowly and silently.

# Control area 4: Human Oversight

- Human in the loop where needed
- Clear escalation paths
- Avoid automation bias
- Training for users and decision makers

# Control area 5: Security and Resilience

- AI systems as part of the attack surface
- Manipulation risks: prompts, data, models
- Secure development and deployment controls
- Monitoring, logging, and anomaly detection
- AI-specific incident response and recovery
- Alignment with ISO IEC 27001 security controls

# Why certification matters

Demonstrates structured control

Builds trust with customers and regulators

Creates internal clarity

Avoids ad hoc compliance panic

# Getting started without overwhelm

| | |
|---|---|
| Map | Map AI use cases and suppliers |
| Extend | Extend existing ISO 27001 processes |
| Start | Start with governance, not tooling |
| Build | Build internal competence through training |

# Key takeaways

- AI control is a governance challenge
- ISO 27001 is necessary but not sufficient
- ISO 42001 closes the gap
- Certification supports credibility and readiness

# Upskill your career with PECB Skills

**15-minute courses on:**

- AI
- Cybersecurity
- Data Protection
- Auditing
- Information Security

**Earn CPDs** for each competency and Get Certified

PECB Skills


# THANK YOU

✉ n.claes@myrnacoachingconsulting.be

in https://www.linkedin.com/in/nathalieclaes/