MITRATECH

CHECKLIST

TPRM Compliance Guide: ISO 42001 - Artificial Intelligence Management Systems (AIMS)

Table of Contents

The AI Balancing Act: Innovate and Regulate

Artificial Intelligence (AI) is transforming how organizations operate, creating new efficiencies while introducing unique governance, risk, and compliance (GRC) challenges. Because of this, organizations must understand how to develop the necessary AI governance policies to use the technology safely and securely. ISO/IEC 42001:2023 is the first global standard for establishing an Artificial Intelligence Management System (AIMS), designed to help organizations address concerns around AI ethics, transparency, bias, safety, and privacy.

Note: *This guide does not constitute legal or professional advice. Organizations should consult with internal audit teams to address specific compliance needs.*

What is ISO 42001?

ISO/IEC 42001:2023 is an international standard developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) that provides guidance for establishing, implementing, maintaining, and continually improving an AIMS. It includes controls for ethical use, data quality, transparency, accountability, and third-party oversight. Like all ISO standards, ISO 42001 is voluntary, but it is quickly becoming a global benchmark for AI governance.

ISO 42001 Overview

ISO/IEC 42001 is modeled on the Plan-Do-Check-Act (PDCA) cycle and shares a common structure with other ISO management system standards like ISO 27001. ISO 42001 is structured with detailed annexes and core clauses that provide guidance for implementation. The structure encourages integration with other compliance frameworks and supports cross-functional governance.

Scope & Applicability

ISO 42001 applies to AI providers, producers, and users of AI systems regardless of origin or use case. AI used via SaaS, third-party APIs, or internal models can all fall within scope. The standard also extends to non-technical departments using AI tools (e.g., marketing) as part of the evaluation.

Alignment with Other Standards/Regulations

ISO 42001 harmonizes with ISO 27001 (Information Security), ISO 27701 (Privacy), and ISO 23894 (AI Risk Management). It complements multiple global frameworks and regulations, including but not limited to the NIST AI RMF, the EU AI Act, and DORA, allowing a single governance structure to serve multiple frameworks.

Why ISO 42001 Matters for Risk Management Teams

AI introduces various types of risks — from bias in algorithms and data misuse to regulatory exposure and reputational harm. The widespread use of large language models (LLMs), such as Claude, ChatGPT, and Gemini, is already creating new vulnerabilities, unearthing risks that IT security teams scramble to navigate. ISO 42001 provides a future-ready, auditable framework to: AI ethics, transparency, bias, safety, and privacy.

- Manage AI risk across the AI system's lifecycle
- Embed ethical principles and transparency
- Comply with regulations like the EU AI Act
- Build trust with stakeholders

ISO 42001 & Third-Party Risk Management

ISO/IEC 42001 fundamentally expands the scope of third-party risk management programs by formalizing AI-specific requirements across the supplier lifecycle. It requires organizations to assess and manage not just traditional security and compliance risks, but also the ethical, operational, and societal risks introduced by vendors' AI systems.

For TPRM teams, this means extending due diligence questionnaires to evaluate a supplier's AI governance maturity, monitoring ongoing changes to third-party AI models, and embedding contractual provisions that enforce transparency, explainability, and incident response obligations.

Going forward, TPRM programs must treat AI vendors as critical control points, integrating ISO 42001-aligned criteria into onboarding, monitoring, and audit processes to meet growing regulatory demands and ensure AI supply chain resilience.

Mapping Mitratech TPRM Capabilities to ISO 42001 Standards

The summary table below maps capabilities in the Mitratech Third-Party Risk Management Platform to select third-party, vendor, and supplier controls present in ISO 42001.

Note: *This table should not be considered definitive guidance. For a complete list of controls, please review the complete ISO standards in detail and consult your auditor.*

ISO 42001 Controls	How Mitratech Helps
Clause 6.1: Actions to address risks and opportunities	
6.1.2 AI risk assessment *"Organizations shall determine the risks and opportunities that need to be addressed to give assurance that AI management systems can achieve their results, prevent or reduce undesired effects, and achieve continual improvement."* *"The organization shall define and establish an AI risk assessment process that analyses the AI risks to:* *1) assess the potential consequences to the organization, individuals and societies that would result if the identified risks were to materialize;* *2) assess, where applicable, the realistic likelihood of the identified risks;* *3) determine the levels of risk"*	Mitratech partners with you to build a comprehensive third-party risk management (TPRM) program aligned with your broader artificial intelligence management systems program, based on proven best practices and extensive real-world experience. As part of the process, Mitratech can help to define: • Risk scoring and thresholds based on your organization's risk tolerance • Assessment and monitoring methodologies based on third-party criticality • Risk mitigation and remediation strategies
Annex A Control A.10 – Third-party and Customer Relationships	
A.10.2 Allocating responsibilities *"The organization shall ensure that responsibilities within their AI system lifecycle are allocated between the organization, its partners, suppliers, customers and third parties."*	Our experts collaborate with your team on defining and implementing TPRM processes and solutions; selecting risk assessment questionnaires and frameworks; and optimizing your program to address the entire third-party risk lifecycle – from sourcing and due diligence to termination and offboarding – according to your organization's risk appetite. As part of this process, Mitratech can help you define: • Clear roles and responsibilities (e.g., RACI) • Third-party inventories • Risk scoring and thresholds based on your organization's risk tolerance

	• Assessment and monitoring methodologies based on third-party criticality • Fourth-party mapping • Sources of continuous monitoring data (cyber, business, reputational, financial) • Key performance indicators (KPIs) and key risk indicators (KRIs) • Governing policies, standards, systems, and processes to protect data • Compliance and contractual reporting requirements against service levels • Incident response requirements • Risk and internal stakeholder reporting • Risk mitigation and remediation strategies
A.10.3 Suppliers *"The organization should establish a process to ensure that its usage of services, products or materials provided by suppliers aligns with the organization's approach to the responsible development and use of AI systems."*	Mitratech standardizes assessments against ISO best practices and other information security control frameworks, providing internal audit and IT security teams with a central platform for measuring and demonstrating adherence to secure software development and software development lifecycle (SDLC) practices. For organizations with limited resources and expertise, Mitratech can manage the third-party risk lifecycle on your behalf – from onboarding suppliers and collecting evidence, to providing remediation guidance and reporting on contract SLAs. As a result, you reduce vendor risk and simplify compliance without burdening internal staff.

Best Practice Recommendations for TPRM Leaders

The following list offers practical strategies for managing risks, ensuring transparency, and aligning programs with ISO 42001 standards.

- ☐ Clearly define the scope: internal AI use (e.g., usingChatGPT) vs. AI in customer-facing products (e.g., in-house models)
- ☐ Use Statements of Applicability (SOAs) to transparently document what's in-scope and how it's controlled
- ☐ Implement consistent risk assessment criteria for evaluating third-party AI systems
- ☐ Verify that third-party AI algorithms are accountable, fair, and free from bias
- ☐ Monitor and improve third-party AI systems through regular evaluations and updates
- ☐ Assess and manage risks associated with data used by third-party AI systems, focusing on data quality, privacy, and security
- ☐ Ensure that third-party AI systems adhere to ethical principles and maintain transparency in their operations
- ☐ Add AI scoping questions to your intake form to capture model type, data sensitivity, and decision criticality
- ☐ Publish an AI supplier code of conduct aligned with ISO 42001 Annex A principles (fairness, transparency, privacy, security)
- ☐ Require a Statement of Applicability or ISO 42001 certificate from critical AI vendors by a defined deadline
- ☐ Integrate AI incident clauses into your existing breach notification SLA
- ☐ Review the supplier tiering model quarterly to capture changes in AI usage

By embedding these enhancements, your TPRM program will not only satisfy ISO 42001 auditors but also provide a forward-looking defense against the unique, rapidly evolving risks that AI introduces into the extended enterprise. Look for solutions that offer automated evidence collection, continuous monitoring capabilities, and map risk assessment to relevant frameworks and regulations to satisfy auditors, reduce risk exposure, and stay compliant.

Looking Ahead: Turning These Insights into Action

ISO 42001 is a foundational AI governance standard increasingly seen as essential, transitioning from a "nice-to-have" to a baseline requirement for any AI-driven product strategy.

It requires structured risk and compliance processes that span the entire AI lifecycle, encompassing ethics, third-party oversight, and performance management. Risk and impact assessments must expand beyond classic cybersecurity and move into model fairness, data provenance, and human oversight as core considerations. Continuous vendor monitoring is mandatory; hidden AI in third-party tools (think shadow AI and fourth-party AI dependencies) is now a top governance gap.

Risk leaders should act now to future-proof their organizations' AI strategies and demonstrate trust, accountability, and compliance. Certification is less about a compliance badge and more about accelerated market trust amid tightening regulation.

Incorporating ISO 42001 into third-party risk management programs enhances an organization's ability to govern AI responsibly, mitigate potential risks, and foster confidence among stakeholders.

MITRATECH

About Mitratech

Mitratech is a proven global technology partner for legal, risk, compliance, and HR professionals seeking to maximize productivity, control expense, and mitigate risk by deepening operational alignment, increasing visibility, and spurring collaboration across an enterprise. Mitratech serves over 24,000 organizations worldwide, spanning more than 160 countries.

Learn more at Mitratech.com.

EMPOWER. AUTOMATE. ELEVATE.