BARR ADVISORY

2024 Whitepaper

Everything You Need to Know About ISO 42001

Table of Contents

Introduction

ISO 42001

ISO recently released ISO 42001, a new standard designed to help implement safeguards for the security, safety, privacy, fairness, transparency, and data quality of artificial intelligence (AI) systems. ISO 42001 includes best practices for an AI management system—otherwise known as AIMS—and was created to help organizations that use AI responsibly perform their roles in using, developing, monitoring, or providing products or services.

In this whitepaper, we'll break down ISO 42001's risk management features, unique safeguards, and structure of the upcoming framework.

> ***"The widespread adoption of AI increases the likelihood of large-scale data breaches where massive amounts of personal information are compromised, leading to severe consequences for individuals and organizations.***
>
> Steve Ryan, Attest Manager at BARR Advisory

ISO 42001 AI Management System

As a new ISO management system standard (MSS), ISO 42001 will take a risk-based approach in applying the requirements for AI use.

What are risks posed by third parties?

One of the most notable features of ISO 42001 is that it's been drafted in such a way as to integrate with other existing MSS, such as:

- ISO 27001 for **information security**
- ISO 27701 for **privacy**
- ISO 9001 for **quality**

If your organization opts to adhere to ISO 42001, you'll be expected to focus your application of the requirements on features unique to AI and the resulting issues and risks that arise with its use.

Since organizations should consider the management of issues and risks surrounding AI a comprehensive strategy, adopting an AIMS can enhance the effectiveness of an organization's existing management systems in the areas of information security, privacy, and quality, as well as your overall compliance posture.

ISO 42001 AI Safeguards

As AI continues to evolve, the ISO 42001 framework can help organizations implement safeguards for certain AI features that could create additional risks within a particular process or system.

Take a look at some examples of features that require specific safeguards:

Automatic Decision-Making

When done in a non-transparent way, automatic decision-making may require specific administration and oversight beyond traditional IT systems.

Data Analysis, Insight, and Machine Learning

When employed in place of human-coded logic to design systems, these features change how such systems are developed, justified, and deployed in ways that may require different protections.

Continuous Learning

AI systems that perform continuous learning change their behavior during use and require special considerations to ensure their responsible use continues in their constantly changing behavior.

ISO 42001 Subject Matter

ISO 42001 Controls

ISO 42001 controls touch on the following areas:

- Policies related to AI
- Internal organization
- Resources for AI systems
- Impact analysis of AI systems on individuals, groups, and society
- AI system life cycle
- Data for AI systems
- Information for interested parties of AI systems
- Use of AI systems
- Third-party relationships
- New ISO 42001 Annexes

ISO 42001 is key for any AI-powered organization. Completing an ISO 42001 compliance assessment or gap assessment with BARR Advisory will help your organization understand what is required to achieve ISO 42001 certification and uncover potential nonconformities that your team can work to remediate before beginning the certification process.

Frequently Asked Questions

Who should pursue ISO 42001 certification?

ISO 42001 was designed to serve organizations of all sizes and across all industries that participate in the use or development of AI-powered products and services. Additionally, organizations should consider ISO 42001 certification if they wish to demonstrate to internal and external stakeholders their ability to manage AI for decision-making, data analysis, or continuous learning.

What are the benefits of ISO 42001 compliance?

Achieving compliance with ISO 42001 not only offers a competitive advantage to AI-powered businesses, but also positions your organization as one that prioritizes the ethical and responsible use of AI. Designed to integrate with standards such as ISO 27001 and ISO 27701, the framework serves as a seamless and smart addition to a modern, comprehensive compliance program.

How long is an ISO 42001 certification valid?

Like other ISO/IEC cybersecurity frameworks, ISO 42001 certification remains valid for three years after the initial issuance date. In the interim, your organization will work with your chosen certification body to complete regular surveillance audits to maintain your certification.

How does ISO 42001 align with ISO 27001?

While the two frameworks differ widely in scope, there are some areas of overlap. The ISO 42001 framework pertains solely to AI management systems (AIMS). By contrast, ISO 27001 standards cover an organization's information security management system (ISMS). Both, however, are designed to help organizations mitigate risks and promote security, privacy, and transparency with customers and stakeholders.

Is a gap assessment required to achieve certification?

While completing a gap assessment is not required to achieve ISO 42001 certification, it can reveal deficiencies in your AIMS ahead of time and make for a smoother, more predictable certification process.

BARR Advisory's expert team can help you simplify the path to ISO 42001. We will assess your organization's alignment with ISO 42001 standards and provide a detailed report attesting to their findings once you've made the decision to pursue ISO 42001 compliance. While not a formal certification, the resulting report will provide assurance to customers and stakeholders that your organization is staying ahead of the curve when it comes to the ethical and secure use of developing technologies like AI.

About BARR Advisory

BARR Advisory is a cloud-based security and compliance solutions provider specializing in cybersecurity and compliance for companies with high-value information in cloud environments like AWS, Microsoft Azure, and Google Cloud Platform. A trusted advisor to some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements in highly regulated industries including technology, financial services, healthcare, and government.

Our Services

- **SOC Examinations**
  [SOC 1, SOC 2, SOC 3, SOC for Cybersecurity]
- **Healthcare Services**
  [HIPAA/HITRUST]
- **ISO 27001 Assessments**
- **FedRAMP Security Assessments**
- **PCI DSS Assessment Services**
- **Penetration Testing and Vulnerability Assessments**
- **Cybersecurity Consulting and vCISO Services**
- **Compliance Program Assistance**

Connect with BARR

Want to learn more about our ISO 42001 services? Contact us today.