safeshield®

A Practical Guide to the EU AI Act

How ISO/IEC 42001 Can Help You Achieve Complience

June 2025

What is the EU AI Act?

+ What is the EU AI Act?

Proposed by the European Commission and passed by the European Parliament, the EU AI Act was first adopted in 2024 and will be enforceable by 2026. The Act aims to ensure that AI systems are "safe, transparent, traceable, non-discriminatory, and environmentally friendly."

+ Does the Act apply to my organization?

The Act applies to any organization whose AI systems operate within the EU or serve users within the EU.

+ How does the Act work?

The Act offers a risk-based classification system ranging from "Unacceptable Risk" at the top end, and "Minimal Risk" at the bottom. Depending on an AI system's risk level, the responsible organization will need to comply with certain rules and obligations.

+ Are there any repercussions for non-compliance?

Many organizations will avoid strict regulations under the Act; however, it's important to be aware of these classifications to avoid hefty fines and other legal repercussions.

4 Risk Levels of the EU AI Act

Unacceptable Risk

Unacceptable risk is completely prohibited under the EU AI Act and typically applies to governments or law enforcement. This category exists primarily to preserve human dignity and privacy. Systems classified as unacceptable are things like real time biometric surveillance (facial recognition used to identify individuals during protests) or manipulative AI (AI driven advertising that relies heavily on psychological manipulation, commonly directed towards children in the form of games etc.).

High Risk

This category is the most likely to apply to business. High risk systems are heavily regulated under the Act. Finance, healthcare and employment are all areas that are most commonly affected. Examples include AI that screen resumes, manages credit scoring, autonomous driving systems or medical diagnostic aids.

Businesses are mandated by The Act to employ strict controls to mitigate the risks associated with these high-risk technologies. These controls include risk management systems, fully documented, thorough record keeping, and post-market monitoring after the deployment of these technologies.

Limited Risk

Limited Risk technologies are not inherently harmful but do still require transparency under the EU AI Act. To comply with The Act, users must be informed they are interacting with an AI; users must be allowed to opt out of interacting with an AI wherever possible and must be able to request human interaction if appropriate. There must also be disclosure and transparency whenever content has been generated by an AI (this applies to video, image, and audio, etc.). Examples of Limited Risk technologies include chatbots, AI generated content and recommendation engines for things like product suggestions.

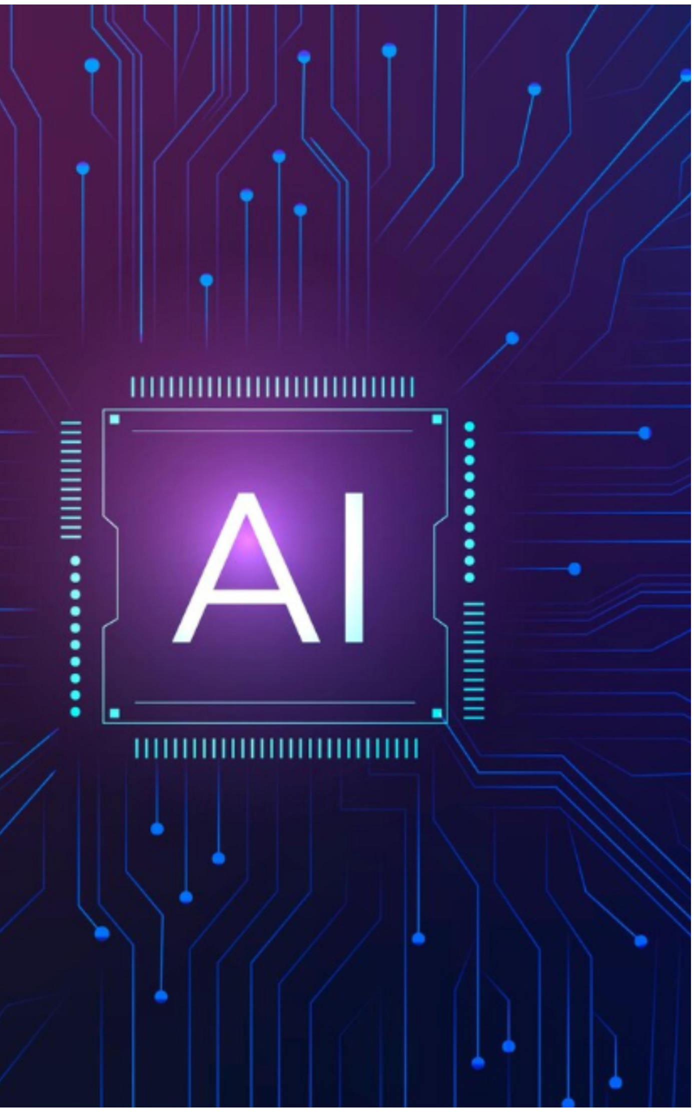
Minimal Risk

Minimal Risk technologies (like spam filters) are unregulated under The Act but do have voluntary guidelines associated with them. There is no legal mandate to adhere to these guidelines, though they are encouraged.

Guidelines include voluntary adherence to codes of conduct such as ISO/IEC 42001 and following ethical principles, such as data privacy and fairness.

How Adopting the ISO/IEC 42001 Standard Can Help

ISO/IEC 42001 is the first of its kind and stands as the first international standard for AI management systems (AIMS).



- **Transparency**
  Clear communication of AI functions and decisions

- **Accountability**
  Assignment of responsibilities within the organization

- **Human Oversight**
  Defined thresholds for intervention and escalation

- **Data Governance**
  Responsible data use and quality management

- **Continual Improvement**
  Ongoing performance reviews and process enhancements

ISO/IEC 42001 aligns perfectly with the EU AI Act, and compliance with the standard will ensure your business meets the legal requirements of the EU AI Act. The table below shows how ISO/IEC 42001 aligns with the EU AI Act:

EU AI Act Requirement	ISO/IEC 42001 Support
Risk management system	Core structure of ISO/IEC 42001
Documentation and record-keeping	Important part of the AIMS process
Human oversight	Mandatory part of ISO/IEC 42001
Transparency and user disclosure	Supported through operational guidelines
Post-market monitoring and continual improvement	Core principle of ISO/IEC 42001

Compliance with the EU AI Act will soon become a legal requirement for any business employing the use of AI that operates in Europe or that serves users in the EU.

If your business operates in or serves the EU, it's vital to start preparing now. ISO/IEC 42001 offers the most comprehensive, actionable path to ensure your business is ready. Achieving ISO/IEC 42001 compliance:

- Simplifies your regulatory response,
- Builds strong, reliable internal AI governance,
- Demonstrates your commitment to responsible innovation.

The ISO/IEC 42001 standard lays the foundation for compliant, trustworthy AI systems both today and in the future.

Frequently Asked Questions

+ Does the EU AI Act apply to companies outside the EU?

Yes. The EU AI Act applies to any organization that places AI systems on the EU market, uses AI systems within the EU, or whose AI outputs affect individuals within the EU, regardless of where the company is based.

+ What if we use third-party or pre-built AI tools?

You are still responsible. Even if your organization uses third-party AI systems (such as SaaS tools with embedded AI), you may be classified as a "deploying entity" under the Act. That means you're accountable for how those systems are used and must ensure they meet regulatory requirements.

+ How can I tell if our AI system is High Risk?

High-risk systems are those used in important sectors such as healthcare, employment, education, law enforcement, and/or finance. If your AI influences decisions about people's rights, safety, or opportunities, it likely falls into the high-risk category. The EU Commission maintains a list of high-risk use cases that can be used as a guide.

+ Is ISO/IEC 42001 certification mandatory under the EU AI Act?

No, it is not mandatory—but it is highly recommended. ISO/IEC 42001 provides a structured, internationally recognized framework to help meet the legal requirements of the EU AI Act. Adopting it can simplify your compliance process and demonstrate good faith in regulatory efforts.

+ How long does ISO/IEC 42001 certification typically take for an organization?

The timeline varies based on your organization’s size and readiness. For most mid-sized companies, it typically takes between 8 and 12 months to prepare for and complete certification. Leveraging expert training and guidance can significantly accelerate this process.

+ Where can I learn more?

Safeshield offers both self-paced and expert-led ISO/IEC 42001 professional certification programs that empower individuals and teams to confidently navigate AI governance and compliance. Whether you're seeking foundational training or pursuing more advanced skills as an Artificial Intelligence Management Systems implementer or auditor, we have a course to fit your needs.

Visit us at https://www.safeshield.cloud/ai-grc-certifications

Thank You

About Us

SafeShield specializes in cybersecurity and compliance consulting, providing comprehensive solutions to help businesses safeguard against potential cyber threats and compliance risks. Our services include:

- ISMS Implementation
- Risk assessments
- Security audits
- Security training for employees and executives
- More

Visit us at https://www.safeshield.cloud for more information or to view our library of training courses and personalized services.