ISO/IEC 42001

As the cybersecurity landscape undergoes rapid evolution, the integration of Artificial Intelligence (AI) has emerged as a pivotal component. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have introduced ISO/IEC 42001, the world's first AI management system standard. This groundbreaking standard provides organizations with a structured approach to managing AI projects, balancing innovation with governance, and addressing unique challenges such as ethical considerations, transparency, and continuous learning.

Definition of Standard

What is ISO/IEC 42001?

ISO/IEC 42001 specifies requirements for establishing, implementing, maintaining, and continually improving an Artificial Intelligence Management System (AIMS) within organizations. It is designed for entities providing or utilizing AI-based products or services, ensuring responsible development and use of AI systems.

Who is ISO/IEC 42001 for, and does it apply for all AI Systems?

ISO/IEC 42001 is applicable to organizations of any size involved in developing, providing, or using AI-based products or services. It is relevant across all industries and is applicable to public sector agencies as well as companies or non-profits. Yes, it's designed to be applicable across various AI applications and contexts.

Services offered by Tevora

Readiness Assessment: An assessment of your current environment to see how ready they are for the ISO/IEC 42001 standard. Upon completion, a list of gaps will be presented on what items the organization must address to pursue the actual certification process.

Consulting Support: Post-gap assessment to help create policies, procedures, and implement controls that comply with ISO/IEC 42001 standards. This will include the creation of AIMS, SOA, and other mandatory documents.

Internal Audit: Detailed internal audit for the requirements of the standard and then prepare a report to be distributed internally and with external certification bodies on the current state of AIMS.

AI REGULATIONS

NIST AI Risk Management Framework (AI RMF 1.0): In January of this year, NIST released this new framework to better manage risks to individuals, organizations, and society associated with AI. For voluntary use, the NIST AI RMF can improve the incorporation of trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems.

Biden Executive Order (October 2023): This extensive order issued by President Biden builds on previous initiatives and provides comprehensive strategies to help harness the potential of AI, while at the same time managing its associated risks.

EU AI Act: At the time of this blog's publication, the EU is also in the process of finalizing its own AI use regulation that is centered around excellence and trust and aims to boost research and industrial capacity while ensuring safety and fundamental rights.

Standard Overview:

The standard has been drafted to follow the same structure and integrate with existing standards such as ISO 27001 (Information Security) and ISO 27701 (Privacy). While considering requirements of information security and privacy, ISO/IEC 42001 does not require organizations to have these standards as prerequisites.

What is an AIMS?

An AI management system, as specified in ISO/IEC 42001, is a set of interrelated elements intended to establish policies, objectives, and processes concerning the responsible development, provision, or use of AI systems. It provides requirements and guidance for establishing, implementing, maintaining, and continually improving an AI management system within the context of an organization.

Structure:

The standard is broken down into the following

- Management Clauses
- Annex A - control requirement
- Annex B - implementation guidance
- Annex C - potential AI related objectives & risk
- Annex D - use of AIMS across domains & sectors

Management Clauses, Annex A and B are requirements while Annex C and D are informative

Timeline of Standard

There are currently no accreditation rules published governing procedures for certification bodies to perform audits to the new standard. It will take between 3 to 12 months for Certification Bodies to be able to provide certification depending on the accreditation body. Organizations can use this time period to start preparing for and implementing AIMS. They can leverage internal consulting like Tevora to help set up all the applicable documentation needed to comply with ISO/IEC 42001.

TEVORA Compromise Elsewhere.

Tevora is a global leader in enterprise cybersecurity, risk, and compliance services. Founded in 2003, Tevora's team of expert consultants is devoted to supporting the CISO in protecting their organizations from digital threats, creating more secure and compliant business operations. With 20 years of consistent growth, Tevora has accumulated numerous awards and recognitions for growth and industry leadership. Most notably, Tevora has been recognized as one of Inc 5000's fastest growing companies for 9 years since 2014. Today, Tevora boasts over 1000 enterprise clients and robust practices around compliance, risk, threat management, and cyber solution integration.

Go forward. **We've got your back.**