International Journal of Recent Advances in Multidisciplinary Topics
Volume 6, Issue 4, April 2025
https://www.ijramt.com | ISSN (Online): 2582-7839

Understanding Risk Management: ISO 42001 vs ISO 27001

Shashank Sambamoorthy[1], Sambamoorthi Subramaniam[2*]
[1]Cyber Security Practitioner & Strategist, Orlando, USA
[2]SME-Cyber Security, VCISO, Chennai, India

***Abstract*: Both ISO 42001-2023 (Artificial Intelligence Management System - AIMS) and ISO 27001:2022 (Information Security Management System - ISMS) include comprehensive requirements for risk management as part of their planning processes. While both standards follow a similar Plan-Do-Check-Act (PDCA) cycle and emphasize the importance of addressing risks and opportunities, they differ in their specific focus and the types of risks they address.**

***Keywords*: Artificial Intelligence Management System (AIMS), Information Security Management System (ISMS), International Organization for Standardization (ISO), Risk Management.**

1. Introduction

This article explores the similarities and differences of addressing risk management in ISO 42001-2023 (Artificial Intelligence Management System - AIMS) and ISO 27001:2022 (Information Security Management System - ISMS).

2. Similarities in Risk Management Planning

A. Consideration of Context and Interested Parties

Both standards require the organization to consider external and internal issues (Clause 4.1 in both) and the requirements of interested parties (Clause 4.2 in both) when planning and determining the risks and opportunities that need to be addressed.

B. Objectives of Addressing Risks and Opportunities

In both standards, the purpose of addressing risks and opportunities is to ensure that the management system can achieve its intended results, prevent or reduce undesired effects, and achieve continual improvement.

C. Planning Actions

Both ISO 42001 and ISO 27001 require the organization to plan actions to address these risks and opportunities, integrate these actions into their respective management system processes, and evaluate the effectiveness of these actions.

D. Alignment with ISO 31000

The risk assessment and treatment process in ISO 27001 is explicitly stated to align with the principles and generic guidelines provided in ISO 31000. Similarly, the risk management planning in ISO 42001 aligns with the general risk management principles outlined in ISO 31000.

E. Consideration in Objectives

Both standards require that organizational objectives (AI objectives in ISO 42001 and information security objectives in ISO 27001) take into account applicable requirements and the results from risk assessment and risk treatment.

3. Key Differences and Specifics

A. Scope of Risks

ISO 42001 focuses on "AI risks"9. These are risks that could prevent or achieve intended AI objectives and relate to the potential consequences to the organization, individuals, and society resulting from the development, deployment, or use of AI systems.

It also emphasizes an "AI system impact assessment" to understand the potential consequences for individuals, groups, or societies10. Annex C of ISO 42001 provides examples of potential AI-related organizational objectives and risk sources, such as accountability, availability and quality of training and test data, fairness, privacy, robustness, safety, security, and transparency.

ISO 27001 focuses on "information security risks". These are risks associated with the loss of confidentiality, integrity, and availability of information within the scope of the information security management system15. Annex A of ISO 27001 provides a comprehensive list of information security controls across organizational, people, physical, and technological domains to address these risks.

B. Risk Assessment Process

While both require a defined risk assessment process, ISO 42001 specifies that the process should be "informed by and aligned with the AI policy (see 5.2) and AI objectives (see 6.2). It also highlights the need for repeated AI risk assessments to produce "consistent and comparable results" and specifically mentions utilizing an "AI system impact assessment" when assessing consequences.

ISO 27001's risk assessment process requires establishing and maintaining "information security risk criteria" including risk acceptance criteria and criteria for performing risk

*Corresponding author: saamba@gmail.com

assessments.

C. Risk Treatment Process

ISO 42001 requires the organization to select appropriate "AI risk treatment options" considering options provided in Annex A9. It also necessitates obtaining "approval from the management for the AI risk treatment plan and acceptance of the residual AI risks"

ISO 27001 requires selecting appropriate "information security risk treatment options", taking account of risk assessment results, and determining all "controls that are necessary" to implement the chosen options.

It also mandates a comparison with the controls in Annex A to ensure no necessary controls have been omitted and the creation of a "Statement of Applicability" detailing the chosen controls, justifications, implementation status, and reasons for exclusion of Annex A controls.

While ISO 42001's Annex A provides control objectives and controls, it does not explicitly require a "Statement of Applicability" in the same way ISO 27001 does.

D. Focus of Annex A

ISO 42001's Annex A (normative) provides "Reference control objectives and controls" organized by objectives related to policies, internal organization, resource management, assessing impacts of AI systems, AI system lifecycle, data for AI systems, information for interested parties, and use of AI systems. These are directly related to the management of AI.

ISO 27001's Annex A (normative) provides an "Information security controls reference" that lists a comprehensive set of 93 information security controls categorized under Organizational controls, People control, Physical controls, and Technological controls. These are broader in scope, covering general information security practices.

4. Conclusion

In summary, while both ISO 42001 and ISO 27001 require robust risk management planning, ISO 42001 is specifically tailored to address the unique risks and opportunities associated with artificial intelligence systems, including their societal impact. It emphasizes AI-specific risk assessment informed by AI policies and objectives and provides AI-focused control objectives in its Annex A.

ISO 27001, on the other hand, focuses on managing risks to the confidentiality, integrity, and availability of information assets and offers a broader set of information security controls in its Annex A, along with the specific requirement for a Statement of Applicability.

References

[1] ISO 42001-2023 (Artificial Intelligence Management System - AIMS).
[2] ISO 27001:2022 (Information Security Management System - ISMS).
[3] ISO 31000-2018 (Risk Management guidelines).