Summary

Presentation

The Operational Guide to the Update of the Information Security Management System (ISMS) according to the ISO 27001:2000 standard at AMD 1/2024, relating to climate change, represents a fundamental innovation for organizations that aim to align their information security strategies with rapidly evolving global environmental challenges. This guide was developed to provide entities with a clear and detailed path to integrate climate change considerations into their ISMS, recognizing the growing impact that climate has on information security and business continuity.

AMD 1/2024 emphasizes the importance of considering climate change as a critical factor in risk assessment processes, business continuity planning and

risk mitigation strategy. With the introduction of this document, organizations are encouraged to take a proactive approach in managing climate-related risks, incorporating new assessment methodologies and specific adaptation strategies.

In this introduction, we will explore the key changes and additions provided by the AMD, highlighting how organizations can apply these new guidelines to improve the resilience and sustainability of their ISMS. The guide specifically addresses the needs of a changing environment, providing tools and techniques to ensure information security remains robust in the face of threats from climate change.

This actionable guide is essential for information security managers, risk professionals and business decision makers seeking to anticipate and mitigate the impact of climate change on their operations. By adopting the practices recommended in this document, organizations will not only strengthen their information security but also contribute to the global fight against climate change by demonstrating a commitment to sustainability and corporate social responsibility.

What is AMD 1/2024 of ISO/IEC 27001:2022?

AMD 1 ISO 27001 is an amendment to the ISO 27001 standard that introduces climate change requirements into the information security management system. It is officially known as ISO/IEC 27001:2022 Amd 1/2024

What has changed?

The change consists of adding climate change requirements to the ISO 27001 standard.

Clauses 4.1 and 4.2 are amended as shown below

4.1 Understand the organization and its context.

The organization must determine the external and internal issues that are relevant to its purpose and that influence its ability to achieve the intended outcome(s) of its management system.

Addition – "The organization will need to determine whether climate change is a relevant issue."

4.2 Understand the needs and expectations of stakeholders.

The organization must determine: (i) the interested parties that are relevant to the management system; (ii) the relevant requirements of such interested parties; (iii) which of these requirements will be met through the management system.

Added – "NOTE: Relevant stakeholders may have requirements related to climate change"

Indirectly there can also be an impact on other requirements such as:

information security management system policy (requirement 5.2);

objectives and planning for their achievement (requirement 6.2);

analysis of risks and opportunities (requirement 6.1);

competence and awareness (requirements 7.2 and 7.3);

documented information (requirement 7.5);

operational activities (requirements 8.1, 8.2 and 8.3);

monitoring, measurement, analysis and evaluation (requirement 9.1.3);

internal audit (requirement 9.2);