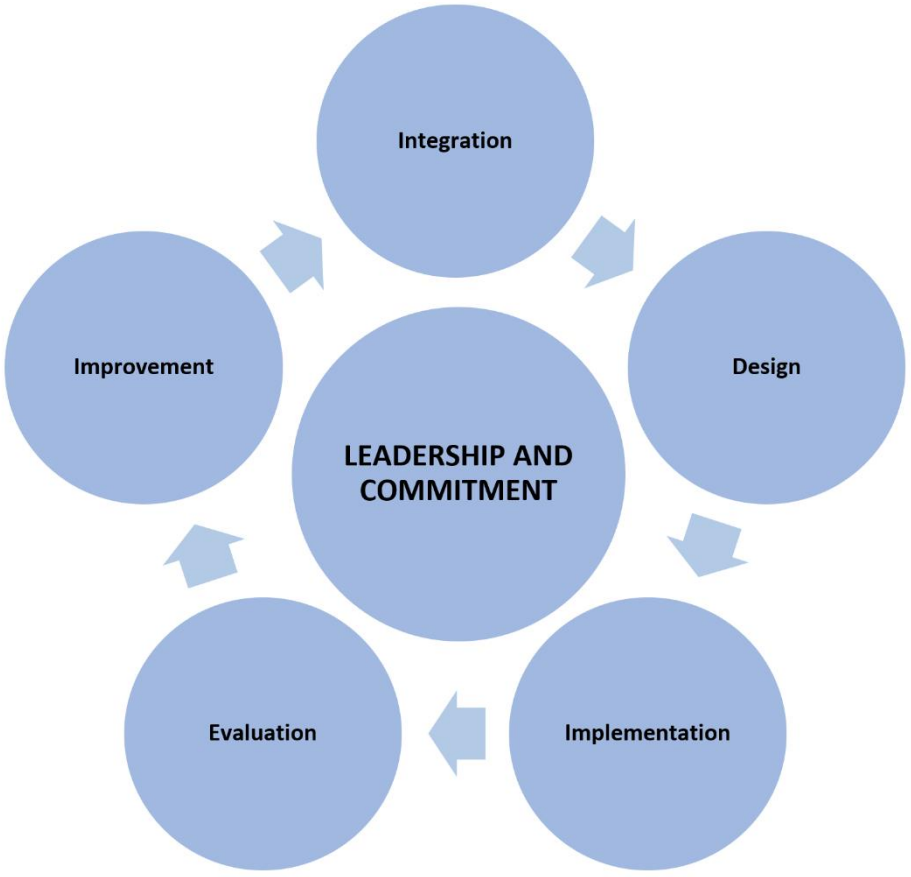
WHAT IS ISO 31000 STANDARD?

ISO 31000 is an international standard developed by the International Organization for Standardization (ISO) that provides principles, guidelines, and a framework for risk management. It was first published in 2009 and has since been revised in 2018.

The ISO 31000 standard aims to help organizations of all types and sizes to effectively identify, assess, and manage risks in a structured and systematic manner. It provides a common language and approach to risk management, enabling organizations to improve decision-making, increase resilience, and protect their objectives from potential threats and uncertainties.

RISK MANAGEMENT FRAMEWORK

The ISO 31000 standard provides a framework for risk management. By establishing and implementing a risk management framework according to ISO 31000 principles, organizations can systematically identify and address risks, make informed decisions, and improve their ability to achieve their objectives despite uncertainties and challenges.



Visualization of framework for risk management by ISO 31000

KEY PRINCIPLES OF EFFECTIVE RISK MANAGEMENT

ISO 31000 provides also principles for effective risk management. Key principles are:

Integration: Risk management should be integrated into all aspects of the organization, including strategic planning, decision-making, and operational processes.

Risk-based approach: Organizations should adopt a systematic and structured process to identify, assess, and manage risks across all levels of the organization.

Customization: The risk management process should be tailored to the organization's specific needs, context, and objectives.

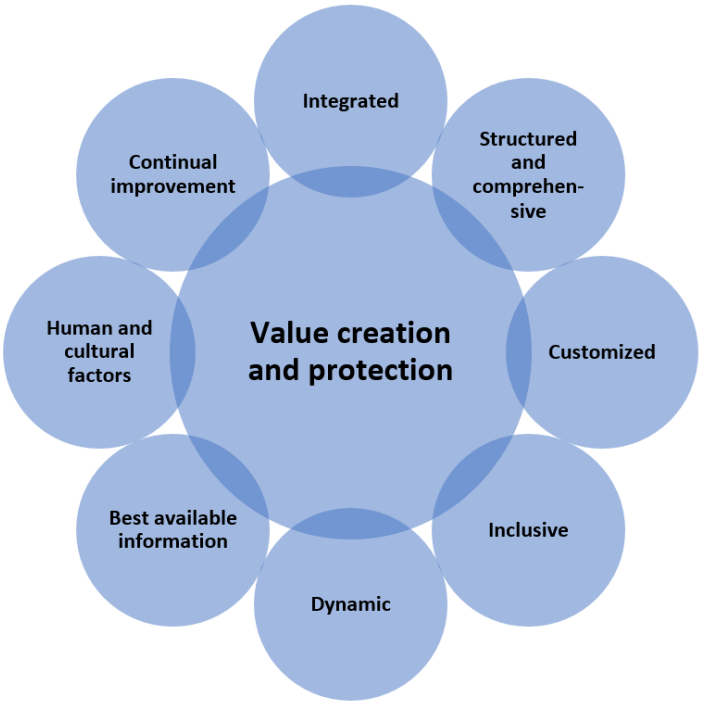
Inclusivity: All stakeholders, both internal and external, should be involved in the risk management process to ensure a comprehensive understanding of risks and potential impacts.

Dynamic and iterative: Risk management should be a continuous process that adapts to changes in the internal and external environment, allowing for ongoing improvement.

Transparent communication: Effective communication about risks, their potential consequences, and risk management strategies is essential for informed decision-making.

Human and cultural factors: Consideration should be given to human behaviour, culture, and the organization's values in managing risks effectively.

Continual improvement: The organization should regularly review and enhance its risk management framework to ensure its effectiveness and relevance.



Visualization of key principles for effective risk management by ISO 31000

By adhering to these principles, organizations can establish a robust and proactive approach to managing risks, leading to better decision-making and safeguarding their objectives.

You can read more about key management principles for effective risk management by ISO 31000 in Handbook developed by INCLUS*:* *https://inclus.com/en/iso-31000-risk-management-principles/*

RISK MANAGEMENT PROCESS

The risk management process outlined in ISO 31000 can be summarized as follows:

Establish the context: Understand the organization's objectives, stakeholders, and the external and internal factors that can influence the risk management process.

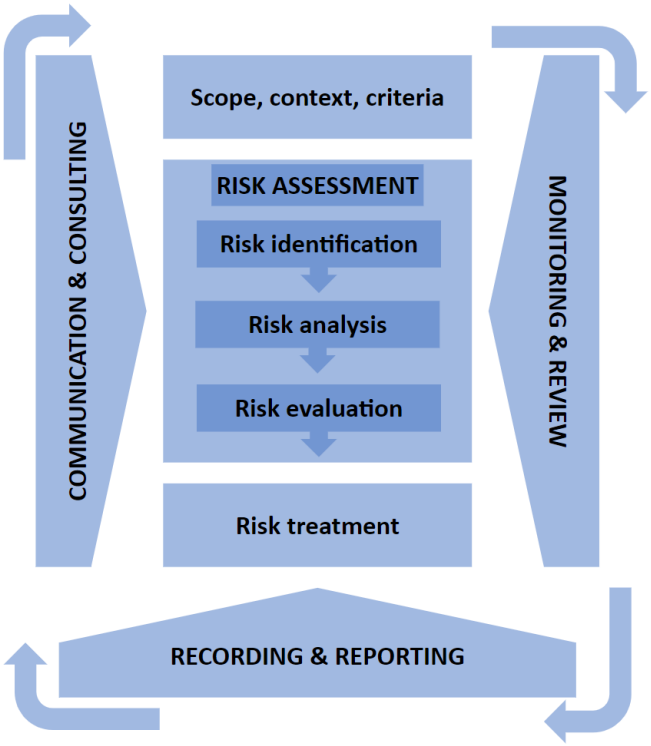
Risk identification: Identify risks that could impact the achievement of objectives. This involves systematically identifying potential risks across the organization.

Risk analysis: Assess the identified risks by analyzing their likelihood of occurrence, potential impact, and any existing controls. This step helps understand the nature and characteristics of each risk.

Risk evaluation: Evaluate the assessed risks against predefined criteria to determine their significance. This process involves comparing risks to determine their priority for further action.

Risk treatment: Develop and implement risk treatment plans. This step involves selecting and implementing appropriate risk response options, such as avoiding, reducing, transferring, or accepting risks.

Monitor and review: Continuously monitor and review the effectiveness of the risk management process. This includes monitoring the outcomes of risk treatment actions, reviewing the risk landscape, and making necessary adjustments.



Visualization of risk management process by ISO 31000

The ISO 31000 standard emphasizes the importance of an iterative and ongoing risk management process that is embedded within the organization's decision-making and planning processes. It promotes a systematic and proactive approach to identify, assess, and manage risks, ultimately helping organizations make informed decisions and improve their resilience.

WHAT IS ISO 31000 STANDARD RELATION TO SECURITY RISK MANAGEMENT?

ISO 31000 is a generic risk management standard that can be applied to various domains, including **security risk management**. When it comes to security risk management, ISO 31000 provides a foundation and guidance for organizations to identify, assess, and manage security risks in a systematic and structured manner.

Here are a few key points highlighting the relation of ISO 31000 to security risk management:

Holistic approach: ISO 31000 promotes a holistic approach to risk management, considering all potential risks that can impact an organization, including security risks. It emphasizes integrating security risk management into the overall risk management framework of the organization.

Contextual understanding: ISO 31000 emphasizes the importance of understanding the context within which security risks exist. This involves considering the organization's objectives, stakeholders, legal and regulatory requirements, and the specific security threats and vulnerabilities relevant to the organization's operations.

Understanding the context implies considering several factors that could have an impact on the company's organizational risks. These factors may include, for example:

- The organization's objectives: It is important to align risk management efforts with the organization's objectives, both from an economic and business model standpoint, including the company's values. This entails considering how risks may affect the achievement of those objectives and ensuring that risk management strategies are taken into account along with the organizational goals.

- Stakeholders: Organizations have stakeholders who may be affected by or have an impact on their activities, such as employees, customers, suppliers, shareholders, regulators and the community.

- Legal requirements: Organizations operate within a legal and regulatory framework (regional, national, European and international) that sets standards and obligations for safety and risk management. Understanding these requirements is essential to ensure compliance and avoid legal and regulatory issues, otherwise the company may face fines for administrative violations and, in some countries that recognize it, criminal liability not only for their employees, but also for the legal entities themselves.

- Security threats and vulnerabilities: Organizations face a wide range of security threats, such as cyber-attacks, physical breaches, natural disasters or internal fraud. It is important to identify and assess the specific threats and vulnerabilities that are relevant to the organization's operations. This includes considering the potential impact and likelihood of these risks occurring.

Risk assessment: ISO 31000 provides guidance on conducting risk assessments, which involves identifying and evaluating security risks. It encourages organizations to use systematic processes to assess the likelihood and potential impact of security risks on the achievement of objectives.

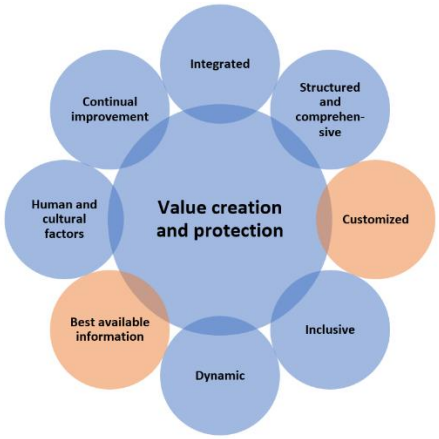
Risk treatment: ISO 31000 assists in the development and implementation of risk treatment plans, including security risk treatment. This involves selecting and implementing appropriate security controls and countermeasures to mitigate, transfer, or accept security risks based on the organization's risk appetite and objectives.

Integration with security management frameworks: ISO 31000 can be integrated with existing security management frameworks, such as ISO 27001 (Information Security Management System) or sector-specific security standards, to enhance the organization's overall security risk management practices.

By incorporating the principles and guidance of ISO 31000 into their security risk management processes, organizations can establish a structured, systematic, and proactive approach to identifying, assessing, and managing security risks effectively. It helps organizations to better protect their assets, operations, and stakeholders from security threats and vulnerabilities.

RELATION OF PROJECT MATERIALS TO ISO 31000 RISK MANAGEMENT PROCESS

The materials found in the SECUREU website are designed according to the framework, principles and management process steps of the ISO 31000 standard. With the published materials (videos, articles, assignments) you will find a visual indication that will explain which step of the risk management framework, values or process the relevant material referred to.



For example, best practice article, task or video published on SECUREU project webpage and marked with such icon will explain two ISO 31000 key principles of risk management - **Transparent communication** and **Customization.**