

# ISO 31000 guide: Steps used in all types of organizations in Latin American Countries



Edmundo Lizarzaburu<sup>a</sup>  | Monica Chavez<sup>a</sup> | Conrado Garcia<sup>b</sup> | Eduardo Noriega<sup>c</sup> | David Tinoco<sup>a</sup>

<sup>a</sup>Esan University, Peru.

<sup>b</sup>Universidad de Valladolid, Spain.

<sup>c</sup>Universidad Cesar Vallejo, Peru.

**Abstract** This paper highlights the crucial role of adopting ISO 31000 as a comprehensive and flexible risk management standard for organizations throughout Latin America. ISO 31000 provides a globally recognized framework for tackling various challenges, such as regulatory pressures, economic fluctuations, and operational inefficiencies. By embedding risk management into day-to-day operations and strategic decision-making, organizations can strengthen their resilience and improve decision-making processes. The study examines key elements of ISO 31000, such as risk identification, assessment, and response strategies, which include mitigation, transfer, acceptance, or elimination. It stresses the importance of stakeholder engagement to ensure effective communication and consultation at every phase. The iterative nature of risk management outlined in ISO 31000 promotes continuous improvement and alignment with organizational objectives. Through a qualitative analysis of case studies from Peru, Mexico, and Brazil in both the public and private sectors, this paper demonstrates how organizations adapt ISO 31000 to their specific economic, cultural, and legal contexts. These adaptations enhance risk visibility, build stakeholder trust, and support long-term sustainability. The findings reveal significant benefits, such as improved business continuity and a better capacity to address financial and operational uncertainties. Despite its adaptability, the successful implementation of ISO 31000 requires addressing regional challenges, including resource constraints and evolving regulations. The paper calls for ongoing training and awareness efforts to ensure the framework's widespread adoption and effectiveness. In conclusion, ISO 31000 is an essential tool for strengthening risk management practices, empowering Latin American organizations to navigate uncertainties and achieve sustainable growth.

**Keywords:** risk management, organizational resilience, business continuity, Latin America, governance

## 1. Introduction

The International Organization for Standardization (ISO) introduced the ISO 31000:2009 Risk Management Principles and Guidelines to provide a structured framework for risk management applicable to organizations of all types and sizes (ISO, 2009). This guidance was updated in 2018 to address evolving organizational challenges and ensure its relevance across diverse sectors (Hopkin, 2018; ISO 2018; Settembre-Blundo et al., 2021). ISO 31000 serves as a crucial framework for systematically managing risks in Latin America, a region marked by economic instability, political challenges, and natural disasters (Abel et al., 2011; Pakhchanyan, 2016). The framework offers practical tools for integrating risk management into key organizational processes, including strategic planning, operational management, and project execution (Barafort et al., 2018). These include tactics and decisions, operations, functionalities, processes, projects, assets and producer functionalities (Tiwari, et al., 2023).

It is important to note that there are some aspects of risk that can be difficult to define. However, it is imperative that both the private and public sectors consider risk in order to create value through ethical behavior and establish a framework to manage them (Fan and Stevenson, 2018).

The structure of this paper is as follows. Section 2 reviews the relevant literature, focusing on the definition of risk and benefits of risk management. Section 3 analyses the methodology that has been used to conduct research on risk management, based on the ISO 31000 guide. Section 4 explains the principles of risk management and the application of each. Section 5 describes the risk management framework while Section 6 describes its process. Finally, Section 7 presents the conclusion of this research.

## 2. Literature Review

The evolution of risk management highlights its critical role in organizational success. Over time, frameworks like ISO 31000 have provided standardized approaches to addressing uncertainties and achieving continuous improvement (Baranoff,



2001; Bernal et al., 2011; Hardjomidjojo et al., 2022). Risks, as defined by Martínez and Pastor (2018), encompass events that can positively or negatively impact the objectives of both public and private organizations. Managing these risks requires the implementation of preventive strategies to enhance efficiency, governance, and stakeholder management (ISO, 2018). Effective risk management focuses on principles such as traceability, due diligence, and proportionality. These principles enable organizations to develop tailored approaches that align with their unique contexts, allowing for the efficient allocation of resources to address risks, recognize opportunities, and minimize operational losses (Aven & Renn, 2010; Oyede & Aderibidge, 2022). Additionally, risk management fosters improved decision-making processes and enhances operational performance. Although ISO 31000 is widely recognized for its adaptability, its implementation must consider organizational-specific factors such as leadership, management structures, information systems, and policy frameworks. Support from senior management is essential to embed risk management into organizational culture and processes. As AL-Kiyumi (2021) emphasizes, organizations must also adapt their risk management practices to evolving regional contexts, accounting for economic, cultural, and regulatory changes.

### 2.1. Definition of risk

Baranoff (2001) defines risk as any event that introduces uncertainty or unpredictability into an outcome. The International Organization for Standardization (ISO) elaborates on risk management as a coordinated effort to control an organization's risks, as outlined in ISO 31000, first published in 2009 and updated in 2018 (ISO, 2009, 2018). Understanding risk appetite and risk tolerance is fundamental to effective risk management (Borek et al., 2013; Aven, 2017). Risk appetite reflects the degree to which an individual or organization is willing to embrace risk, whereas risk tolerance defines the threshold within which the organization is comfortable operating (Berger et al., 2022). Fernandez and Bernard (2014) argue that risk management involves a comprehensive evaluation of potential risks throughout a project's life cycle. They highlight the necessity of identifying appropriate responses to minimize the likelihood and impact of adverse events (Renn, 2017, 2020). This process is iterative and begins with defining the scope and objectives of risk management (Pritchard & PMP, 2014). Organizations often adopt standardized risk management frameworks, such as ISO 31000, to address the inherently high-risk nature of certain projects (Fernandez & Bernard, 2014; Barafort et al., 2018; Berger et al., 2022). Standardization helps ensure consistency, clarity, and accountability in managing risks across various organizational processes and industries.

### 2.2. Benefits of risk management

The ISO 31000 standard offers numerous benefits to organizations, serving as a comprehensive framework for effective risk management (Borek et al., 2013; Djapic et al., 2016; Gallati, 2022). By providing clear guidelines, it enables businesses to manage their operations safely and effectively while ensuring compliance with best practices. The standard also outlines the essential components of a risk management system that every risk manager should consider (ISO, 2009, 2018). Effective risk management begins with identifying and addressing potential risks, ultimately creating an environment where risks are minimized (Björnsdottir et al., 2022). Additionally, ISO 31000 emphasizes process improvement, enhancing operational effectiveness, and reducing losses, thereby contributing to greater organizational efficiency and resilience (Sadgrove, 2016; Berger et al., 2022).

## 3. Methodology

Conducting a literature review is a critical component of any academic research process, as it provides the foundation for understanding existing knowledge and identifying research gaps (Cooper, 1988). This essay outlines a systematic methodology for performing an effective literature review, emphasizing the importance of selecting appropriate sources, evaluating study quality, and synthesizing findings. To achieve this, it is essential to precisely define the research topic and establish clear boundaries for the review. As Hart (1998) highlights, a well-defined research problem serves as a guide for the literature search, helping researchers focus on collecting relevant and meaningful information. The process of identifying relevant sources often relies on academic databases, digital libraries, and peer-reviewed scientific journals, which are valuable tools for locating high-quality studies (Palmer, 2005). According to Boote and Beile (2005), the strategic selection of keywords and search terms is fundamental to identifying the most pertinent literature within a specific area of interest.

A crucial aspect of the methodology involves defining inclusion and exclusion criteria for selecting sources. These criteria ensure that only studies aligned with the research objectives are considered. As Snyder (2019) suggests, applying these criteria is vital for maintaining the coherence and relevance of the review. Furthermore, Tranfield, Denyer, and Smart (2003) emphasize the role of quality and relevance standards in preserving the integrity of the review. Similarly, Fink (2005) and Green et al. (2006) advocate for the critical evaluation of literature to ensure the reliability and validity of findings.

### 3.1. The ISO 31000 standard

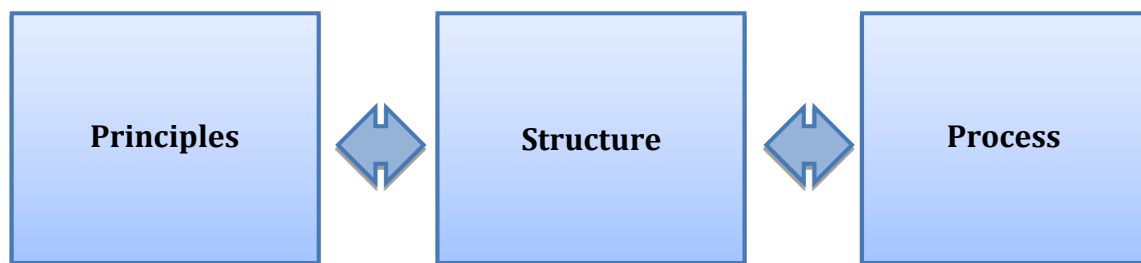
The ISO 31000 guide establishes a comprehensive set of standards for risk management, emphasizing that collaborative implementation is often the most effective approach (Earle, 2010; Fan & Stevenson, 2018; Hardjomidjojo et al., 2022). This

framework supports organizations in developing tailored risk management strategies that align with their unique needs and contexts. Unlike prescriptive guidelines, ISO 31000 provides a flexible approach, enabling organizations to define their own benchmarks based on its principles (Van Greuning & Bratanovic, 2020). By doing so, organizations can effectively manage and control uncertainty in various situations (ISO, 2009, 2018). ISO 31000 defines risk as the effect of uncertainty on achieving objectives, emphasizing its role in creating challenges for individuals or organizations striving to meet their goals (Djapic et al., 2016; Hopkin, 2018). Several key aspects of this definition include:

- Deviations from expected outcomes: Risk arises when actual results differ from anticipated objectives.
- Multidimensional objectives: Risks may impact various areas, such as economic, environmental, financial, and safety concerns, and operate across strategic, operational, and organizational levels.
- Event-based possibilities: Risk involves specific events, their probabilities, and potential consequences for a project or organization's objectives.
- Probability and environmental factors: Risk represents a combination of the likelihood of an event and its environmental effects.
- Uncertainty and its causes: Lack of information, knowledge, or understanding can lead to uncertainty, which increases the difficulty of anticipating and addressing potential consequences.

### 3.1.1. ISO 31000 standard components

Hutchins (2018) states that the ISO 31000 standard for risk management has three related components, which are presented on figure 1.



**Figure 1** Risk Management components (own elaboration). *Source:* UNE-ISO 31000 (2018): Risk management. Principles and guidelines.

To effectively manage risk, organizations must understand how their structure, processes, and principles interrelate and function together (Green & Adams, 2006; Borguesi & Gaudenzi, 2012; Borek et al., 2013; Gallati, 2022). Each of these components plays a vital role, and they must be applied in a balanced and integrated manner. According to ISO 31000, risk management should be implemented iteratively to assist businesses in decision-making, enhance the likelihood of achieving objectives, and deepen their understanding of potential opportunities and risks (Hassani & Hassani, 2016; Barafort et al., 2018; Gallati, 2022). Despite its flexibility, ISO 31000 remains an essential resource for risk assessment programs, especially those seeking external guidance or aiming to align with international standards (Landoll, 2021). Its application helps organizations maintain robust management and governance principles, ensuring that risk management practices are aligned with organizational objectives and sustainability (Aven & Renn, 2010; Renn, 2017; Björnsdottir, 2022).

## 4. Key Definitions and for The Manual in Companies

The ISO 31000 guide, published in 2018, aims to establish the principles and steps necessary for organizations, both public and private, as well as government entities across various sectors, to develop their own risk management methodologies (Barafort et al., 2018; Hoplon, 2018; Hubbard, 2020). The guide includes definitions that help mitigate risks and provide preventive actions, which are essential for addressing events that may lead to the failure of achieving set objectives. The 2018 ISO guide provides the following key definitions:

- Risk: The deviation from the forecast, which can be either positive or negative, and generates uncertainty regarding the achievement of organizational objectives. Risk applies at different levels and across various aspects of an organization.
- Risk management: The process of controlling risks by coordinating the organization's activities to minimize potential negative impacts.
- Stakeholder: Any organization or individual who is, or perceives themselves to be, affected by a decision or action taken by the organization.
- Risk sources: Elements that individually or jointly cause risks within an organization.
- Event: A change in circumstances that may be either expected or unforeseen. Events are not always inevitable; they may be anticipated but not predicted.

- **Consequence:** The outcome of an event that affects the organization's objectives, with effects ranging from negative to positive.
- **Probability:** The likelihood of potential events occurring within a given range of possibilities.
- **Control:** The measures taken to maintain or alter the level of risk associated with a particular situation or decision.

## 5. Principles of Risk Management

The ISO 31000:2018 standards provide a comprehensive framework for risk management, emphasizing the importance of integrating various principles and practices to achieve effective risk control (Fan & Stevenson, 2018; Hutchins, 2018). Successful risk management requires careful consideration of all guiding principles, which should be consistently applied to ensure organizational efficiency (Jaafari, 2001; Stoneburner et al., 2002; Martínez Hernández, 2018). These objectives may vary depending on the risk management framework adopted by individuals within the organization (Hopkin, 2018), but they must be aligned with the organization's goals. Effective risk management involves analyzing results, integrating findings into the risk management process, assigning responsibilities, providing ongoing training, collaborating with third parties, and continuously monitoring performance (Hopkin, 2018; Oyede & Aderibigbe, 2022). Establishing a risk culture is essential, as it fosters a clear framework for managing uncertainty, ensuring organizational resilience and informed decision-making (MacDonald et al., 2012; Martínez et al., 2018; Poljanšek et al., 2019). Since risk management is a cross-functional aspect of business operations, adaptability and dynamism are crucial to meeting challenges across all levels of an organization. This requires having access to the best available information to make well-informed decisions.

### 5.1. Principle 1: Integrated

Every organization must incorporate risk management into its processes, including strategic planning and other significant activities (Pakhchanyan, 2016). The main objective of risk management is to protect the organization's reputation and create value by identifying potential risks associated with its decisions and actions (Sadgrove, 2016; Renn, 2020).

### 5.2. Application of principle 1

When engaging in decision-making activities, organizations must assess the associated risks (Edwards & Bowen, 2013; ISO, 2018). Since organizations cannot regulate external changes, they are always exposed to risk. A risk management plan is essential for mitigating these risks (Lam, 2014). Ambiguity is inherent in organizational environments, where processes and activities occur both internally and externally (Sadgrove, 2016). To instill a strong sense of responsibility for managing risks, it is crucial to integrate risk management frameworks into organizational information systems (Hiles, 2012; ISO, 2018).

### 5.3. Principle 2: Structured and Comprehensive

To achieve optimal efficiency and consistency, risk management must be performed in a systematic, methodical, and predictable manner (Saunders et al., 2021). This approach produces reliable results that can be compared across various projects.

### 5.4. Application of principle 2

To ensure successful implementation, organizations must adopt a comprehensive risk management plan (Hopkin, 2018). Such a plan involves making informed decisions and assessing the risks involved to determine the effectiveness of each choice (Haines, 2011). Timing is crucial in risk assessment; determining when to assess risks is vital to identifying the best approach for mitigation (Borghesi & Gaudenzi, 2012; Aven, 2016).

### 5.5. Principle 3: Adapted

Risk management frameworks must be aligned with organizational objectives and goals, and adapted to both internal and external environments (Tiwari, 2023).

### 5.6. Application of principle 3

ISO 31000 offers a comprehensive framework suitable for any organization, regardless of the risks it faces (Tiwari et al., 2023). However, each organization's unique culture, risk assessment criteria, and operating environment necessitate a customized approach (Albakri et al., 20014). Flexibility and adaptability are crucial for tailoring the risk management framework to meet specific organizational needs (Van Der et al., 2015).

### 5.7. Principle 4: Inclusive

Risk management should involve all relevant stakeholders to remain current and effective (ISO, 2009, 2018). Stakeholders include anyone involved in decision-making at any level of the organization, and they must be represented in determining risk criteria (Poljanšek et al., 2019).

#### *5.8. Application of principle 4*

Organizations should use reflective tools to inform and consult with stakeholders (Jaafari, 2001; Leitch, 2010; Hubbard, 2020). Ensuring that all relevant parties are included in the decision-making process increases the effectiveness of risk management and builds confidence in its outcomes (MacDonald et al., 2012). This principle also requires addressing privacy, security, and confidentiality concerns when implementing risk management theories.

#### *5.9. Principle 5: Dynamic*

Risk management must reflect the speed of organizational change and anticipate disruptions (Stulz, 2008). When changes occur, organizations must react swiftly to stay informed and prepared.

#### *5.10. Application of principle 5*

Risk management processes should account for new objectives or circumstances, both internal and external (Chapman & Ward, 2003). Changes such as new suppliers or legal requirements can alter risk management strategies (Hopkins, 2018; Saunders et al., 2021). Regular monitoring of key metrics is necessary to evaluate whether expectations are met, ensuring ongoing improvements (Marchetti, 2011; Van Greuning & Bratanovic, 2020).

#### *5.11. Principle 6: Best available information*

Effective risk management requires access to a variety of data sources, including historical information, expert opinions, forecasts, and stakeholder input (ISO, 2009, 2018).

#### *5.12. Application of principle 6*

Risk management decisions must be based on the most current information available (Hurne & Gutteling, 2008). The collection of new data is crucial for understanding and mitigating risk (Borek et al., 2013). Clear and precise criteria ensure more reliable risk assessments (Aven, 2017).

#### *5.13. Principle 7: Human and cultural factors*

Understanding how stakeholders perceive the organization and its objectives is crucial for determining how those objectives can be achieved (Earle, 2010). Risk management also considers human skills, intentions, and the surrounding cultural and social context, which can influence decision-making and the identification of risks (Sadgrove, 2016). This principle applies at all stages of risk management, from risk identification to response planning.

#### *5.13. Application of principle 7*

It is essential to recognize that opinions and perceptions can be shaped by human and cultural factors, which affect how risks are viewed and addressed (Tsohou et al., 2006). Common errors in risk management include biases stemming from misunderstandings of time, political or social contexts, failure to recognize warnings, or neglecting the perspectives of others (Hopkins, 2018). By considering these factors, organizations can develop a more holistic understanding of risks and ensure that diverse viewpoints are incorporated into the decision-making process. Effective risk management requires awareness of these influences and integrating them into the risk assessment and mitigation strategies.

#### *5.14. Principle 8: Continuous improvement*

Risk management processes must be continuously updated and refined based on experience and evolving circumstances (Rasmussen & Suedung, 2000). Establishing continuous improvement plans ensures that risk management practices evolve, promoting maturity in management systems and agility in responding to new challenges. Continuous improvement helps build more adaptable teams capable of reacting effectively to unforeseen events.

#### *5.15. Application of principle 8*

Continuous improvement strengthens risk management by reducing uncertainty, facilitating better decision-making, and responding to emerging opportunities. Improved agility allows organizations to act quickly while maintaining flexibility to find and leverage new opportunities. This does not mean taking unnecessary risks, but rather ensuring the adaptive process remains robust and effective (Hopkin, 2018). Organizations should incorporate continuous improvement goals into their risk

management policies, ensuring that these objectives are communicated both formally and informally to employees to encourage ongoing refinement and adaptation (Hopkin, 2018).

By focusing on continuous improvement, organizations create a more resilient risk management framework that can evolve in line with changing circumstances and objectives. Having an integrated risk management approach will allow organizations to focus their resources on preventive rather than corrective actions, which would have a positive impact on the use of resources for mitigation plans or so-called treatments.

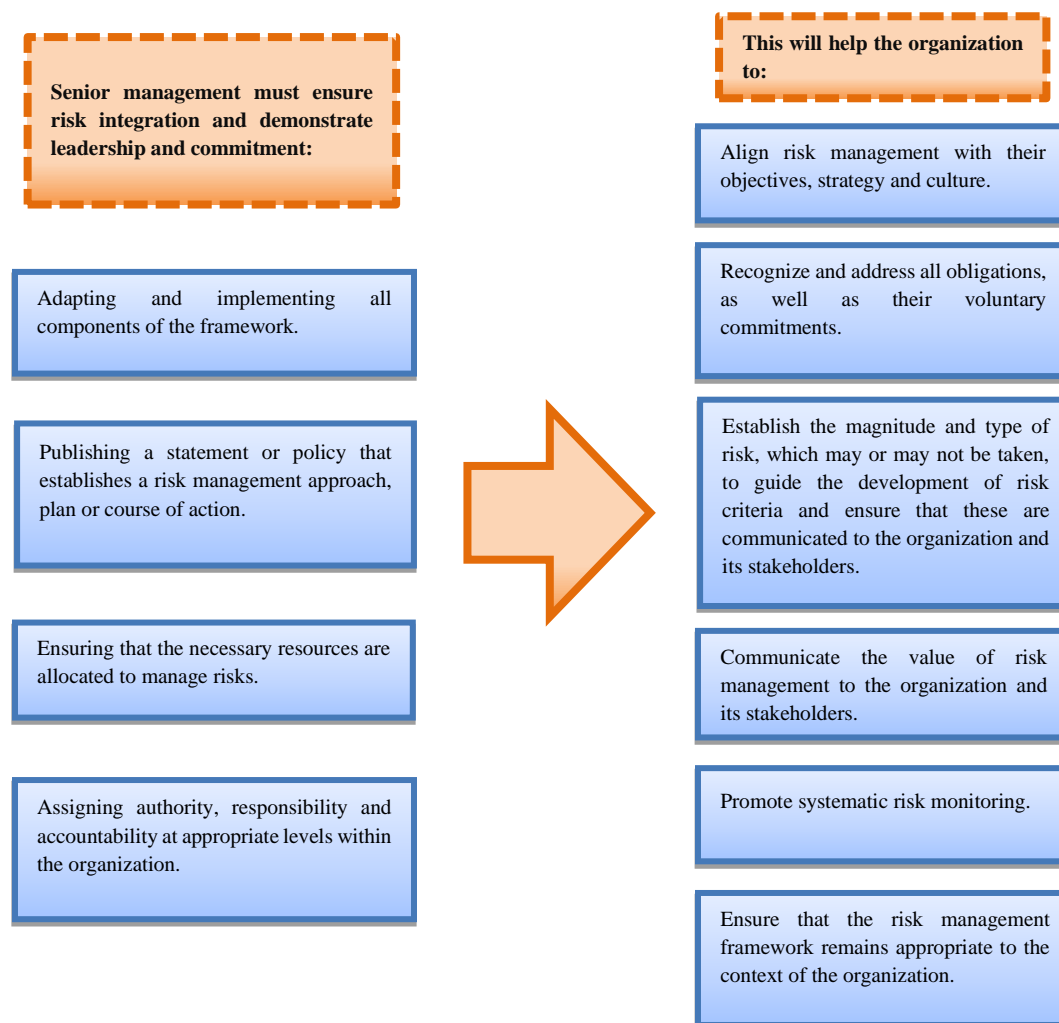
In general, a pure risk is a combination of the probability or frequency of an event and its consequences, which is usually negative. In this article, risk management is defined as a set of financial or operational activities that maximize the value of a company, and that seek to mitigate events that generate non-fulfillment of objectives. Managers' risk behavior (risk appetite and aversion) and corporate governance also affect the choice of risk management activities.

### 6. Risk Management Framework

Organizational risk management requires a robust support structure to function effectively. Any ongoing organizational process must be continually improved and adapted to meet evolving challenges (Salmeron & Lopez, 2010). This can be achieved by implementing best practices and fostering a culture of continuous improvement (Hopkin, 2018). Effective risk management frameworks demand strong corporate governance to ensure their success (Brown et al., 2009; ISO, 2018).

#### 6.1. Leadership and commitment

Risk management requires a strong commitment from organizational leadership to meet objectives. This is so because institutions must set clear goals for risk management and allocate the necessary resources to ensure its effectiveness (Hopkin, 2018). The role of leadership in establishing a risk-aware culture and making risk management a priority is essential for achieving organizational goals, those roles are presented on figure 2.



**Figure 2** The role of top management in risk management (own elaboration). *Source:* UNE-ISO 31000 (2018): Risk management. Principles and guidelines.



## 6.2. Integration

Successful risk management programs require a comprehensive understanding of the organization's context and environment (Hopkin, 2018). This includes an awareness of the organization's goals, methods, and scale. Every aspect of the organization's structure must engage with risk management (Monahan, 2008). Furthermore, all employees share a responsibility for managing risk, emphasizing that risk management is a collective responsibility across the organization (Power, 2007).

Creating an integrated risk management process requires continuous adaptation to the culture and evolving needs of the organization (ISO, 2009). Risk management should be considered an integral part of the organization's purpose, direction, leadership, operations, and overall goals (Stoneburner et al., 2002). It must permeate all levels of the organization to ensure its long-term success and sustainability (Saeidi et al., 2019, Douglas, 2020).

## 6.3. Design

The design of risk management consists of the following elements presented on figure 3.



**Figure 3** Risk management design components (own elaboration). *Source:* UNE-ISO 31000 (2018): Risk management. Principles and guidelines.

## 6.4. Implementation

To effectively manage risk, an organization must establish a comprehensive risk management framework, determining when, how, and by whom the plans will be implemented across all areas (Djapic et al., 2016; Hopkin, 2018). The organization must also define flexible processes that can be adjusted as necessary and assess their existing risk management methods (Tiwari et al., 2023). Successful implementation requires a clear understanding and commitment from all stakeholders, ensuring that the organization is prepared for unexpected uncertainties that may arise (O'Malley, 2013; Aven, 2016). This approach guarantees that risk management remains an ongoing, dynamic process throughout the organization.

## 6.5. Evaluate

To evaluate the efficiency of the risk management framework, the organization should:

- Review the risk controls currently implemented.
- Identify gaps or deficiencies in the risk management process.
- Analyze the impact of the framework on the organization's operations.
- Conduct periodic risk assessments and update the framework as needed.
- Assess whether the framework supports the achievement of organizational objectives.

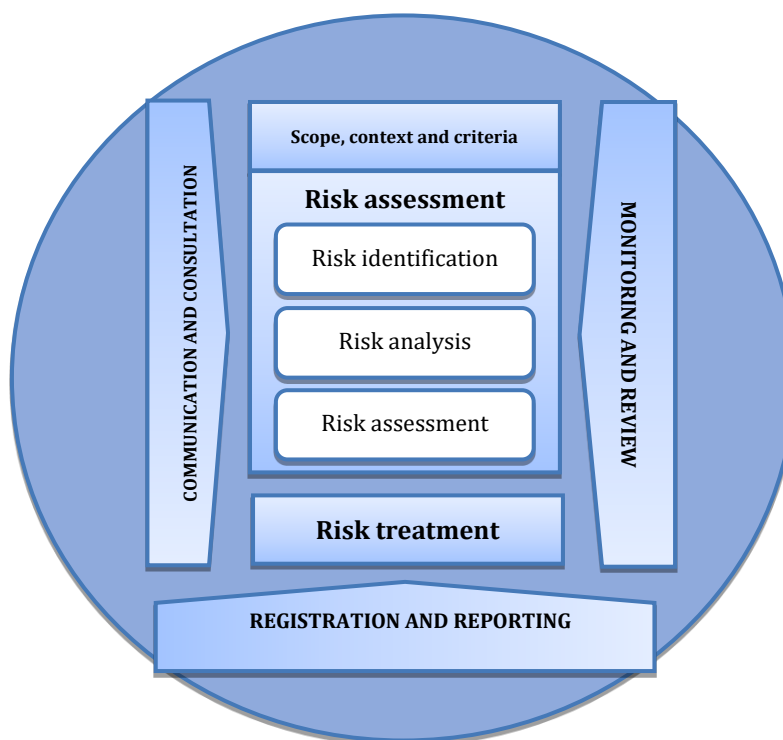
The framework's purpose, implementation plans, performance indicators, and expected outcomes should be evaluated periodically to measure the overall effectiveness of the risk management framework (Albakri et al., 2014; Leveson, 2015; ISO, 2018).

### 6.6. Improvement

- **Adaptation:** Organizations must continuously adjust their risk management framework in response to both internal and external changes (Borek et al., 2013; Hopkin, 2018). This ensures that the framework remains relevant and capable of generating greater value.
- **Continuous improvement:** Risk management frameworks must evolve continuously to address new opportunities and emerging issues (Palmer, 2005; Power, 2007; IRM, 2018). Regular updates and improvements are necessary to enhance the effectiveness of these frameworks (Dafikpaku et al., 2011). All risk management functions require adequate resources from senior management and regulatory bodies, including funding for personnel, tools, processes, and methods to manage risk (Gallati, 2022).
- **Understanding the organization and its context:** It is essential to understand both the external environment and internal operations when developing a risk management framework (ISO, 2018; Luneau & Fourniau, 2021). An organization's context is a critical factor in effective risk management and decision-making, involving an understanding of both internal and external elements that influence operations, goals, and overall performance (ISO, 2018; Fan & Stevenson, 2018).

## 7. The Risk Management Process

ISO 31000 defines risk management as "unified activities that control the organization with respect to risk" (Barafort et al., 2019). It involves the consistent application of policies, procedures, and practices related to risk consultation, communication, context development, assessment, treatment, monitoring, review, evaluation, recording, and reporting (Fink, 2005; ISO, 2009, 2018). The risk management process is presented below on figure 4.



**Figure 4** Risk management process (own elaboration). *Source:* UNE-ISO 31000 (2018): Risk management. Principles and guidelines.

### 7.1. Scope, Context, and Criteria

An effective risk assessment process must be adaptable to meet specific risk criteria across different contexts (Brooks, 2003; Cokins, 2009; Renn, 2017, 2020). Risk management needs to be flexible in order to account for the various contexts surrounding risk assessment and treatment (Aven, 2016; ISO, 2018). This highlights the importance of establishing the principle of scope, context, and criteria in the risk management framework (Schuitema & Hooks, 2024).

#### 7.1.1. Scope definition

Risk management applies at various levels within the organization, so it is essential to properly define its scope when implementing the process (ISO, 2018; Stoneburner et al., 2022). This definition should align with the process objectives and the organization's overall goals.

#### 7.1.2. External context

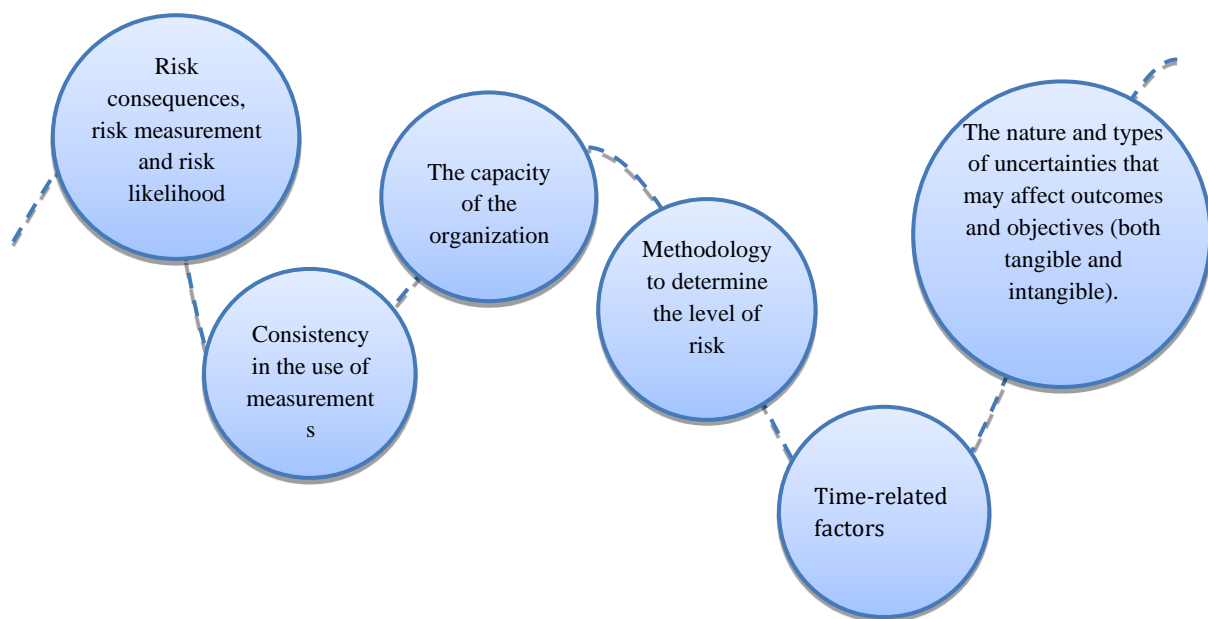
Environments where the company seeks to define and achieve its objectives: Social and cultural environment, Political environment, Legal and regulatory environment, Economic and financial environment, Technological environment, Key drivers and trends affecting the organization's objectives, Relationships with external stakeholders (Arena et al., 2010; Hiles; 2012; Hernandez et al., 2013; ISO 2018).

#### 7.1.3. Internal context

Internal environments where the company seeks to define and achieve its objectives: Vision, mission and values of the organization, Culture of the organization (Kucuk, et. al, 2017). Standards, guidelines and models adopted in the organization, Data, information systems and information flow, Organizational structure, roles and responsibilities, Policies, objectives and techniques implemented to achieve them, Capacity and knowledge of human resources, Relations with internal stakeholders, Contractual relationships and commitments, Interdependencies and interconnections, other groups that have an impact on the organization's objectives (Sadgrove, 2016; Saunders, et al., 2021).

#### 7.1.4. Definition of risk criteria

The risk criteria should be defined to assess the significance of risks and support decision-making processes effectively, those considerations are presented on figure 5.



**Figure 5** Considerations for defining risk criteria (own elaboration). *Source:* UNE-ISO 31000 (2018): Risk management. Principles and guidelines.

#### 7.2. Risk identification

To achieve their objectives, organizations must identify the potential risks and challenges that could hinder their progress (Van Greuning & Bratanovic, 2020). Effective risk identification allows organizations to address potential barriers before they escalate into significant problems (Duque-Grisales & Aguilera-Caracuel 2021).

#### 6.7. Risk analysis

Risk analysis is the process of examining the nature and characteristics of risks. It involves identifying the sources, probabilities, scenarios, controls, and potential outcomes of risks (Monahan, 2008; Aven, 2012; Lam, 2014; Pakhchanyan, 2016; Hopkin, 2018). The complexity and level of detail in risk analysis can vary depending on the purpose and the reliability of the available data (Abdymomunov & Mihov, 2019). The primary goal of risk analysis is to understand the risk's nature, sources, consequences, probabilities, events, and scenarios (Borghesi & Gaudenzi, 2012; Leveson, 2015; Landoll, 2021).

### 6.8. Risk assessment

To determine which risks require attention and prioritization, the analysis generates criteria to assess the severity and significance of the identified risks (Power, 2007; Aven, 2012; ISO, 2018). If the analysis results deviate from the established criteria, the organization must take additional actions to refine the risk assessment (Monahan, 2008; National Research Council et al., 2009; O'Malley, 2013; Sadgrove, 2016; Renn, 2020). The risks initially identified are known as inherent risks. The level of risk or severity is calculated by multiplying the probability of occurrence or frequency by the impact or consequence (Hopkins, 2018; Tiwari et al., 2023). Once the risks are documented, communicated, and validated by the relevant authorities, stakeholders can decide on the appropriate course of action (Aven, 2012; Van Der Vegt et al., 2015; ISO, 2018).

### 6.9. Risk treatment

After calculating the severity of risks, the next step is to design action plans that aim to mitigate the risks, starting with the most severe (those deemed intolerable), then addressing tolerable risks, and finally reviewing those that are considered acceptable (Salmeron & Lopez, 2010; Leveson, 2015; Kucuk et al., 2017; Landoll, 2021). Risk accumulation involves analyzing risks thoroughly and determining whether they are acceptable or unacceptable (Rasmussen & Suedung, 2000; Aven, 2012; ISO, 2018; Poljanšek et al., 2019).

Once deemed acceptable, the risk is implemented and evaluated. This process must be repeated until the risk no longer poses a significant threat to individuals or the organization (Van Greuning & Bratanovic, 2020). The two variables with which the risks are measured are the level of probability of occurrence and the impact or consequence, the value of each one, it is recommended between 1 and 5. The multiplication of both allows us to obtain the level of risk or severity, which ranges from 1 as a minimum value to 25 as a maximum level. The important thing is that with these values there are three groups of risks, non-tolerable, tolerable and acceptable, which allows the next stage to be deployed, such as the development of action or mitigation plans or treating the risks.

### 6.10. Recording and reporting (database)

Recording and reporting involve sharing information regarding risk management efforts across the organization to enhance management's understanding of the situation (Borguesi & Gaudenzi, 2012; Hopkin, 2018; Hubbard, 2020). This transparency fosters closer interaction with relevant parties. Importantly, reporting and logging involve all individuals engaged in the risk management process (Abdymomunov & Mihov, 2019; Saunders et al., 2021; Nademar, 2024). Key factors to consider in reporting include:

- Stakeholders and their specific information needs and requirements
- The cost, frequency, and timing of the report
- The methodology used for reporting
- The relevance of the information to the organization's objectives and decision-making (Tiwari et al., 2023; Schuitema & Hooks, 2024).

### 7.7. Communication and consultation

The primary objective of risk management is to provide information that explains the rationale behind decisions, including associated risks (Aven & Renn, 2010). This information aims to enhance understanding, guiding individuals to seek consultation and stay vigilant about potential risks (Renn, 1998, 2020; Luneau & Fourniau, 2021). Throughout the risk management process, communication and consultation with stakeholders are essential (Luneau & Fourniau, 2021; Berger et al., 2022; Curti et al., 2023). Effective coordination ensures timely, relevant, and accurate exchange of information, fostering informed decision-making and a collaborative approach to managing uncertainties (Schuitema & Hooks, 2024). Transparent communication empowers decision-makers to address risks more effectively (Aven & Renn, 2010; Hiles, 2012; IRM, 2018; Snyder, 2019).

### 7.8. Monitoring and review

The goal of using process metrics is to improve the quality and efficiency of the design, implementation, and results of risk management processes (Haimes, 2005, 2011; Abdymomunov & Mihov, 2019; Tiwari et al., 2023). This requires gathering and analyzing information, recording results, and providing feedback throughout the process. Regular review and analysis of performance results should be integrated into the organization's management, measurement, and reporting activities. Key goals for risk monitoring and review include:

- Accessing additional information about specific risk assessments to improve efficiency.
- Leveraging the understanding of events, changes, trends, successes, and failures for the organization's benefit.

- Identifying relevant changes in the external context and fluctuations in the organization's internal state to prioritize risk treatment changes.
- Recognizing emerging risk trends to address them proactively.

## 8. Final Considerations

The ISO 31000 guide provides organizations with a structured approach to develop an efficient, tailored risk management strategy. It enables organizations to allocate resources effectively, manage risks, and recognize both opportunities and threats, ultimately improving operational efficiency and reducing losses. While ISO 31000 is recognized for its versatility, it must be tailored to the specific leadership, management practices, information processes, and policies of each organization.

Risk management is particularly valuable for businesses in developing countries, where the identification and assessment of risks—such as political instability, regulatory changes, or resource constraints—are crucial for maintaining operations. By understanding and evaluating these risks systematically, organizations can reduce their impact and protect their operations from potential disruptions.

Response planning is a crucial component of risk management. This entails laying down steps to address risks that have been recognized, such as acceptance, transfer, mitigation, or elimination strategies. Proactive and efficient risk management is ensured for enterprises through effective reaction planning. Furthermore, communicating with both internal and external stakeholders is essential to comprehending and managing risks. This partnership improves risk management and encourages well-informed decision-making.

Organizations must incorporate risk management into their culture to ensure long-term sustainability. Embedding preventive measures into organizational culture enables companies to reduce the impact of unexpected events and achieve their goals more effectively. Future research should investigate how risk management fosters strategic planning across short, medium, and long terms to prevent incidents and minimize potential harm.

Risk management is indispensable for the sustainability and growth of companies in emerging economies. In volatile economic, political, and financial environments, risk management practices are essential to mitigate potential threats and seize available opportunities. Implementing preventive measures and contingency plans helps businesses forecast and manage future challenges, improving organizational resilience and adaptability while minimizing the likelihood of financial losses and reputational damage.

Furthermore, risk management contributes to enhancing the efficiency and effectiveness of business operations. By identifying and prioritizing significant risks, organizations can optimize resource allocation, focus efforts on critical areas, and maximize growth opportunities, even in uncertain and ever-changing environments. Improving a company's credibility and capacity to engage stakeholders is another significant advantage of risk management (Nademar, 2024). Companies that prioritize security and corporate integrity enhance their brand reputation, foster positive relationships with investors and customers, and secure long-term growth.

Research into how small and medium-sized enterprises (SMEs) in Latin America implement ISO 31000 can offer valuable insights. Compared to larger firms, SMEs often face distinct resource limitations and operational challenges, making their adoption of risk management practices particularly instructive. Additionally, studies on how Latin American cultures influence the adoption and modification of ISO 31000 norms can shed light on the role of managerial techniques, corporate culture, and risk perception in the region. Sector-specific research on industries like mining, banking, agriculture, and healthcare can highlight challenges, best practices, and regulatory impacts unique to these sectors.

ISO 31000 can also be integrated with other frameworks commonly used in Latin America, such as ISO 14001 (environmental management) and ISO 9001 (quality management). Research in this area can explore conflicts, synergies, and solutions for harmonizing multiple standards. Longitudinal studies could assess how the implementation of ISO 31000 improves organizational resilience and performance over time, especially in the context of Latin American countries.

Further research could investigate the role of emerging technologies, such as artificial intelligence and blockchain, in enhancing risk management practices aligned with ISO 31000 in Latin American organizations. Additionally, exploring the impact of legal and regulatory frameworks on the adoption and implementation of ISO 31000 can provide valuable insights into compliance requirements, government incentives, and regulatory barriers.

In conclusion, risk management is essential for the success and sustainability of organizations in emerging economies. By adopting proactive and systematic approaches to identifying, assessing, and mitigating risks, organizations can strengthen their management capabilities, improve operational resilience, and capitalize on growth opportunities in dynamic and competitive business environments.

## 9. Future Research Directions

Future research should explore the effects of risk management on small and medium-sized businesses (SMEs), particularly in sectors that contribute significantly to the GDP of Latin American countries and generate formal employment.

This paper outlines the components that SMEs must incorporate into their risk management manuals to ensure comprehensive and transversal risk management practices. Researchers can also test this model in various empirical settings, such as other developing economies or specific sectors of the economy. Within the framework of protection and value creation, an important component to investigate is the development and potential updating of the ISO 31000 guide.

### Ethical Considerations

Not applicable.

### Conflict of Interest

The authors declare no conflicts of interest.

### Funding

This research did not receive any financial support.

### References

- Abdymomunov, A., & Mihov, A. (2019). Operational risk and risk management quality: Evidence from US bank holding companies. *Journal of Financial Services Research, 56*(1), 73-93.
- Abel Bernal, Carlos Rosen, Enrique Yacuzzi y Espedito Passarella. (2011). Ideas innovadoras para una mejor práctica de negocios. *Revistas de temas de management, 3*, 12.
- Albakri, S. H., Shanmugam, B., Samy, G. N., Idris, N. B., & Ahmed, A. (2014). Security risk assessment framework for cloud computing environments. *Security and Communication Networks, 7*(11), 2114-2124.
- AL-kiyumi, R. K., AL-hattali, Z. N., & Ahmed, E. R. (2021). Operational risk management and customer complaints in Omani banks. *Journal of Governance and Integrity, 5*(1), 200-210.
- Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organizations and Society, 35*(7), 659-675.
- Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research, 253*(1), 1-13.
- Aven, T. (2017). How some types of risk assessments can support resilience analysis and management. *Reliability Engineering & System Safety, 167*, 536-543.
- Aven, T., & Renn, O. (2010). Risk management and governance: Concepts, guidelines and applications (Vol. 16). *Springer Science & Business Media*.
- Barafort, B., Mesquida, A. L., & Mas, A. (2018). Integrated risk management process assessment model for IT organizations based on ISO 31000 in an ISO multi-standards context. *Computer Standards & Interfaces, 60*, 57-66.
- Barafort, B., Mesquida, A. L., & Mas, A. (2019). ISO 31000-based integrated risk management process assessment model for IT organizations. *Journal of Software: Evolution and Process, 31*(1), e1984.
- Baranoff, E.G. (2001), "The risk balls game: transforming risk and insurance into tangible concepts", *Risk Management and Insurance Review, Vol. 4 No. 2*, pp. 51-58.
- Berger, A. N., Curti, F., Mihov, A., & Sedunov, J. (2022). Operational risk is more systemic than you think: Evidence from US bank holding companies. *Journal of Banking & Finance, 143*, 106619.
- Björnsdóttir, S. H., Jensson, P., Thorsteinsson, S. E., Dokas, I. M., & de Boer, R. J. (2022). Benchmarking ISO Risk Management Systems to Assess Efficacy and Help Identify Hidden Organizational Risk. *Sustainability, 14*(9), 4937.
- Borek, A., Parlikad, A. K., Webb, J., & Woodall, P. (2013). Total information risk management: maximizing the value of data and information assets. *Newnes*.
- Borghesi, A., & Gaudenzi, B. (2012). Risk management: How to assess, transfer and communicate critical risks (Vol. 5). *Springer Science & Business Media*.
- Brooks, N. (2003). Vulnerability, risk and adaptation: A conceptual framework. *Tyndall Centre for climate change research working paper, 38*(38), 1-16.
- Chapman, C., & Ward, S. (2003). Project risk management processes, techniques and insights. *John Wiley & Sons Ltd*.
- Cokins, G. (2009). Performance management: Integrating strategy execution, methodologies, risk, and analytics. *John Wiley & Sons*.
- Cooper, H. M. (1988). Organizing knowledge synthesis: A taxonomy of literature reviews. *Knowledge in Society, 1*(1), 104-126.
- Curti, F., Gerlach, J., Kazinnik, S., Lee, M., & Mihov, A. (2023). Cyber risk definition and classification for financial risk management. *Journal of Operational Risk, 18*(2).
- Dafikpaku, E., Eng, M. B. A. B., & Mcmi, M. (2011, March). The strategic implications of enterprise risk management: A framework. *In ERM Symposium (Vol. 48)*.
- Djapic, M., Lukic, L., & Pavlovic, A. (2016). Technical product risk assessment: standards, integration in the erm model and uncertainty modeling. *International Journal for Quality Research, 10*(1), 159.
- Douglas, M. (2020). Risk as a forensic resource. *In Risk Management (pp. 1-16)*. *Routledge*.
- Duque-Grisales, E., & Aguilera-Caracuel, J. (2021). Environmental, social and governance (ESG) scores and financial performance of multilatinas: Moderating effects of geographic international diversification and financial slack. *Journal of Business Ethics, 168*(2), 315-334.
- Earle, T. C. (2010). Trust in risk management: A model-based review of empirical research. *Risk Analysis: An International Journal, 30*(4), 541-574.
- Edwards, P., & Bowen, P. (2013). Risk management in project organisations. *Routledge*.
- Fan, Y., & Stevenson, M. (2018). A review of supply chain risk management: definition, theory, and research agenda. *International journal of physical distribution & logistics management, 48*(3), 205-230.

- Fernández Sanz, Luis; Bernad Silva, Pedro. (2014). Gestión de riesgos en proyectos de desarrollo de software en España: estudio de la situación. *Revista Facultad de Ingeniería Universidad de Antioquia*, núm. 70, 233-243.
- Fink, A. (2005). Conducting research literature reviews: From the Internet to paper. *Sage Publications*.
- Gallati, R. R. (2022). Risk management and capital adequacy. McGraw-Hill.
- Green, B. N., Johnson, C. D., & Adams, A. (2006). Writing narrative literature reviews for peer-reviewed journals: Secrets of the trade. *Journal of Chiropractic Medicine*, 5(3), 101-117.
- Haimes, Y. Y. (2005). Risk modeling, assessment, and management. *John Wiley & Sons*.
- Haimes, Y. Y. (2011). Risk modeling, assessment, and management. *John Wiley & Sons*.
- Hardjomidjojo, H., Pranata, C., & Baigorria, G. (2022, July). Rapid assessment model on risk management based on ISO 31000: 2018. In *IOP Conference Series: Earth and Environmental Science (Vol. 1063, No. 1, p. 012043)*. IOP Publishing.
- Hart, C. (1998). Doing a literature review: Releasing the social science research imagination. *Sage Publications*.
- Hassani, B., & Hassani, B. K. (2016). Scenario analysis in risk management. *Springer International Publishing Switzerland*.
- Hiles, A. (2012). Enterprise risk management. *The definitive handbook of business continuity management*, 1-21.
- Hopkin, P. (2018). Fundamentals of risk management: understanding, evaluating and implementing effective risk management. *Kogan Page Publishers*.
- Hubbard, D. W. (2020). The failure of risk management: Why it's broken and how to fix it. *John Wiley & Sons*.
- Hutchins, G. (2018). ISO 31000: 2018 enterprise risk management. *Greg Hutchins*.
- Huurne, E. T., & Gutteling, J. (2008). Information needs and risk perception as predictors of risk information seeking. *Journal of risk research*, 11(7), 847-862.
- IRM. (2018). Standard Deviations: A Risk Practitioners Guide to ISO 31000. *Institute of Risk Management*.
- ISO, I. (2009). Risk management—Principles and guidelines. *International Organization for Standardization, Geneva, Switzerland*.
- ISO. (2018). Risk management - Guidelines. *Geneva: International Organization for Standardization (ISO)*.
- Jaafari, A. (2001). Management of risks, uncertainties and opportunities on projects: time for a fundamental shift. *International journal of project management*, 19(2), 89-101.
- Kucuk Yilmaz, A., Flouris, T., Yilmaz, A. K., & Flouris, T. (2017). Enterprise risk management in terms of organizational culture and its leadership and strategic management. *Corporate risk management for international business*, 65-112.
- Lam, J. (2014). Enterprise risk management: from incentives to controls. *John Wiley & Sons*.
- Landoll, D. (2021). The security risk assessment handbook: A complete guide for performing security risk assessments. *CRC press*.
- Leitch, M. (2010). "ISO 31000:2009 – the new international standard on risk management: Perspective", *Risk Analysis*, Vol. 30 No. 6, pp. 887-892.
- Leveson, N. (2015). A systems approach to risk management through leading safety indicators. *Reliability engineering & system safety*, 136, 17-34.
- Luneau, A., & Fourniau, J. M. (2021). Involving stakeholders in the risk regulation process: the example of ANSES. *Journal of Risk Research*, 24(6), 740-755.
- MacDonald, N. E., Smith, J., & Appleton, M. (2012). Risk perception, risk management and safety assessment: what can governments do to increase public confidence in their vaccine system?. *Biologicals*, 40(5), 384-388.
- Marchetti, A. M. (2011). Enterprise risk management best practices: From assessment to ongoing compliance. *John Wiley & Sons*.
- Martínez Hernández, Rosalba, & Pastor Pérez, María del Pilar. (2018). Relationship between risk and innovation: Risk perception by project managers. *Journal of technology management & innovation*, 13(2), 94-103.
- Monahan, G. (2008). Enterprise risk management: A methodology for achieving strategic objectives. *John Wiley & Sons*.
- Nandemar, D. (2024). Fraud risk judgments performance: The role of audit technology, task structure, and auditor competence. *Multidisciplinary Science Journal*, 6(9), 2024180-2024180.
- National Research Council, Division on Earth, Life Studies, Board on Environmental Studies, & Committee on Improving Risk Analysis Approaches Used by the US EPA. (2009). *Science and decisions: advancing risk assessment*.
- O'Malley, P. (2013). Risk and responsibility. In *Foucault and political reason* (pp. 189-207). Routledge.
- Oyede, S. A., & Aderibigbe, F. O. (2022). Moderating Effect of Internal Control Activities on Risk Assessment and Performance of Insurance Companies in Nigeria. *Gusau International Journal of Management and Social Sciences*, 5(1), 1-18.
- Pakhchanyan, S. (2016). Operational risk management in financial institutions: A literature review. *International Journal of Financial Studies*, 4(4), 20.
- Palmer, C. L. (2005). Scholarly work and the shaping of digital access. *Journal of the American Society for Information Science and Technology*, 56(11), 1140-1153.
- Poljanšek, K., Casajus Valles, A., Marin Ferrer, M., De Jager, A., Dottori, F., Galbusera, L., ... & Wood, M. (2019). *Recommendations for national risk assessment for disaster risk management in EU. Luxembourg, Publications Office of the European Union*.
- Power, M. (2004). The risk management of everything. *The Journal of Risk Finance*, 5(3), 58-65.
- Power, M. (2007). Organized uncertainty: Designing a world of risk management. *Oxford University Press, USA*.
- Pritchard, C. L., & PMP, P. R. (2014). Risk management: concepts and guidance. *CRC Press*. The goal of using process metrics is to improve the quality and efficiency of the design, implementation and results of a process.
- Rasmussen, J., & Suedung, I. (2000). Proactive risk management in a dynamic society. *Swedish Rescue Services Agency*.
- Renn, O. (1998). The role of risk perception for risk management. *Reliability engineering & system Safety*, 59(1), 49-62.
- Renn, O. (2017). Risk governance: coping with uncertainty in a complex world. *Routledge*.
- Renn, O. (2020). Risk communication: Insights and requirements for designing successful communication programs on health and environmental hazards. In *Handbook of risk and crisis communication* (pp. 80-98). Routledge.
- Sadgrove, K. (2016). The complete guide to business risk management. *Routledge*.

- Saeidi, P., Saeidi, S. P., Sofian, S., Saeidi, S. P., Nilashi, M., & Mardani, A. (2019). The impact of enterprise risk management on competitive advantage by moderating role of information technology. *Computer standards & interfaces*, 63, 67-82.
- Salmeron, J. L., & Lopez, C. (2010). A multicriteria approach for risks assessment in ERP maintenance. *Journal of systems and software*, 83(10), 1941-1953.
- Sanchez, H., Robert, B., Bourgault, M., & Pellerin, R. (2009). Risk management applied to projects, programs, and portfolios. *International journal of managing projects in Business*, 2(1), 14-35.
- Saunders, A., Cornett, M. M., & Erhemjants, O. (2021). *Financial institutions management: A risk management approach*. McGraw-Hill.
- Schuitema, G., & Hooks, T. (2024). Promoting voluntary risk detection behaviour: an intervention study based on trending social norms combined with emotional appeals. *Journal of Risk Research*, 1–16.
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of business research*, 104, 333-339.
- Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *Nist special publication*, 800(30), 800-30.
- Stulz, R. M. (2008). Risk management failures: What are they and when do they happen?. *Journal of Applied Corporate Finance*, 20(4), 39-48.
- Tiwari, S., Sharma, P., Choi, T. M., & Lim, A. (2023). Blockchain and third-party logistics for global supply chain operations: Stakeholders' perspectives and decision roadmap. *Transportation Research Part E: Logistics and Transportation Review*, 170, 103012
- Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management*, 14(3), 207-222.
- Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2006). Formulating information systems risk management strategies through cultural theory. *Information Management & Computer Security*, 14(3), 198-217.
- Van Der Vegt, G. S., Essens, P., Wahlström, M., & George, G. (2015). Managing risk and resilience. *Academy of Management Journal*, 58(4), 971-980.
- Van Greuning, H., & Bratanovic, S. B. (2020). Analyzing banking risk: a framework for assessing corporate governance and risk management. *World Bank Publications*.