Harmony Alliance Guides:
Risk Management

Risk Management

THE SOCIAL POLICY GROUP

Risk Management

Securing the Continued and Future Success of the Organisation

Risk is defined as the uncertainty in achieving the organisation's objectives, measured in terms of impact and probability. Risk management is the process of mitigating that uncertainty to ensure the future success of the organisation.

Effective risk management starts with the Board and is a critical responsibility of management. It involves identifying, assessing, and addressing risks that could impede the organisation's ability to meet its goals and objectives. By actively managing risk, organisations can better prepare for potential challenges and create a solid foundation for future growth and success.

This guide covers the essential aspects of risk management, offering strategies for identifying and handling risks.

What is Risk?

For many, risk is seen as something dangerous to be avoided. However, risk is more than just a threat. The word "risk" comes from the early Italian verb *riscare*, meaning 'to dare'—taking action despite uncertainty about the outcome, whether good or bad.

According to **AS ISO 31000:2018 standard for risk management**, risk is defined as *"the effect of uncertainty on objectives"*.[1]

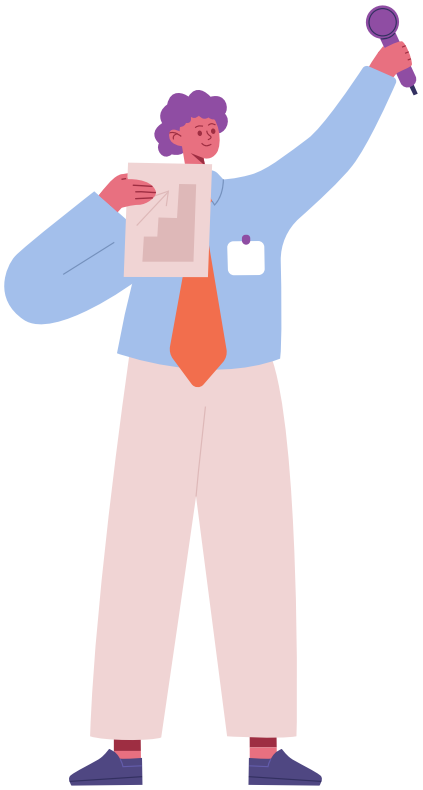
In reality, decisions cannot be made, and any organisation cannot move forward, without taking risks. Rejecting all opportunities in the name of 'managing risk' is not fulfilling the goals of good governance or good management.

What is Risk Management?

The **AS ISO 31000:2018 standard** defines risk management as *"a coordinated set of activities to direct and control an organisation with regard to risk"*. It is a fundamental responsibility for governance and management. As part of the organisation's process, risk management can be broken down into six activities:

1. Understanding the context.
2. Identifying risks and determining tolerances.
3. Measuring, quantifying, and assessing risks.
4. Making decisions on how to manage risks.
5. Monitoring and reporting risks.
6. Overseeing, evaluating, assessing, and refining the risk management process/system.

Risk management is an essential aspect of good governance and effective management. It aims to eliminate or reduce the likelihood of harm to people, property or the business (whether financial, reputation, or otherwise). It should be applied whenever there is a risk of undesired or unexpected outcomes that could have a significant impact.

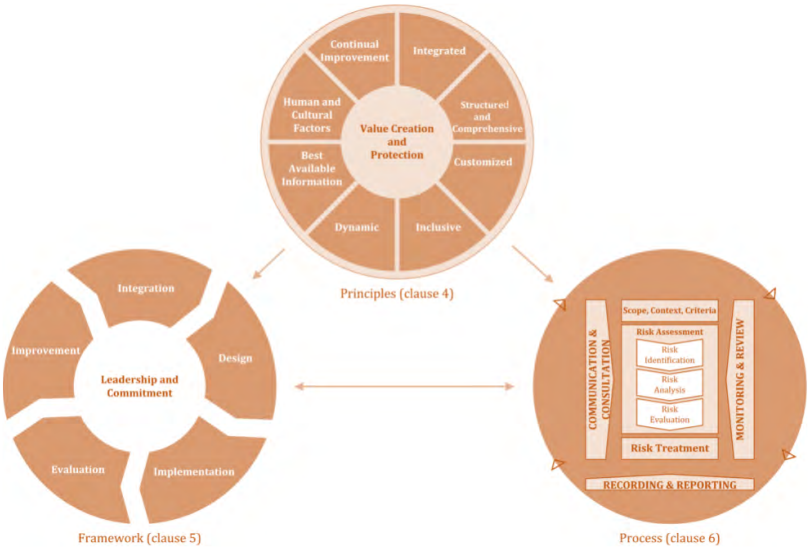


1. Standards Australia, AS ISO 31000:2018, Risk Management - Guidelines

Risk Management

Risk Management Framework - AS ISO 31000:2018

Risk management is essential for not-for-profit (or for-purpose) organisations to ensure the continuity of their mission and the protection of resources. A structured risk management process, in alignment with the **AS ISO 31000:2018** framework, helps organisations navigate uncertainties and achieve their objectives.



Effective risk management is about creating and protecting value. The following principles, as outlined in the **AS ISO 31000:2018 standard**, provide the foundation for a strong risk management process:

1. **Integrated**
   Risk management should be embedded in all organisational activities and decision-making processes. It is not a standalone function but a core part of the organisation's operations.
2. **Structured and Comprehensive**
   A structured, organised approach to risk management leads to consistent and reliable outcomes, ensuring all aspects of risk are addressed systematically.
3. **Customised**
   The risk management process must be tailored to the organisation's unique context, including its goals, internal environment, and external factors. This ensures that the approach is relevant and proportional to the risks faced.
4. **Inclusive**
   Involving stakeholders in the risk management process ensures that their perspectives, knowledge, and concerns are considered. This helps improve awareness and leads to better-informed decisions.
5. **Dynamic**
   Risks evolve as the organisation's internal and external environment changes. Effective risk management is flexible and responsive, constantly monitored and adapted to emerging risks.
6. **Best Available Information**
   Risk management relies on up-to-date, accurate information, including historical data, current insights, and future projections. It is essential to acknowledge any uncertainties and limitations in the available information to make informed decisions.
7. **Human and Cultural Factors**
   Human behaviour and organisational culture play a key role in how risks are identified, assessed, and managed. Understanding these factors is critical at every stage of the risk management process.
8. **Continual Improvement**
   Risk management processes should be continuously improved through learning from experience, feedback, and changing circumstances. This ensures the process remains effective and relevant over time.

Risk Management

Risk Management Roles of the Board

Risk management begins with the Board's leadership and oversight.

The Board has the following key responsibilities:

- **Set the Risk Appetite:** Define the level of risk the organisation is willing to accept in pursuit of its objectives.
- **Establish the Risk Management Structure:** Determine the most appropriate framework and processes for managing risk, ensuring both the Board and management are aligned and equipped to address risks effectively.
- **Embed Risk Management into Governance:** Integrate risk management into the organisation's governance practices to ensure both current and emerging risks are identified, understood, and addressed.
- **Monitor and Report on the Risk Management System:** Oversee the implementation and performance of the risk management system, ensuring it operates effectively and reporting progress regularly.

It is essential that these roles are carried out within the context of the organisation's culture. Even the most well-designed risk management systems will not succeed unless the culture actively supports the organisation's risk appetite, structure, processes, and systems.

Risk Appetite and its Connection to Strategy

One of the most critical aspects of risk management is determining the organisation's risk appetite. This is typically established by the Board, often in collaboration with management. Risk appetite can take various forms; for example, some organisations create a risk appetite statement that outlines their tolerance for risk across different areas.

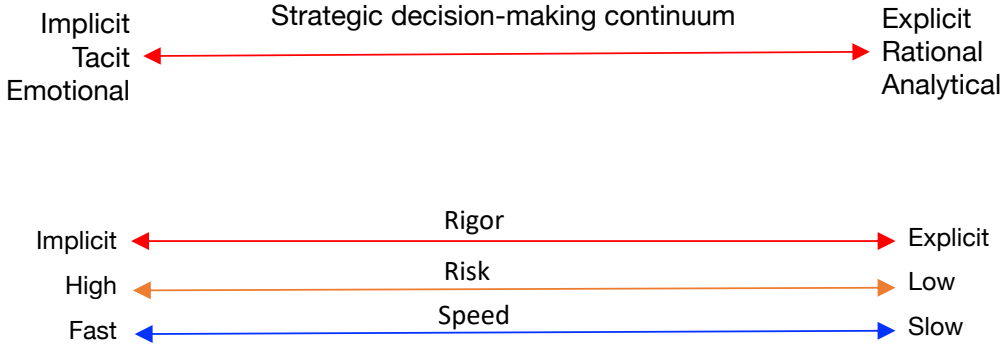
For instance, the organisation may have a higher tolerance for risk in new business ventures, such as mergers and acquisitions, but have zero tolerance for risk in areas like Workplace Health and Safety.

Once defined, the risk appetite sets clear boundaries for decision-making regarding risk. As a result, the risk appetite is intrinsically linked to the development of the organisation's strategy, guiding decisions in alignment with the level of risk the organisation is willing to take on.

The Decision-Making Continuum

The decision-making continuum describes how Boards, managers, and leadership teams approach decisions. It ranges from implicit, gut-feeling decisions (which can sometimes be emotional) at one end, to highly explicit, rational, and analytical decisions at the other.

The trade-off between rigour, speed, and risk is an essential aspect of this continuum.



Risk Management

Bias Towards Explicit Decision-Making

In many organisations, decision-making tends to lean toward the explicit end of the continuum. This often involves rigid processes and controls designed to ensure decisions are rational and minimise risk. For instance, business plans are required, spreadsheets are filled out, analyses can become overly detailed, and decisions are scrutinised through multiple layers of signoffs. For larger decisions, the process may even involve consulting with external firms at considerable expense to provide strategic recommendations.

While these steps ensure thoroughness and risk mitigation, the question remains:

Does this result in more effective decision-making?

The answer is not clear-cut. Research into the quality of decision-making is limited, as it may be difficult to separate the decision itself from its execution. However, one key finding from strategic management research is that the quality of a decision is closely tied to how quickly the decision is made. The problem is processes that demand explicit decision-making tend to slow down the decision-making process. While some decisions benefit from more deliberation, in general, making a decision in a timely manner is often more effective.

Trade-offs Between Speed and Risk

The natural assumption might be that moving down the continuum toward faster decision-making means higher risk, but effective decision-making is not simply about moving faster.

Three Types of Decision-Making Archetypes

Organisations typically operate with one of three decision-making archetypes:

1. **Slow:** Decisions are made with extensive analysis and process, often at the expense of timeliness.
2. **Accelerated:** A balance between speed and thoroughness, decisions are made faster with adequate analysis.
3. **Fast:** The ideal approach. Managers shift along the continuum as needed, making decisions quickly and with confidence, based on available information. They dive deep into areas where they lack knowledge and move quickly when the probability of success is high (generally when the probability is above 70%).

Managers who adopt the **"Fast"** approach update their **tacit knowledge** by staying actively engaged with both internal and external stakeholders. They have systems in place to monitor relevant information, tapping into competitive knowledge sources. They make decisions that align with the organisation's **risk appetite**, balancing speed, risk, and rigour.

In these cases, **strategic thinking** is not hindered by overly complicated processes. Instead, the decision-making system is aligned with the focus on making informed, timely decisions, while managing risks in accordance with the organisation's established risk appetite. This allows leaders to move confidently on the decision-making continuum and adapt based on the situation at hand.

Risk Management

Risk Taking

As previously mentioned, an overemphasis on strict compliance with processes and procedures can stifle innovation, creativity, and strategic thinking—critical elements of competitive advantage. This focus on compliance can sometimes hinder value creation, which is contrary to the goal of risk management as outlined in **AS ISO 31000:2018**.

Board members of not-for-profit (or for-purpose) organisations must recognise that risk management is not about eliminating risk entirely. Rather, it is about managing the risks taken in pursuit of the organisation's strategic objectives. This is where the Board's role in establishing a clear **risk appetite** and fostering a supportive culture becomes crucial.

A defined risk appetite provides clarity and empowers the organisation to take calculated risks within certain boundaries. These boundaries might include avoiding unacceptable risks, such as breaching organisational delegations of authority or violating laws and regulations. With a clear risk framework in place, the organisation can make informed decisions that balance risk-taking with value creation, ensuring progress while protecting against potential setbacks.

Types of Risk

There are three main types of risk that organisations face:

1. **Strategic Risk** Strategic risks are those that could affect the organisation's ability to achieve its goals and objectives. These risks tend to have significant consequences and are typically discussed at the Board level.	Examples of strategic risks include: • Climate change impacts. • Change in consumer and competitor behaviour. • Shifts in government policy. • Economic fluctuations, both positive and negative. • Failure to act on strategic opportunities or threats. • Loss of the CEO or other key leadership.
2. **Financial Risk** Financial risks are those that affect the organisation's financial stability, particularly its ability to remain solvent.	Examples of financial risks include: • Overdue creditors and debtors. • Project budget overruns. • Change to interest rates or currency and commodity markets. • Increased costs or expense blowouts in the cost of doing business (CODB).
3. **Operational Risk** Operational risks relate to the day-to-day functions of the organisations and include risks arising from failed internal processes, people, systems or external events. These risks are primarily managed by the organisation's management team with the Board providing oversight.	Examples of operational risks include: • Workplace health and safety (WHS) issues. • Loss of key personnel. • Legal compliance challenges. • Industrial action. • Equipment or systems failure. • Cybersecurity failures. • Payroll process failures.

Risk Management

Within any of the abovementioned types of risks, reputational risk may emerge. There are issues that, when publicised—particularly on social media or in major news outlets—can damage the organisation's reputation. Reputational risks are often tied to community or social expectations and can stem from any of the risk types outlined above.

Not every risk requires the same level of management or attention. Successful organisations focus their efforts on the risks that are the most critical to their sustainability and growth.

Risk Management Structures

Risk management structures and mechanisms for coordinating and ensuring risk management functions within an organisation will differ depending on the organisation's size and nature. A large, publicly listed company will likely have an extensive and comprehensive structure, while smaller not-for-profits (or for-purpose) organisations, such as those in the settlement sector, will have simpler structures. Regardless of size, these structures must be fit for purpose and add value. They are established by the Board and operated by management.

Several key elements of a risk management structure can be implemented, depending on the size and form of the organisation:

a. Committees

Boards can establish committees to delegate specific risk responsibilities and oversee particular areas of risk. These committees may include:

- Audit & Risk.
- Finance.
- Workplace Health and Safety (WHS).
- Clinical governance.
- Environmental Risk.
- Quality.

The composition of these committees should ensure relevant expertise is provided by membership. Each committee should have a clear Terms of Reference to define its responsibilities and purpose, while also acknowledging that the Board holds overall responsibility for the committee's actions.

b. Internal Audit Function

An internal audit function plays a critical role in the risk management structure by conducting compliance audits, post-implementation reviews, and operational reviews throughout the year. Some organisations outsource their internal audit function to specialised expertise. It is important to note that internal audits differ from external audits, which are required by law in many public and not-for-profit (or for-purpose) organisations.

c. External Audit

External audits provide an independent opinion on the organisation's financial health, typically conducted annually. External auditors confirm whether the financial statements are accurate and whether the organisation's financial systems and governance processes are sound. These auditors are independent of the organisation and assess the strength of financial controls.

d. Risk Management Documents

Several key documents make up an organisation's risk management framework:

- **Risk Appetite Statement:** As discussed earlier, the Board is responsible for determining the organisation's risk appetite, which outlines the level of risk the organisation is willing to accept.
- **Risk Management Policy:** This document clearly articulates the organisation's approach to risk management, including roles and responsibilities. It should

Risk Management

be communicated at all levels of the organisation and to key stakeholders. Some government contracts in social services may require such a policy to be in place and regularly reviewed by the Board and management.

- **Risk Management Framework:** This framework defines how risk management processes are integrated into the organisation. It should outline how risk management is embedded within the organisation's culture.
- **Risk Registers:** These registers detail identified risks, their ratings, controls, associated costs, and the plans in place to reduce risks to acceptable levels.
- **Risk Profile:** Ideally, this is expressed visually, such as through heat maps, to illustrate the organisation's overall risk landscape.
- **Risk Reports:** These are reports presented to the Board, striking a balance between highlighting critical risks that need Board-level attention and those that can be managed at the management level.

Risk Assessment

The basic steps of risk assessment include:

1. **Identifing the risk:** Recognise potential risks that could impact the organisation.
2. **Conducting risk analysis:**
   - Determine the **consequence** (impact) of the risk.
   - Determine **likelihood** (probability) of the risk occurring.
   - Map the **impact** vs. the **probability** on a risk matrix.
3. **Evaluating the risk level and actions:** Assess the severity of the risk and decide on the necessary actions to mitigate it.
4. **Reviewing the effectiveness of existing controls:** Examine the current controls in place to manage the risk.
5. **Developing actions if controls are unsatisfactory:** If the current controls are insufficient, create and implement actions to address the identified gaps.

Dealing with Risk

There are four ways to deal with risk.

1. **Treatment:** This involves risk mitigation (risk reduction). It includes steps to reduce either the probability or the impact of the risk. Boards and management work systematically to reduce either the impact and/or the likelihood of the risk occurring. The level of risk remaining after internal controls are applied is known as 'residual risk'. Residual risk is often the acceptable level of risk and aligns with the organisation's risk appetite.
2. **Avoidance:** This is achieved by not starting or continuing with an activity or by removing the source of the risk altogether.
3. **Sharing:** This involves transferring the risk to a third party, usually achieved through insurance or contracts.
4. **Acceptance**: In some cases, no action is taken, and the risk is accepted. This is usually the case when organisations believe they can withstand the consequences.

Risk Management

Some risks will always remain high due to the nature of the business, and these must be accepted by Boards and management.

Risk management is a broad and detailed area of governance and management.

Other Harmony Alliance Guides in the Risk Management Series

- Identifying, Analysing & Evaluating Risk
- Risk and Culture
- Crisis Management
- Emerging Risks
- Business Continuity Planning - Overview
- Pandemic Planning