PRINCIPLE 5

Risk management

Board decision-making is informed by an understanding of risk and how it is managed

5.1 The board oversees a risk management framework that aligns to the purpose and strategy

5.2 Directors seek and are provided with information about risk and how it is managed

5.3 The board periodically reviews the risk management framework

Risk is inherent in all human endeavours – including in the activities of organisations. The role of the board is to understand the organisation's risk, to make decisions based on this understanding and to oversee a framework that manages risk on an ongoing basis. Risk is not something to be avoided, but to be understood and leveraged in pursuit of an organisation's purpose.

"The best laid schemes of mice and men
Go often awry."

Robert Burns, To a Mouse, 1785

What is risk?

The International Organisation for Standardisation (ISO) defines risk as "the effect of uncertainty on objectives" (*AS/NZS ISO 3100 Risk management*). This is a useful definition as it helps to explain why risk is important to governance – it must be understood and considered in decision-making so that the organisation achieves its purpose with an acceptable degree of certainty.

Importantly, risk is not inherently bad. It arises because the future is unknowable and therefore the outcomes of decisions are always uncertain to some extent.

Risk is typically characterised by considering examples of events that could occur, their likelihood and the consequence of their impact. These examples are colloquially called 'risks'. For example, hypothetical risks could be that a building burns down or that a funding contract is not renewed. It is important to note that these are only illustrations that help to understand risk and are only relevant in the context of the making of a particular decision.

It is easy to confuse these example 'risks' with 'risk.' Risk refers to the uncertainty that is inherent in all decisions because they must be made on the basis of certain assumptions.

All decisions are based on assumptions about:

- Internal factors (such as structure, staff skills and resource availability);
- External factors (such as the regulatory environment, funding availability, interest rates); and
- Wider factors (such as political changes, public sentiment about donations, or climate change).

What is a risk management framework?

The way that organisations take uncertainty into account when they make decisions is called 'risk management.' The goal of risk management is to increase the certainty that a decision's intended outcome will be achieved. It involves the identification, evaluation and prioritisation of risks.

Risk management should not be considered as a discrete activity. Rather, it should be embedded in the practices, processes and policies within an organisation that are concerned with making decisions and ensuring that these decisions continue to be valid.

Risk management happens in all organisations because people consider, to some extent, what they need to do to make sure their decisions achieve their intended outcome. This approach may be ad hoc and inconsistent across the organisation, but it is always happening.

However, organisations can adopt more formal processes to facilitate better management of risk. This is called developing a risk management framework.

The Australian/New Zealand Standard on Risk management defines a risk management framework as:

> **AS/NZS ISO 31000:2009 RISK MANAGEMENT – PRINCIPLES AND GUIDANCE**
>
> A risk management framework is a set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

There is no one-size-fits-all approach to developing a risk management framework. Large organisations may have highly-developed approaches, systems and processes which are supported by both internal and external professional advisers. Smaller organisations facing simpler decisions may adopt more informal approaches, relying on their own experience, judgement and common sense to manage risk.

Benefits of risk management

The purpose of risk management is to support more informed decision-making. When a decision is made based on an understanding of risk and how it is managed, the chances that it will contribute to achieving the

organisation's purpose will improve. Ultimately, risk management aims to increase the certainty that an organisation's purpose will be achieved.

Risk management enables the organisation to:

- Challenge assumptions in decision-making;
- Take actions that will increase the likelihood that a desired outcome will be achieved;
- Identify early signs that an undesirable event may occur and take pre-emptive action to address it;
- Learn from successes and failures in a way that improves decision-making over time; and
- Consider whether previous decisions remain valid and, if necessary, revise them.

The board's role in risk management

The board's role is to oversee a framework that manages risk as an integral part of the decision-making process both at the board level and throughout the organisation.

Risk management is not a separate activity of the board. While the board may contribute to identifying risks, it can be a distraction for boards to spend time reviewing lists of hypothetical risks and the steps that might be taken to prevent them.

When the board makes a decision, they should ask management what actions they will take so that the intended outcomes of the decision will be achieved with an acceptable level of certainty. The steps taken by management to identify and control the uncertain elements of implementation is part of risk management. Boards should be satisfied that these steps are sufficient and in alignment with their expectations.

The board should also monitor the outcomes of decisions they make. Where the context for decisions changes or the assumptions on which they are made become invalid, the board may seek to alter these decisions or take new actions so that the desired outcomes remain sufficiently certain.

Reviewing the risk management framework

The board should periodically review how well the organisation is managing risk as part of decision-making. This should involve reviewing the risk management framework that enables this to occur.

How a review is undertaken, by whom and with what frequency will depend on the nature of the organisation and its circumstances. For example, if an organisation has been subject to significant change, it may require a more thorough or frequent review of its risk management framework.

In undertaking a review of the risk management framework, directors should ask:

?	*Is there clarity about how risk is managed in the organisation?*
?	*Is the risk management framework appropriate for the decisions the organisation faces?*
?	*How effectively has risk management been applied to past decisions?*

Responding to risk

It is important to note that the purpose of risk management is not to minimise or eliminate risk. This approach can seriously undermine an organisation's ability to achieve its purpose. There are several different approaches an organisation can take in responding to risk:

- Avoidance – an organisation can avoid risks by discontinuing the activity that generates the risk;
- Treatment – taking steps to control either the likelihood, or the consequence of the risk if it occurs;
- Transference – passing the risk on to another party such as outsourcing the activity or acquiring insurance; and
- Acceptance – accepting that a risk may eventuate and putting plans in place to respond if does.

Risk appetite

One of the most important roles of the board in risk management is in developing an understanding about the nature and the extent of risk the organisation is prepared to accept in pursuit of its purpose. This is often called defining a 'risk appetite.' The risk appetite provides parameters within which management can pursue the organisation's purpose.

It is critical that the organisation's risk appetite is aligned with its purpose. If an organisation is not prepared to accept enough risk, it may be inefficient in pursuing its purpose; if it accepts too much risk it may be exposed to undesirable consequences that undermine its performance.

Defining and documenting the organisation's appetite for risk supports the development of an appropriate risk culture which aligns to and supports the purpose and strategy. Boards must be careful that they are not so concerned with negative risk that opportunities are missed, but they can also not have such a disregard for risk as to expose the organisation to serious harm. Striking an effective balance between the two is the hallmark of a sound risk appetite. The board's role in culture is discussed in greater detail in *Principle 10: Culture*.

Risk management committee

Many organisations will establish a committee to assist the board in exercising due care, diligence and skill in relation to risk management. In smaller organisations it is common for the risk management committee to be combined with other committee functions such as the audit committee.

Objectives for a risk management committee may include:

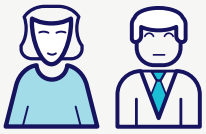
- Advising the board on the effectiveness of the risk management framework;
- Supporting provision of accurate, relevant and timely information about risk;
- Examining previous decisions to see how risk was managed as part of making those decisions;
- Monitoring and reviewing safety systems throughout the organisation;
- Oversight of insurance programs to maintain appropriate coverage;
- Monitoring the organisation's business continuity processes; and
- Developing and maintaining an appropriate risk culture that is embedded through the organisation.

In larger and more complex organisations, staff involved in the management of risk may also be involved with or have reporting lines to the risk management committee.

"Boards must be careful that they are not so concerned with negative risk that opportunities are missed, but they can also not have such a disregard for risk as to expose the organisation to serious harm. Striking an effective balance between the two is the hallmark of a sound risk appetite."

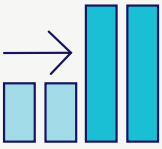
QUESTIONS FOR DIRECTORS

- IS THE BOARD AWARE OF HOW RISK IS MANAGED IN THE ORGANISATION?

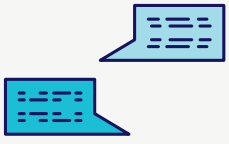


- IS THERE A SHARED UNDERSTANDING OF THE ORGANISATION'S RISK APPETITE?

- HOW OFTEN SHOULD THE BOARD UNDERTAKE A REVIEW OF THE RISK MANAGEMENT FRAMEWORK?



- IS THE RISK MANAGEMENT FRAMEWORK ALIGNED TO THE ORGANISATION'S PURPOSE?



- DOES THE BOARD HAVE ACCESS TO EXTERNAL PROFESSIONAL ADVICE ON RISK MANAGEMENT?

CASE STUDIES

HelpfulCare

In making or reviewing decisions, the board of HelpfulCare regularly questions management about how risk has been understood and responded to. The consideration of uncertainty is part of its formal decision-making processes.

The board has also established a risk management committee whose purpose is to assist the board with its oversight responsibility. The risk management committee reviews decisions made by the board to consider whether risk has been properly considered, and there is a sufficient degree of certainty of achieving the desired outcome.

At their annual strategy day, the board and management test the objectives of the strategic plan to understand the uncertainties that could affect the achievement of their goals. If there is not sufficient certainty, objectives are adjusted to make their outcomes more certain or other, ancillary actions agreed upon (to help increase the level of certainty).

The board of HelpfulCare engage the services of external consultants to undertake an annual review of their framework for managing risk. The risk management committee works with the consultants to agree actions that should be taken to enhance the effectiveness of risk management in the organisation.

The Friendlies

The Friendlies manage risk as an integral part of decision-making. Their directors examine the assumptions involved about uncertainty in the internal and external environment as part of their decision-making process.

The board works to make sure that their decisions remain relevant and that the desired outcomes continue to be sufficiently certain. To do this they receive and consider reports on:

- Whether the implementation of their decisions proceeded as intended;
- Whether any ancillary actions were also properly implemented; and
- Whether changes in the operational context have affected or could affect the outcome of their decisions.

In response to these reports, the board sometimes adjusts their decisions or authorises ancillary action to make sure their goals are achieved with sufficient certainty.

Every two years an ad hoc committee of the board of the Friendlies formally reviews how risk has been managed as part of past decision-making. Where there is adequate documentation past decisions are examined using the criteria above.