WHAT GOOD LOOKS LIKE

Risk management

What is risk management?

Risks are defined as the effect of uncertainty on objectives.[1] Risk can be negative (a threat) or positive (an opportunity). Risk management refers to activities carried out to reduce the impact of uncertainty to an acceptable level, or to take advantage of opportunities.

Why does good risk management matter?

Effective risk management helps to:

- increase the likelihood of meeting strategic and operational objectives;
- improve identification of opportunities and threats;
- establish a consistent and reliable basis for decision-making and planning;
- ensure compliance with legislation, rules, regulations, and standards; and
- improve organisational resilience.

About this guide

This guide is for governors and senior managers. It poses questions and provides some of the indicators of whether your organisation meets our definition of what good looks like. It can help you work out whether your risk management is effective.

Effective risk management

A good approach to risk management comprises four elements:

- a **framework** – policies, procedures, tools, and templates;
- the right **infrastructure** – the right number of staff with the right skills, knowledge, and experience, and access to the right information;
- being able to **apply** policies consistently and well; and
- ensuring that senior managers and governors have the information they need to **monitor** and **review** risks and how they are being managed.

Where to find out more

Risk management principles and guidelines – ISO

Risk management – Office of the Auditor-General

Useful guides for audit committees – Office of the Auditor-General

1 AS/NZS ISO 31000:2009.

	10 questions	Indicators of what good looks like
Framework	**1. Do you have an up-to-date risk management framework?**	· Framework for risk management to be embedded throughout the organisation. · Framework states that all staff have a role and duty to identify risk. · Risk information helps inform decision-making and accountability.
	2. Do you have an organisational risk management policy?	· Formally adopted policy incorporates the principles of effective risk management described in AS/NZS ISO 31000:2009.[2] · Policy clearly states the organisation's objectives and commitment to risk management. It sets expectations and defines accountability, systems, and responsibility. It also establishes how risk management performance is measured and reported.
Infrastructure	**3. Do you have the right staff, with the necessary skills, experience, and competence?**	· Clear responsibility for developing, implementing, and maintaining the risk management framework. · Staff are fully aware of the risks, controls, and tasks they are accountable for. · Risk owners have sufficient authority, time, training, and resources.
	4. Do you have effective systems and processes in place to manage risk?	· Risks are formally recorded in a risk register with their rating, treatment, status, and owner. · Up-to-date information and knowledge management systems are used by risk owners to inform decision-making.
Application	**5. Has your organisation established the risk context?**	· Clear, logical, and relevant structure is used for categorising risks (for example, strategic, tactical, operational, financial, or political risks). · Clearly articulated criteria for evaluating significance of risks (including how likelihood and impact are defined). · Risk appetite and/or tolerances are clearly stated.
	6. Is there an effective process for identifying risks?	· Comprehensive process for identifying sources of risk, their causes, and potential consequences. · Risk identification considers knock-on effects of consequences and cumulative effects of potential scenarios.
	7. Is there an effective process for analysing and evaluating risks?	· Formal assessment of risk likelihood and consequences is consistent with the risk context. · Effectiveness and efficiency of existing controls is considered. · Formal analysis of risk against established criteria and appetite to determine which risks need treatment.
	8. Is a full range of risk treatments considered and used?	· Full range of potential risk treatments (including avoidance, reduction, sharing, and retaining) are used according to their effectiveness. · Residual risk levels are tolerable and consistent with risk appetite. · Application and effectiveness of risk treatments regularly monitored.
Monitor and review	**9. Is there a clear commitment to risk management at governance level?**	· Key indicators demonstrate to governors that risk is within appetite. · Clear understanding of key strategic, operational, and financial risks enables good quality discussion. · Audit and risk committee or similar oversees risk management.
	10. Is the risk management framework monitored, reviewed, and continually improved?	· Periodic and ad-hoc reviews provide the foundation for continuous learning about risk. · Progress with improvement initiatives is tracked and monitored.

2 Although there is an International Standard 31000:2018, ISO 31000:2009 remains relevant in New Zealand.