clearview

Best practice guide to risk management

Risk management is central to the effective running of any organisation, and best practice risk management is simply good management. This best practice guide gives an introduction to risk management and provides best practice guidance on the main elements of an organisation’s risk management framework.

Contents

1 Risk management overview

1.1 What is risk?

Risk can be defined as the threat that an action or event will adversely affect your organisation’s ability to achieve its current and future objectives.

Your organisation is no different to any other organisation, in that it is continuously exposed to an endless number of new, or changing, threats, vulnerabilities and opportunities that may affect its operations and the fulfilment of its strategic objectives. Identification of these threats, vulnerabilities and opportunities are the only way to understand the likelihood (probability) and consequence (impact) of the risk involved and determine the appropriate controls and actions that you should undertake to manage and mitigate them.

1.2 Risk appetite

Risk appetite is a core consideration in any organisation’s risk management approach. Your organisation’s risk appetite outlines the level of exposure to risk that your organisation is prepared to accept or tolerate in order to achieve your strategic objectives, before action is deemed necessary to reduce it. The resources available for managing risk are finite and so the aim is to achieve an optimum response to risk. This management of risk should be prioritised in accordance with the evaluation of the probability of a risk occurring, and the potential impact if it does.

The term ‘risk appetite’ therefore refers to the level of risk your organisation is prepared to accept or tolerate after internal control is exercised (i.e. the residual risk). If the residual assessment is higher than the risk appetite, further action should be taken to reduce the likelihood and/or impact of the risk occurring, ensuring that additional controls are put in place. If this not possible, contingency plans should be put in place. If the risk is too high and your organisation doesn’t have the appropriate risk appetite, you may decide to stop the activity that caused the risk to arise.

1.3 Why manage risks?

The management of risk is the balancing of a number of interwoven elements which interact with each other. It is essential that the risk management process is embedded throughout your organisation, its management and staff.

The goals of risk management are to:

- take a proactive approach, anticipating and influencing events before they happen;
- facilitate better informed decision making;
- improve contingency planning;
- avoid unnecessary problems;
- set demanding performance targets; and
- set appropriate corporate ethics.

2 Risk management process

Risk management involves the evaluation of how a wide range of possible events and scenarios will affect your organisation’s strategy and its execution and the ultimate impact on your organisation’s value.

Risk management is the process by which we:

- identify risks in relation to the achievement of our objectives and goals;
- assess their relative likelihood and impact;
- respond to the risks identified, taking into account our assessment and risk appetite;
- review and report on risks – to ensure the risk register is up to date, to gain assurance that responses are effective, and identify when further action is necessary.

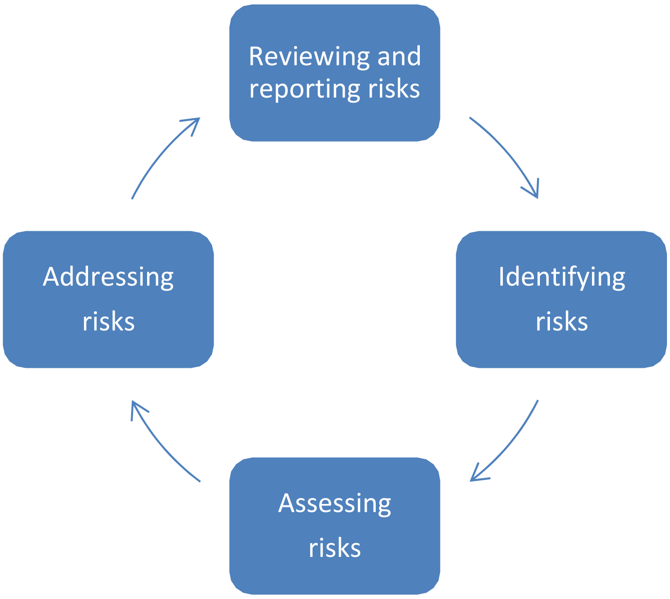


Figure 1: The Risk management process

2.1 *Identifying risks*

Identifying risks is the first step in building your organisation’s risk register. In identifying risks, you should consider both strategic and operational risks and who has ownership and responsibility for ensuring that each risk is managed and monitored over time.

Who will identify your strategic risks? And when? And how? Who will identify your operational risks? And how frequently (annual or ongoing) will these be reviewed?

When identifying the risks that could impact your business you should consider: people, information and data, buildings, work environment and associated utilities, facilities, equipment, ICT systems, transportation, finance, partners and suppliers and brand and reputation.

2.2 Assessing risks

An assessment of the likelihood of a risk occurring and its relative impact should be undertaken, with all risks being scored in terms of their likelihood and potential impact.

Examples of impact criteria to assess risks against could include financial, governance, regulatory, reputational, customer, environmental and service interruption.

Each risk should be assessed in terms of its ‘inherent/raw risk’ - the exposure arising from a specific risk before you have implemented any controls/action to manage the risk (worst case scenario); and also the ‘residual risk’ which relates to the impact and probability of the risk after controls have been implemented and action has been taken (target/residual/best case scenario). It is important to note that in some cases, controls may have limited impact, thus there may be no, or only a small, reduction of the risk in the residual assessment.

2.3 Addressing risks

The aim of addressing risks is to turn uncertainty to your organisation’s benefit by constraining threats and taking advantage of opportunities. This is often defined at the treatment of risk. Risk treatment is the process of selecting and implementing measures to address the risk.

The response to each risk must be determined by the risk’s nature and outcome of the risk assessment. The degree of attention required should be proportionate to the level of the risk and the costs and benefits involved in any action to reduce the risk.

There are typically 5 key aspects to addressing risk:

1. **Tolerate** - The risk may be tolerable without any further action being taken (or your ability to take action is limited, or the cost of action is disproportionate to the potential benefit gained). In tolerating the risk this can be done with or without monitoring.
2. **Treat** – Action is taken to constrain the risk to an acceptable level.
3. **Transfer** – Transfer risks to a third party to mitigate risk , for example to an insurance company.
4. **Terminate** – Terminate the activities causing the risk.
5. **Take the opportunity** – This is not an alternative to those above, rather it is an option which should be considered whenever tolerating, transferring or treating a risk. The option is to take the opportunity whilst being fully aware of the risks.

Once the approach to addressing each risk has been determined, it is vital to identify the required controls and actions. Who will identify the controls and actions, and when? Who will be responsible for them? Who will review the effectiveness of these, and identify any further actions, hence adding assurance.

2.4 Reviewing and reporting risks

Effective risk management requires a reporting, monitoring and review structure to ensure that your risks are effectively identified and assessed and that appropriate controls are in place. The management of risks has to be reviewed and reported on for two reasons:

1. to monitor whether or not your risk profile is changing; and
2. to gain assurance that your risk management activity is effective, and to identify when/where further action is necessary.

All elements of your risk management process should be reviewed at least once a year including risks, risk controls and risk assurances. The risk controls themselves should be reviewed at least on a biannual basis.

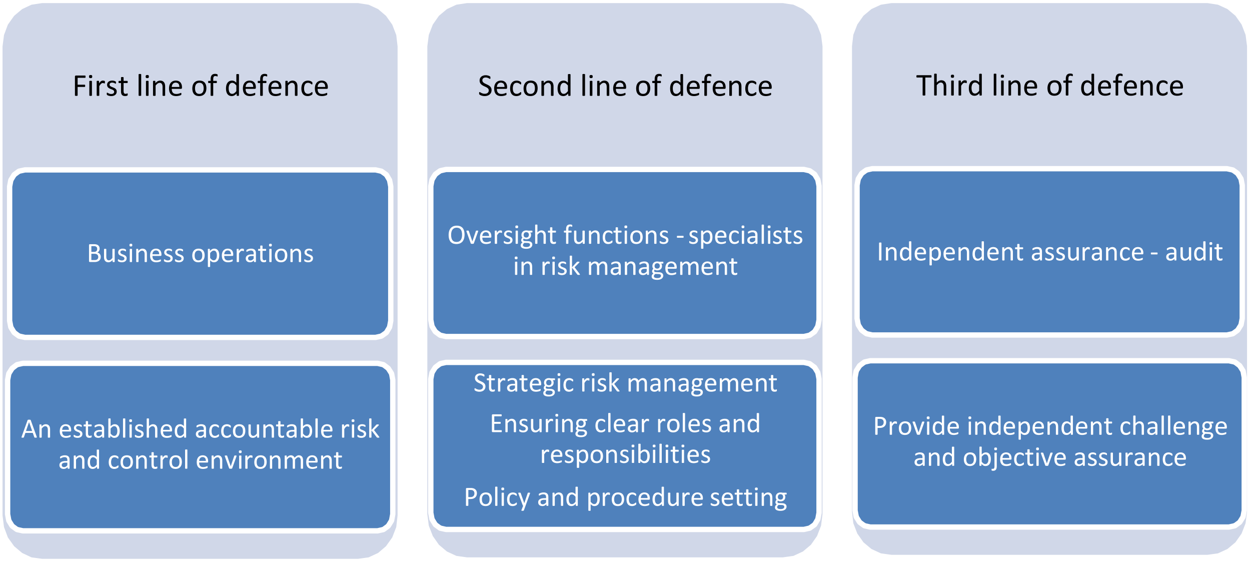
2.5 Risk assurance

Implementing an effective assurance system, including monitoring, auditing and assuring controls will help prevent any nasty surprises and improve the overall effectiveness of management. Assurances should ensure that controls are in place and are working effectively for your organisation. Three lines of defence is an approach you could consider:

First line of defence: In this line of defence managers provide assurance through identifying risks, implementing controls and reporting on progress within their functional areas.

Second line of defence: The second line of defence is provided by functions that oversee or specialise in risk management and compliance whom provide an oversight of business processes and risks. It is important that the second line of defence ensures there are clearly defined roles and responsibilities for risk management; that risks are strategically aligned; your policies are regularly reviewed; and risk management governance and assurance adds value to your organisation.

Third line of defence: The third line of defence is provided by functions that offer independent assurance, above all audit. The role of internal/external audit is to provide independent challenge and objective assurance.



First line of defence	Second line of defence	Third line of defence
Business operations	Oversight functions - specialists in risk management	Independent assurance - audit
An established accountable risk and control environment	Strategic risk management Ensuring clear roles and responsibilities Policy and procedure setting	Provide independent challenge and objective assurance

The use of the three lines of defence to understand the system of internal control and risk management is a great starting point to help ensure effective risk management and control. It should however, not be regarded as an automatic guarantee of success. All three lines need to work effectively with each other in order to create the right conditions.

3 Key principles in managing risks

There are a number of key principles to ensure are in place and demonstrable:

3.1 Aspirations and risk appetite

What is the risk appetite of your organisation? Has this been assessed in relation to the internal and external environment? Is this regularly reviewed, and aligned to your organisational ambitions?

3.2 Ownership and accountability

Have the risks been allocated to an individual for overarching management and responsibility? Have controls been identified and put in place? Are there any associated actions with relevant timescales and delegated responsibility?

3.3 Monitoring and review

There is an implicit need to regularly monitor and review risks, to monitor whether or not you risk profile is changing, and to gain assurance that risk management is effective. Are risks regularly reviewed as part of a formal process? What is the process? Do others understand and follow this process?

3.4 Support and reinforcement

Are staff given adequate training to fulfil the actions required? Use existing mechanisms such as internal audit to help assess risks and identify necessary controls. What are the existing mechanisms for managing risks? Are assurances in place?

4 What can go wrong?

Some of the common problems that impede effective risk management are:

- Thinking it will be easy. It is not. Effective risk management needs commitment, clear communication, tough decision-making and a clear focus on outcomes, time and resources.
- Thinking it is something you do in addition to the “real work”. This is the real work.
- Side-lining it – making it the responsibility of one person or team.
- Failure to understand the different working processes and practices of different parts of the organisation.
- Expecting the system to do the hard thinking – identifying and assessing risk is not an easy task. Remember you may not be able to eliminate all risks.
- Not being prepared to tackle difficult issues.

- Not keeping your risks under review.
- Failing to invest the necessary resources in support, training and communication.
- Failing to involve staff or prepare them for change.

5 The key role of leaders

To be effective, risk management needs visible, enthusiastic and unrelenting commitment from your board and executive team. Leaders should show, by their actions as well as their words, that:

- Managing risk is important.
- Risk management is carried out within a culture of clear and open communication and learning.
- Board members, executives and managers regularly reflect on what they need to do differently as a board, as a team and as individuals.

6 Conclusion

In order to manage risks well, risk management should be an integral part of strategic and operational management embedded throughout your organisation. You should ensure that all levels within your organisation receive the appropriate information from the risk management process to effectively manage your organisation and deliver its strategic objectives.