# Risk management guide

*Risk is defined as the effect of uncertainty on objectives. An effect is a deviation from the expected. It can either be positive, negative or both, and can address, create or result in opportunities and threats.*

*The role of Board, Executives and leaders is not to eliminate risk but to manage risk. They interpret how much risk is appropriate for the organisation to ensure its objectives are achieved. Risk management is about value creation and protection – it requires leadership, commitment, and an inte grated approach.*

*Note: This is intended as a guide only and not a comprehensive list of compulsory requirements. It will need to be adapted to take your organisation's unique circumstances into consideration.*

## Risk Management Development

- Start with a plan: what is required for your organisation to manage its risk, how you will develop the key components, prioritise these activities and set timeframes
- Get the right people involved: engage the Board, Executives and Leaders to support and guide the development, and the people within the organisation who will manage the risks
- Develop the tools: define and develop the essential risk tools to support the risk framework
- Communicate the plan: identify who needs to know and understand the plan, and how will it be communicated
- Monitor and review the program

 

## Start the Build

Commence building the essential risk tools for the risk framework

- Define the Risk Assessment
- Create a Risk Register
- Create an education and awareness program

## Assess the Risks

Utilise the risk register to record the key assessment elements for each risk. The risk assessment process addresses key questions and supports decision making.

1. Risk Identification – identify the types or categories of risks, and the key risks of the organisation
2. Risk Analysis – define the risk criteria by which risks are expressed, developing the impact and likelihood guide rails by which to evaluate risks
3. Risk Evaluation – prioritise risks and determine actions
4. Risk Treatment – identify and decide the treatment options

### Risk Identification

Identify the risk categories relevant to your organisation. Common categories include: Financial, Strategic, Legal and regulatory, Work health and safety, Reputation, Operational, and Stakeholder

Identify the key risks for the organisation, considering

- What can go wrong, when, how
- Potential cost to time, money, performance
- How likely is it to happen
- Source of the risk

## Risk Analysis

Risks are usually expressed in terms of their sources, potential events, their consequences or impacts, and their likelihood or probability. Risks are analysed for both cause and effect, such as what could go wrong and potential effects, and why might it go wrong and potential causes.

## Risk Criteria

Understanding the likelihood or probability of a risk occurring and the consequence or impact of that ris k is part of the assessment. This is done by defining each of the criteria and ratings, taking into consideration the organisation's size, culture, values, objectives and activities, the overarching risk assessment criteria, and any risk management contro ls already in place.

| Rating | Likelihood | Consequence |
|---|---|---|
| 1 | Highly Unlikely | Insignificant |
| 2 | Unlikely | Minor |
| 3 | Possible | Moderate |
| 4 | Likely | Major |
| 5 | Almost Certain | Extreme |

## Risk Evaluation

Use the risk register to record each key risk and capture key elements. Components within the risk register may include

- Risk Category
- Risk Statement summarising the risk
- Controls currently in place
- Initial risk rating for likelihood and consequence, and overall risk rating
- Risk owner
- Treatment Plan
- Residual risk rating for likelihood and consequence after treatment plan is considered, with the overall residual risk rating

 

## Risk Treatment

Determine  how to treat each risk, using the following commonly used options to help determine the approach.

- Avoid – don't do it
- Reduce – procedures, safety protocols
- Transfer or Share – insurance, agreements
- Retain – control, absorb, small consequence

## Monitor, Manage and Communicate

Risk management includes the coordination of activities and allocation of resources to minimise, monitor and control the organisations risks, and maximise the opportunities.

Executives, Board and Leaders monitor the performance of the risk management system, requiring appropriate reporting to conduct oversight and ensure alignment to risk appetite. Reporting includes activities outside of agreed levels, non-conformance, escalating or de-escalating risks, and new risks.

Ongoing education and communication with stakeholders is required throughout the entire risk management process.  Everyone in the organisation is responsible for managing risk.  Successful risk management occurs when it is built into the culture of an organisation.

## References


- Governance Hub, Australian Charities and Not-for-Profit Commission
- Risk Management, Australian Institute of Company Directors
- Running the Risk?, Volunteering Australia
- Psychosocial Hazards Fact Sheet, WorkSafe Victoria
- Prevent and Manage Risk of Mental Injury in your Small Business, Worksafe Victoria