Mentorloop Risk Management Process

Mentorloop

Risk Management Process

Overview

Our Risk Management Process has been developed in accordance with the guidelines of ISO 31000:2018.

The Risk Management Process consists of the following steps:

- Identify
- Analyse
- Control
- Monitor & Review
- Report

Risk events must be captured in the Risk Register (see Appendix 1.1) and maintained throughout the process.

Identify

The purpose of risk identification is to find, recognise and describe risks that might help or prevent an organisation achieving its objectives. Relevant, appropriate and up-to-date information is important in identifying risks.

In identifying risk, the organisation will consider:

- Causes and events
- Threats and opportunities
- Vulnerabilities and capabilities
- Changes to internal and external context
- Indicators of emerging risks
- Limitations of knowledge and reliability of information
- Biases and assumptions of those involved

To formally identify a risk to be managed, staff must document the following in the Risk Register:

- Event & Cause
    - A brief description of the risk (*what* it is)
    - The root cause of the risk (*how* or *why* it may occur)
- Risk Owner
    - The person or team responsible for the risk and ensuring that it is effectively managed.

Analyse

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness.

In collaboration with the risk owner and stakeholders, the risk management team must identify, agree upon and document in the Risk Register (see appendix 1.1) the following:

- Inherent Likelihood Rating
    - Risk Likelihood Rating (appendix 1.2) inherent to this risk event if no controls were in place.
- Inherent Consequence Rating
    - Risk Consequence Rating (appendix 1.3) inherent to this risk event if no controls were in place.
- Inherent Risk Rating
    - Calculated Risk Rating (appendix 1.4) determined by Inherent Likelihood Rating and Inherent Consequence Rating
- Existing Controls
    - What existing controls have been established to mitigate the risk event and how effective do we believe those controls are.
- Residual Likelihood Rating
    - Risk Likelihood Rating (appendix 1.2) as it applies to the risk event with the existing controls in place.
- Residual Consequence Rating
    - Risk Consequence Rating (appendix 1.2) as it applies to the risk event with the existing controls in place
- Residual Risk Rating
    - Calculated Risk Rating (appendix 1.4) determined by Residual Likelihood Rating and Residual Consequence Rating

Evaluate

The purpose of risk evaluation is to support decisions. It involves comparing the results of the risk analysis to determine where additional action is required.

The team will make a decision to:

- Do nothing further
- Consider treatment/control options
- Undertake further analysis to better understand the risk
- Maintain existing controls
- Reconsider objectives

The outcome of risk evaluation should be recorded in the Risk Register and, as appropriate, communicated with and approved by the relevant areas of the organisation.

Treatment

The purpose of risk treatment is to select and implement options for addressing risk.

Risk treatment is an iterative process that involves:

- Formulating and selecting treatment options
- Planning and implementing risk treatment
- Assessing the effectiveness of that treatment
- Deciding whether or not the remaining risk is acceptable
- If not acceptable, taking further treatment

There may be multiple risk treatment options selected for a single risk event and treatment options are not necessarily mutually exclusive. Risk treatment options may include but are not limited to the following:

- Avoiding the risk by not pursuing the activity that gives rise to the risk
- Taking or increasing risk in order to pursue an opportunity
- Removing the risk source
- Changing the likelihood
- Changing the consequence
- Sharing/transferring the risk
- Retaining and accepting the risk by informed decision.

The team will select appropriate treatment options and document in the Risk Register the following:

- Action
    - What specific treatment option will be implemented to prevent and/or mitigate the risk event
    - How it will be implemented
    - The expected outcomes of implementing this treatment option
- Owner
    - Which individual is responsible for the action
- Date
    - When the treatment option is to be implemented by

Monitoring and Reviewing

The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes.

It is the responsibility of the designated Risk Owner to continually:

- Review and maintain the accuracy of risk details in the Risk Register, including:

    - Event and cause
    - Likelihood, consequence and risk ratings
    - Existing controls and their effectiveness
- Manage the implementation of the selected treatment options to ensure they are:
    - Being delivered within the documented timelines
    - Achieving their expected outcomes with regards to risk control and mitigation
- Communicate progress and any changes to stakeholders as appropriate

Reporting

All risks currently being managed by our Risk Management Process must be documented in the Risk Register at all times. As per *monitoring and reviewing* it is the responsibility of the Risk Owner to ensure that this information is kept up to date and accurate at all times.

It is also the responsibility of the designated Risk Owner to:

- Provide reports and updates to assure the organisation and key stakeholders that risks are being appropriately managed and treated
- Inform internal stakeholders of their responsibilities as they pertain to the treatment and management of specific risks, such that they
    - Understand existing controls
    - Are aware of their responsibilities in relation to selected treatment options
    - Are able to make informed decisions in relation to organisational objectives with a clear understanding of the risk and its consequences

The frequency and method may vary to reflect the significance of its risk.

Management must be aware of and involved in any decisions to communicate risk to external stakeholders.

Appendices

1.1 Example Risk Register

Event & Cause	Owner	Inherent Likelihood Rating	Inherent Consequence Rating	Inherent Risk Rating	Existing Controls	Residual Likelihood Rating	Residual Consequence Rating	Residual Risk Rating	Actions
Brief description of the risk event and its potential origins.	Who is responsible for this risk and its control.	See appendix 1.2	See appendix 1.3	See appendix 1.4	What treatments and controls are currently in place to manage this risk and what is their effectiveness?	See appendix 1.2	See appendix 1.3	See appendix 1.4	Additional actions approved to mitigate risk. Identify WHAT, WHO and WHEN.

1.2 Risk Likelihood Matrix

Rating	Description	Probability
Rare	Incident is possible in exceptional circumstances.	1 in 5+ years
Unlikely	Incidents are unlikely to occur	1 in 3-5 years
Possible	Incidents will possibly occur less frequently than once every 2 years	1 in 2-3 years
Likely	Incidents are likely to occur each year	1 per year
Almost certain	Incidents will occur frequently each year	Multiple times each year

1.3 Risk Consequence Matrix

Rating	Description
Insignificant	Issue of little concern to stakeholders
Minor	Isolated issues that may cause small disruptions
Moderate	An issue that will require attention and may cause concern or inconvenience to stakeholders
Major	An issue that will require urgent attention and will have lasting impact on stakeholders
Catastrophic	An issue that poses an existential threat to the organisation

1.4 Risk Level Matrix

	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Moderate	Moderate	High	High	High
Likely	Moderate	Moderate	Moderate	High	High
Possible	Low	Moderate	Moderate	Moderate	High
Unlikely	Low	Low	Moderate	Moderate	Moderate
Rare	Low	Low	Low	Low	Moderate