Risk management procedures

Purpose and scope

In accordance with the BizOps Enterprises risk management policy, these procedures describe the organisation's standard process for risk management, including:

1. Risk identification
2. Risk rating
3. Risk controls
4. Risk monitoring and reporting

A standard approach to risk management allows risks to be correctly prioritised across all of BizOps's operations.

Responsibilities

The risk management policy committee oversees risk management and implementation on behalf of the board and the Chief Executive Officer.

All BizOps employees are responsible for applying risk management principles and practices in their work areas. Management is responsible for ensuring risk management principles are applied.

Employees must report risks and participate in risk management training.

Risk management process

A risk to BizOps is any event or action that could have a negative impact on the organisation. This includes events that could lead to:

- death or injury
- financial loss to BizOps
- damage to BizOps's reputation or adverse media coverage
- damage to the physical environment, including land, water or air quality
- failure to meet regulatory or legislative requirements.

The risk management policy specifies that:

- all business activities must undergo risk assessment prior to commencing and then undergo risk management throughout
- risk identification, analysis, evaluation and treatment must be reported and recorded in the BizOps risk register.

Risk management procedures

1. Risk identification

Risk identification is a structured approach to identifying the events that, if they were to occur, could have a negative impact on the organisation.

2. Risk rating

Risk rating is a process to analyse and understand each of the risks, including understanding what causes the risk to occur and what controls are already in place to manage the risk. Risk assessment also determines:

- how severe a potential impact could be
- the likelihood of the organisation being negatively impacted in this way.

Once the potential impact and likelihood have been assessed, the risk assessment process considers whether the risk is acceptable to BizOps, or whether further treatments are required to reduce the level of risk.

All identified risks shall be assessed to determine the overall ranking for the risk. Risks are ranked in the following four categories:

- Extreme
- High
- Medium
- Low

The ranking of a risk determines:

- the nature of further action that is required
- the urgency with which further action should be undertaken
- the reporting requirements for the risk, including who the risk is reported to
- how the risk is monitored.

All risks within BizOps are ranked using a common scale that assesses:

- the potential consequences if the risk were to occur
- the likelihood of BizOps being impacted in that way.

A common approach to risk ranking is necessary to ensure that the largest risks to BizOps can readily be identified and risk management can be prioritised in a way that has the greatest overall benefit to the organisation.

The following tables show how the consequences and likelihood of risks are assessed.

Consequence table

Consequence	Consequence category				
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Financial	<$5k	>$5k <$10k	>$10k <$100k	>$100k <$300k	>$300k
Reputation/market disruption	Isolated complaints from individuals; minor local media coverage	Adverse capital city/state media coverage; ongoing complaints	Loss of market opportunity or some loss of reputation; adverse national media attention	Reputation damage or loss of major opportunity that has a major impact on BizOps's operations	Will impact future business operations in catastrophic way; continuous public criticism
Regulatory and legislative	Minor breaches by individual staff members	Organisational breach	Penalties for breach of Act or legislation; third-party claims	Major fines for breaches; multiple third-party claims	Severe fines and/or prison sentences
Environmental	Brief spill incident contained onsite with no environmental harm	Minor onsite spill incident; pollutant contained and cleaned up immediately	Release of pollutant or environmental incident; moderate environmental harm	Large spill or environmental incident and significant associated cost	Long-term environmental damage with ongoing liabilities and/or possible EPA closure for undisclosed period
Safety	Treated with first aid	Medical attention required	Hospital treatment and ongoing rehabilitation	Hospital treatment and possible serious permanent injury	Loss of a life

Likelihood table

Likelihood rating is based on the number of times within a specified period that a risk may occur either as a consequence of business operations or through failure of operating systems, policies or procedures.

Rating	Description	Probability
Expected	Expected to occur in most circumstances	> 80%
Probable	Will probably occur in most circumstances	50%–80%
Possible	Might occur within a 1–2 year time period	21%–49%
Improbable	Could occur during a specified time period	5%–20%
Rare	May only occur in exceptional circumstances	< 5%

The risk rank is determined by combining the consequence and likelihood as shown as follows:

Level of likelihood	Level of impact				
	1 (Insignificant)	**2 (Minor)**	**3 (Moderate)**	**4 (Major)**	**5 (Catastrophic)**
A (Expected)	Medium	Medium	High	Extreme	Extreme
B (Probable)	Medium	Medium	Medium	High	Extreme
C (Possible)	Low	Medium	Medium	High	High
D (Improbable)	Low	Low	Medium	Medium	High
E (Rare)	Low	Low	Low	Medium	Medium

Assessing likelihood

When assessing likelihood, it is important to note that the likelihood score for a risk needs to reflect the likelihood of the consequence occurring, rather than the likelihood of the risk occurring.

For example, there may be a risk that staff are injured as a result of a fire emergency. The consequences of a fire may range from a relatively minor injury to death, depending on the circumstances of the fire.

While fire emergencies are fortunately not common within BizOps, the likelihood of staff dying as a result of a fire is considered to be likely. There are therefore a number of ways of scoring this risk.

Type of incident	Consequence	Likelihood	Risk score
Minor incident	Minor injury to individuals Consequence: Moderate	Possible	Medium
Serious incident	Serious harm to individual Consequence: Major	Possible	High
Fatality	Fatality as a result of the fire Consequence: Catastrophic	Possible	High

Overall it is clear that this risk would be considered to be Medium to High. To highlight the serious nature of the risk, it would therefore be appropriate to give this risk the risk scoring that shows the High risk rating, and therefore score this risk with a consequence of Catastrophic and a likelihood of Possible.

3. Risk controls

Controls represent a whole range of actions, measures and strategies taken by management and employees to eliminate or reduce risks. The process of determining risk controls includes assessing the consequences and likelihood of the risk and evaluating how to treat the risk. This could include:

- avoiding the risk
- mitigating the risk
- transferring the risk
- accepting the risk.

A process should then be followed to identify efficient and effective ways to mitigate the risk. This can occur by either:

- removing the risk
- reducing the likelihood of the risk impacting BizOps
- reducing the consequences if the risk were to occur
- a combination of these approaches.

Consider the hierarchy of control:

- Elimination
- Substitution
- Engineering controls
- Administrative controls
- Personal protective equipment

4. Risk monitoring and reporting

Risk monitoring and reporting involves a process of regular review to ensure that:

- new risks are identified and considered as they arise
- existing risks are monitored to identify any changes that may impact the organisation
- new risk controls are being implemented
- existing risk controls are still in place and working effectively
- information about risks is adequately communicated.

All risks rated as moderate, significant or high in the risk identification process will be reviewed by the risk management policy committee regularly. This review will be via either:

- the risk manager reporting on new risks identified by staff during the course of their work since the last committee meeting
- risk owners providing a report on the status of their assigned risk to the committee (see below)
- the risk manager reporting on reviews of the risk register following a Structured Risk Identification Workshop each year, or any review of the risk register by the Executive.

The risk owner’s reports to the committee should outline that the risk controls are to indicate:

- causes of the risk
- implication of the risk with amendment to existing controls (if they exist)
- what any existing mitigating controls are
- what actions are being undertaken to put further controls in place, or maintain existing controls, and by when
- who is responsible for ensuring the controls are in place.