Risk Management Policy

Objective

Risk Management is a process that assists our organisation to predict future events that may impact (positively or negatively) on activities and to take appropriate actions to address the impact of these events. Risk is defined as the "effect of uncertainty on objectives".

Risk Management Framework

Our Organisation has designed a framework in accordance with the AS/NZS ISO 31000:2018 International Risk Management Standard and the AS/NZS 5050:2010 Business Continuity Standard which assists our organisation to manage its Seven Step Risk Management Process and ensures that information about risk is adequately reported and used as a basis for decision making and accountability at all relevant organisational levels.

International standard for Risk Management (AS/NZS ISO 31000:2009) Building Blocks

- **9 Principles** which an organisation should follow in order to effectively manage risk
- **A Management Framework** which provides the foundations that will allow an organisation to embed risk management at all levels throughout the organisation
- **A Seven-Step Process** designed to assist an organisation effectively manage risk on a day to day basis.

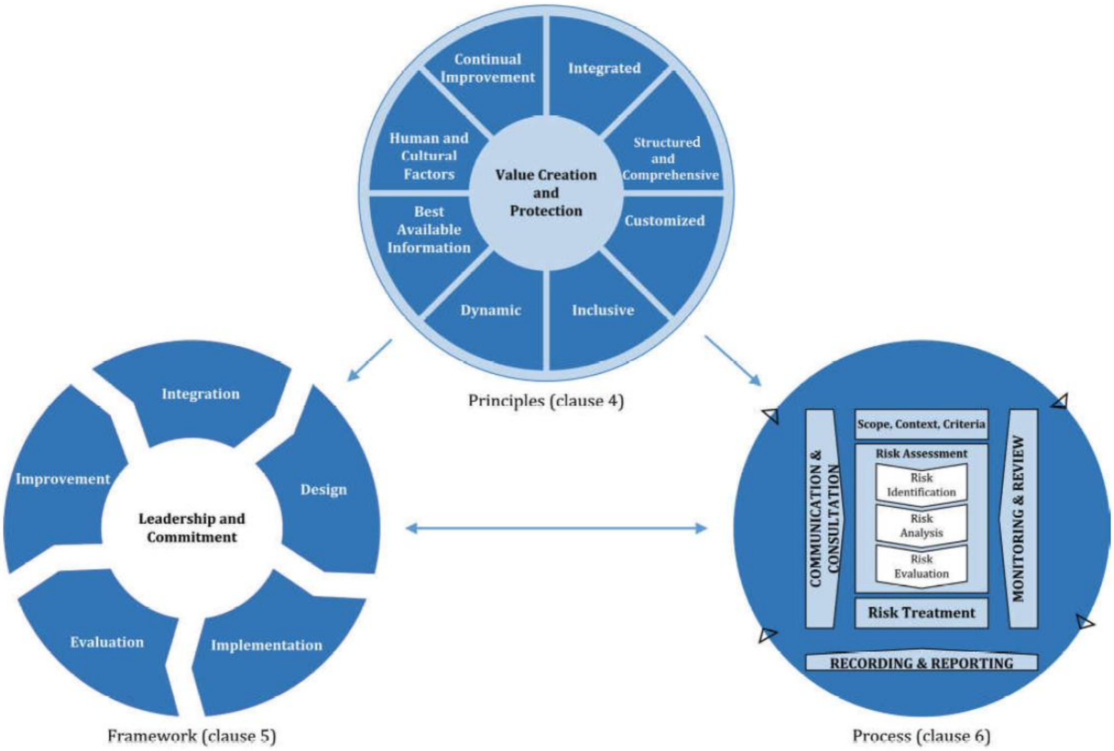

Diagram taken from ISO 31000:2018 Standards

Who is responsible for Risk Management?

Risks arise at every level of business, from the implementation of high-level strategies through to the physical security and safety of our working environment.

As such it is the responsibility of every person within our organisation to be aware of risks and to provide feedback with respect to perceived risks, either by notifying a member of the our Executive directly, or within the context of more formal risk identification processes.

Responsibilities of the Board

The Board is responsible for:

- approving and overseeing the implementation and maintenance of this Risk Management Program
- ensuring that it receives regular reports on the risk profile of the company
- ensuring that management has sufficient resources in place and staff are adequately skilled and qualified to manage and control risks
- ensuring that those policies and procedures that are designed to mitigate risks are readily accessible by employees
- promoting a risk management culture within the organisation
- Establishing clear delineations of lines of responsibility for managing the end to end risk process.

Responsibilities of Management

Management is responsible for:

- establishing and implementing this Risk Management Program and the policies and procedures that are required to effectively manage risk within our organisation
- promoting a risk management culture within our organisation
- establishing clear delineations of lines of responsibility for managing the end to end risk process
- continuously monitoring changes in our organisation's activities and ensuring that risks arising from any significant changes are considered within the risk framework
- Ensuring that the policies and procedures are carried out efficiently and effectively.

Responsibilities of the Risk Manager

- The Executive has overall responsibility for our organisation's risk management and will delegate responsibility for this role to the Risk Manager.

- The Risk Manager reports to the CEO, the Risk & Compliance Committee and the Board.

The Risk Manager is responsible for ensuring that the:

- establishment and implementation of this Risk Management Program and the policies and procedures that are required to effectively manage risk within our organisation
- promoting a risk management culture within our organisation establishing clear delineations of lines of responsibility for managing the end to end risk process
- continuously monitoring changes in our organisation's activities and ensuring that risks arising from any significant changes are considered within the risk framework
- service streams conduct all relevant risk assessments at all times
- maintaining our organisation's Risk Register
- ensuring that risk controls and treatment plans are carried out efficiently and effectively
- preparing risk management reports for management and the board
- providing input on all risk issues
- reviewing the overall effectiveness of this Risk Management Program

Mandate and commitment

Our organisation recognises that in order to implement and effectively maintain a Risk Management Program, a strong and sustained commitment from management is required. This commitment is demonstrated by the:

- formulation of the Risk Management Program which substantially meets the guidelines as set out in the International Risk Management Standard AS/NZ ISO 31000: 2018
- Formulation of a compliance framework which substantially meets the guidelines as set out in the Australian Compliance Standard. Our organisation Compliance framework is designed to ensure legal and regulatory, organisational and contractual compliance
- formulation of a Business Continuity Program which substantially meets the guidelines as set out in the Australian Business Continuity Standard
- formal endorsement of our organisation's Risk Management, Business Continuity Management and Compliance frameworks by the Board of Directors
- implementation of quality system, that allows us to capture risks and compliance tasks, assign them to responsible individuals, monitor individual performance, and report in real time

- development of internal risk management and compliance training programs to enable the alignment of our organisation’s culture and our strategic goals and objectives with our Risk Management Program
- regular reporting with respect to risk and compliance across our organisation

Ratified by	Board
Person responsible	Risk Committee
Version	2
Next Review	September 2020

Procedure for Risk Scoring in matrix

This following information is a guide to the scoring of a risk at the organisation and how it will be managed in the IONMY system. All risks have the capability to become an issue should they not be addressed, and scoring to ensure it is addressed is critical to keep business flowing and achieving targets based on legislation and accreditation.

	Impact				
Likelihood	**1 Insignificant**	**2 Minor**	**3 Moderate**	**4 Major**	**5 Extreme**
A - Almost Certain	Medium (A1)	Medium (A2)	High (A3)	Critical (A4)	Critical (A5)
B - Likely	Low (B1)	Medium (B2)	High (B3)	High (B4)	Critical (B5)
C - Possible	Low (C1)	Medium (C2)	Medium (C3)	High (C4)	High (C5)
D - Unlikely	Low (D1)	Low (D2)	Medium (D3)	Medium (D4)	High (D5)
E - Rare	Low (E1)	Low (E2)	Low (E3)	Medium (E4)	High (E5)

Risk rating scale

The risk rating scales will allow you to rate identified risks, analyse and evaluate them, and then identify risk management priorities. As with the context, you should identify a number of new risks that are specific to your organisation and how it operates. Each identified risk in the risk audit should be rated. These ratings describe:

- The likelihood of the risk event occurring (occurrence)
- The loss or damage impact if the risk event occurred (severity)
- The risk priority scales. The risk priority will be rated according to the potential loss or damage impact, the degree of urgency required to address the risk and the level of importance in the decision to take action to manage the risk.

Likelihood Definitions

A	Almost Certain	Not unusual to happen. Risk has more than 80% chance of occurring, or it is almost certain to occur in the next three months.
B	Likely	Known to occur or has happened in the past. Risk has 60-80% chance of occurring, or is likely to occur in the next six months.
C	Possible	May occur. Risk has a 30-60% chance of occurring, or may occur within one year.
D	Unlikely	Not likely to occur. Risk has 5-30% chance of occurring, or may occur within the next three years.
E	Rare	May occur in exceptional circumstances (would be considered highly unusual). Risk has less than 5% of occurring

Impact Definitions

1	Insignificant	Physical Assets: Localised damage, easily repaired. Business Interruption: Minimal, no long term effect. Reputation/market share: No media reports Financial Assets: Insignificant financial loss (up to $5K)
2	Minor	Physical Assets: Minor damage, repairable. Business Interruption: one week or less, minor long term effect. Reputation/market share: Short-term local media attention. Financial Assets: Minor financial loss in a single event. (up to $10K)
3	Moderate	Physical Assets: Significant damage to property or equipment. Repairable. Business Interruption: More than 1 week. Probable long term impact on profitability. Reputation/market share: Medium-term local media attention. Financial Assets: Moderate financial loss in one single event. (up to $100K)
4	Major	Physical Assets: Extensive damage to property and equipment. Repairs difficult. Business Interruption: Up to 3 months. Significant long-term impact on profitability. Reputation/market share: National media attention. Loss of clients. Financial Assets: Major financial loss in one single event. (up to $1 Mil)
5	Extreme	Physical Assets: Total loss of buildings, equipment, records Business Interruption: Extended interruption, full recovery unlikely. Reputation/market share: Extended national media attention. Irreparable damage. Clients lost. Financial Assets: Financial failure of the company. (> $1 Mil)

All risks are scored in the above manner, and entered into the Management system. These are reviewed based on their matrix rating, and a mitigation applied by the business and endorsed by management.

Actions to follow regarding risk rating

Low	Manage by routine procedure. Manage trending data
Medium	Specify Management Accountability & responsibility. Monitor & Plan
High	Escalate to Senior Management – Implement detailed action plan
Critical	Escalate to CEO. Implement detailed action plan

Risk Categories

This following information is a list of categories that risks are assigned under when they are created in the system. The heading at a high level indicates the set of guidelines for reporting. The subset is a guide for the type of assessment for the risk that is being put into the system.

These headings and sub headings are to be used when classifying the risk reported. This way, the appropriate risks can be assigned together in the correct group, reported correctly and given the priority they require within the business.

If you have any questions, please contact your supervisor and they will ensure you are given the correct information. Please ensure all risks are treated seriously, as left untouched they can quickly become an issue which can damage the company in many ways, such as legally, credibility and socially.

Risk Area	**i.on my Risk Categories**	**Examples of areas to consider within each category**
Operational	Client safety and clinical care	Client safety including medication safety, response to complaints and concerns Protection of children and clients who are unable to care for themselves Support appropriate to needs including referral to other services
Operational	Workforce	Organisational culture Recruitment and selection Learning and professional development Performance management Succession Planning Workplace relations including grievances Claims
Operational	Communication and Information	Access and controls Information and data management system Hardware/Software Privacy and confidentiality Release of information Record management Risk communication Staff communication Technology Digital information security
Operational	Facilities and assets	Security Assets management Repairs and maintenance Capital works Procurement
Operational	Emergency Management	Business continuity planning and management Natural disasters Man-made disasters
Compliance	Legal	Litigation Contract management Intellectual property Regulatory compliance Contract compliance
Financial	Finance	Operational budget and financial performance Administration Procurement of goods and services, maintenance and contracts management Fraud Insurance

Risk Area	i.on my Risk Categories	Examples of areas to consider within each category
Work Health & Safety	Work Health and Safety	Workplace Health and Safety Workers compensation and injury management Contractor compliance
Work Health & Safety	Environmental	Waste management
Strategy	Leadership and Management	Effective leadership Enquiries and Ministerial External and internal auditing Governance structures, delegations and financial management Legislative and regulatory compliance Monitoring performance Political circumstances Reputation and image Strategic and operational planning
Reputational	Community Expectations	Access to services Client engagement and empowerment Client feedback, cultural and special needs Excellent care and services Protection of vulnerable people