**[Organisation name/logo]**

**Risk Management Policy**

**Version: [Year/no]**

**Document status: Draft or Final**

**Date issued: [date]**

**Approved by: [insert organisation name]’s Board of Directors on [date]**

**Date for review: [date]**

**Record of policy development:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version number** | **Date of issue**  | **Lead author/ reviewer**   | **Significant changes on previous version** |
| **[Yr/no]**  | **[Date]** | **[Name/role]** | **[For example, incorporate changes to new legislation]** |
|  |  |  |  |
|  |  |  |  |

***Note\****

*All material provided by the Network of Alcohol and other Drugs Agencies (NADA) is for guidance purposes only. As this template has been developed to meet the needs of a diverse range of services, not all content may be relevant to your service.* ***Organisations are encouraged to review the material in relation to your organisation’s individual circumstances and edit, add and delete content to ensure relevancy.***

*While every effort has been made to present all information accurately, the Network of Alcohol and other Drugs Agencies (NADA), its employees and related parties, accept no liability for, and do not indemnify against, any loss, damage or injury that may result from any actions taken based on the information contained in this document.*

*All notes (like this one) should be considered and deleted before finalising the policy, and the contents list should be updated as changes are made and when content is finalised.*

*\*Please delete note before finalising this policy.*

***Note\****

*To update the contents list when all content has been finalised, right click on the contents list and select ‘update field’, an option box will appear, select ‘Update entire table’ and ‘Ok’.*

*To use the contents list to skip to relevant text, use* ***Ctrl and click*** *to select the relevant page number.*

*\*Please delete note before finalising this policy.*

**CONTENTS**

[SECTION 1: Policy statement 3](#_Toc185843628)

[1.1 Purpose and scope 3](#_Toc185843629)

[1.2 Definitions 3](#_Toc185843630)

[1.3 Principles 4](#_Toc185843631)

[1.4 Governance 4](#_Toc185843632)

[1.5 Outcomes 5](#_Toc185843633)

[1.6 Delegations 5](#_Toc185843634)

[1.7 Policy implementation 5](#_Toc185843635)

[1.8 Risk Management 5](#_Toc185843636)

[SECTION 2: Risk Management Framework 6](#_Toc185843637)

[2.1 Risk management framework 6](#_Toc185843638)

[2.3 Roles and Responsibilities 8](#_Toc185843639)

[SECTION 3: Risk management processes 9](#_Toc185843640)

[3.1 Communication and consultation 9](#_Toc185843641)

[3.2 Establishing risk context 10](#_Toc185843642)

[3.3 Risk identification 10](#_Toc185843643)

[3.4 Risk assessment 11](#_Toc185843644)

[3.4.1 Risk matrix 11](#_Toc185843645)

[3.4.2 Risk likelihood 12](#_Toc185843646)

[3.4.3 Risk impact 12](#_Toc185843647)

[3.4.4 Risk rating 12](#_Toc185843648)

[3.5 Risk treatment 13](#_Toc185843649)

[3.6 Risk management plans 14](#_Toc185843650)

[3.7 Risk monitoring and reviewing 14](#_Toc185843651)

[3.8 Reporting and record-keeping 15](#_Toc185843652)

[3.8.1 Risk register 15](#_Toc185843653)

[3.8.2 Compliance register 15](#_Toc185843654)

[SECTION 4: REFERENCES 16](#_Toc185843655)

[4.1 Supporting documents 16](#_Toc185843656)

[4.2 Related internal policies 16](#_Toc185843657)

[4.3 External references 16](#_Toc185843658)

# SECTION 1: Policy statement

**[Insert organisation name]** (‘**organisation’**) is committed to effective risk management as a strategy for protecting the organisation, board, employees, workers, clients, stakeholders, visitors, students, volunteers and the community from unnecessary injury, loss or damage relating to the business and activities the organisation undertakes.

In particular:

* We are committed to protecting the wellbeing, health and safety of clients and staff in the delivery of our services, and in all their interactions with **[organisation name]**
* Risk management is embedded in the key decision and approval processes of all business processes and functions
* Employees proactively identify risks; our culture promotes awareness of potential risk exposures and any opportunities created by risks
* We are compliant with all legislation and regulatory obligations that apply to **[organisation name]**.
* The risk appetite of the Board for the major risk classes to which **[organisation name]** is exposed, is documented and regularly revisited in the Board Appetite Risk Statement-part of this document.

## 1.1 Purpose and scope

This Risk Management Policy (the Policy) affirms (**[organisation name]**) commitment to effective risk management. It deﬁnes the policy, governance, and broad accountabilities which **[organisation name]** maintains to effectively manage risks. It lays the foundation of the Risk Management Framework and defines the key actions to support effective risk management.

This policy applies to the Board of Directors, all staff, students, volunteers and contractors of **[organisation name]**. It applies to all work performed, as well as related activities such as work-related functions, travel, conferences and any other circumstance when a person is representing **[organisation name]**.

This policy does not provide detailed guidance on:

* human resources management – refer to the Human Resources Management Policy
* workplace environment and safety – refer to the Work Health and Safety (WHS) Policy
* financial operations – refer to the Financial Management Policy.

## 1.2 Definitions

|  |  |
| --- | --- |
| **Clinical Incident** | Any unplanned event resulting in, or having the potential to harm a client |
| **Clinical Risk Management** | Clinical risk management is concerned with improving the quality and safety of services by identifying the circumstances and opportunities that put clients at risk of harm and then acting to prevent or control those risks |
| **Compliance Register** | A register that assists an organisation to comply with its legal, regulatory and financial obligations |
| **Likelihood** | Probability or chance of something happening |
| **Impact** | Actual or potential impact that would or may occur |
| **Risk** | Chance of something happening that will impact on objectives, measured in terms of likelihood and impact |
| **Risk Assessment** | Process of analysing and evaluating the likelihood and impact of potential risks |
| **Risk Incident** | Realisation or occurrence of a risk impact |
| **Risk Management** | Process of identifying, assessing and judging risks, assigning ownership, taking actions to mitigate them, monitoring and reviewing progress |
| **Risk Register** | Tool for documenting risks, and actions to manage each risk. As risks are identified they are logged on the register, and actions are taken to respond to the risk. |
| **Risk Treatment** | Identifying and implementing actions to eliminate risks or reduce impacts |

## 1.3 Principles

The following principles guide **[insert organisation name]**’s risk management policy,:

* Risk management applies to all aspects ofthe organisation’sbusiness and activity
* Risk management is a shared responsibility of all staff, management, volunteers, student placements and Board members
* Risk management is a continuous improvement process, where the organisation continually strives to reduce and manage the likelihood and negative impact of risks
* Staff, Board members, volunteers and students are provided with training and other support to assist them in managing risk in their roles.

## 1.4 Governance

The Board is ultimately responsible for how **[insert organisation name here]** manages risk. To discharge its accountabilities and responsibilities, the Board:

* Determines **[organisation name]**’s risk appetite
* Oversees risk management activities through [Board meetings/subcommittee or other]
* Delegates responsibility for the implementation of the risk management policy, frameworks and the effective mitigation of risks to the CEO/Manager
* The CEO/Manager reports regularly to the Board on the risk posture of the organisation.

The risk management policy is reviewed annually, and approved by the Board.

## 1.5 Outcomes

The outcomes of this policy are that **[organisation name]:**

* Makes informed business, operational and service delivery decisions while remaining fully aware of risks and opportunities
* Staff, management and Board members understand their roles and responsibilities in relation to risk management
* Risks and risk impact are minimised through compliance with relevant regulatory, legal and financial obligations, and implementation of risk treatments.

This policy is measured annually by the number and costs of avoidable risks, outside of Board appetite, occurring within a financial year.

## 1.6 Delegations

Delegations relevant to the organisation are detailed in the governance policy.

## 1.7 Policy implementation

This policy is endorsed by the **[insert applicable committee]** and approved by the Board.

* **[Organisation name]** implements organisational risk management by monitoring risk in a number of ways, such as: monitoring risk and compliance through the risk and compliance registers
* Risk management issues are part of the **[include applicable committees, staff meeting and or Board group]** as a standing agenda item.
* Use of this policy should be referenced in relevant **[organisation name]** policies, procedures and other supporting documents, to ensure staff are familiar with it, and that it is actively used
* This policy will be reviewed every **[insert timeframe]**, as mentioned in the policy review schedule for the organisation. A risk incident and/or legislative change may prompt a review sooner.

## 1.8 Risk Management

**[organisation name]** develops and implements risk management strategies and process informed by this policy and in compliance with relevant legislation.

The risk management policy is included in **[organisation name]**’s policy review schedule where all policies are reviewed every **[Insert frequency]** at a minimum, or following significant operational, policy or legislative requirements.

Risks are also actively managed through **[organisation name]**’s risk and compliance register reviewed at board meetings.

# SECTION 2: Risk Management Framework

## 2.1 Risk management framework

This Policy is supported by the risk management framework (the framework) which is broadly compliant to the *ISO Standard 31000:2018 Risk Management – Guidelines*. Changes have been made to account for the nature of **[organisation name]**’s activities and the risks to which the organisation is exposed.

The Framework guides the implementation and execution of effective risk management and has the following components:



| **Component** | **Contents**  |
| --- | --- |
| **Risk Management Policy and** **Board Risk Appetite Statement (RAS)** | This document:* Defines the policy, governance, and broad accountabilities which **[organisation name]** maintains to effectively manage risks.
* Defines the risk appetite of the Board for each class of risk. The RAS is the basis for setting acceptable levels of risk tolerance and thresholds and informs decision making.
 |
| **Risk Management Procedure** | This document:* Describes the risk management processes used at **[organisation name]**.
* Provides the “how to” information to help employees manage risk.
 |

|  |  |
| --- | --- |
| **Risk Management Tools** | Tools to facilitate risk management and reporting, such as:* Risk registers to record risks, rate them and record mitigation.
* Risk assessment templates to assess risks and the incident management processes.
 |
| **HR and Operations Policies and Procedures** | Provides policy and processes and tools to manage and safeguard employees and business activities. |
| **Compliance Policies & Procedures** | Provides policy and processes and tools to ensure that **[organisation name]** remains compliant will all relative legislation and regulations. |
| **Business Continuity & Crisis Management** | Provides the formal framework to guide **[organisation name]** through business disruptions and crisis events. |

**Key actions**

In addition to this Policy and the Risk Management Framework, good risk management at **[organisation name]** is supported by:

* A comprehensive set of policies and procedures, that cover, but are not limited to: quality management, code of conduct, business continuity, incidents, complaints, whistle-blower, wh&s, privacy, financial controls, conflicts of interest and technology.
* An effective Board, staff, student and volunteer induction & training program that includes management of risks and clarification of roles and responsibilities.
* Regular and effective communication from the CEO about the importance of effective risk management and our culture.
* Ongoing review of risks, their assessment and mitigation strategies to ensure risks are maintained at acceptable levels.
* Effective risk mitigations that do not excessively hinder performance of everyday activities, and the exploration of new opportunities and strategies to improve stakeholder outcomes.
* Objective and transparent Board reporting as to **[organisation name]**’s risk posture.

Effective risk management relies on more than policy. It requires a positive culture where employees are empowered to identify and manage risks to better protect our customers. Processes and communication channels support this culture with leaders who role model effective attitudes and behaviour.

## 2.3 Roles and Responsibilities

|  |  |
| --- | --- |
| **Board**  | * The Board is ultimately accountable for risk management and delegates oversight to the [insert relevant committee]. Delegates responsibility for the implementation of the risk management framework and effective risk mitigation to the CEO/Manager
* Endorses and complies with Risk Management Policy
 |
| **Finance, Risk, Audit and Compliance sub-committee (FRAC)\*** | * Reviews the effectiveness of the Risk Management Framework, including this Policy.
* Oversees and monitors the organisational management’s effectiveness in managing key risks and internal controls.
* Monitor and contribute to internal risk treatment strategies and activities, including regular review of the Risk Register
* Reviewing [organisation name]’s compliance with relevant statutory and regulatory requirements
 |
| **CEO/ Manager** | * The CEO is responsible for ensuring that risk management practices are established and maintained in accordance with this Policy and regularly reporting the risk posture to the Board and relevant committees.
* Responsible to promote a positive risk culture that encourages identification and management of risk.
* Ensure all staff, Board members, students and volunteers are aware of [organisation name]’s approach to risk management
 |
| **Supervisors** | * Responsible to ensure risk management principles, appetite, framework and processes are communicated, and implemented into strategy, business decisions and daily operations.
* Identify, assess, and manage risks and controls within their area of responsibility, including maintaining adequate policies and procedures.
* Maintain the risk and compliance register.
* Ensure all staff comply with this policy.
 |
| **[Organisation name] staff**  | * All employees are aware of and understand this Policy and the Risk Management Framework. Staff actively live the Policy Statement and apply the processes to effectively manage risks in their daily work.
* Take personal ownership for risk identification and reporting in their work and surroundings. Where appropriate, keep relevant records
* [Insert any other staff role responsibilities as required]
 |

***\*Note*** *While the FRAC Committee is included in the above table, we recognise that not all organisations will have a FRAC as part of their Board. Some organisations may instead have a differently titled working group or sub-committee. Please edit this policy to ensure consistency with the circumstances of your own organisation. \*Please delete this note before finalising this policy.*

# SECTION 3: RISK management processes

This section ensures that **[insert organisation name]** develops and implements consistent risk management strategies and processes to effectively manage and treat risk, in order to safely enhance the organisation’s operation and achieve its strategic goals.

This section provides guidance on the plans, processes and tools that the organisationadopts to identify, assess, treat and monitor risks.

This section ensures that the organisation:

* Provides reliable administrative tools and reporting methods
* Confirms that the risk management strategy and activities are informed by its Personnel, clients and the broader community
* Ensures that risk management processes support and enhance the services provided to its clients
* Has a structure for the continuing review of risk
* Provides ongoing safe operations for Personnel, clients and the broader community.

## 3.1 Communication and consultation

Communication and consultation is undertaken with the organisation’s personnel to ensure understanding and engagement in risk management.

Communication mechanisms include:

* Orientation processes for new Board members, staff, and clients entering the service
* Agenda items and discussion at staff and team meetings, e.g. WHS, budgets, client related incidents
* Regular staff and supervisor meetings to review work plans and activities, together with incident management
* CEO/Manager reporting to the Board, and regular review of the risk register.

The organisation implements diverse consultation methods to seek feedback from its clients and Personnel. This may include:

* Staff and Board leadership and participation in policy development
* Staff and Board leadership and participation in risk management and risk incident review
* Client meetings
* Workshops
* Surveys
* **[Insert other consultation method].**

Communication and consultation is undertaken with external stakeholders (if appropriate) as part of **[insert organisation name]** business. Mechanisms include:

* Briefing and planning meetings as part of project development, implementation and evaluation
* Strategic planning
* Performance reporting to funding bodies
* Annual reports
* Surveys and evaluations
* **[Insert other consultation method].**

## 3.2 Establishing risk context

Risk management considers the context in which **[insert organisation name]** operates and how these characteristics and capabilities influence and inform risk responses. This could include assessing:

|  |  |
| --- | --- |
| **Strategic or external context:** | * Operational, regulatory, financial and political environment
* Business drivers
* Opportunities and threats
* Stakeholders.
 |
| **Organisational or internal context:** | * The organisation’s goal and outcomes
* Organisation al culture
* Strengths and weaknesses within the organisation
* Existing systems and processes
* Stakeholders
* Available resources.
 |
| **Risk management context:** | * The organisation‘s size, organisational structure and location
* Governance structure
* Management expertise
* Clinical service delivery
* Workforce capacity
* Assets.
 |

## 3.3 Risk identification

**[Insert organisation name]** identifies risks through formal and informal processes such as: targeted consultation, observation of workplace practice, monitoring of regulatory requirements, organisational system reviews, regular audits (e.g. WHS, policy compliance), analysis of information gathered relating to WHS incidents and strategic and project planning.

Organisational risks are categorised and summarised as follows:

|  |  |
| --- | --- |
| **Type** | **Area/item compromise** |
| **Strategic**  | * Goal and intended outcomes of the organisation
* Intellectual property
* Reputation
* Organisation and sector positioning
* Resourcing, growth and improvement
* **[Insert other item].**
 |
| **Compliance**  | * Entity legislation (e.g. incorporations, co-operatives or others)
* Contractual obligations
* Insurance
* Taxation
* Employment legislation (refer to the Human Resources policy)
* Work health safety legislation (refer to the Work Health Safety policy )
* **[Insert other item].**
 |
| **Financial**  | * Fraud
* Income, budget and expenditure operations
* Debt collection
* Governance and management by Board
* **[Insert other item].**
 |
| **Operational**  | * Governance
* Service delivery (e.g. clinical, projects, programs)
* General equipment, resources and facilities
* Human resource management
* Information management
* Break-in, theft, and fire
* **[Insert other item].**
 |
| **Market/environmental/ external risks**  | * Natural disasters or major storms
* Changes in government and/or government policy
* Major legislation change
* **[Insert other item].**
 |

## 3.4 Risk assessment

The risk assessment matrix, risk likelihood and rating tables below are applied to all identified risks to determine their level of risk based on two categories: likelihood and impact.

Risk assessment also includes reviewing existing controls, whether specific to that risk or by default.

### 3.4.1 Risk matrix

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Likelihood** | Almost certain | Low Medium | Medium | Medium -High | High | High |
| Likely | Low | Low - Medium | Medium | Medium -High | High |
| Possible | Low | Low | Medium | Medium -High | High |
| Unlikely | Low | Low | Low - Medium | Medium | Medium -High |
| Rare | Low | Low | Low | Medium | Medium -High |
|  |  | Minimal | Minor | Moderate | Significant | Severe |
|  |  | **Impact** |

### 3.4.2 Risk likelihood

|  |  |
| --- | --- |
| **Rating** | **Description** |
| **Almost certain** | 90% or greater probability  | Expected to occur in most circumstances |
| **Likely** | 50-90% probability  | Will probably occur in most circumstances |
| **Possible** | 20-50% probability  | Could occur at some time |
| **Unlikely** | 10-20% probability  | Not expected to occur |
| **Rare** | <10% probability  | Would occur only in exceptional circumstances |

### 3.4.3 Risk impact

|  |  |
| --- | --- |
| **Rating** | **Description** |
| **Severe** | Business objectives and/or continuing viability is threatened | Death or serious injury to a person  |
| **Significant**  | Business objectives are not met | Serious injury or illness requiring medical treatment with permanent consequences |
| **Moderate**  | Business objectives may be threatened | Injury or illness requiring medical treatment |
| **Minor** | Business objectives require monitoring | Minor injuries  |
| **Minimal** | Business objectives unlikey to be affected | Minor first aid injury |

### 3.4.4 Risk rating

The risk rating assists **[insert organisation name]** in determining if the risk is acceptable or unacceptable. A low rating risk may be expected and acceptable with minimal treatment response, whereas a high rating risk is not acceptable and therefore requires a response to minimise or eliminate risk.

|  |  |
| --- | --- |
| **High** | Requires immediate action to mitigate the risk |
| **Medium-High** | Requires short-term action to mitigate the risk  |
| **Medium** | Requires medium-term action to mitigate the risk (work within other priorities) |
| **Low-Medium** | May require attention  |
| **Low** | Manage by routine procedure |

## 3.5 Risk treatment

Risk treatment involves identifying and implementing actions to eliminate risks or reduce their impacts. In treating risk the organisation, board and staff members ensure that:

* The cost of implementing risk treatments is balanced with the expected and actual risk reduction outcomes
* If eliminating risk is to discontinue an activity, remove an identified risk item, or avoid new or potential risks
* Risk reduction activity involves implementing reasonable and practical steps to reduce risks and minimise loss, injury or harm. For example, where transport of heavy boxes is unavoidable, a trolley and safe lifting training is provided
* Major risks and their responding treatments are logged in the organisation’s Risk Register
* Risks that are substantially mitigated by the existence of a specific organisational policy or listed in the organisation’s Compliance Register may not be required to be recorded in the Risk Register
* Risk specific to client service delivery are managed under a clinical risk management framework
* Risks specific to individual projects are identified and responded to through project implementation; these may not be required to be recorded in the Risk Register.

Risk Treatment should adopt the hierarchy for controlling Risks:

* Eliminate the hazard
* Substitute the hazard for something safer
* Isolate the hazard from people
* Use engineering controls
* Use administrative controls
* Use personal protective equipment.

The diagram below depicts the organisation’s risk management process.

**Monitor and review**

**Identify risk**

Strategic

Compliance

Financial

Operational

Market/environmental

**Assess risk**

Likelihood

Impact

Existing controls

Risk rating

**Treat risk**

Identify and implement actions

Eliminate risk

Reduce risk impact

**Establish risk context**

Strategic/external

Organisational/internal

Risk management

**Communicate and consult**

## 3.6 Risk management plans

**[Insert organisation name]** implements risk management plans for specific activities that carry likely or almost certain risk which are inherent in working with our clients. The plans provide specific guidance to staff in managing concerns that are likely to arise when providing direct client services.

## 3.7 Risk monitoring and reviewing

**[Insert organisation name]** monitors and reviews risks and their treatment strategies as part of effective risk management and ongoing quality improvement.

Monitoring and reviewing activities include:

* Re-consideration of the contexts, rating, treatment and responsibilities.
* Risks identified through the organisation’s risk register and compliance register are reviewed and updated **[insert timeframe; for example, monthly]** by the **[insert allocated position; for example, Work Health and Safety officer]**.
* The Board reviews the organisation’s risk register and compliance register **[insert timeframe; for example, monthly]** through Board and other relevant meetings.
* Previously identified risks may become de-activated through a monitoring and review process, where the likelihood and impact of loss, injury or harm is assessed as non-existent or negligible.
* WHS risks are reviewed **[insert timeframe; for example, quarterly]** through workplace audits and other WHS strategies.
* Clinical risk is monitored and reviewed regularly through **[insert mechanisms, for example case meetings, clinical supervision]**. Risk management plans are developed and regularly reviewed for the delivery of services to those areas where risk is likely or almost certain.
* Risks that are assessed as specific to individual projects are reviewed through project mechanisms such as scheduled milestone checks, progress reporting, advisory group meetings, stakeholder feedback, outcome monitoring, and end-of-project evaluation.
* The organisation’s risks are also reviewed and their status is updated following a risk incident, such as a clinical incident, workplace accident, cuts to funding, damage to reputation, or not meeting taxation compliance requirements.
* **[Insert other activities].**

## 3.8 Reporting and record-keeping

Risks identified in the organisation’s risk register and the compliance register are reported to the Board **[insert timeframe; for example, monthly]** by the CEO/Manager in the scheduled Board meetings. Related discussion and outcomes are recorded in Board and relevant minutes.

Risk management discussion and outcomes from staff meetings are recorded in meeting minutes.

### 3.8.1 Risk register

The Organisation’s risk register details major risks, their rating, controls and treatments, as well as responsibilities and timeframes.

* All risks listed in the risk register are allocated a unique risk identification number.
* De-activated risk identification numbers are maintained on the risk register for reference as required.
* Electronic copies of **[insert timeframe; for example, monthly]** reviewed and updated risk register are saved in accordance with the Information and Communication Technology policy.

### 3.8.2 Compliance register

The compliance register details compliance obligations in relation to: insurance, incorporation, taxation, performance agreements, and WHS.

Electronic copies of **[insert timeframe; for example, monthly]** reviewed and updated compliance register are saved in accordance with the Information and Communication Technology policy.

# SECTION 4: REFERENCES

## 4.1 Supporting documents

* Risk register
* Compliance register

## 4.2 Related internal policies

* Governance policy
* Financial Management policy
* Human Resources policy
* Work Health and Safety policy
* Privacy and Confidentiality policy
* ICT policy

## 4.3 External references

* [ISO Standard 31000: 2018 Risk Management- Guidelines](https://www.iso.org/standard/65694.html)
* [Risk Management and Quality Improvement Handbook July 2013](https://www.scribd.com/document/258260724/Risk-Management-and-Quality-Improvement-Handbook-July-2013)
* *Associations Incorporation Act 1984* (NSW) No 143
* *Corporations Act 2001* (Cth) No 50
* *Work Health and Safety Act 2011* (NSW)